McGILL UNIVERSITY

FACULTY OF SCIENCE

DEPARTMENT OF
MATHEMATICS AND STATISTICS

MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

Information for Students
(Winter Term, 2001/2002)

W. G. Brown

April 16, 2002

Originally mounted on the Web at the following URL:

http://www.math.mcgill.ca/brown/math340.2001-02.pdf

(Items marked ‡ not distributed in hard copy)

Contents

1 General Information **1**
1.1 Instructor, Tutor, and Times . 1
1.2 Calendar Description 1
1.3 Tutorials 1
1.4 Homework 2
1.4.1 Rules for submission of homework 2
1.5 Term Mark 2
1.6 Final Grade 3
1.7 Printed and Web-based Materials 3
1.7.1 Required Text-Book . . 3
1.7.2 Web-based and/or Printed Notes 3
1.7.3 Web address 3
1.8 Test and Examinations 4
1.8.1 Class Test 4
1.8.2 Supplemental Examination 4
1.8.3 Extra Work Option . . 4
1.8.4 Machine Scoring 4
1.9 Calculators 4

2 Timetable **5**

3 First Problem Assignment **7**

4 Multiplicative inverses modulo n **10**

5 Second Problem Assignment **11**

6 Consequences of the ring axioms **14**
6.1 Assuming and/or proving properties of 0_R and, where it exists, 1_R, in a ring R 14
6.2 Closure under operations . . . 14

7 Two non-isomorphic rings **16**

8 Different ring structures on the same cartesian product **16**

9 Third Problem Assignment **18**

10 Detailed syllabus corresponding to textbook chapters 1 – 4‡ **21**
10.1 Chapter 1, Arithmetic in $\mathbb{Z}$ Revisited, and applicable appendices 21
10.1.1 Logic and Proof, [19, Appendix A, p. 493] . . 21
10.1.2 The Division Algorithm, [19, §1.1] 21
10.1.3 Well Ordering and Induction, [19, Appendix C, p. 519] 21
10.1.4 Divisibility, [19, §1.2, p. 7] 22
10.1.5 Primes and Unique Factorization, [19, §1.3, p. 15] 22
10.1.6 Primality Testing, [19, §1.4, p. 20] 22
10.1.7 Sets and Functions, [19, Appendix B, p. 504] . . 22
10.1.8 Equivalence Relations, [19, Appendix D, p. 527] 22
10.1.9 Congruence and Congruence Classes, [19, §2.1, p. 24] 22
10.2 Chapter 2: Congruence in $\mathbb{Z}$ and Modular Arithmetic 23
10.2.1 Modular Arithmetic [19, §2.2, p. 31] 23
10.2.2 The Structure of $\mathbb{Z}_p$ When p is Prime [19, §2.3, p. 37] 23
10.3 Chapter 3: Rings 23
10.3.1 Definition and Examples of Rings [19, §3.1, p. 42] 23
10.3.2 Basic Properties of Rings [19, §3.2, p. 56] . 24

10.3.3 Isomorphisms and Homomorphisms [19, §3.3, p. 66] 24
10.4 Chapter 4: Arithmetic in $F[x]$. 24
10.4.1 Polynomials [19, Appendix G, p. 542] 24
10.4.2 Formal Power Series (§A.7.3) 25
10.4.3 Polynomial Arithmetic and the Division Algorithm $F[x]$ [19, §4.1, p. 81] 25
10.4.4 Divisibility in $F[x]$ [19, §4.2, p. 90] 26
10.4.5 Irreducibles and Unique Factorization [19, §4.3, p. 94] 26
10.4.6 Polynomial Functions, Roots, and Reducibility [19, §4.4] 26
10.4.7 Irreducibility in $\mathbb{Q}[x]$ [19, §4.5, p. 107] 26
10.4.8 Irreducibility in $\mathbb{R}[x]$ and $\mathbb{C}[x]$ [19, §4.6, p. 115] 26

11 Solutions, First Problem Assignment‡ 28

12 Fourth Problem Assignment 39

13 Solutions, Second Problem Assignment‡ 40

14 Class Tests ‡ 51
14.1 Version 1 51
14.2 Version 2 56
14.3 Version 3 61
14.4 Version 4 66

15 Plagiarism in student solutions to Assignment 2‡ 71

16 Solutions, Third Problem Assignment‡ 72

17 Detailed syllabus corresponding to textbook chapters 5, 6, 7, 8, 13‡ 82
17.1 Chapter 5, Congruence in $F[x]$, and Congruence-Class Arithmetic 82
17.1.1 Congruence in $F[x]$, and Congruence Classes [19, §5.1, p. 119] 82
17.1.2 Congruence-Class Arithmetic [19, §5.2, p. 123] 82
17.1.3 The Structure of $F[x]/(p(x))$ when $p(x)$ is Irreducible [19, §5.3, p. 128] 82
17.2 Chapter 6, Ideals and Quotient Rings 83
17.3 Chapter 7, Groups [19, p. 160] 83
17.3.1 Definitions and Examples of Groups [19, §7.1] 83
17.3.2 Basic Properties of Groups [19, §7.2, p. 174] 83
17.3.3 Subgroups [19, §7.3, p. 181] 83
17.3.4 Isomorphisms and Homomorphisms [19, §7.4, p. 191] 83
17.3.5 Congruence and Lagrange's Theorem [19, §7.5, p. 199] 83
17.3.6 Normal Subgroups [19, §7.6, p. 208] 84
17.3.7 Quotient Groups [19, §7.7, p. 216] 84
17.3.8 Quotient Groups and Homomorphisms [19, §7.8, p. 222] 84
17.3.9 The Symmetric and Alternating Groups [19, §7.9] 84

17.3.10 The Simplicity of A_n [19, §7.10, p. 239] 84
17.4 Chapter 8, Topics in Group Theory [19, p. 245] 84
17.4.1 Direct Products [19, §8.1] 84
17.4.2 Finite Abelian Groups [19, §8.2, p. 252] 84
17.4.3 The Sylow Theorems [19, §8.3, p. 282] 84
17.4.4 Conjugacy and the Proof of the Sylow Theorems [19, §8.4, p. 267] 85
17.4.5 The Structure of Finite Groups [19, §8.5, p. 275] 85
17.5 [19, Chapters 9 - 12] 85
17.6 Chapter 13, The Chinese Remainder Theorem [19, p. 406] . 85
17.6.1 Proof of the Chinese Remainder Theorem [19, §13.1] 85
17.6.2 Applications of the Chinese Remainder Theorem [19, §13.2, p. 412] . 85

18 Fifth Problem Assignment 86

19 Solutions to Problems on the Class Test 89

20 Solutions, Fourth Problem Assignment‡ 95

21 Solutions, Fifth Problem Assignment‡ 100

22 References 901

A Notes on Algebra‡ 1001
A.1 Theory of Numbers 1001
A.1.1 Introduction 1001
A.1.2 The number systems . . 1001
A.1.3 Other notational conventions 1004
A.1.4 Divisibility of integers . 1004
A.1.5 The Division "Algorithm". Bases of Notation. 1005
A.1.6 Greatest Common Divisor 1011
A.1.7 Algebraic operations on sets of integers 1018
A.1.8 Primes 1021
A.1.9 Congruences 1026
A.2 Functions etc. 1037
A.2.1 Set Theory 1037
A.2.2 Basic Definitions 1037
A.2.3 Function Composition . 1039
A.3 Permutation Groups 1043
A.3.1 Permutations 1043
A.3.2 Multiplication (Composition) of Permutations 1048
A.3.3 Groups of permutations 1052
A.3.4 Invariance under a Permutation Group 1055
A.3.5 Conjugacy classes of permutations 1061
A.3.6 Even and Odd Permutations. The Alternating Group. 1064
A.3.7 The Cycle Index of a Permutation Group‡ . . 1065
A.3.8 The "Graph Isomorphism Problem"‡ 1071
A.4 Binary Operations; Semigroups and Monoids 1072
A.4.1 Introduction 1072
A.4.2 Semigroups 1072
A.4.3 Monoids 1080
A.4.4 Subsemigroups, Submonoids, Generators . . 1086
A.4.5 Commutative Semigroups and Monoids . . 1088
A.4.6 Direct products 1089
A.4.7 Naming conventions . . 1090

A.5 Groups 1091
A.5.1 Inverses 1091
A.5.2 Objects and Morphisms 1097
A.5.3 Kernel and image of a homomorphism. 1102
A.5.4 Action of a group on itself 1106
A.5.5 Normal Subgroups. Quotient Groups 1116
A.5.6 Generators and Relations. Cyclic Groups. . . 1119
A.5.7 Group Presentations . . 1124
A.5.8 The Quaternion Group 1125
A.6 Abelian Groups 1127
A.6.1 Direct Sums. The Fundamental Theorem. . . . 1127
A.6.2 Euler's "Totient" Function. Fermat's "Little" Theorem. 1128
A.6.3 Public Key Cryptography: The RSA Cryptosystem 1136
A.6.4 Primitive Roots modulo n. The Discrete Logarithm 1138
A.6.5 Homomorphisms 1141
A.7 Rings and Fields 1146
A.7.1 Rings 1146
A.7.2 Ring Homomorphisms. Subrings. Ideals 1149
A.7.3 Polynomials and Power Series 1152
A.7.4 Factorization of Polynomials 1156
A.7.5 Fields 1157

B 1997 Problem Assignments, with Solutions‡ 2001
B.1 First 1997 Problem Assignment 2001
B.2 Second 1997 Problem Assignment 2007
B.3 Third 1997 Problem Assignment 2013
B.4 Fourth 1997 Problem Assignment 2020
B.5 Fifth 1997 Problem Assignment 2028
B.6 Sixth 1997 Problem Assignment 2035

C 1998 Problem Assignments, with Solutions‡ 2042
C.1 First 1998 Problem Assignment 2042
C.2 Second 1998 Problem Assignment 2049
C.3 Third 1998 Problem Assignment 2055
C.4 Fourth 1998 Problem Assignment 2063
C.5 Fifth 1998 Problem Assignment 2071

D 1999 Problem Assignments, with Solutions‡ 2079
D.1 First 1999 Problem Assignment 2079
D.2 Second 1999 Problem Assignment 2086
D.3 Third 1999 Problem Assignment 2092
D.4 Fourth 1999 Problem Assignment 2096
D.5 Fifth 1999 Problem Assignment 2100

E 2000 Problem Assignments, with Solutions‡ 2108
E.1 First 2000 Problem Assignment 2108
E.2 Second 2000 Problem Assignment 2117
E.3 Third 2000 Problem Assignment 2125
E.4 Fourth 2000 Problem Assignment 2130
E.5 Fifth 2000 Problem Assignment 2137

F 2000/2001 Problem Assignments, with Solutions‡ 2146
F.1 First 2000/2001 Problem Assignment‡ 2146
F.2 Second 2000/2001 Problem Assignment‡ 2150
F.3 Third 2000/2001 Problem Assignment‡ 2154
F.4 Fourth 2000/2001 Problem Assignment‡ 2162

G Some Class Tests from Previous Years, with Solutions‡ 2167
G.1 1991 Class Test 2167
G.2 1997 Class Test 2169
G.3 1998 Class Tests 2174
G.3.1 Version 1 2174

G.3.2 Version 2 2178
G.3.3 Version 3 2181
G.3.4 Version 4 2184
G.4 1999 Class Tests 2186
G.4.1 Version 1 2186
G.4.2 Version 2 2189
G.5 2000 Class Tests 2191
G.5.1 Problems on monoids . 2192
G.5.2 Group homomorphisms 2192
G.5.3 Solution of congruences 2194
G.5.4 Cosets of subgroup in a group 2194
G.6 2001 Class Tests 2195
G.7 2001 Homework Tests 2202

H Some Examinations from Previous Years, Without Solutions‡ 2206
H.1 Final Examination, Spring, 1991 2206
H.2 Final Examination, Spring, 1997 2207
H.3 Supplemental/Deferred Examination, August, 1997 2208
H.4 Final Examination, Spring, 1998 2210
H.5 Supplemental/Deferred Examination, August, 1998 2211
H.6 Final Examination, Spring, 1999 2213
H.7 Supplemental/Deferred Examination, Spring, 1999 2214
H.8 Final Examination, Spring, 2000 2215
H.9 Supplemental/Deferred Examination, August, 2000 2217
H.10 2000/2001 Final Examination . 2218
H.11 2000/2001 Supplemental/Deferred Examination . . . 2219

1 General Information

Distribution Date (1st version): Monday, January 7th, 2002
(all information is *subject to change*)
The Course Outline for the course can be considered to be pages 1 – 4 of these notes.

1.1 Instructor, Tutor, and Times

INSTRUCTOR:	Professor W. G. Brown
OFFICE:	BURN 1224
OFFICE HOURS	W 14:30→15:30 h.; F 10→11 h.
(subject to change):	or by appointment
OFFICE TELEPHONE:	398–3836
E-MAIL:	BROWN@MATH.MCGILL.CA
CLASSROOM:	ENGMC 204
CLASS HOURS:	MWF 11:30 — 12:30 h.
TUTOR:	Mr. Matthew Greenberg
OFFICE:	BURN 1036
E-MAIL:	GREENBERG@MATH.MCGILL.CA
TUTORIAL ROOM:	BURN 1B36
TUTORIAL TIME:	W 15:30 — 17:30 h.
OFFICE HOURS:	W 09:00 – 11:00 h.

1.2 Calendar Description

189-340B ABSTRACT ALGEBRA AND COMPUTING. (3 credits; Prerequisites: 189-240, 189-223 (or 189-236); for Major and Honours students in Computer Science only. Others with the Instructor's permission.) Basic number theory: divisibility, Euclid's algorithm, congruences, Fermat's "little" theorem, primality testing, factorization. Commutative rings: basic definitions, (integers), gaussian integers, polynomial rings, euclidean rings, finite fields. Groups: symmetry groups, permutation groups. Additional topics.

1.3 Tutorials

While attendance is optional, students are urged to take advantage of a service that was requested by students for many years before being implemented. The tutorials are intended to hone your skills in problem solving. The teaching assistant conducting the tutorials will discuss a variety of problems, not only those on the current problem

assignment. The first tutorial will be on January 16th, 2002; there will be no tutorial (and no office hours) during Study Week.

1.4 Homework

There will be approximately 5 homework assignments. The material on these assignments forms an integral part of the course. Students must not, however, assume that the assignments represent an exhaustive list of the types of problems they should be able to solve: the assignments are only a sampling. Nor should any conclusions been drawn from the absence of certain syllabus topics from assignment questions.

Because of limited grading time the grader may have to select only a portion of each student's submitted problems for grading. The recorded numerical grade for the assignments may be relatively insignificant; but students should be sure that they understand the problems and their solutions.

1.4.1 Rules for submission of homework

1. Late homework will not necessarily be accepted or graded.
2. *Print* student name and student number on every page.
3. Use paper approximately $8\frac{1}{2}$ inches $\times$ 11 inches.
4. Pages should be securely stapled.
5. While students are not discouraged from discussing assignment problems with their colleagues, solutions handed in should be each student's own work.[1]

1.5 Term Mark

Graded out of 30, the TERM MARK will be the sum of the HOMEWORK GRADE (out of 10) and the TERM TEST GRADE (out of 20).

[1]From the Handbook on Student Rights and Responsibilities:

> "No student shall, with intent to deceive, represent the work of another person as his or her own in any...assignment submitted in a course or program of study or represent as his or her own an entire essay or work of another, whether the material so represented constitutes a part or the entirety of the work submitted."

See also the "Student Guide to Avoid Plagiarism", at

http://www.mcgill.ca/arts_science/academic/plagiarism.htm

1.6 Final Grade

The final grade will be a *letter* grade, computed from

$$\boxed{\max\{\text{Examination mark}, (.7 \times \text{Examination mark}) + \text{Term Mark}\}}$$

1.7 Printed and Web-based Materials

1.7.1 Required Text-Book

Thomas W. Hungerford, *Abstract Algebra, An Introduction (Second Edition)*, Saunders College Publishing, Harcourt Brace College Publishers (1990); ISBN 0-03-010559-5 (hardbound) [19].[2]

1.7.2 Web-based and/or Printed Notes

Students may be provided, from time to time, with notes which will be available in printed form and/or on the Web. Such notes are intended to complement and supplement material in the required text-book, and/or discussed in the lectures, and should be treated as an integral part of the syllabus. Notes will usually bear a "Distribution Date". While some notes may be available on the Web in advance of this date, students are cautioned that notes not yet distributed may be in preliminary form, subject to change and correction before distribution. Even after distribution, errors in printed materials — there are certain to be errors — may be corrected only in the Web-based version. Also on the Web will be solved problem assignments, solved class tests, examinations (without solutions) and full copies of printed notes from previous years. These are not required for the present course, but are being made available for students who wish to use them.

1.7.3 Web address

Materials are available at the following URL:

http://www.math.mcgill.ca/brown/math340b.html

Files from years before 1999/2000 are in "PostScript" format, ($\cdots$.ps). Files for 2001/2002 will be in "PDF" format ($\cdots$.pdf), as were the notes from last year. An appendix to the current year's notes will contain assignments from previous years, and old examinations and tests. Some of these files are very long.

The notes will also be available via a link from the WebCT URL:

[2]This is the first time this book has been used in this course; however, it has been in use at McGill in another course.

http://webct3/mcgill.ca

but most other features of WebCT will not be implemented.[3]

1.8 Test and Examinations

1.8.1 Class Test

One class test will be will be administered, during a regular class hour; tentatively the date of the test is set as Monday, March 4th, 2002. Any further change in this date will be announced in the lectures. Please note that the last date to drop the course precedes the date of the test. No provision will normally be made for a "make-up" test for a student absent during the test.

1.8.2 Supplemental Examination

"Will there be a supplemental examination in this course." Yes.

1.8.3 Extra Work Option

"Will students with marks of D, F, or J have the option of doing additional work to upgrade their mark?" No.

1.8.4 Machine Scoring

"Will the final examination be machine scored?" No.

1.9 Calculators

The use of calculators, computers, notes, or other aids will not be permitted at the test or examination.

[3]WebCT is the proprietary system of Web Course Tools that has been implemented by McGill University. Every McGill student and staff member has been assigned a Global UserID for Version 3 of WebCT. The WebCT UserID is identical to McGill's new Permanent E-mail Alias and follows the general convention of first name followed by a period, and then last name. WebCT UserID's are based on an individual's official McGill records and must be all lowercase, with spaces converted to the underscore (_) character. For example: Jim McGill would use james.mcgill as his WebCT 3 UserID.

2 Timetable

Distribution Date: 4th version: Monday, March 18th, 2002. (Subject to continual revision through the term.) [Section numbers refer to the text-book.][4]
This being the first year that the textbook is being used in this course, the selection of materials and the timing must be considered provisional, and subject to change.

MONDAY	WEDNESDAY	FRIDAY
JANUARY		
7 **§1.1, Appendix C (review)**	9 **§1.2**	11 **§1.2, §1.3** ▣1
Tutorials begin week of January 14th, 2002		
14 **§1.3, §1.4, Appendix B (review, pp. 508–518)**	16 **§2.1, Appendix D (review)**	18 **§2.2**
Course changes must be completed on MARS by Jan. 20, 2002		
21 **§2.3**	23 **§3.1** ▣2	25 **§3.1, §3.2** ①1
Deadline for withdrawal with fee refund = Jan. 27, 2002		
28 **§3.2**	30 **§3.3**	
FEBRUARY		
		1 **§4.1**
Verification Period: February 4–8, 2002		
4 **§4.1**	6 **§4.2** *CLASS IN SADB M-1 11:30*	8 **§4.3** ②2 ▣3
11 **§4.4**	13 **§4.4**	15 **§4.6**
18 **§5.1**	20 **§5.2**	22 **§5.3** ③3 ▣4
Deadline for withdrawal (with W) from course via MARS = Feb. 24		
Study Break: February 25–March 1, 2002 No lectures, no office hours, no tutorials!		
25 **NO LECTURE**	27 **NO LECTURE**	

Page 6 of the timetable will be circulated later in the term. It is expected that the remaining lectures will be devoted to parts of the following sections: 7.1, 7.2, 7.3, 7.4, 7.5, 7.9, 8.1, 8.2, 10.6, 12, 13.1, 13.2, 14.1, 14.2, 16.

[4]Notation: ▣# = distribution of assignment #
ⓝ = assignment #n due at tutorials this week
Ⓡ = Read Only
X = reserved for eXpansion or review
$\mathcal{N}$ = distributed notes

UPDATED TO April 16, 2002

MONDAY		WEDNESDAY		FRIDAY	
MARCH					
				1	**NO LECTURE**
4	**§7.1, §7.2**	6	**§7.1, §7.2**	8	**§7.3**
11	**§7.4 (part)**	13	**CLASS TEST**	15	**§7.4 (part)** ④
18	**§7.5 (part)** ⑤	20	**§7.9 (part), §8.1**	22	**§8.2**
25	**X**	27	**§13.1**	29	**NO LECTURE**
APRIL					
1	**NO LECTURE**	3	**§13.1**	5	**§13.1** ⑤
Last tutorials during the week of April 8th, 2002					
8	**§13.1, X**	10	**X**	12	**X**
15	**X**				

3 First Problem Assignment

Distribution Date: Friday, January 11th, 2002
Solutions are to be submitted on Friday, January 25th, 2002.

1. (a) [19, Exercise 1.2.A1(h)] Use the Euclidean Algorithm to calculate $(12378, 3054)$. (This can be done by hand, but you may wish to use a calculator; in any case show all your work, systematically.)

   (b) [19, Exercise 1.2.B15(h)] Use the preceding computations (by "back substitution") to determine a decomposition of $(12378, 3054)$ in the form

   $$(12378, 3054) = 12378u + 3054v \tag{1}$$

   (c) Find another decomposition in form (1).

2. [19, Exercise 1.3.B22(b), p. 19]

   (a) Prove that there are no nonzero integers a, b such that $a^3 = 2b^3$. [Hint: Use the Fundamental Theorem of Arithmetic or [19, Theorem 1.8, p. 15].]

   (b) Prove that $\sqrt[3]{2}$ is irrational. [Hint: Use proof by contradiction. Assume that $\sqrt[3]{2} = \frac{a}{b}$, with $a, b \in \mathbb{Z}$ and use part (a) to reach a contradiction. Show first that it is possible to assume that $(a, b) = 1$, by using the result of [19, Exercise 1.2.B16, p. 13] without proof.]

3. (a) [19, Exercise 1.2.B20(a), p. 13],[19, Exercise 2.1.B22, p. 30] If $a^2 \equiv 1 \pmod 2$, prove that $a^2 \equiv 1 \pmod 4$.

   (b) (cf. [19, Exercise 1.1.B8, p. 7], [19, Exercise 1.2.B20(b), p. 13]) If $a^2 \equiv 1 \pmod 2$, prove that $a^2 \equiv 1 \pmod 8$. [Hint: Use the fact that one of any two consecutive integers is even.]

4. [19, Exercise ApB.B24, p. 517] Determine whether the given operation on $\mathbb{R}$ is commutative (that is, $(\forall a)(\forall b)[a * b = b * a]$) and whether it is associative (that is, $(\forall a)(\forall b)(\forall c)[a * (b * c) = (a * b) * c]$).

   (a) $a * b = 2^{ab}$

   (b) $a * b = ab^2$

   (c) $a * b = 0$

   (d) $a * b = (a + b)/2$

   (e) $a * b = 1$

(f) $a * b = b$

(g) $a * b = a^2 + b^2$

(h) (This example is not from the textbook.) $a * b = \sqrt{a^2 + b^2}$

5. [19, Exercise ApB.B28, p. 517]

   (a) Let $f : B \to C$ and $g : C \to D$ be functions such that $g \circ f$ is injective. Prove that f is injective.

   (b) Give an example of the situation in part (a) in which g is not injective. Your example should be "best possible" in that you should make $|B \cup C \cup D|$ as small as possible for such a counterexample.

6. (a) (cf. [19, Exercise ApD.A6, p. 531]) For any integer m, let $m\mathbb{Z}$ denote the set of integer multiples of m. Prove that the following relation on the points in the coordinate plane $\mathbb{R}^2$ is an equivalence relation:

$$(x, y) \sim (u, v) \quad \text{iff} \quad ((x - u) \in 3\mathbb{Z}) \wedge ((y - v) \in 2\mathbb{Z}) \,. \tag{2}$$

   (b) Show that every equivalence class $[(x, y)]$ under $\sim$ has a member (called a *representative*) in the rectangle $R = \{(x, y) : 0 \leq x < 3, 0 \leq y < 2\}$. In particular, find the *representative* of $[(-2, \pi)]$ in this rectangle.

   (c) For the relation $\sim$ defined above, let us define a measure of "distance" on the equivalence classes of the points of $\mathbb{R}^2$ under $\sim$. For classes $[(x, y)]$ and $[(u, v)]$ define the distance $d([(x, y)], [(u, v)])$ to be the minimum distance in $\mathbb{R}^2$ between any point in $[(x, y)]$ and any point in $[(u, v)]$.[5] Suppose that 7 points are placed anywhere in $\mathbb{R}^2$. Show that, with the preceding definition of distance, there must be two of these points whose distance is less than $\sqrt{2}$. [Hint: Divide the rectangle R into 6 squares of side 1, and show that at least two of the points have a representative in the same unit square. Then observe — without proof — that the maximum distance between two points in the square is attained when the points are at opposite corners.]

   (d) Show that the following relation on the points in $\mathbb{R}^2$ is *not* an equivalence relation, explaining precisely which property/properties of an equivalence relation fail/fails to hold:

$$(x, y) \backsim (u, v) \quad \text{iff} \quad ((x - v) \in 3\mathbb{Z}) \wedge ((y - u) \in 2\mathbb{Z}) \,. \tag{3}$$

[5] An equivalent way of looking at this definition is to think of rolling the plane into a cylinder whose axis is parallel to the x-axis, and whose circumference is 2, and then "identifying" pieces of this cylinder of length 3 (measured along the axis); except for the fact that the surface is deformed, this could also be achieved by taking a 3-unit length and gluing together the two circular boundaries to form a torus.

7. [19, Exercise ApC.B14, p. 525] At a social bridge party every couple plays every other couple exactly once. Assume there are no ties.

   (a) If n couples participate, prove that there is a "best" couple u in the following sense: for every couple v *distinct from*[6] u, u beats v or u beats a couple that beats v.

   (b) Show by example (for any n) that there may be more than one "best" couple.

   - Hint: (A convenient way to represent this type of bridge party is a *tournament*, which is a directed simple graph in which the couples are the vertices, and an edge is directed a to b if couple b defeats couple a.) Prove the claim by induction on n. Take the case $n = 1$ as the Basis Step. In the inductive step, after making the induction hypothesis, select any couple a, and prove the existence of a couple b which is "best" for all couples except possibly a. Then show that, if b is not "best" for all the couples, then a is "best".
   - The use of the English superlative "best" is unfortunate, since it suggests uniqueness.

8. [19, Exercise 1.2.A8, p. 13] If $r \in \mathbb{Z}$ and r is a non-zero solution of $x^2 + ax + b = 0$, (where $a, b \in \mathbb{Z}$), prove that $r|b$.

9. (a) [19, Exercise 1.4.A4] Verify that $2^5 - 1$ and $2^7 - 1$ are prime, but that $2^{11} - 1$ is not prime.

   (b) [19, Exercise 1.4.B7] Let $p > 1$. If $2^p - 1$ is prime, prove that p is prime. [Hint: Prove the contrapositive, i.e., if p is composite, so is $2^p - 1$.]

   (c) [19, Exercise 1.4.B9] If $k \geq 1$, and $2^k + 1$ is prime, prove that $k = 2^t$ for some t. [Hint: Verify that, if n is odd, $x^n + 1 = (x + 1)\left(x^{n-1} - x^{n-2} + \ldots - x + 1\right)$. Factorize k by dividing out 2 repeatedly until it can be written in the form $k = 2^t \ell$, where ℓ is odd.]

10. (a) Work out the addition and multiplication tables of $\mathbb{Z}_6$.

    (b) [19, Exercise 2.2.B6, p. 36] Prove or disprove: If $ab = 0$ in $\mathbb{Z}_n$, then $a = 0$ or $b = 0$.

[6] Note that this essential exclusion was overlooked in the textbook.

4 Multiplicative inverses modulo n

Let n be a non-zero integer. The statement at the bottom of [19, p. 11], and applied in Problem 1b of Assignment 1 (these notes, 3) [19, Exercises 1.2.A1(b)], is sometimes called *Bézout's Theorem". By "back substitution" in the equations developed when the Euclidean algorithm is executed on a and n, one can express (a, n) in the form*

$$(a, n) = au + nv \tag{4}$$

where u, v are integers. When a and n are relatively prime[7], (4) implies that

$$au \equiv 1 \pmod{n}. \tag{5}$$

An integer u with this property is called a *multiplicative inverse of a modulo*[8] n; we also say that $[u]$ is a (multiplicative)[9] inverse of $[a]$.

Equation (5) also *implies* that $(a, n) = 1$, since it implies the existence of an integer v such that $au - 1 = n \cdot (-v)$, or (4): any divisor of both a and n will also divide 1. We have thus proved the following

4.0.0.1 THEOREM. *An integer a has a multiplicative inverse iff $(a, n) = 1$.*

The procedure described above enables us to solve modulo n any equation of form (5). If we are given an equation of the form

$$au \equiv b \pmod{n} \tag{6}$$

to solve for u (where a, b, n are fixed integers, and $(a, n) = 1$), we can first solve (5), and then multiply the solution by b.

But what happens if $(a, n) \neq 1$? If $(a, n)|b$, we can first use the Euclidean algorithm to solve

$$\frac{a}{(a, n)}u \equiv \frac{b}{(a, n)} \left(\mathrm{mod} \frac{n}{(a, n)} \right).$$

and then multiply the solutions by (a, n). But, what if $(a, n) \not| b$. Then solving congruence (6) would be equivalent to finding integers u and v such that $au = b - nv$, i.e. such that $b = au + nv$. Here any common divisor of a and n would have to divide their linear combinations, including b; we have thus proved the following theorem:

4.0.0.2 THEOREM. *$au \equiv b \pmod{n}$ has a solution iff $(a, n) \mid b$.*

---

[7] We can also say "When a is *relatively prime to n...*"

[8] Latin, for *to the modulus*

[9] This word is often suppressed. Later we shall have occasion to speak also of an *additive* inverse; where neither adjective is present, one should assume that *multiplicative* is intended.

5 Second Problem Assignment

Distribution Date: Wednesday, January 23rd, 2002
Solutions are to be submitted on Friday, February 8th, 2002

The lecture in this course on Wednesday, February 6th, will be held in SADB M-1.

1. [3, Exercise 2.3.B7] In each of the following cases, solve the equation completely. Express your solution x as a congruence class $[u]$, where u is a representative of your choice; then describe precisely the membership of that class; for example, $[5]_2$ consists of all the integers expressible in the form $5 + 2n$, i.e., all the odd integers. Wherever a multiplicative inverse is required, you are expected to formally apply the Euclidean algorithm to find it.

   (a) $7x = 2$ in $\mathbb{Z}_{24}$

   (b) $34x = 1$ in $\mathbb{Z}_{97}$

   (c) $15x = 5$ in $\mathbb{Z}_{63}$

2. [19, Exercise 2.3.B11(b)] Showing all your work, solve the congruence $25x \equiv 10 \pmod{65}$. (Do not use [19, Exercise 2.3.B9].)

3. In each of the following cases, determine whether the given subset of the given ring constitutes a subring. Use the criteria of [19, Theorem 3.2, p. 49].

   (a) [19, Exercise 3.1.A5(b), p. 51] The subset of all matrices of the form $\begin{pmatrix} a & b \\ 0_{\mathbb{Z}} & c \end{pmatrix}$ (called *upper triangular matrices* in the ring $M(\mathbb{Z})$ of 2×2 integer matrices.

   (b) [19, Exercise 3.1.A6, p. 51] The subset $\{1, -1, i, -i\}$ of the ring $\mathbb{C}$.

   (c) [19, Exercise 3.1.A9, p. 51] The subset of $\mathbb{R}$ consisting of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{R}$.

4. (a) [19, Exercise 3.1.B24, p. 53] The addition table and part of the multiplication table for a three-element ring are given below. Use the distributive laws to complete the multiplication table.

$+$	r	s	t
r	r	s	t
s	s	t	r
t	t	r	s

$\cdot$	r	s	t
r	r	r	r
s	r	t	
t	r		

(b) Determine which element of the ring is the zero element.

(c) Show that this ring is isomorphic to $\mathbb{Z}_3$.

5. Prove that a ring R with a multiplicative identity 1_R cannot possess another element x with the same property, i.e. an element $x \neq 1_R$ such that $(\forall a \in R)[ax = a = xa]$.

6. (a) [19, Exercise 3.2.A11(a), p. 63] Prove that if a and b are units in a ring R with identity, then ab is also a unit, and its inverse is $b^{-1}a^{-1}$.

   (b) [19, Exercise 3.2.A11(b), p. 63] Give an example of two units a, b in some ring R such that $(ab)^{-1} \neq a^{-1}b^{-1}$.

   (c) [19, Exercise 3.2.A10, p. 63] Prove or disprove: The set of units in a ring R with identity is a subring of R.

7. (a) [19, Exercise 3.1.B27] Prove [19, Theorem 3.1, p. 49]: *Let R and S be rings. Define addition and multiplication in the Cartesian product set $R \times S$ by*

$$(r, s) + (r', s') = (r + r', s + s') \tag{7}$$
$$(r, s)(r', s') = (rr', ss') \tag{8}$$

   Then $R \times S$ is a ring, and its zero is $(0_R, 0_S)$. [Note that there are 8 properties to check.]

   (b) Prove that $R \times S$ is commutative if *and only if* R and S are both commutative.

   (c) Prove that, if R and S respectively have identities, 1_R, and 1_S, then $R \times S$ has an identity, and it is

$$1_{R \times S} = (1_R, 1_S)\,.$$

8. In a ring R with identity 1_R, the *characteristic* is defined to be the smallest integer n — if there is one — with the property that the sum of n copies of 1_R is 0_R; if there is no such integer, the characteristic is said to be 0. The sum of n copies of any element $x \in R$ is denoted by nx; thus a positive characteristic n is the smallest positive integer such that $n1_R = 0_R$ [19, p. 65]. Observe without proof [19, Exercise 3.2.B31(a)] that $\mathbb{Z}$ has characteristic 0, and that $\mathbb{Z}_n$ has characteristic n.

   (a) [19, Exercise 3.2.B31(b)] Determine the characteristic of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

   (b) [19, Exercise 3.2.B32] Prove that a finite ring with identity has characteristic n for some $n > 0$.

   (c) [19, Exercise 3.2.B33(a), p. 65] Prove that, in a ring R with identity 1_R and finite characteristic $n > 0$, $(\forall a \in R)[na = 0_R]$.

(d) [19, Exercise 3.2.B33(b), p. 65] Prove that, if R is an integral domain with identity 1_R and finite characteristic $n > 0$, n must be a prime.

(e) [19, Exercise 3.1.B29(a), p. 53]Use the preceding result to show that $\mathbb{Z}_4 \times \mathbb{Z}_6$ is not an integral domain. Then prove this result in another way, by exhibiting a *zero divisor* in the ring.

9. (cf. [19, Exercise 3.3.B33]) Show that the first ring is not isomorphic to the second.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and the ring $M(\mathbb{Z}_2)$ of 2×2 matrices with entries from $\mathbb{Z}_2$. [Hint: There are many ways to attack a problem of this type. The basic idea is to find some property that is preserved under isomorphism, and then to show that the two rings differ in this property. One property that one might wish to consider is the cardinality, but here the two rings have the same cardinality. Another approach could be based on looking at the set of *idempotents* — the members of the set $S = \{x | xx = x\}$. Show that, if there exists an isomorphism, it must map the set of idempotents of one ring on to the idempotents in the other ring. Then show that, in the present case, the cardinalities of the sets of idempotents are different.]

(b) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.

(c) $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$. (Hint: One of these rings is a field, the other is not.)

6 Consequences of the ring axioms

Distribution Date: Web — 28 January, 2002; lecture — 28 January, 2002; hard copy — 30 January, 2002

6.1 Assuming and/or proving properties of 0_R and, where it exists, 1_R, in a ring R

The properties of the additive identity, and, where it exists, the multiplicative identity will be seen to be very similar to the properties we are accustomed to for 0 and 1 in $\mathbb{R}$. While we have apparently assumed little about these elements (in Axioms 4 and 5, for 0_R, and in Axiom 10 for 1_R [19, §3.1, pp. 42-43]) many properties can be derived from the assumed *axioms*.

As an example, we derived in the lecture of Friday, January 25th, 2002, the property that $(\forall a)[a \cdot 0_R = 0_R]$. The derivation obtained at that time served the purpose of showing how mathematicians may explore possible ways of proving theorems; however, the proof finally obtained was not elegant; here is a somewhat cleaner proof:

$$\begin{aligned}
b \cdot 0_R &= b \cdot 0_R + 0_R \quad \text{by Axiom 4, with } a = b \cdot 0_R \\
&= b \cdot 0_R + ((b \cdot 0_R) + (-(b \cdot 0_R))) \quad \text{by Axiom 5 with } a = b \cdot 0_R \\
&= (b \cdot 0_R + b \cdot 0_R) + (-(b \cdot 0_R)) \quad \text{by Axiom 2} \\
&= b \cdot (0_R + 0_R) + (-(b \cdot 0_R)) \quad \text{by distributive law} \\
&= b \cdot 0_R + (-(b \cdot 0_R)) \quad \text{by Axiom 4 with } a = 0_R \\
&= 0_R \quad \text{by Axiom 5 with } a = b \cdot 0_R
\end{aligned}$$

Proceeding in a similar way (that is, by carefully choosing specific values for the quantified variables in the axioms), one can develop proofs for the other parts of [19, Theorem 3.5, p. 57]. In a similar way one can prove properties that one might expect to hold for 1_R. (For example, we can prove that $\forall a[(-1_R)a = -a]$.)

6.2 Closure under operations

In the definitions we saw for a ring [19, §3.1, p. 42] Axioms ##1,6 respectively postulate "closure" under the binary operations of addition and multiplication. These axioms are not needed at this point, as a *binary operation* on R is *defined* [19, Appendix B, p. 510] to mean a function from $R \times R$ to R, so the image of the function — i.e. respectively the *sum* and *product* — must be in the codomain of the function. Thus a ring is simply a set R and two binary operations satisfying the remaining 6 axioms. Let's use a notation $(R, +, \times)$ to denote a ring with underlying set R, where the operations are respectively $+$ and $\times$, each acting on $R \times R$ and taking their values in R.

The situation changes when we come to define a *subring* of a ring $(R, +, \times)$. Here we wish to consider a subset $S \subseteq R$, where the operations of addition and multiplication are the *restrictions* of the corresponding operations on R. For example, we wish to add two elements of S by considering them to be elements of R, and applying the addition rule $+$ of the ring R. In general, when we operate by $+$ on a pair of elements of S, their sum must be in R, but it need not happen that the sum is in S; when that is the case for all such pairs of elements, we say that $+$ is *closed under* $+$. In symbols: S is defined to be *closed under addition* $+$ if $(\forall a \in S)(\forall b \in S)[a + b \in S]$; an analogous definition is used for closure of S under $\times$.

It may happen that, using the defined operations on S and the defined element 0_R, and, for every $a \in S$, the defined additive inverse $-a$ (known to be unique by [19, p. 56, Theorem 3.3]) the structure with underlying set S will still be a ring. When that happens we call $(S, +, \times)$ a *subring of the ring* $(R, +, \times)$.[10]

6.2.0.3 THEOREM. *(cf. [19, Theorem 3.2, p. 49]) A subset S of the underlying set R of a ring $(R, +, \times)$ is a* subring *of $(R, +\times)$ if and only if:*

1. *S is closed under $+$;*
2. *S is closed under $\times$;*
3. *$0_R \in S$;*
4. *$(\forall a \in R)[-a \in S]$; equivalently, one may say that S is closed under the taking of the additive inverse.*

Because this theorem *characterizes* the notion of being a subring, we may find it convenient to use the four conditions as a *definition* of a subring. The characterization is not the "slickest" possible one, however.

6.2.0.4 EXERCISE. Show that, in Theorem 6.2.0.3, if we know that $S \neq \varnothing$, we don't need the third condition. Then explain why this observation requires that $S \neq \varnothing$.

[10] More precisely, it is the structure $(S, + \mid_{S\times S}, \times \mid_{S\times S}))$ since the domains of the functions have changed. The notation $f|_{S\times S}$ where $f : R \times R \to R$ is some function, means that the domain of f has been *restricted*. (Even this improved statement is still technically incorrect, as the codomain of the restriction is usually taken to be the codomain of the original function; here we wish to reduce the codomain also. These technical difficulties with terminology should not cause any problems at the level of this course.)

7 Two non-isomorphic rings

Distribution Date: Friday, February 1st, 2002

We prove that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$. These two rings both have cardinality 4, so there will certainly exist bijections between them; we need to prove that none of the bijections $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ has the two defining properties

$$f(a+b) = f(a) + f(b) \tag{9}$$
$$f(ab) = f(a) \cdot f(b) \tag{10}$$

All members (a_1, a_2) of $\mathbb{Z}_2 \times \mathbb{Z}_2$ have the property that $(a_1, a_2) + (a_1, a_2) = (a_1 + a_1, a_2 + a_2) = (0, 0)$, since all computations of coordinates are performed modulo 2. Any function $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$, will have the property that $f((a_1, a_2) + (a_1, a_2)) = f((0, 0))$. But one of the basic properties of any isomorphism is that 0 is carried on to 0; a generalization of this is proved in [19, Theorem 3.12(1), p. 72].[11] Since f is a homomorphism, it follows by property (9) that

$$f((a_1, a_2)) + f((a_1, a_2)) = 0$$

But f is a bijection, so every element b of $\mathbb{Z}_4$ must appear as an image of the form $b = f((a_1, a_2))$.[12] Thus we would have proved that every element $b \in \mathbb{Z}_4$ has the property that $b + b = 0$. But we know that this is not true; for example, $[1]_4 + [1]_4 = [2]_4$, and $[2]_4$ is not the same as $[0]_4$ — its elements are not multiples of 4. From this contradiction we may conclude that the two rings are not isomorphic.

The preceding is certainly not the only possible proof that the given rings are not isomorphic. An "exhaustive" solution could be based on testing each one of the 4! bijections; this would be inelegant, and could not be generalized to a problem of comparing two *infinite* rings, whereas the solution above would have infinite analogues.

8 Different ring structures on the same cartesian product

We have defined, in the lectures, the cartesian product $R \times S$ of two given rings, by "coordinate-wise" operations based on the operations in R and S. But it is possible to

[11] The proof in the textbook is formulated for a more general type of function, called a *homomorphism*. However, the details of the proof on page 73 hold, in particular, for isomorphisms.

[12] In practice mathematicians usually do not bother writing double sets of parentheses; so we would usually write $f(a_1, a_2)$ instead of $f((a_1, a_2))$.

impose other ring structures on the same underlying *set* $R \times S$.[13] One example is the *trivial* structure, in which all products are defined to be zero. Convince yourself that the definition $(a_1, b_1) \cdot (a_2, b_2) = (0_R, 0_S)$ actually defines a valid product (when combined with the usual definition of addition.)

Another interesting example will be given in the lectures. We shall show how the complex number field and the Cartesian product field can both be considered to have underlying *sets* $\mathbb{R} \times \mathbb{R}$.

[13]Remember — we use the symbol $R \times S$ to denote both the Cartesian product set of the two underlying sets, and the Cartesian product ring. In practice, if no statement to the contrary is given, you should assume that the ring structure is the that given in [19, Theorem 3.1, p. 49].

9 Third Problem Assignment

Distribution Date: Mounted on the Web on Thursday, February 7th, 2002
Distributed in hard copy on Monday, February 11th, 2002
Solutions are to be submitted on Friday, February 22nd, 2002
NOT LATER THAN THE END OF THE LECTURE

1. (cf. [19, Exercise 4.1.A6]) In which of the following cases is the given set a subring of the indicated ring? If it is a subring, prove that fact; if it is not, provide a counterexample, or prove the fact in some other way.

   (a) All polynomials in $\mathbb{R}[x]$ with constant term $0_{\mathbb{R}}$.

   (b) All polynomials of degree 2 in $\mathbb{C}[x]$.

   (c) All polynomials in $\mathbb{Z}[x]$ in which the coefficients of all even-degree terms are zero.

   (d) All polynomials in $\mathbb{Z}[x]$ in which the coefficients of all odd-degree terms are zero.

   (e) The zero polynomial, together with all non-zero polynomials in $\mathbb{Z}[x]$ in which the coefficient of the highest-degree term is non-negative.

   (f) The zero polynomial, together with all non-zero polynomials in $\mathbb{Z}[x]$ in which the coefficient of the highest-degree term is non-zero.

2. (In this problem we will be working with the complex numbers, defined as the points in the set $\mathbb{R} \times \mathbb{R}$, endowed with the usual (vector) definition of addition, but with the multiplication rule given in the lectures. The complex number we write as (a, b) can also be denoted by, for example, $a + b\sqrt{-1}$, or by $a + bi$.)

   (a) Show that the function $f : \mathbb{C} \to \mathbb{C}$ given by $(x, y) \mapsto (x, -y)$ defines an isomorphism.[14]

   (b) Show that the function $f : \mathbb{C} \to \mathbb{C}$ given by $(x, y) \mapsto (-x, -y)$ *does not* define an isomorphism.

3. (In the following problem the "long" divisions should be carried out showing all intermediate steps, for example, using the notation at the bottom of [19, p. 85].)

   Find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x) \cdot q(x) + r(x)$, and $r(x) = 0$ or $\deg r(x) < \deg g(x)$:

   (a) [19, Exercise 4.1.A5(b), p. 88] $f(x) = x^4 - 7x + 1$, and $g(x) = 2x^2 + 1$ in $\mathbb{Q}[x]$.

[14] An isomorphism of a ring or field or graph or... with itself is called an *automorphism*.

(b) [19, Exercise 4.1.A5(d), p. 88] $f(x) = 4x^4+2x^3+6x^2+4x+5$ and $g(x) = 3x^2+2$ in $\mathbb{Z}_7[x]$.

4. Use the Euclidean algorithm to find the greatest common divisor of the given polynomials over the given fields, and then — in parts (a) and (b) only — to express that greatest common divisor as a sum of multiples of the given polynomials (as described in [19, Theorem 4.5, p. 92]).

   (a) [19, Exercise 4.2.A5(b), p. 94] $f_1(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $g_1(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.

   (b) $f_2(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $g_2(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Z}_2[x]$. (Over this field, 2 is the same as 0, 5 is the same as 1, etc.)

   (c) $f_3(x) = x^4 + ix + 1$ and $g_3(x) = x^2 - (1 + i)x + 1$ in $\mathbb{C}[x]$.
   (Here i denotes the point $(0, 1)$ in the complex plane; a real number x is to be interpreted as the complex number $(x, 0)$. Observe that the inverse of $x + yi$, where not both x and y are 0, is $\frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$.
   While the complex numbers in this problem do not appear to be particularly abstruse, the computations can be expected to be unpleasant. The purpose is for students to face the realities of arithmetic in $\mathbb{C}$.)

5. Proceeding recursively, starting with the set $\{1\}$ consisting of the only monic irreducible polynomial of degree 0, we wish to determine the set S_n of irreducible polynomials in $\mathbb{Z}_2[x]$ of degree n, where $n \leq 3$ The recursion is based on the fact that the degree of a product of polynomials is the sum of their degrees [19, Theorem 4.2, p. 84].

   Polynomials of degree 0 are the non-zero constants, and the only one which is monic is the constant 1.

   Polynomials of degree 1 all have the form $a_0 + a_1x$, where $a_1 \neq 0$. There is only one non-zero element in this field, so $a_1 = 1$. But there are two possible values for a_0. Could either of these polynomials be reducible, i.e. the product of two polynomials of lower degree? The only lower degree available is degree 0, and the product of two polynomials of degree 0 again has degree 0. Hence neither of these polynomials is reducible, and we have $S_1 = \{x, 1 + x\}$.

   Carry this reasoning on to determine the members of S_2 and S_3.

6. (a) [19, Exercise 4.4.A4(a), p. 104] Determine all values of k, if any, for which $x - 2$ is a factor of $x^4 - 5x^3 + 5x^2 + 3x + k$ in $\mathbb{Q}[x]$.

   (b) [19, Exercise 4.4.A4(b), p. 104] Determine all values of ℓ, if any, for which $x + 1$ is a factor of $x^4 + 2x^3 - 3x^2 + \ell x + 1$ in $\mathbb{Z}_5[x]$.

(c) [19, Exercise 4.4.A7, p. 104] Use the Factor Theorem to show that $x^7 - x$ factors in $\mathbb{Z}_7[x]$ as

$$x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$$

without doing any polynomial multiplication. Explain why your argument could not be applied to the polynomial $x^{14} - x^2$.

7. [19, cf. Exercise 4.4.B8, p. 105] For each of the following polynomials, using the Factor Theorem or otherwise, determine whether it is irreducible in the given ring of polynomials:

   (a) $x^2 + 7$ in $\mathbb{R}[x]$

   (b) $x^2 - 7$ in $\mathbb{Q}[x]$

   (c) $x^2 + 7$ in $\mathbb{C}[x]$

   (d) $2x^3 + x^2 + 2x + 2$ in $\mathbb{Z}_5[x]$

   (e) $x^4 + x^2 + 1$ in $\mathbb{Z}_3[x]$

   (f) $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$

   (g) $x^4 + x^2 + 1$ in $\mathbb{R}[x]$.

10 Detailed syllabus corresponding to textbook chapters 1 – 4

Distribution Date: Draft version posted on the Web on Sunday, February 17th, 2002.
E.&O.E.[15]

Unless otherwise noted, all material is taken from the textbook.

10.1 Chapter 1, Arithmetic in $\mathbb{Z}$ Revisited, and applicable appendices

10.1.1 Logic and Proof, [19, Appendix A, p. 493]

This material was discussed in 189-240A. It is not examination material in this course in itself, but involves skills that are essential to understanding the material in this course.

10.1.2 The Division Algorithm, [19, §1.1]

Our theory begins with the *Well-Ordering Axiom*. This is a property we *postulate* for the natural numbers. (You should be familiar with the term *well ordered* from Mathematics 189-240A, a prerequisite to this course, cf. [35, Definition 4, p. 416].) You should understand the Division Algorithm in $\mathbb{Z}$; its proof was discussed in the lectures. The Division Algorithm is not stated in an "algorithmic" form, and should be considered an "existence" theorem. However, implementation of the algorithm for integers written in, say, the decimal system, can be viewed as algorithmic; think of the methods of "long division" that you learned in school. It is these methods that we will be generalizing later, in [19, §4.1], to a division algorithm for polynomials with coefficients taken from some field.

10.1.3 Well Ordering and Induction, [19, Appendix C, p. 519]

The Principle of Mathematical Induction [19, Theorem C.1, p. 520] should be familiar from Mathematics 189-240A. The Principle of Complete Induction [19, Theorem C.2, p. 522] is what was called "The Second Principle of Mathematical Induction" in [35, §3.2]. You should know that these principles are logically equivalent, and that they can be derived from the Well Ordering Axiom. You will not be expected to be able to prove these equivalences, but you could be expected to be able to write rigorous induction proofs in solving problems.

[15] "Errors and omissions excepted". This is the first version of this document, and there could be errors and/or omissions.

10.1.4 Divisibility, [19, §1.2, p. 7]

Concepts to be mastered: divisibility, divisor, greatest common divisor, relatively prime pairs of integers, Euclidean algorithm. [19, Theorem 1.3] characterizes (a, b) as the smallest positive member of the set of linear combinations of a and b (with integer coefficients). The definition of (a, b) can be replaced by an equivalent definition, given as [19, Corollary 1.4 to Theorem 1.3, p. 10]; that is, the characterization in this corollary can be used in place of the original definition. Students should know [19, Theorem 1.5] and its proof: *If* $a \mid bc$ *and* $(a, b) = 1$, *then* $a \mid c$. (The proof is important because it illustrates a use for the characterization of the g.c.d. as a linear combination. It is also significant because the proof does not require use of the Fundamental Theorem of Arithmetic.)

The concept of *least common multiple* may be mentioned, and could be needed in applications later [19, Exercise 1.2A31, p. 14].

10.1.5 Primes and Unique Factorization, [19, §1.3, p. 15]

Students should be comfortable with the concept of *primes*; often we intend to restrict a discussion to only the positive primes. [19, Theorem 1.8, p. 15] extends [19, Theorem 1.5, p. 10]. Students should read the proof of the [19, Fundamental Theorem of Arithmetic, p. 17], but will not be expected to memorize its proof.

10.1.6 Primality Testing, [19, §1.4, p. 20]

Students should know [19, Theorem 1.13, p. 20], which serves to justify the Sieve of Eratosthenes. They should also be aware that this result is thousands of years old! The concepts of Mersenne and Fermat primes are discussed in problems on Assignment 1.

10.1.7 Sets and Functions, [19, Appendix B, p. 504]

Most of this material was covered in 189-240A [35, §1.6, p. 46]. You are expected to be comfortable with these concepts whenever they appear.

10.1.8 Equivalence Relations, [19, Appendix D, p. 527]

This concept was studied in 189-240A, in [35, §6.5 and elsewhere].

10.1.9 Congruence and Congruence Classes, [19, §2.1, p. 24]

Students should be thoroughly familiar with this section, cf. [35, pp. 120-122]. Note that, eventually, we use replace the symbol $\oplus$ by $+$, and $\odot$ by $\cdot$ or even just by juxtaposition. Students should understand clearly the definitions of $\oplus$ and $\odot$, why there is a need for

preparation before stating these definitions. You should not memorize the proofs of the parts of [19, Theorem 2.7, p. 34], but should be able to product a proof of a problem of these types spontaneously.

10.2 Chapter 2: Congruence in $\mathbb{Z}$ and Modular Arithmetic

10.2.1 Modular Arithmetic [19, §2.2, p. 31]

Note the conventions:

- When we wish to specify modulus n for a congruence class $[a]$ we may write $[a]_n$; usually the modulus can be determined from the context, and, in such cases, we may suppress the subscript.
- We usually write $+$ instead of $\oplus$; instead of $\odot$ we may write $\cdot$ or $\times$ or simply juxtapose the factors.
- We often denote $[a]$ simply by a; in this notation we could write, for example, $1 + 1 = 0$ (instead of $[1]_2 \oplus [1]_2 = [0]_{\mathbb{Z}_2}$ or $= 0_{\mathbb{Z}_2}$) in $\mathbb{Z}_2$.
- We may use exponential notation in the obvious way, writing, for example, 3^2 instead of $3 \cdot 3$. The properties of the exponentials can be proved by induction; there are no surprises.

10.2.2 The Structure of $\mathbb{Z}_p$ When p is Prime [19, §2.3, p. 37]

It is suggested that, in addition to becoming familiar with the theorems in this section in their stated forms, students rephrase each of the theorems in the language of congruences, and also in terms of equations in $\mathbb{Z}$. For example, [19, Theorem 2.11(1), p. 39] reads *Let a, b, n, be integers with $n > 1$, and let $d = (a, n)$. Then the equation $[a]x = [b]$ has solutions in $\mathbb{Z}_p$ iff $d|b$.* In terms of congruences it could read (replacing x by $[u]$) *Let a, b, n, be integers with $n > 1$, and let $d = (a, n)$. Then the congruence $au \equiv b \pmod{n}$ has solutions $u \in \mathbb{Z}$ iff $d|b$.*[16] A formulation in terms of an equation would be *Let a, b, n, be integers with $n > 1$, and let $d = (a, n)$. Then the equation $au = b + kn$ has solutions $(u, k) \in \mathbb{Z} \times \mathbb{Z}$ iff $d|b$.*

10.3 Chapter 3: Rings

10.3.1 Definition and Examples of Rings [19, §3.1, p. 42]

Students should read all the examples. Note that axioms ##1, 8 of closure are not required in the definition of a ring, since a *(binary) operation* on a set R is, by definition,

[16] This result, with this type of formulation, was proved in these notes as Theorem 4.0.0.2.

required to take its values in R. [19, Theorem 3.2, p. 49] may be used as a *definition* of a subring, replacing the definition in the textbook just before the *enunciation* of the theorem. In class we considered the significance of the requirement in an integral domain R, and particularly a field R, that $0_R \neq 1_R$. We also proved the uniqueness of the additive and multiplicative identities (if the latter exists) and the uniqueness of additive and multiplicative inverses (if the latter exist).

The ring $\mathbb{C}$ of complex numbers will be defined first as a structure built on the Cartesian produce set $\mathbb{R} \times \mathbb{R}$, with the usual vector addition rule, but with the multiplication rule $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. This should be seen to be equivalent to the treatment in the textbook example [19, p. 47], where one considers "objects" of the form $a + bi$, where $a, b \in \mathbb{R}$. Here i denotes the point $(0, 1) \in \mathbb{R} \times \mathbb{R}$, and $+$ denotes the addition operation in the ring we have constructed. A subring of our ring is the set $\{(x, 0) : x \in \mathbb{R}\}$, which is isomorphic to the ring $\mathbb{R}$, and $a + bi$ may be interpreted as the sum $(a, 0) + (0, b)$. What we have described here is an *isomorphism* between two ways of expressing the field $\mathbb{C}$. We will also consider another formulation of $\mathbb{C}$, where the points are matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ and prove the obvious isomorphism. (The isomorphism is described in [19, pp. 47-48], but with b replaced by $-b$; it was discussed at length in the lecture of February 6th, 2002.)

10.3.2 Basic Properties of Rings [19, §3.2, p. 56]

We did not study [19, Theorem 3.11, p. 61] *Every finite integral domain R is a field.* Perhaps we shall return to prove this theorem when we study groups.

10.3.3 Isomorphisms and Homomorphisms [19, §3.3, p. 66]

We have not studied *homomrphisms* yet, but we did consider *isomorphisms*, which are bijective homomorphisms. It suffices to consider the homomorphism theorems only in the special case of isomorphisms. (This omission was to simplify the treatment, by reducing the abstraction and the class time required.)

10.4 Chapter 4: Arithmetic in $F[x]$

10.4.1 Polynomials [19, Appendix G, p. 542]

For a commutative ring R the set of polynomials may be defined in several equivalent ways. Students need not be familiar with all the material in this appendix, but should understand clearly the need for definitions of the ring operations, and the nature of those definitions, involving "term-by-term" sums and the "Cauchy" (convolution) product, although they need not remember these terms. The familiar properties of polynomials,

seen earlier in calculus courses, can be justified algebraically in this way. (Recall, for example, the expansion of rational functions of polynomials into "partial fractions", where the determination of the numerators of the fractions can involve equating coefficients of corresponding powers of the indeterminate of two "equal" polynomials.) Another treatment of this subject may be found in these notes §A.7.3.

10.4.2 Formal Power Series (§A.7.3)

This topic is not discussed in the textbook, and so will only be referred to in passing. Student should understand the definitions. Formal power series with real coefficients have been seen by student in course 189-240A, where they were used as ordinary and exponential generating functions for sequences of real numbers. We may use either of the notations $R[[x]]$ and $R\{x\}$ for the ring of formal power series in an indeterminate x over the ring R, and will interpret the ring $R[x]$ as the subring of this ring consisting of the series wherein all but a finite number of coefficients are 0_R.

10.4.3 Polynomial Arithmetic and the Division Algorithm $F[x]$ [19, §4.1, p. 81]

Students may follow the practice of the book, of not assigning a degree to the 0 polynomial; or, alternatively, define the degree of 0 to be $-\infty$. In this latter alternative one is working in an extension of the ring $\mathbb{Z}$, wherein the operations of addition and multiplications are not defined for certain excluded pairs, e.g. we do not give a meaning to $(-\infty) + \infty$. We do not assign a meaning to this sum because, no matter which element of the extended ring to which we might wish to assign this value, we would arrive at contradictions to the ring properties that we wish to preserve. So $\mathbb{Z} \cup \{-\infty, \infty\}$ is not a ring! But it is still possible do carry out meaningful computations there, as students should have seen in their calculus courses.

Some of the concepts in this and subsequent sections are meaningful for polynomials with coefficients coming from a general ring; but, for the most part, we will require that the ring of coefficients R of $R[x]$ have additional properties: we usually want to have $1_R \in R$; in this course we will study only polynomial rings where the ring is commutative, although students may see results concerning the ring $M(\mathbb{R})[x]$ in their linear algebra course; we shall usually require that the ring be an *integral domain*, in order that the theorem that the degree of a product of polynomials is the sum of the degrees of the factors should hold; and some of our results may hold only when the coefficients come from a field.

10.4.4 Divisibility in $F[x]$ [19, §4.2, p. 90]

In order to render unique the greatest common divisor of two polynomials, not both 0, we "normalize" by requiring that the polynomial be *monic*, that is, that its leading coefficient — the coefficient of the highest power of the indeterminate having a non-zero coefficient — be 1. Of course, we do not use this concept unless the ring R has a 1_R.

10.4.5 Irreducibles and Unique Factorization [19, §4.3, p. 94]

We may deviate from the language of the textbook, and include non-zero constant polynomials among those called *irreducible*. Students should be familiar with the properties of polynomials over a field that are analogous to the factorization of integers into powers of primes.

10.4.6 Polynomial Functions, Roots, and Reducibility [19, §4.4]

The distinction between *polynomials* in $R[x]$ and *polynomial functions* $f : ER \to R$ will not be stressed. The spirit of the treatment we are following is that the properties of polynomials learned in calculus courses can be proved rigorously, if time permitted that in the course, and students should not be uncomfortable relying on their intuition when working with polynomials *over a field*. However, students should try to analyze the operations they perform on polynomials to see where the filed properties are needed, as opposed to taking polynomials over general rings. The Remainder Theorem and Factor Theorem will be proved and applied. Students should observe that polynomials of degree 4 or greater may be reducible even though they may have no roots.

10.4.7 Irreducibility in $\mathbb{Q}[x]$ [19, §4.5, p. 107]

Contrary to the information in the first timetable circulated, this section may be omitted. It is suggested that students read [19, Theorem 4.20 (Rational Root Test), p. 107], although this will not be examination material.

10.4.8 Irreducibility in $\mathbb{R}[x]$ and $\mathbb{C}[x]$ [19, §4.6, p. 115]

The *automorphism* of $\mathbb{C}$ given by *conjugation* $(x, y) \mapsto \overline{(x, y)} = (x, -y)$, (equivalently $x + iy \mapsto x - iy$) was discussed in the lecture of February 15th, 2002. It was proved that polynomials in $\mathbb{R}[z]$, when interpreted as polynomials in $\mathbb{C}[z]$, have, corresponding to any root $x + iy$ a root $x - iy$. The implications to irreducibility of real polynomials was discussed.

(This page has been left blank intentionally.)

11 Solutions, First Problem Assignment

Distribution Date: Mounted on the Web on Tuesday, February 19th, 2002
Solutions were to be handed in on Friday, January 25th, 2002
(First version, subject to correction of misprints and errors.)

1. (a) [19, Exercise 1.2.A1(h)] Use the Euclidean Algorithm to calculate $(12378, 3054)$. (This can be done by hand, but you may wish to use a calculator; in any case show all your work, systematically.)

   (b) [19, Exercise 1.2.B15(h)] Use the preceding computations (by "back substitution") to determine a decomposition of $(12378, 3054)$ in the form

   $$(12378, 3054) = 12378u + 3054v \tag{11}$$

   (c) Find another decomposition in form (11).

   Solution:

   (a)

   $$\begin{aligned} 12378 &= 3054 \cdot 4 + 162 \\ 3054 &= 126 \cdot 18 + 138 \\ 162 &= 138 \cdot 1 + 24 \\ 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 + 0 \\ \Rightarrow (12378, 3054) &= 6 \end{aligned}$$

   (b)

   $$\begin{aligned} 6 &= 24 - 18 \cdot 1 = 24 - (138 - 24 \cdot 5) \cdot 1 \\ &= 138 \cdot (-1) + 24 \cdot 6 = 138 \cdot (-1) + (162 - 138 \cdot 1) \cdot 6 \\ &= 162 \cdot 6 + 138 \cdot (-7) = 162 \cdot 6 + (3054 - 162 \cdot 18) \cdot (-7) \\ &= 3054 \cdot (-7) + 162 \cdot 132 = 3054 \cdot (-7) + (12378 - 3054 \cdot 4) \cdot 132 \\ &= 12378 \cdot 132 + 3054 \cdot (-535) \end{aligned}$$

   (c) Suppose that we have two decompositions,

   $$\begin{aligned} (12378, 3054) &= 12378 \cdot 132 + 3054 \cdot (-535) \\ (12378, 3054) &= 12378u + 3054v \end{aligned}$$

Subtracting yields $0 = 12378 \cdot (132 - u) + 3054 \cdot (-535 - v)$, or, after division by $(12378, 3054) = 6$, $0 = 2063 \cdot (132 - u) + 509 \cdot (-535 - v)$. In this last equation, 509 divides the second summand, so it must divide the first; but, as it is relatively prime to 2063, it must divide $132 - u$ [19, Theoroem 1.5, p. 10]; so there exists an integer k such that $132 - u = 509k$, i.e.

$$u = 132 - 509k\,; \tag{12}$$

this implies that $535 + v = 2036k$, so

$$v = -535 + 2063k\,. \tag{13}$$

Conversely, it is easy to see that any value of k satisfying (12) and (13) will yield a decomposition of the form (11). We have, in this example, sketched a proof of a general theorem: if $u = u_0$, $v = v_0$ is one decomposition of the form $(a, b) = au + bv$, then the most general solution is of the form $u = u_0 + k\frac{b}{(a,b)}$, $v = v_0 - k\frac{a}{(a,b)}$.

The problem asked for just one solution other than that found earlier: we could take any integer value of k except $k = 0$. For example, $k = 1$ yields the solution $u = -377$, $v = 1528$, i.e.,

$$(12378, 3054) = 12378 \cdot (-377) + 3054 \cdot 1528\,.$$

2. [19, Exercise 1.3.B22(b), p. 19]

   (a) Prove that there are no nonzero integers a, b such that $a^3 = 2b^3$. [Hint: Use the Fundamental Theorem of Arithmetic or [19, Theorem 1.8, p. 15].]

   (b) Prove that $\sqrt[3]{2}$ is irrational. [Hint: Use proof by contradiction. Assume that $\sqrt[3]{2} = \frac{a}{b}$, with $a, b \in \mathbb{Z}$ and use part (a) to reach a contradiction. Show first that it is possible to assume that $(a, b) = 1$, by using the result of [19, Exercise 1.2.B16, p. 13] without proof.]

   Solution:

   (a) **Solution using Fundamental Theorem:** We may factorize a and b so that $a^3 = 2b^3$ may be rewritten in the form

   $$\left(\frac{a}{(a,b)}\right)^3 (a,b)^3 = 2\left(\frac{b}{(a,b)}\right)^3 (a,b)^3 \tag{14}$$

   and then divide out the common factor $(a, b)^3$ to obtain

   $$\left(\frac{a}{(a,b)}\right)^3 = 2\left(\frac{b}{(a,b)}\right)^3 \tag{15}$$

Now rename $a' = \frac{a}{(a,b)}$ and $b' = \frac{b}{(a,b)}$, so that the equation becomes

$$(a')^3 = 2\,(b')^3 \tag{16}$$

Both a' and b' admit decompositions into products of powers of primes, unique up to the order in which they are written. The decomposition on the right side of equation (16) contains a 2, hence 2 must appear in the prime decomposition of a'. But that means that the left side will be divisible by 2^3, so the right side also is divisible by 2^3. One of these 2's comes from the first factor; the other two 2's come from $(b')^3$, so 2 must be a prime in the decomposition of b'. But this means that both a' and b' are even, and that contradicts the conclusion of [19, Exercise 1.2.B16] that they should be relatively prime.

From this contradiction we conclude that there do not exist a and b such that $a^3 = 2b^3$.

We could also argue in the following way by considering the prime decompositions of the two sides of equation (16). The exponent of the prime 2 on the left side of the equation $a^3 = 2b^3$ must be 3 times the exponent of 2 in a, so it is congruent to 0 modulo 3; the exponent of 2 on the right side will be 1 plus 3 times the exponent of 2 in b; from this contradiction we conclude that the original equation is not valid.

Solution using Theorem 1.8: Since 2 divides $2b^3$, it must divide a^3, which may be interpreted as a product $a \cdot a^2$; hence $2|a$ or $2|a^2$; in the latter case we may interpret a^2 as a product $a \cdot a$ and apply the reasoning again, to conclude that $2|a$. But, if $a = 2a_1$, then $4c^3 = b^3$, so a similar argument yields the fact that $2|b$ so b is of the form $2b_1$. Hence, dividing both sides of the equation by 2^3, we obtain $a_1^3 = 2b_1^3$. Considering the set of ordered pairs (a, b) of positive integers such that $a^3 = 2b^3$, let S be the set of integers that appear as the first coordinate of the ordered pairs. By the Well-Ordering Axiom, this set has a smallest element, say a_0, so that there exists a positive integer b_0 such that $a_0^3 = 2b_0^3$. Then the preceding argument leads us to the ordered pair $(\frac{a_0}{2}, \frac{b_0}{2})$, contradicting the minimality of a_0. We must conclude that there exists no solution in positive integers to the equation $a^3 = 2b^3$.

(b) If $\sqrt[3]{2}$ is expressible as a ratio of integers, $\frac{a}{b}$, then $2 = \frac{a^3}{b^3}$, and hence $a^3 = 2b^3$. But this contradicts (a). From this contradiction we conclude that no such integers a, b can exist, i.e. that $\sqrt[3]{2}$ is not rational.

3. (a) [19, Exercise 1.2.B20(a), p. 13],[19, Exercise 2.1.B22, p. 30] If $a^2 \equiv 1 \pmod 2$, prove that $a^2 \equiv 1 \pmod 4$.

(b) (cf. [19, Exercise 1.1.B8, p. 7], [19, Exercise 1.2.B20(b), p. 13]) If $a^2 \equiv 1 \pmod 2$, prove that $a^2 \equiv 1 \pmod 8$. [Hint: Use the fact that one of any two consecutive integers is even.]

Solution:

(a) Could a be even? If it were, then a^2 would also be even, contradicting the hypothesis. So $a \equiv 1 \pmod 2$, and $(\exists m)[a = 2m + 1]$. But then $a^2 = 1 + 4(m^2 + m) \equiv 1 \pmod 4$.

(b) As before, $a^2 = 1 + 4m(m+1)$. But one of m, $m+1$ is even, so their product is even, and $4m(m+1)$ is divisible by $4 \times 2 = 8$.

4. [19, Exercise ApB.B24, p. 517] Determine whether the given operation on $\mathbb{R}$ is commutative (that is, $(\forall a)(\forall b)[a * b = b * a]$) and whether it is associative (that is, $(\forall a)(\forall b)(\forall c)[a * (b * c) = (a * b) * c]$).

(a) $a * b = 2^{ab}$

(b) $a * b = ab^2$

(c) $a * b = 0$

(d) $a * b = (a + b)/2$

(e) $a * b = 1$

(f) $a * b = b$

(g) $a * b = a^2 + b^2$

(h) (This example is not from the textbook.) $a * b = \sqrt{a^2 + b^2}$

Solution:

(a) The operation is commutative since multiplication of real numbers is commutative. More precisely,

$$\begin{aligned} a * b &= 2^{ab} \\ &= 2^{ba} \quad \text{by commutativity of multiplication in } \mathbb{R}^2 \\ &= b * a \end{aligned}$$

We can prove that the operation is *not* associative by providing a counterexample: $0 * (0 * 1) = 2^{0\cdot(0*1)} = 2^{0\cdot 2^{0\cdot 1}} = 2^{0\cdot 2^0} = 2^{0\cdot 1} = 2^0 = 1$, but $(0 * 0) * 1 = 2^{(0*0)\cdot 1} = 2^{2^{0\cdot 0}\cdot 1} = 2^{2^0\cdot 1} = 2^{1\cdot 1} = 2^1 = 2$.

(b) In this case the lack of symmetry in the definition should immediately alert you to the failure of commutativity, which we demonstrate with a counterexample: $1*3 = 1\cdot 3^2 = 9 \neq 3 = 3\cdot 1^2 = 3*1$. Nor is this relation associative: $(1*1)*3 = (1\cdot 1^2) * 3 = 1 * 3 = 1 \cdot 3^2 = 9 \neq 81 = 1 \cdot 9^2 = 1 * 9 = 1 * (1 \cdot 3^2) = 1 * (1 * 3)$.

(c) This "trivial" law of combination is both commutative and associative, since the image of the function * consists of just one point: all functions have to point to the same unique point.

(d) **Commutativity:** By commutativity of addition of real numbers $a*b = \frac{a+b}{2} = \frac{b+a}{2} = b*a$.

Associativity: Here is a counterexample: $(0*0)*1 = \frac{\frac{0+0}{2}+1}{2} = \frac{1}{2} \neq \frac{1}{4} = \frac{0+\frac{0+1}{2}}{2} = 0*(0*1)$

(e) Use the same reasoning as expressed above in part 4c. This law of combination is also both commutative and associative.

(f) **Commutativity:** Here is a counterexample to commutativity: $0*1 = 1 \neq 0 = 1*0$.

Associativity: This operation is, indeed, associative, since, for all a, b, c, $(a*b)*c = b*c = c = b*c = a*(b*c)$.

(g) This operation is commutative, since, by commutativity of addition in $\mathbb{R}$, $a^2+b^2 = b^2+a^2$. It is not associative; for example, $(0*0)*3 = (0^2+0^2)^2+3^2 = 9$, but $0*(0*3) = 0^2+(0^2+3^2)^2 = 81$.

(h) Commutativity follows a similar proof to the preceding example. But this operation *is* associative:

$$\begin{aligned}(a*b)*c &= \sqrt{a^2+b^2}*c \\ &= \sqrt{(\sqrt{a^2+b^2})^2+c^2} \\ &= \sqrt{(a^2+b^2)+c^2} \\ &= \sqrt{a^2+(b^2+c^2)} \quad \text{by associativity of + in R} \\ &= a*(\sqrt{b^2+c^2})^2 = a*(b*c)\end{aligned}$$

5. [19, Exercise ApB.B28, p. 517]

(a) Let $f : B \to C$ and $g : C \to D$ be functions such that $g \circ f$ is injective. Prove that f is injective.

(b) Give an example of the situation in part (a) in which g is not injective. Your example should be "best possible" in that you should make $|B \cup C \cup D|$ as small as possible for such a counterexample.

Solution:

(a) For any $b_1 \in B$ and $b_2 \in B$,

$$\begin{aligned} f(b_1) = f(b_2) &\Rightarrow g(f(b_1)) = g(f(b_2)) \\ &\Rightarrow (g \circ f)(b_1) = (g \circ f)(b_2) \\ &\qquad \text{by definition of } g \circ f \\ &\Rightarrow b_1 = b_2 \quad \text{since } g \circ f \text{ is injective} \end{aligned}$$

(b) Since g is not injective, its domain needs to have more than one point: let $C = \{\ell, m\}$. In order for it not to be injective, we have to map both points to the same point of D; thus D cannot be empty — let's take $D = \{d\}$, and let g be the "constant" function that maps all points of C to d. We can arrange for a counterexample by taking $B = \varnothing$, in which case $g \circ f$ is an "empty" function, since there are no points to map: such a function is "vacuously" injective. If this counterexample is not satisfying[17], we could take $B = \{b\}$ and map it under f to just one of the points of C, say $f(b) = \ell$. Then $g \circ f$ must be injective, since its domain has only one point, but g is not injective.

6. (a) (cf. [19, Exercise ApD.A6, p. 531]) For any integer m, let $m\mathbb{Z}$ denote the set of integer multiples of m. Prove that the following relation on the points in the coordinate plane $\mathbb{R}^2$ is an equivalence relation:

$$(x, y) \sim (u, v) \quad \text{iff} \quad ((x - u) \in 3\mathbb{Z}) \wedge ((y - v) \in 2\mathbb{Z})\,. \tag{17}$$

(b) Show that every equivalence class $[(x, y)]$ under $\sim$ has a member (called a *representative*) in the rectangle $R = \{(x, y) : 0 \leq x < 3, 0 \leq y < 2\}$. In particular, find the *representative* of $[(-2, \pi)]$ in this rectangle.

(c) For the relation $\sim$ defined above, let us define a measure of "distance" on the equivalence classes of the points of $\mathbb{R}^2$ under $\sim$. For classes $[(x, y)]$ and $[(u, v)]$ define the distance $d([(x, y)], [(u, v)])$ to be the minimum distance in $\mathbb{R}^2$ between any point in $[(x, y)]$ and any point in $[(u, v)]$.[18] Suppose that 7 points are placed anywhere in $\mathbb{R}^2$. Show that, with the preceding definition of distance, there must be two of these points whose distance is less than $\sqrt{2}$. [Hint: Divide the rectangle R into 6 squares of side 1, and show that at least

[17] NOTE TO THE GRADER: Please accept either version of this counterexample as the "best possible" counterexample.

[18] An equivalent way of looking at this definition is to think of rolling the plane into a cylinder whose axis is parallel to the x-axis, and whose circumference is 2, and then "identifying" pieces of this cylinder of length 3 (measured along the axis); except for the fact that the surface is deformed, this could also be achieved by taking a 3-unit length and gluing together the two circular boundaries to form a torus (the surface of a doughnut).

two of the points have a representative in the same unit square. Then observe — without proof — that the maximum distance between two points in the square is attained when the points are at opposite corners.]

(d) Show that the following relation on the points in $\mathbb{R}^2$ is *not* an equivalence relation, explaining precisely which property/properties of an equivalence relation fail/fails to hold:

$$(x, y) \backsim (u, v) \quad \text{iff} \quad ((x - v) \in 3\mathbb{Z}) \wedge ((y - u) \in 2\mathbb{Z}) \,. \tag{18}$$

Solution:

(a) **Reflexive:** For any point $(x, y) \in \mathbb{R}^2$, $x - x = 0 = 0 \cdot 3$ and $y - y = 0 = 0 \cdot 2$; thus $(x, y) \sim (x, y)$.

Symmetric: Suppose that $(x, y) \sim (u, v)$. By definition this implies that $\exists m, n \in \mathbb{Z}$ such that $x - u = 3m$, $y - v = 2n$. Then $u - x = 3 \cdot (-m)$ and $v - y = 2 \cdot n$. By definition, these two properties are equivalent to $(u, v) \sim (x, y)$.

Transitive: Suppose that $(x, y) \sim (u, v)$ and that $(u, v) \sim (r, s)$, where $x, y, u, v, r, s \in \mathbb{R}$. Then there exist integers a, b, c, d such that

$$x - u = 3a \tag{19}$$
$$y - v = 2b \tag{20}$$
$$u - r = 3c \tag{21}$$
$$v - s = 2d \tag{22}$$

Then

$$(19),\ (21) \Rightarrow x - r = 3(a + c) \text{ and } y - s = 2(b + d)$$

which together imply that $(x, y) \sim (r, s)$.

(b) Every point (x, y) is equivalent to all points $(x + 3m, y + 2n)$, where m and n are any integers. If we subtract from x the integer $3 \left\lfloor \frac{x}{3} \right\rfloor$, we obtain a real number x_0 such that $0 \leq x_0 < 3$; x_0 is the remainder upon division of x by 3. Similarly, if we subtract from y the integer $2 \left\lfloor \frac{y}{2} \right\rfloor$, we obtain a real number y_0 such that $0 \leq y_0 < 2$; y_0 is the remainder upon division of y by 2; thus $(x, y) \sim (x_0, y_0)$, where $(x_0, y_0) \in R$. In particular,

$$[(-2, \pi)] = \{(-2 + 3m, \pi + 2n) : m, n \in \mathbb{Z}\}$$

Among the members of this equivalence class is $(-2 + 3, \pi - 2)$, lying in the designated rectangle. This point is a *representative* of the class in the sense that

$$[(-2, \pi)] = \{(-2 + 3m, \pi + 2n) : m, n \in \mathbb{Z}\} = [(-2 + 3, \pi - 2)] \,.$$

(c) This is a simple application of the Pigeonhole Principle. There are six squares in R having sides parallel to the coordinate axes and vertices being integer coordinates. More precisely, each of these squares should be considered as containing its bottom edge and its left edge, but not the other two sides. Among seven equivalence classes under $\sim$, each containing precisely one point in R, there must be at least 2 having their representatives in the same square. The maximum distance between two points in a square would be $\sqrt{2}$, *if the entire boundary were included*; but, if only the bottom and left sides are included, then this maximum will not be attained: that is, two points must be strictly less than $\sqrt{2}$ units apart. Hence the distance between the two corresponding equivalence classes must be less than $\sqrt{2}$. Compare [31, 14th Putnam Competition (1954) Problem #2, pp. 387–388].

(d) This relation is not reflexive; for example, $(1,0) \not\backsim (1,0)$. Nor is it symmetric. For example, $(1,0) \backsim (0,4)$ since $1 \equiv 4 \pmod 3$ and $0 \equiv 0 \pmod 2$; but $(0,4) \not\backsim (1,0)$ since $4 \not\equiv 1 \pmod 2$. We can find a counterexample to transitivity by taking a point off this line. For example, $(1,0) \backsim (0,1)$ and $(0,1) \backsim (1,0)$, but $\neg((1,0) \backsim (1,0))$.

7. [19, Exercise ApC.B14, p. 525] At a social bridge party every couple plays every other couple exactly once. Assume there are no ties.

(a) If n couples participate, prove that there is a "best" couple u in the following sense: for every couple v *distinct from*[19] u, u beats v or u beats a couple that beats v.

(b) Show by example (for any n) that there may be more than one "best" couple.

- Hint: (A convenient way to represent this type of bridge party is a *tournament*, which is a directed simple graph in which the couples are the vertices, and an edge is directed a to b if couple b defeats couple a.) Prove the claim by induction on n. Take the case $n = 1$ as the Basis Step. In the inductive step, after making the induction hypothesis, select any couple a, and prove the existence of a couple b which is "best" for all couples except possibly a. Then show that, if b is not "best" for all the couples, then a is "best".
- The use of the English superlative "best" is unfortunate, since it suggests uniqueness.

Solution:

[19] Note that this essential exclusion was overlooked in the textbook.

(a) **Basis Step:** If there is only one couple u, then there exists no couple v distinct from u so the desired property holds.

Induction Step: Suppose that the property holds for all parties with n couples, and assume there are $n+1$ couples, where $n > 0$. Select *any* couple a, and apply the induction hypothesis to the remaining n couples. There will exist a couple b which beats some of the couples — say c_i, $(i = 1, ..., k)$ and is beaten by the remaining couples, d_j, where, for each j there exists a c_{i_j} $(1 \leq i_j \leq k)$ which beats d_j $(j = 1, ..., n-k-1)$. There are three cases:

Case I: b **beats** a**.** In this case b is "best" for the party of $n+1$ couples.

Case II: a **beats** b**, but one of** c_i $(i = 1, \ldots, k)$ **beats** a**.** In this case b is again "best" for the party, since it beats a couple that beats a.

Case III: a **beats** b**, and none of** c_i $(i = 1, \ldots, k)$ **beats** a**.** In this case a beats all of the couples that b beats, and also b itself; and we know that each of d_j is beaten by couple c_{i_j} beaten by a $(j = 1, \ldots, n-k-1)$. So this time a is "best".

(b) If there are only one or two couples, then there is just one that is "best". But, if there are three couples, consider the *cyclically oriented tournament* in which a defeats b, which defeats c, which defeats a. Then all three of the couples are "best". (The other tournament with three vertices, the *transitively oriented tournament* does have a unique "best" vertex.)

8. [19, Exercise 1.2.A8, p. 13] If $r \in \mathbb{Z}$ and r is a non-zero solution of $x^2 + ax + b = 0$, (where $a, b \in \mathbb{Z}$), prove that $r|b$.

Solution: The hypothesis states that $r^2 + ar + b = 0$, so $b = r(r + a)$, expressing b as a multiple of r, which is equivalent to stating that $r|b$.

9. (a) [19, Exercise 1.4.A4] Verify that $2^5 - 1$ and $2^7 - 1$ are prime, but that $2^{11} - 1$ is not prime.

(b) [19, Exercise 1.4.B7] Let $p > 1$. If $2^p - 1$ is prime, prove that p is prime. [Hint: Prove the contrapositive, i.e., if p is composite, so is $2^p - 1$.]

(c) [19, Exercise 1.4.B9] If $k \geq 1$, and $2^k + 1$ is prime, prove that $k = 2^t$ for some t. [Hint: Verify that, if n is odd, $x^n + 1 = (x+1)\left(x^{n-1} - x^{n-2} + \ldots - x + 1\right)$. Factorize k by dividing out 2 repeatedly until it can be written in the form $k = 2^t \ell$, where ℓ is odd.]

Solution:

(a) $2^5 - 1 = 31$. By [19, Theorem 1.13, p. 20], we need only look for prime factors not exceeding $\lfloor \sqrt{31} \rfloor = 5$. It's not even; it's not divisible by 3 since the sum of

its digits (4) is not divisible by 3; it's not divisible by 5 since all such integers end in 0 or 5 (when written in the decimal system).

$2^7 - 1 = 127$. Here we look for prime factors not exceeding $\lfloor\sqrt{127}\rfloor = 11$. It is not even, and not divisible by 3 by the test used above [19, Exercise 1.2.B32, p. 14]. There are simple tests for divisibility by[20] 5 and 11 that may be discussed in the lectures. When divided by 7 the remainder is 1. Thus 127 is also prime.

But $2^{11} - 1 = 2047$. Its primality can be tested by dividing by primes not exceeding its square root, hence not exceeding 45 (or 43, since 44 and 45 are evidently not primes). We find, after trying all primes 2, 3, 5, 7, 11, 13, 17, 19, that $2047 = 23 \cdot 89$.

(b) See the sketch of solution in [19, p. 555]. The polynomial $x^{mn} - 1$ can be factored as the product of $x^m - 1$ and $(x^m)^{n-1} + (x^m)^{n-2} + \ldots + x^m + 1$. The factorization of the polynomial implies a factorization of the integer obtained by giving x, m, and n positive integer values. However, for the purpose of proving primality, we need to ensure that both of the factors are greater than 1. Here we are taking $x = 2$: the factorization will be non-trivial iff[21] $m > 1$ and $n > 1$ — i.e. iff the integer mn is not prime. Primes of the form $2^p - 1$ are called *Mersenne* primes.

(c) This time we consider factorization of a polynomial $x^{mn} + 1$. First observe that $y^n + 1$ *where* n *is odd* factorizes as $y^n + 1 = (y+1)(y^{n-1} - y^{n-2} + \ldots - y + 1)$. Substitution of $y = x^m$ produces a factorization of $x^{mn} + 1$. Thus we see that $x^{mn} + 1$ factorizes whenever the product mn is odd — i.e. whenever both factors m, n are odd! When we substitute $x = 2$ we obtain a factorization of $2^{mn} + 1$. We have to observe that the factorization is *non-trivial*, that is, that neither of the factors is 1. When m and n are both greater than 1, both factors $2^m + 1$ and $\left((2^m)^{n-1} - (2^m)^{n-2}\right) + \ldots + \left((2^m)^2 - 2^m\right) + 1$ are greater than 1. Thus the only way in which $2^k + 1$ can be prime is for $k = 0$ or $k = 1$ or k cannot be factorized into a product with an odd factor exceeding 1; by the Fundamental Theorem of Arithmetic, this is equivalent to stating that k must be a positive power of 2.

Primes that have the form $2^k + 1$ are called *Fermat* primes, in deference to Pierre Fermat, who believed that *all* integers of this form are[22].

---

[20] See the preceding paragraph.

[21] The *iff* does not show that this is a criterion for primality, since $2^p - 1$ could have a different type of factorization, even where p is a prime — and this has been demonstrated when $p = 11$.

[22] They are not all prime. For example [28, Problem 47, p. 18],

$$2^{32} + 1 = \left(2^9 + 2^7 + 1\right)\left(223 - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^9 - 2^7 + 1\right)$$

10. (a) Work out the addition and multiplication tables of $\mathbb{Z}_6$.

    (b) [19, Exercise 2.2.B6, p. 36] Prove or disprove: If $ab = 0$ in $\mathbb{Z}_n$, then $a = 0$ or $b = 0$.

Solution:

(a)

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) There is a counterexample in the preceding multiplication table: $[2] \odot [3] = [0]$.

[6, Chapter XV. Fermat Numbers $F_n = 2^{2^n} + 1$.]

12 Fourth Problem Assignment

Distribution Date: Mounted on the Web on Thursday, February 21st, 2002
Solutions are to be submitted by Friday, March 15th, 2002
(subject to correction)

1. (a) Prove that the polynomial $x^4 + x^3 + x^2 + x^1 + x^0$ is irreducible in $\mathbb{Z}_2[x]$ by assuming that it has a factorization, and deriving a contradiction. You will have to consider various types of possible factorizations. (You will see a different proof of this result in the solutions to Assignment 2.)
   (b) Using the Euclidean Algorithm, determine the inverse to the congruence class $[x^3 + x^2 + x^0]$ in the ring $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x^1 + x^0)$.
   (c) In each of the congruence classes $[x^1]$, $[x^3]$, $[x^5]$, $[x^9]$ of the ring $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x^1 + x^0)$ determine a member polynomial of degree less than 4.

2. [19, Exercise 5.2.A4] Show that, under congruence modulo x^3+2x+1 in $\mathbb{Z}_3[x]$, there are exactly 27 distinct congruence classes. Describe a system of representatives for these classes.

3. In the following problems each element of the given congruence class ring can be written in the form $[ax + b]$ (Why?). Determine the rules for addition and multiplication of congruence classes. (In other words, if the product $[ax+b]\cdot[cx+d]$ is the class $[rx + s]$, describe how to find r and s from a, b, c, d, and similarly for addition.)
   (a) [19, Exercise 5.2.B8] $\mathbb{Q}[x]/(x^2)$.
   (b) $\mathbb{Z}_3[x]/(x^2 + 1)$. Work out the multiplication table.
   (c) $\mathbb{R}[x]/(x^2 + 1)$. Show that this ring of polynomials is isomorphic to the field $\mathbb{C}$.

4. Find a polynomial in $\mathbb{R}[x]$ that satisfies the given conditions:
   (a) [19, Exercise 4.6.A2(a), p. 118] Monic of degree 3 with 2 and $3 + i$ as roots
   (b) [19, Exercise 4.6.A2(b), p. 118] Monic of least possible degree with $1 - i$ and $2i$ as roots
   (c) [19, Exercise 4.6.A2(c), p. 118] Monic of least possible degree with 3 and $4i-1$ as roots.

5. [19, Exercise 4.6.B8, p. 118] Prove or disprove: Let a and b be real numbers. If $a + bi$ is a root of $x^3 - 3x^2 + 2ix + i - 1 \in \mathbb{C}[x]$, then $a - bi$ is also a root.[23]

[23] We are using the familiar $x + iy$ notation for complex numbers [19, p. 47].

13 Solutions, Second Problem Assignment

Distribution Date: Preliminary version posted on the Web on February 4th, 2002
Solutions were to be submitted on Monday, February 4th, 2002
(E.&O.E. These are unchecked preliminary solutions, and are subject to correction and/or change.)

1. [3, Exercise 2.3.B7] In each of the following cases, solve the equation completely. Express your solution x as a congruence class $[u]$, where u is a representative of your choice; then describe precisely the membership of that class; for example, $[5]_2$ consists of all the integers expressible in the form $5 + 2n$, i.e., all the odd integers. Wherever a multiplicative inverse is required, you are expected to formally apply the Euclidean algorithm to find it.

   (a) $7x = 2$ in $\mathbb{Z}_{24}$

   (b) $34x = 1$ in $\mathbb{Z}_{97}$

   (c) $15x = 5$ in $\mathbb{Z}_{63}$

   Solution:

   (a) We apply the Euclidean algorithm:

$$\begin{aligned} 24 &= 7 \cdot 3 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 37 &= 1 \cdot 3 + 0 \\ \Rightarrow 1 &= 7 + 3 \cdot (-2) = 7 + (24 - 7 \cdot 3)(-2) \\ &= 24 \cdot (-2) + 7 \cdot 7 \\ \Rightarrow 7 \cdot 7 &\equiv 1 \pmod{24} \end{aligned}$$

   so 7 is a multiplicative inverse of 7. If we multiply both sides of the given equation by 7, we obtain $49x = 14$, i.e. $[49][x] = [14]$, which is equivalent to $[1][x] = [14]$, or $[x] = [14]$; i.e. $x = \{14 + 24n | n \in \mathbb{Z}\}$.

   (b) We apply the Euclidean algorithm:

$$\begin{aligned} 97 &= 34 \cdot 2 + 29 \\ 34 &= 29 \cdot 1 + 5 \\ 29 &= 5 \cdot 5 + 4 \\ 57 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

$$\begin{aligned}
\Rightarrow 1 &= 5 - 4 \cdot 1 = 5 - (29 - 5 \cdot 5) \cdot 1 \\
&= 29 \cdot (-1) + 5 \cdot 6 = 29 \cdot (-1) + (34 - 29) \cdot 6 \\
&= 34 \cdot 6 + 29 \cdot (-7) = 34 \cdot 6 + (97 - 34 \cdot 2) \cdot (-7) \\
&= 97 \cdot (-7) + 34 \cdot 20
\end{aligned}$$

We multiply the given equation by 20 to obtain, after reduction $x \equiv 20 \pmod 9$7, so the solution set is $x = \{20 + 97n | n \in \mathbb{Z}\}$.

(c) Here $(15, 63) = 3$, which is not a divisor of 5. We are looking for integers x such that $15x = 5 + 63k$. Since $63k$ is a multiple of 5, and $(5, 63) = 1$, k must be of the form $k = 5\ell$ [19, Theorem 1.5, p. 10], so $3x = 1 + 63\ell$. But this implies that $1 = 3(x - 21)$. Since 1 is not a multiple of 3, there are no solutions to this congruence!

2. [19, Exercise 2.3.B11(b)] Showing all your work, solve the congruence $25x \equiv 10 \pmod{65}$. (Do not use [19, Exercise 2.3.B9].)

Solution: We wish to find all integers x such that $25x = 10 + 65k$, where $k \in \mathbb{Z}$. This equation is equivalent to $5x = 2 + 13k$; equivalently, we are solving the congruence

$$5x \equiv 2 \pmod{13}. \tag{23}$$

Since $(5, 13) = 1$, this congruence will have solutions. We begin by applying the Euclidean algorithm:

$$\begin{aligned}
13 &= 5 \cdot 2 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0 \\
\Rightarrow 1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 \\
&= 5 \cdot (-1) + 3 \cdot 2 = 5 \cdot (-1) + (13 - 5 \cdot 2) \cdot 2 \\
&= 13 \cdot 2 + 5 \cdot (-5)
\end{aligned}$$

When we multiply congruence (23) by -5, we obtain $x \equiv 2 \cdot (-5) \equiv -10 \equiv 3 \pmod{13}$. The solution set is $\{3 + 13n | n \in \mathbb{Z}\}$.

3. In each of the following cases, determine whether the given subset of the given ring constitutes a subring. Use the criteria of [19, Theorem 3.2, p. 49].

(a) [19, Exercise 3.1.A5(b), p. 51] The subset of all matrices of the form $\begin{pmatrix} a & b \\ 0_{\mathbb{Z}} & c \end{pmatrix}$ (called *upper triangular matrices* in the ring $M(\mathbb{Z})$ of 2×2 integer matrices.

(b) [19, Exercise 3.1.A6, p. 51] The subset $\{1, -1, i, -i\}$ of the ring $\mathbb{C}$.

(c) [19, Exercise 3.1.A9, p. 51] The subset of $\mathbb{R}$ consisting of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{R}$.

Solution:

(a) **closure under addition.** The sum of two upper triangular matrices $\begin{pmatrix} a_1 & b_1 \\ 0_{\mathbb{Z}} & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0_{\mathbb{Z}} & c_2 \end{pmatrix}$, is the matrix $\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0_{\mathbb{Z}} & c_1 + c_2 \end{pmatrix}$, which is again upper triangular.

closure under multiplication. The product of two upper triangular matrices $\begin{pmatrix} a_1 & b_1 \\ 0_{\mathbb{Z}} & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0_{\mathbb{Z}} & c_2 \end{pmatrix}$ is the matrix $\begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0_{\mathbb{Z}} & c_1c_2 \end{pmatrix}$, which also has a zero in position (2,1), so it also is upper triangular.

zero element. The zero matrix has, in particular, a zero in position $(2, 1)$.

additive inverse. The additive inverse of a matrix $\begin{pmatrix} a & b \\ 0_{\mathbb{Z}} & c \end{pmatrix}$ is evidently $\begin{pmatrix} -a & -b \\ 0_{\mathbb{Z}} & -c \end{pmatrix}$, which is also upper triangular.

Since the criteria of the theorem are satisfied, the subset is a subring.

(b) The subset does not contain $0_{|mathbbC}$, so it cannot be a subring.

(c) **closure under addition.** $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = ((a_1+a_2)+(b_1+b_2)\sqrt{2})$, which is again in the subset.

closure under multiplication. $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2})$, which is again in the subset.

zero element. The zero element of the parent ring is equal to $0+0\sqrt{2}$, which is in the subset.

additive inverse. The additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2}$, which is in the subset.

4. (a) [19, Exercise 3.1.B24, p. 53] The addition table and part of the multiplication table for a three-element ring are given below. Use the distributive laws to complete the multiplication table.

$+$	r	s	t
r	r	s	t
s	s	t	r
t	t	r	s

$\cdot$	r	s	t
r	r	r	r
s	r	t	
t	r		

(b) Determine which element of the ring is the zero element.

(c) Show that this ring is isomorphic to $\mathbb{Z}_3$.

Solution:

(a) (This is not the only possible correct solution.) The first missing entry in the multiplication table is $s \cdot t$. From the addition table we learn that $t = s + s$, hence

$$\begin{aligned} s \cdot t &= s \cdot (s + s) \\ &= (s \cdot s) + (s \cdot s) \quad \text{Distributive Laws} \\ &= t + t \quad \text{Multiplication Table} \\ &= s \quad \text{Addition Table.} \end{aligned}$$

Similarly, $t \cdot s = (s + s) \cdot s = (s \cdot s) + (s \cdot s) = t + t = s$. Finally, $t \cdot t = (s + s) \cdot t = (s \cdot t) + (s \cdot t) = s + s = t$.

(b) Only one row of the table has all entries the same — a feature that must be present for the zero element; hence r is the zero element.

(c) The element t can be observed as having the properties of a multiplicative identity. Thus the isomorphism — it if exists — must be given by $r \leftrightarrow 0$, $t \leftrightarrow 1$, and so the remaining elements must be paired: $s \leftrightarrow 2$. When the tables are rewritten with this labelling, the isomorphism is evident. (There are more elegant ways of proving this.)

5. Prove that a ring R with a multiplicative identity 1_R cannot possess another element x with the same property, i.e. an element $x \neq 1_R$ such that $(\forall a \in R)[ax = a = xa]$.

Solution: We prove that any x with the property $(\forall a \in R)[ax = a = xa]$ must coincide with 1_R:

$$\begin{aligned} x &= 1_R x \quad \text{since } 1_R \text{ is an identity} \\ &= 1_R \quad \text{since } x \text{ is an identity} \end{aligned}$$

The uniqueness of the multiplicative identity — if one exists — justifies the use of the definite article: we may now speak of *the* multiplicative identity. The multiplicative identity is often called the *unity* element. (Do not confuse this term with a *unit* element, which [19, p. 60] is any element possessing a [multiplicative] inverse.)

6. (a) [19, Exercise 3.2.A11(a), p. 63] Prove that if a and b are units in a ring R with identity, then ab is also a unit, and its inverse is $b^{-1}a^{-1}$.

(b) [19, Exercise 3.2.A11(b), p. 63] Give an example of two units a, b in some ring R such that $(ab)^{-1} \neq a^{-1}b^{-1}$.

(c) [19, Exercise 3.2.A10, p. 63] Prove or disprove: The set of units in a ring R with identity is a subring of R.

Solution:

(a) By the theory on [19, pp. 59-60] a multiplicative inverse, it if exists, is unique. We compute the products $(ab)(b^{-1}a^{-1})$ and $(b^{-1}a^{-1})(ab)$ and show that both are equal to 1_R. This will show that $b^{-1}a^{-1}$ is *an* inverse of ab, and hence it is *the* inverse.

$$\begin{aligned}
(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \quad \text{associativity of multiplication} \\
&= (a(bb^{-1}))a^{-1} \quad \text{associativity of multiplication} \\
&= (a1_R)a^{-1} \quad \text{definition of } b^{-1} \\
&= aa^{-1} \quad 1_R \text{ is the multiplicative identity} \\
&= 1_R \quad \text{definition of } a^{-1}; \\
(b^{-1}a^{-1})(ab) &= ((b^{-1}a^{-1})a)b \\
&= (b^{-1}(a^{-1}a))b \\
&= (b^{-1}1_R)b \\
&= b^{-1}b \\
&= 1_R
\end{aligned}$$

(b) The counterexample has to come from a non-commutative ring. We take, for example, the ring $M(\mathbb{Z})$, having identity element $1_{M(\mathbb{Z})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. If $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, where $a^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $b^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, then $ab = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, and $ba = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Then $a^{-1}b^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$, and $b^{-1}a^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$. $ab\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}ab$, so the inverse of ab is $\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$. But $ab\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}ab = \begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix}$, so $a^{-1}b^{-1}$ acts as neither a *left inverse* nor as a *right inverse*.

(c) While the set of units is "closed under multiplication", in the sense that the product of two units is again a unit, the set is not closed under addition. For

example, the sum of a unit a and its additive inverse $-a$ is 0_R. The product of any element with 0_R is 0_R [19, Theorem 3.5(1)]. This leads to a contradiction if we can show that $0_R \neq 1_R$. Try to show that the only ring with identity in which $0_R = 1_R$ is the ring consisting of only one element.)

7. (a) [19, Exercise 3.1.B27] Prove [19, Theorem 3.1, p. 49]: *Let R and S be rings. Define addition and multiplication in the Cartesian product set $R \times S$ by*

$$(r, s) + (r', s') = (r + r', s + s') \tag{24}$$
$$(r, s)(r', s') = (rr', ss') \tag{25}$$

Then $R \times S$ is a ring, and its zero is $(0_R, 0_S)$. [Note that there are 8 properties to check.]

(b) Prove that $R \times S$ is commutative if *and only if* R and S are both commutative.

(c) Prove that, if R and S respectively have identities, 1_R, and 1_S, then $R \times S$ has an identity, and it is

$$1_{R \times S} = (1_R, 1_S)\,.$$

Solution:

(a) We have to check each of the axioms in the definition of a ring [19, p. 42].

Closure under addition. The defined value for the sum is an ordered pair in $R \times S$. Another way of expressing this property is that the addition function is "well defined".

Associativity of addition. Let $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$. Then

$$\begin{aligned}
& (r_1, s_1) + ((r_2, s_2) + (r_3, s_3)) \\
= \; & (r_1, s_1) + (r_2 + r_3, s_2 + s_3) \quad \text{by definition (24) of } + \text{ in } R \times S \\
= \; & (r_1 + (r_2 + r_3), s_1 + (s_2 + s_3)) \quad \text{by definition (24) of } + \text{ in } R \times S \\
= \; & ((r_1 + r_2) + r_3, (s_1 + s_2) + s_3) \quad \text{by associativity of } + \text{ in } R \text{ and } S \\
= \; & (r_1 + r_2, s_1 + s_2) + (r_3, s_3) \quad \text{by definition (24) of } + \text{ in } R \times S \\
= \; & ((r_1, s_1) + (r_2, s_2)) + (r_3, s_3) \quad \text{by definition (24) of } + \text{ in } R \times S
\end{aligned}$$

Commutativity of addition. Let $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Then

$$\begin{aligned}
& (r_1, s_1) + (r_2, s_2) \\
= \; & (r_1 + r_2, s_1 + s_2) \quad \text{by definition (24) of } + \text{ in } R \times S \\
= \; & (r_2 + r_1, s_2 + s_1) \quad \text{by commutativity of } + \text{ in } R \text{ and } S \\
= \; & (r_2, s_2) + (r_1, s_1) \quad \text{by definition (24) of } + \text{ in } R \times S
\end{aligned}$$

Additive identity (=zero element). Let $(r, s) \in R \times S$. Then

$$\begin{aligned}(r,s) + (0_R, 0_S) &= (r + 0_R, s + 0_S) \quad \text{by definition of } + \text{ in } R \times S \\ &= (r,s) \quad \text{properties of } 0_R,\ 0_S \\ &= (0_R + r, 0_S + s) \quad \text{properties of } 0_R,\ 0_S \\ &= (0_R, 0_S) + (r,s) \quad \text{by definition of } + \text{ in } R \times S\end{aligned}$$

Additive inverse. Given any element $(r, s) \in R \times S$, we know from [19, Theorem 3.3, p. 56] that there exist *unique* elements $-r \in R$ and $-s \in S$ such that $r + (-r) = 0_R$, and $s + (-s) = 0_S$. We claim that $(-r, -s)$ is the inverse of (r, s), and prove this by computing the sum:

$$\begin{aligned}(r,s) + (-r,-s) &= (r + (-r), s + (-s)) \quad \text{by definition of } + \text{ in } R \times S \\ &= (0_R, 0_S) \quad \text{by [19, Theorem 3.3, p. 56]}\end{aligned}$$

We don't have to check the sum in the other order, since we have already proved that $+$ is commutative in $R \times S$.

Closure under multiplication. As with the earlier "closure" axiom, we could also formulate this property as stating that the multiplication function given by equation (25) is well defined. Since, for any elements (r_1, s_1), (r_2, s_2) in $R \times S$, $r_1 r_2 \in R$ and $s_1 s_2 \in S$, the ordered pair $(r_1 r_2, s_1, s_2)$ is indeed a member of $R \times S$.

Associativity of multiplication. This proof is analogous to the proof of associativity of $+$ — just replace the $+$ sign[24] by juxtaposition wherever it appears.

Distributivity of multiplication over addition. Let $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$. Then

$$\begin{aligned}&(r_1, s_1)\left((r_2, s_2) + (r_3, s_3)\right) \\ = \ &(r_1, s_1)(r_2 + r_3, s_2 + s_3) \quad \text{by definition (24) of } + \text{ in } R \times S \\ = \ &(r_1(r_2 + r_3), s_1(s_2 + s_3)) \quad \text{by definition (25)} \\ = \ &(r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) \quad \text{by distributivity in } R,\ S \\ = \ &(r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3) \quad \text{by definition (24)} \\ = \ &(r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3) \quad \text{by definition (25)}\end{aligned}$$

The other distributive law may be proved analogously.

[24] Actually, there are 3 different $+$ signs in the proof in question: they could have been designated more precisely as $+_R$, $+_S$, and $+_{R \times S}$. They are different functions because they have different domains and different codomains.

(b) If. Suppose that R and S are both commutative (i.e. that multiplication is commutative in both rings.) Let $(r_1, s_1), (r_2, s_2) \in R \times S$. Then

$$\begin{aligned}(r_1, s_2)(r_2, s_2) &= (r_1 r_2, s_1 s_2) \quad \text{by (25)} \\ &= (r_2 r_1, s_1 s_2) \quad \text{by commutativity of } R \\ &= (r_2 r_1, s_2 s_1) \quad \text{by commutativity of } S \\ &= (r_2, s_2)(r_1, s_1) \quad \text{by definition (25)}\end{aligned}$$

Only if. Suppose that $R \times S$ is commutative. Let $r_1, r_2 \in R$. Then

$$\begin{aligned}(r_1 r_2, 0_S) &= (r_1, 0_S)(r_2, 0_S) \quad \text{by definition (25)} \\ &= (r_2, 0_S)(r_1, 0_S) \quad \text{by commutativity of } R \times S \\ &= (r_2 r_1, 0_S) \quad \text{by definition (25)}\end{aligned}$$

By definition of $R \times S$, the ordered pairs $(r_1 r_2, 0_S)$ and $(r_2 r_1, 0_S)$ are equal precisely when their first coordinates are equal and their second coordinates are equal. Since the second coordinates are identical, this is no surprise; but the equality of the first coordinates is precisely the property we are seeking,

$$r_1 r_2 = r_2 r_1 \,,$$

showing that R is commutative. An analogous proof would show that S is commutative.

(c) Let (r, s) be any element of $R \times S$. Then

$$\begin{aligned}(r, s)(1_R, 1_S) &= (r1_R, s1_S) \quad \text{by definition (25)} \\ &= (r, s) \quad \text{property of } 1_R \text{ and } 1_S \\ &= (1_R r, 1_S s) \quad \text{property of } 1_R \text{ and } 1_S \\ &= (1_R, 1_S)(r, s) \quad \text{by definition (25)}\end{aligned}$$

8. In a ring R with identity 1_R, the *characteristic* is defined to be the smallest integer n — if there is one — with the property that the sum of n copies of 1_R is 0_R; if there is no such integer, the characteristic is said to be 0. The sum of n copies of any element $x \in R$ is denoted by nx; thus a positive characteristic n is the smallest positive integer such that $n1_R = 0_R$ [19, p. 65]. Observe without proof [19, Exercise 3.2.B31(a)] that $\mathbb{Z}$ has characteristic 0, and that $\mathbb{Z}_n$ has characteristic n.

   (a) [19, Exercise 3.2.B31(b)] Determine the characteristic of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

   (b) [19, Exercise 3.2.B32] Prove that a finite ring with identity has characteristic n for some $n > 0$.

(c) [19, Exercise 3.2.B33(a), p. 65] Prove that, in a ring R with identity 1_R and finite characteristic $n > 0$, $(\forall a \in R)[na = 0_R]$.

(d) [19, Exercise 3.2.B33(b), p. 65] Prove that, if R is an integral domain with identity 1_R and finite characteristic $n > 0$, n must be a prime.

(e) [19, Exercise 3.1.B29(a), p. 53]Use the preceding result to show that $\mathbb{Z}_4 \times \mathbb{Z}_6$ is not an integral domain. Then prove this result in another way, by exhibiting a *zero divisor* in the ring.

Solution:

(a) In $\mathbb{Z}_4 \times \mathbb{Z}_6$ the identity element, $1_{\mathbb{Z}_4 \times \mathbb{Z}_6}$ is, by Problem 7 above, $(1_{\mathbb{Z}_4}, 1_{\mathbb{Z}_6})$. We observe that, for any integer n, $n(1_{\mathbb{Z}_4}, 1_{\mathbb{Z}_6}) = (n1_{\mathbb{Z}_4}, n1_{\mathbb{Z}_6})$. In order for this sum of n copies to be zero, it will be necessary that both coordinates be zero in the respective rings, i.e. that

$$n1_{\mathbb{Z}_4} = 0_{\mathbb{Z}_4} \quad (26)$$
$$n1_{\mathbb{Z}_6} = 0_{\mathbb{Z}_6} \quad (27)$$

By the Division Algorithm, we can express n in the forms $n = 4a + r$ and $n = 6b + s$, where $0 \leq r \leq 3$ and $0 \leq s \leq 5$. Since the characteristic of $\mathbb{Z}_4$ is 4, equation (26) will hold if and only if r=0; similarly, (27) will hold if and only if $s = 0$. By examining the positive multiples of 4: 4, 8, 12, ..., we see that 12 is the smallest such multiple that is also a multiple of 6. This is the *least common multiple*[25] of 4 and 6, sometimes denoted by lcm(4,6) or $[4, 6]$. This will be the characteristic of the product ring.

(b) If the ring had characteristic 0 there would exist no integer n such that the sum $n1_R$ would be 0_R. That would imply that all the sums in the set $\{n1_R | n = 1, 2, ...\}$ would be distinct, since, if $n1_R = m1_R$ and $m > n$, then, by adding $-m1_R$ to both sides of the equation (i.e. by subtracting $m1_R$ from both sides) we would have $(n - m)1_r = 0$, so the characteristic would be a positive integer not exceeding $n - m$. From this contradiction we conclude that a ring of characteristic 0 has infinitely many elements; so finite rings with identity always have positive characteristic.

(c) na is the sum of n copies of a; we may interpret this as the sum of n copies of the product $1_R a$. But, by the distributive law, $1_R a + 1_R a + ... + 1_R a = (1_R + 1_R + ... + 1_R)a$, i.e. $na = (n1_R)a$. When n is the characteristic of R, $n1_R = 0$, so $na = 0_R a$, which is equal to 0_R, by [19, Theorem 3.5(1), p. 57].

[25] [35, Definition 2.3.7, p. 120], [19, Exercise 1.2.B31, p. 14].

(d) Suppose that $n = ab$, where a, b are integers greater than 1. We shall interpret the sum of ab copies of 1_R in two ways. If we group the ab copies of 1_R into a sums, each consisting of a sum of b copies of 1_R, we have

$$(ab)1_R = a(b1_R)\,.$$

We can also interpret each of the summands $b1_R$ as a sum of products $b(1_R1_R)$, which, by one of the distributive laws, is equal to $1_R(b1_R)$. Then the sum of a such terms can be viewed as the result of application of the other distributive laws, so

$$a(1_R(b1_R)) = (a1_R)(b1_R)\,.$$

We have thus shown that $(a1_R)(b1_R) = (ab)1_R = n1_R = 0_R$. But, since n is the smallest number of copies of 1_R that sum to 0_R, both $a1_R$ and $b1_R$ are non-zero. This contradicts the defining property [19, 11., p. 46] of an integral domain. From this contradiction, we conclude that no non-trivial factorization $n = ab$ exists, i.e. that n is prime.

(e) Since the characteristic of this commutative ring with identity is 12, which is not a prime, the ring cannot be an integral domain.

We can demonstrate this explicitly by exhibiting two non-zero elements whose product is zero. For example

$$(1_{\mathbb{Z}_4}, 0_{\mathbb{Z}_6})(0_{\mathbb{Z}_4}, 1_{\mathbb{Z}_6}) = (0_{\mathbb{Z}_4}, 0_{\mathbb{Z}_4})$$

which is the zero element of the ring.

9. (cf. [19, Exercise 3.3.B33]) Show that the first ring is not isomorphic to the second.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and the ring $M(\mathbb{Z}_2)$ of 2×2 matrices with entries from $\mathbb{Z}_2$. [Hint: There are many ways to attack a problem of this type. The basic idea is to find some property that is preserved under isomorphism, and then to show that the two rings differ in this property. One property that one might wish to consider is the cardinality, but here the two rings have the same cardinality. Another approach could be based on looking at the set of *idempotents* — the members of the set $S = \{x | xx = x\}$. Show that, if there exists an isomorphism, it must map the set of idempotents of one ring on to the idempotents in the other ring. Then show that, in the present case, the cardinalities of the sets of idempotents are different.]

(b) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.

(c) $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$. (Hint: One of these rings is a field, the other is not.)

Solution:

(a) Both of these rings contain precisely $2^4 = 16$ elements. The "additive structures" of the two rings are the same: they both involve ordered 4-tuples of elements of $\mathbb{Z}_2$ — it doesn't matter whether the 4-tuple is written horizontally or in a rectangular array.

However, their "multiplicative structure" is different. This can be shown in various ways. For example, both of these rings have a multiplicative identity. In $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ the identity is $(1, 1, 1, 1)$; in $M(\mathbb{Z}_2)$ the identity is the identity matrix. In the first ring every element is an idempotent. We need only shnw that the number of idempotents in the second ring is different from 16. One element that is not an idempotent is $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, since its square is the zero matrix. If there were an isomorphism from the first ring to the second, this matrix would be the image of an idempotent, and would have to have the property that it is equal to its square; but that is not the case. We conclude that no isomorphism exists.

(b) Here again there are many possible solutions. The basic attack is to exhibit a property that should be preserved under isomorphism, but is different in the two rings. The second ring has the property that it can be generated under addition from one element, for example from $[1]_{16}$; every element is a sum of copies of this element; if there were an isomorphism f from the second to the first, it would induce a similar expression of every element in the first ring as a sum of copies of the image of $[1]_{16}$. But every element in the first ring has the property that the sum of 4 copies is the zero element, $([0]_4, [0]_4)$, which we would usually denote simply by $(0, 0)$. From this contradiction we conclude that no isomorphism exists. [Of course, we could attack this *finite* problem more naïvely, by considering the finite number of possible bijections. But that number is (16)!, and we would have to prove that every one of these functions fails to be an isomorphism. If the rings were infinite, that approach would not be available. Would you be able to prove that the following two rings are not isomorphic: $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}$?]

(c) The first ring is not a field, since it has zero divisors; for example $(1, 0)(0, 1) = (0, 0)$.

14 Class Tests

14.1 Version 1

McGILL UNIVERSITY FACULTY OF SCIENCE

CLASS TEST: MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Wednesday, 13 March, 2002.

TIME: 45 minutes, beginning about 11:35

FAMILY NAME:

MR, MISS, MS, MRS, &c.: SEAT NO.:

GIVEN NAMES:

STUDENT NUMBER: COURSE AND YEAR:

Instructions

1. Fill in the above clearly.
2. All your writing — even rough work — must be handed in.
3. Calculators are not permitted.
4. *Your neighbour's version of this test may not be the same as yours.*
5. This examination booklet consists of this cover, Pages 52 through 54 containing questions; and Page 55, which is blank.
6. Show all your work. All solutions are to be written in the space provided on the page where the question is printed. When that space is exhausted, you may write *on the facing page*. Any solution may be continued on the last page, or the back cover of the booklet, but you must indicate any continuation clearly on the page where the question is printed!
7. You are advised to spend the first few minutes scanning the problems. (Please inform the invigilator if you find that your booklet is defective.)

PLEASE DO NOT WRITE INSIDE THIS BOX

1 /10	2 /10	3 /10				Raw /30	Scaled /20

1. (a) Showing all your work, use the Euclidean Algorithm — no other method will be accepted — to determine integers a and b such that

$$(195, 187) = 195a + 187b\,.$$

   (b) Use your results in (a) to find an integer n such that

$$[n]_{195}[187]_{195} = [1]_{195}\,.$$

2. List the elements of the ring $\mathbb{Z}_2[x]/(x^2+1)$ of congruence classes of polynomials in $\mathbb{Z}_2[x]$ modulo the polynomial x^2+1. Give the addition and multiplication tables of $\mathbb{Z}_2[x]/(x^2+1)$. In these tables you are expected to denote each element in only one way: that is, the same element may not appear in your tables with more than one representation.

3. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = ab^2$$

CONTINUATION PAGE FOR PROBLEM NUMBER

You *must* refer to this continuation page on the page where the problem is printed!

14.2 Version 2

McGILL UNIVERSITY FACULTY OF SCIENCE

CLASS TEST: MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Wednesday, 13 March, 2002.
TIME: 45 minutes, beginning about 11:35

FAMILY NAME:
MR, MISS, MS, MRS, &c.: SEAT NO.:
GIVEN NAMES:

STUDENT NUMBER: COURSE AND YEAR:

Instructions

1. Fill in the above clearly.
2. All your writing — even rough work — must be handed in.
3. Calculators are not permitted.
4. *Your neighbour's version of this test may not be the same as yours.*
5. This examination booklet consists of this cover, Pages 57 through 59 containing questions; and Page 60, which is blank.
6. Show all your work. All solutions are to be written in the space provided on the page where the question is printed. When that space is exhausted, you may write *on the facing page*. Any solution may be continued on the last page, or the back cover of the booklet, but you must indicate any continuation clearly on the page where the question is printed!
7. You are advised to spend the first few minutes scanning the problems. (Please inform the invigilator if you find that your booklet is defective.)

PLEASE DO NOT WRITE INSIDE THIS BOX

1 /10	2 /10	3 /10				Raw /30	Scaled /20

1. Give your choice of three rows of the composition table of the group S_3 of permutations of the set $\{1, 2, 3\}$.

2. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition, and $-$ is the usual operation of subtraction).

$$a * b = a - b$$

3. (a) Showing all your work, use the Euclidean Algorithm — no other method will be accepted — to determine integers a and b such that

$$(209, 182) = 209a + 182b\,.$$

(b) Use your results in (a) to find an integer n such that

$$[n]_{209}[182]_{209} = [1]_{209}\,.$$

CONTINUATION PAGE FOR PROBLEM NUMBER

You *must* refer to this continuation page on the page where the problem is printed!

14.3 Version 3

McGILL UNIVERSITY FACULTY OF SCIENCE

CLASS TEST: MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Wednesday, 13 March, 2002.
TIME: 45 minutes, beginning about 11:35

FAMILY NAME:
MR, MISS, MS, MRS, &c.: SEAT NO.:
GIVEN NAMES:

STUDENT NUMBER: COURSE AND YEAR:

Instructions

1. Fill in the above clearly.
2. All your writing — even rough work — must be handed in.
3. Calculators are not permitted.
4. *Your neighbour's version of this test may not be the same as yours.*
5. This examination booklet consists of this cover, Pages 62 through 64 containing questions; and Page 65, which is blank.
6. Show all your work. All solutions are to be written in the space provided on the page where the question is printed. When that space is exhausted, you may write *on the facing page*. Any solution may be continued on the last page, or the back cover of the booklet, but you must indicate any continuation clearly on the page where the question is printed!
7. You are advised to spend the first few minutes scanning the problems. (Please inform the invigilator if you find that your booklet is defective.)

PLEASE DO NOT WRITE INSIDE THIS BOX

1 /10	2 /10	3 /10				Raw /30	Scaled /20

1. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = a$$

2. Give the addition and multiplication tables of the ring $\mathbb{Z}_3 \times \mathbb{Z}_2$.

3. In the ring $\mathbb{Z}_2[y]$ the polynomials y^3+y+1 and y^3+y^2+1 are relatively prime. Use the Euclidean Algorithm — no other method will be accepted — to determine a polynomial $g(y) \in \mathbb{Z}_2[y]$ such that

$$(y^3 + y + 1)g(y) \equiv 1 \pmod{y^3 + y^2 + 1}$$

in $\mathbb{Z}_2[y]$.

CONTINUATION PAGE FOR PROBLEM NUMBER

You *must* refer to this continuation page on the page where the problem is printed!

14.4 Version 4

McGILL UNIVERSITY FACULTY OF SCIENCE

CLASS TEST: MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Wednesday, 13 March, 2002.
TIME: 45 minutes, beginning about 11:35

FAMILY NAME:
MR, MISS, MS, MRS, &c.: SEAT NO.:
GIVEN NAMES:

STUDENT NUMBER: COURSE AND YEAR:

Instructions

1. Fill in the above clearly.
2. All your writing — even rough work — must be handed in.
3. Calculators are not permitted.
4. *Your neighbour's version of this test may not be the same as yours.*
5. This examination booklet consists of this cover, Pages 67 through 69 containing questions; and Page 70, which is blank.
6. Show all your work. All solutions are to be written in the space provided on the page where the question is printed. When that space is exhausted, you may write *on the facing page*. Any solution may be continued on the last page, or the back cover of the booklet, but you must indicate any continuation clearly on the page where the question is printed!
7. You are advised to spend the first few minutes scanning the problems. (Please inform the invigilator if you find that your booklet is defective.)

PLEASE DO NOT WRITE INSIDE THIS BOX

1 /10	2 /10	3 /10				Raw /30	Scaled /20

1. In the ring $\mathbb{Z}_2[x]$ the polynomials $x^3 + x^2 + x$ and $x^3 + x + 1$ are relatively prime. Use the Euclidean Algorithm — no other method will be accepted — to determine a polynomial $f(x) \in \mathbb{Z}_2[x]$ such that

$$(x^3 + x^2 + x)f(x) \equiv 1 \pmod{x^3 + x + 1}$$

in $\mathbb{Z}_2[x]$.

2. Give the composition table of the group whose elements are $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

3. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = a + b$$

CONTINUATION PAGE FOR PROBLEM NUMBER

You *must* refer to this continuation page on the page where the problem is printed!

15 Plagiarism in student solutions to Assignment 2

Distribution Date: Mounted on the Web on Friday, March 8th, 2002

In the course of their grading of student solutions to Assignment 2, graders identified a number of assignments that exhibited very strong similarities. Students have already been warned earlier in these notes that the University does not tolerate plagiarism. Because the benefits to the students who appear to have plagiarized are so small, it has been decided not to forward the materials to the Faculty's disciplinary officer *at this time*. They will be held in a secure location, and may be passed on if the individuals in question are involved in any future incidents. In the meantime a grade of **0** will be entered for this assignment for each of the students affected. **Students who permitted their work to be plagiarized are, for the purposes of this decision, being treated as plagiarizers.**

There is evidence that some students other than those identified by a grade of zero may have been involved in plagiarism: the papers identified were not sought out for that purpose. All students are warned that future incidents of plagiarism or cheating are likely to be treated with greater severity. While you are encouraged to discuss assignment problems among yourselves, the solutions you write down must be entirely your own.

Students interested in reading the University's regulations can consult [48, Chapter 3, Section A — Rules of Conduct, III Academic Offences, §15. Plagiarism.]

16 Solutions, Third Problem Assignment

(Solutions were to be submitted on Monday, March 4th, 2002)

Distribution Date: Mounted on the Web on Friday, March 8th, 2002
(Preliminary version — subject to correction.)

1. (cf. [19, Exercise 4.1.A6]) In which of the following cases is the given set a subring of the indicated ring? If it is a subring, prove that fact; if it is not, provide a counterexample, or prove the fact in some other way.

   (a) All polynomials in $\mathbb{R}[x]$ with constant term $0_{\mathbb{R}}$.

   (b) All polynomials of degree 2 in $\mathbb{C}[x]$.

   (c) All polynomials in $\mathbb{Z}[x]$ in which the coefficients of all even-degree terms are zero.

   (d) All polynomials in $\mathbb{Z}[x]$ in which the coefficients of all odd-degree terms are zero.

   (e) The zero polynomial, together with all non-zero polynomials in $\mathbb{Z}[x]$ in which the coefficient of the highest-degree term is non-negative.

   (f) The zero polynomial, together with all non-zero polynomials in $\mathbb{Z}[x]$ in which the coefficient of the highest-degree term is non-zero.

   Solution: We shall be applying the characterization of [19, Theorem 3.2, p. 49]. (While the theorem is stated in the textbook only as a *sufficient* condition for a subset to be a subring, it is also *necessary*, by virtue of Ring Axioms ## 1, 4, 5, 6. Thus is is often convenient to use the 4 conditions of the theorem in place of the original *definition* of a subring. The 4 conditions given are, in fact, somewhat redundant; it was shown in the lectures, for example, that, if a subset is known to be non-empty, then it is not necessary to postulate that it contain 0_R, since this will be a consequence of the other axioms.)

   (a) The sum and product of two polynomials with zero constant term is easily seen to have the same property. The zero polynomial has all coefficients zero, so the constant term is *a fortiori* zero. Finally, the additive inverse of a polynomial with constant term 0 has constant term -0, which is also 0. We have shown that this subset is a subring.

   (b) If $f(x)$ is a polynomial of degree 2, then $-f(x)$ will also be a polynomial of degree 2. If the set of these polynomials were closed under addition, then the sum $f(x) + (-f(x))$ would have to have degree 2. But this sum is the zero

polynomial. Your textbook does not consider $0_{\mathbb{R}}$ as a polynomial having a degree.[26]

We can avoid the "difficulty" of a counterexample involving the zero polynomial by taking the polynomials $x^2 + x$ and $-x^2 + x$. Here the sum has degree 1, and so it would not be in the set; i.e. the set is not closed under addition.

(c) The set of polynomials with all coefficients of even degree terms equal to 0 is not closed under multiplication: $1x \cdot 1x = 1x^2$, which is not in the set. Hence this subset is not a subring.

(d) The polynomials whose only non-zero coefficients are among those of the even-degree terms form a set closed under addition, multiplication, and the taking of an additive inverse. One polynomial of this type is the zero polynomial. Thus this set is a subring.

(e) The subset would contain the polynomial $1x^0$; its additive inverse is $-1x^0$, which is not in the subset. Hence the subset is not a subring.

(f) By definition, the highest-degree term of a non-zero polynomial must have a non-zero coefficient. Thus the set consists of *all* polynomials in $\mathbb{Z}[x]$, and is a subring.

2. (In this problem we will be working with the complex numbers, defined as the points in the set $\mathbb{R} \times \mathbb{R}$, endowed with the usual (vector) definition of addition, but with the multiplication rule given in the lectures. The complex number we write as (a, b) can also be denoted by, for example, $a + b\sqrt{-1}$, or by $a + bi$.)

(a) Show that the function $f : \mathbb{C} \to \mathbb{C}$ given by $(x, y) \mapsto (x, -y)$ defines an isomorphism.[27]

(b) Show that the function $f : \mathbb{C} \to \mathbb{C}$ given by $(x, y) \mapsto (-x, -y)$ *does not* define an isomorphism.

Solution: The definition of *isomorphism* is given on [19, p. 69].

(a) f **is injective.**

$$f(a_1, b_1) = f(a_2, b_2)$$

[26] If we were to give a value to this degree, we would have to do so in the "extended" ring $\mathbb{Z}$, and define it to be $-\infty$. The "extended" ring is not a ring at all, since there would be certain pairs of elements on which the operations would not be defined. For example, while we could talk about a new element $-\infty$, as the product of -1 and ∞, we could not talk about the sum of ∞ and $-\infty$; in other words, we would not be able to interpret $-\infty$ as the additive inverse of ∞. While we have proved that, in any ring, $0 \cdot a = 0$, we would not be able to give a value to the product $0 \cdot \infty$. *This subject is not part of the present course.*

[27] An isomorphism of a ring or field or graph or... with itself is called an *automorphism*.

$$\begin{aligned}
&\Rightarrow\ (a_1, -b_1) = (a_2, -b_2) \quad \text{definition of } f\\
&\Leftrightarrow\ (a_1 = a_2) \wedge (-b_1 = -b_2) \quad \text{definition of cartesian product}\\
&\Leftrightarrow\ (a_1 = a_2) \wedge (b_1 = b_2)\\
&\Leftrightarrow\ (a_1, b_1) = (a_2, b_2) \quad \text{definition of cartesian product}
\end{aligned}$$

f **is surjective.** Let (a, b) be any point in $\mathbb{C}$. Then $(a, b) = f(a, -b)$.

f **commutes with addition.** Let $(a_1, b_1) \in \mathbb{C}$ and $(a_2, b_2) \in \mathbb{C}$. Then

$$\begin{aligned}
& f((a_1, b_1) + (a_2, b_2))\\
=\ & f(a_1 + a_2, b_1 + b_2) \quad \text{definition of } + \text{ in } \mathbb{C}\\
=\ & (a_1 + a_2, -(b_1 + b_2)) \quad \text{definition of } f\\
=\ & (a_1 + a_2, (-b_1) + (-b_2))\\
=\ & (a_1, -b_1) + (a_2, -b_2) \quad \text{definition of } + \text{ in } \mathbb{C}\\
=\ & f((a_1, b_1)) + f((a_2, b_2)) \quad \text{definition of } f
\end{aligned}$$

f **commutes with multiplication.** Let $(a_1, b_1) \in \mathbb{C}$ and $(a_2, b_2) \in \mathbb{C}$. Then

$$\begin{aligned}
& f((a_1, b_1) \cdot (a_2, b_2))\\
=\ & f(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \quad \text{definition of } \cdot \text{ in } \mathbb{C}\\
=\ & (a_1a_2 - b_1b_2, -(a_1b_2 + a_2b_1)) \quad \text{definition of } f\\
=\ & (a_1, -b_1) \cdot (a_2, -b_2)) \quad \text{definition of } \cdot \text{ in } \mathbb{C}\\
=\ & f((a_1, b_1)) \cdot f((a_2, b_2)) \quad \text{definition of } f
\end{aligned}$$

(b) The given function is obviously a bijection. It also has the property of commuting with addition. However, it fails to have the necessary property for multiplication. To show that, it suffices to select one suitable pair of complex numbers as a counterexample.

$$f((0, 1) \cdot (0, 1)) = f((-1, 0)) = (1, 0)$$

but

$$f((0, 1)) \cdot f((0, 1)) = (0, -1) \cdot (0, -1) = (-1, 0)\,;$$

or, equivalently, $f(i^2) \neq (f(i))^2$.

3. (In the following problem the "long" divisions should be carried out showing all intermediate steps, for example, using the notation at the bottom of [19, p. 85].)

Find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x) \cdot q(x) + r(x)$, and $r(x) = 0$ or $\deg r(x) < \deg g(x)$:

(a) [19, Exercise 4.1.A5(b)] $f(x) = x^4 - 7x + 1$, and $g(x) = 2x^2 + 1$ in $\mathbb{Q}[x]$.

(b) [19, Exercise 4.1.A5(d)] $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g(x) = 3x^2 + 2$ in $\mathbb{Z}_7[x]$.

Solution:

(a) By the Division Algorithm, $x^4 - 7x + 1 = (2x^2 + 1)\left(\frac{1}{2}x^2 - \frac{1}{4}\right) + \left(-7x + \frac{5}{4}\right)$.

(b) By the Division Algorithm, $4x^4 + 2x^3 + 6x^2 + 4x + 5 = (3x^2 + 2)(6x^2 + 3x + 5) + (5x + 2)$.

4. Use the Euclidean algorithm to find the greatest common divisor of the given polynomials over the given fields, and then — in parts (a) and (b) only — to express that greatest common divisor as a sum of multiples of the given polynomials (as described in [19, Theorem 4.5, p. 92]).

(a) [19, Exercise 4.2.A5(b), p. 94] $f_1(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $g_1(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.

(b) $f_2(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $g_2(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Z}_2[x]$. (Over this field, 2 is the same as 0, 5 is the same as 1, etc.)

(c) $f_3(x) = x^4 + ix + 1$ and $g_3(x) = x^2 - (1 + i)x + 1$ in $\mathbb{C}[x]$.
(Here i denotes the point $(0, 1)$ in the complex plane; a real number x is to be interpreted as the complex number $(x, 0)$. Observe that the inverse of $x + yi$, where not both x and y are 0, is $\frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$.
While the complex numbers in this problem do not appear to be particularly abstruse, the computations can be expected to be unpleasant. The purpose is for students to face the realities of arithmetic in $\mathbb{C}$.)

Solution:

(a)

$$\begin{aligned} x^5 + x^4 + 2x^3 - x^2 - x - 2 &= (x^4 + 2x^3 + 5x^2 + 4x + 4)(x - 1) \\ &\quad + (-x^3 - x + 2) \\ x^4 + 2x^3 + 5x^2 + 4x + 4 &= (-x^3 - x + 2)(-x - 2) + (4x^2 + 4x + 8) \\ -x^3 - x + 2 &= (4x^2 + 4x + 8)\left(-\frac{1}{4}x + \frac{1}{4}\right) \end{aligned}$$

Thus $4x^2+4x+8$ is a common divisor of highest degree. The greatest common divisor $(x^5 + x^4 + 2x^3 - x^2 - x - 2, x^4 + 2x^3 + 5x^2 + 4x + 4)$ is then the *monic*

polynomial obtained from $4x^2 + 4x + 8$ by multiplying by the appropriate element of $\mathbb{Q}$:

$$\frac{1}{4}(4x^2 + 4x + 8) = x^2 + x + 2\,.$$

By "back substitution" we determine that

$$\begin{aligned} x^2 + x + 2 &= \frac{1}{4}(4x^2 + 4x + 8) \\ &= \frac{1}{4}\left((x^4 + 2x^3 + 5x^2 + 4x + 4) + (-x^3 - x + 2)(x + 2)\right) \\ &= \frac{1}{4}((x^4 + 2x^3 + 5x^2 + 4x + 4) + ((x^5 + x^4 + 2x^3 - x^2 - x - 2) \\ &\qquad -(x^4 + 2x^3 + 5x^2 + 4x + 4)(x - 1))(x + 2)) \\ &= (x^5 + x^4 + 2x^3 - x^2 - x - 2)\left(\frac{1}{4}x + \frac{1}{2}\right) \\ &\qquad +(x^4 + 2x^3 + 5x^2 + 4x + 4)\left(-\frac{1}{4}x^2 - \frac{1}{4}x + \frac{3}{4}\right) \end{aligned}$$

(b)

$$\begin{aligned} x^5 + x^4 + x^2 + x &= (x^4 + x^2)(x + 1) + (x^3 + x) \\ x^4 + x^2 &= (x^3 + x)x + 0 \end{aligned}$$

Since $x^3 + x$ is monic,

$$(x^5 + x^4 + x^2 + x, x^4 + x^2) = x^3 + x\,.$$

Note that the greatest common divisor is quite different from that obtained when the polynomials were interpreted as taking their coefficients from $\mathbb{Q}$; even the degree is different!

(c) By the Division Algorithm

$$x^4+ix+1 = (x^2-(1+i)x+1)(x^2+(1+i)x+(-1+2i))+((-4+i)x+(2-2i))$$

To carry out the next step in the algorithm we need to be able to divide $x^2+(1+i)x+(1+2i)$ by $(-4+i)x+(2-2i)$; but this requires observing that $(-4+i)^{-1} = -\frac{4}{17} - \frac{1}{17}i$. By a second application of the Division Algorithm we now obtain

$$\begin{aligned} & x^2 - (1 + i)x + 1 \\ = \;& ((-4 + i)x + (2 - 2i))\left(\frac{1}{17}(-4 - i)x + \frac{1}{17^2}(5 + 99i)\right) + \frac{1}{17^2}(81 - 188i) \end{aligned}$$

We may conclude that $\frac{1}{17^2}(81 - 188i)$ is a multiple of the greatest common divisor, so, scaling it to the associated monic polynomial, we obtain

$$(x^4 + ix + 1, x^2 - (1 + i)x + 1) = 1\,.$$

5. Proceeding recursively, starting with the set $\{1\}$ consisting of the only monic irreducible polynomial of degree 0, we wish to determine the set S_n of irreducible polynomials in $\mathbb{Z}_2[x]$ of degree n, where $n \leq 3$ The recursion is based on the fact that the degree of a product of polynomials is the sum of their degrees [19, Theorem 4.2, p. 84].

   Polynomials of degree 0 are the non-zero constants, and the only one which is monic is the constant 1.

   Polynomials of degree 1 all have the form $a_0 + a_1x$, where $a_1 \neq 0$. There is only one non-zero element in this field, so $a_1 = 1$. But there are two possible values for a_0. Could either of these polynomials be reducible, i.e. the product of two polynomials of lower degree? The only lower degree available is degree 0, and the product of two polynomials of degree 0 again has degree 0. Hence neither of these polynomials is reducible, and we have $S_1 = \{x, 1 + x\}$.

   Carry this reasoning on to determine the members of S_2 and S_3.

   Solution: We consider the possible ways of multiplying polynomials in S_1 to get a polynomial of degree 2: x^2, $(1 + x)^2 = 1 + x^2$, and $x(1 + x) = x + x^2$. The polynomials of degree 2 all have the form $a_0 + a_1x + a_2x^2$, where $a_2 \neq 0$, i.e. where $a_2 = 1$. There are 2×2 possible choices of a_1 and a_2, and 3 of the 4 choices are reducible. The one case remaining — the only *irreducible* polynomial of degree 2 — is $1 + x + x^2$. Thus $S_2 = \{1 + x + x^2\}$.

   Here are the ways in which polynomials in $S_1 \cup S_2$ may be multiplied to produce a polynomial of degree 3: x^3, $(1 + x)^3 = 1 + x + x^2 + x^3$, $x^2(1 + x)^1 = x^2 + x^3$, $x^1(1+x)^2 = x+x^3$ are all the polynomials that factorize into a product of 1st degree polynomials; and $x(1+x+x^2) = x+x^2+x^3$ and $(1+x)(1+x+x^2) = 1+x^3$ are the ways in which the irreducible polynomial of degree 2 can figure in a factorization. In all we have seen 6 reducible polynomials of the form $a_0 + a_1x + a_2x^2 + 1x^3$, but there are $2 \times 2 \times 2$ polynomials of degree 3. The two polynomials missing from our lists of products are $1 + x + x^3$ and $1 + x^2 + x^3$; thus $S_3 = \{1 + x + x^3, 1 + x^2 + x^3\}$.

   While it was not required in the problem, let's multiply members of $S_1 \cup S_2 \cup S_3$ in all possible ways to obtain a polynomial of degree 4. We classify our products by the partition of 4 as a sum of positive integers that corresponds to the multiplicity of its irreducible factors.

$4 = 1 + 1 + 1 + 1$.

$$\begin{aligned} x^4(1+x)^0 &= x^4 \\ x^3(1+x)^1 &= x^3 + x^4 \\ x^2(1+x)^2 &= x^2 + x^4 \\ x^1(1+x)^3 &= x + x^2 + x^3 + x^4 \\ x^0(1+x)^4 &= 1 + x^4 \end{aligned}$$

$4 = 2 + 1 + 1$.

$$\begin{aligned} (1+x+x^2)(x)(x) &= x^2 + x^3 + x^4 \\ (1+x+x^2)(1+x)(1+x) &= (1+x+x^2)(1+x^2) = 1 + x + x^3 + x^4 \\ (1+x+x^2)(x)(1+x) &= (1+x+x^2)(x+x^2) = x + x^4 \end{aligned}$$

$4 = 2 + 2$. $(1 + x + x^2)^2 = 1 + x^2 + x^4$.

$4 = 3 + 1$.

$$\begin{aligned} (1+x+x^3)x &= x + x^2 + x^4 \\ (1+x+x^3)(1+x) &= 1 + x^2 + x^3 + x^4 \\ (1+x^2+x^3)x &= x + x^3 + x^4 \\ (1+x^2+x^3)(1+x) &= 1 + x + x^2 + x^4 \end{aligned}$$

We have accounted for $5 + 3 + 1 + 4 = 13$ polynomials. The $2^4 - 13 = 3$ polynomials of the form $a_0 + a_1x + a_2x^2 + 1x^3$ which are not in our list are the irreducible polynomials of degree 3. By elimination we find the members of S_4 to be $1 + x + x^4$, $1 + x^3 + x^4$, and $1 + x + x^2 + x^3 + x^4$.

6. (a) [19, Exercise 4.4.A4(a), p. 104] Determine all values of k, if any, for which $x - 2$ is a factor of $x^4 - 5x^3 + 5x^2 + 3x + k$ in $\mathbb{Q}[x]$.

   (b) [19, Exercise 4.4.A4(b), p. 104] Determine all values of ℓ, if any, for which $x + 1$ is a factor of $x^4 + 2x^3 - 3x^2 + \ell x + 1$ in $\mathbb{Z}_5[x]$.

   (c) [19, Exercise 4.4.A7, p. 104] Use the Factor Theorem to show that $x^7 - x$ factors in $\mathbb{Z}_7[x]$ as

   $$x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$$

   without doing any polynomial multiplication. Explain why your argument could not be applied to the polynomial $x^{14} - x^2$.

Solution:

(a) We apply the Factor Theorem [19, Theorem 4.15, p. 102] to $f(x) = x^4 - 5x^3 + 5x^2 + 3x + k$. $f(2) = 2^4 - 5 \cdot 2^3 + 5 \cdot 2^2 + 3 \cdot 2 + k = 16 - 40 - 20 + 6 + k = 2 + k$. $x - 2$ is a divisor iff $f(2) = 0$, i.e. iff $2 + k = 0$ or $k = -2$.

(b) Now we apply the Factor Theorem to $g(x) = x^4 + 2x^3 - 3x^2 + \ell x + 1$. $g(-1) = (-1)^4 + 2(-1)^3 - 3(-1)^2 + \ell(-1) + 1 = -3 - \ell$; $x + 1$ is a divisor iff $-3 + \ell = 0$, i.e. iff $\ell = 3$.

(c) We observe that

$$\begin{aligned}
0^7 - 0 &= 0 - 0 = 0 \\
1^7 - 1 &= 1 - 1 = 0 \\
2^7 - 2 &= 128 - 2 = 126 = 7 \cdot 18 \equiv 0 \pmod 7 \\
3^7 - 3 &= 2187 - 3 = 2184 = 7 \cdot 312 \equiv 0 \pmod 7 \\
4^7 - 4 &= (7-3)^7 - (7-3) \equiv -(3^7 - 3) \equiv -0 \equiv 0 \pmod 7 \\
5^7 - 5 &= (7-2)^7 - (7-2) \equiv -(2^7 - 2) \equiv -0 \equiv 0 \pmod 7 \\
6^7 - 5 &= (7-1)^7 - (7-1) \equiv -(1^7 - 1) \equiv -0 \equiv 0 \pmod 7
\end{aligned}$$

showing that $x^7 - x$ has $x - k$ as a factor, where $k = 0, 1, ..., 6$. The product of these factors has degree 7, hence $x^7 - x$ is a non-zero constant multiple of the product; in the field $\mathbb{Z}_2$ there is only one non-zero element, namely 1. Hence $x^7 - x$ is equal to the product.

This reasoning works only because the degree of $x^7 - x$ is equal to the degree of the product: we have argued that the degrees are 7 positive integers whose sum is 7, so each of them is equal to 1.

7. [19, cf. Exercise 4.4.B8, p. 105] For each of the following polynomials, using the Factor Theorem or otherwise, determine whether it is irreducible in the given ring of polynomials:

(a) $x^2 + 7$ in $\mathbb{R}[x]$

(b) $x^2 - 7$ in $\mathbb{Q}[x]$

(c) $x^2 + 7$ in $\mathbb{C}[x]$

(d) $2x^3 + x^2 + 2x + 2$ in $\mathbb{Z}_5[x]$

(e) $x^4 + x^2 + 1$ in $\mathbb{Z}_3[x]$

(f) $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$

(g) $x^4 + x^2 + 1$ in $\mathbb{R}[x]$.

Solution:

(a) For all real numbers x, $x^2 + 7 \geq 0 + 7 = 7$, so no real number r is a root; that implies that there is no factor of the form $x - r$, i.e. no 1st degree factor. But a 2nd degree polynomial can factorize non-trivially only into two factors of degree 1. Hence the polynomial is irreducible over $\mathbb{R}$.

(b) There is no rational square root of 7; (this can be proved with essentially the same proof as was used to show that $\sqrt{2}$ is irrational). Hence there is no 1st degree factor for the given polynomial, and, as it is of degree 2, this would be only way in which it could admit a non-trivial factorization. Therefore $x^2 - 7$ is irreducible over the rationals.

(c) In the field $\mathbb{C}$ there are two square roots of -7, namely $(0, \pm\sqrt{7})$. The polynomial factorizes as

$$x^2 - 7 = (x - (0, -\sqrt{7}))(x + (0, \sqrt{7}))\,.$$

(d) The polynomial $f(x) = 2x^3 + x^2 + 2x + 2$ has degree 3; if it admits a non-trivial factorization, then at least one of the factors will have degree 1. It follows that we can test for irreducibility by applying the Factor Theorem: f will be irreducible iff $f(x) \neq 0$ for all *values* of x. In the following computations, all arithmetic is in $\mathbb{Z}_7$, i.e. integers modulo 5:

$$\begin{aligned}
f(0) &= 2 \cdot 0^3 + 0^2 + 2 \cdot 0 + 2 = 2 \\
f(1) &= 2 \cdot 1^3 + 1^2 + 2 \cdot 1 + 2 = 2 \neq 0 \\
f(2) &= 2 \cdot 2^3 + 2^2 + 2 \cdot 2 + 2 = 26 = 5 \neq 0 \\
f(3) &= 2 \cdot 3^3 + 3^2 + 2 \cdot 3 + 2 = 71 \neq 0 \\
f(4) &= 2 \cdot 4^3 + 4^2 + 2 \cdot 4 + 2 = 2 \cdot (-3)^3 + 4^2 + 2 \cdot 4 + 2 = -28 \neq 0
\end{aligned}$$

As the polynomial has no root in $\mathbb{Z}_5$, it has no 1st degree factor; hence, *because its degree is* ≤ 3, the polynomial is irreducible.

(e) Since $1^4 + 1^2 + 1 = 3 = 0$, this polynomial has a 1st degree factor, $x - 1$ (or, equivalently, $x + 2$, and is reducible.

(f) We find that the polynomial takes on non-zero values at both field elements 0, 1. By the Factor Theorem, this implies that there are no 1st degree factors. But this does not imply that the polynomial is irreducible! In fact, this polynomial is equal to $(x^2 + x + 1)^2$, and it is reducible over $\mathbb{Z}_2$.

(g) In fact, the given polynomial is reducible *over all fields*! This is because

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$$

over all fields. (How can we reconcile the factorization into quadratic factors with the fact that the polynomial has a 1st degree factor over $\mathbb{Z}_3$? Simply because the quadratic factors themselves may admit further factorization over certain fields. Over the reals they are both irreducible; over $\mathbb{Z}_2$ they coincide, and are (is?) irreducible; but, over $\mathbb{Z})_3$, they are both reducible.)

17 Detailed syllabus corresponding to textbook chapters 5, 6, 7, 8, 13

Distribution Date: Incomplete draft version posted on the Web on Thursday, March 14th, 2002.
Updated version posted on Thursday, April 4th, 2002, subject to further tuing or corrections.

Unless otherwise noted, all material is taken from the textbook.

17.1 Chapter 5, Congruence in $F[x]$, and Congruence-Class Arithmetic

Students should understand the nature of the definitions in this chapter, and know the statements of theorems that correspond to theorems already seen for congruence in $\mathbb{Z}$ to an integer modulus. They will not be expected to reproduce the proofs of the theorems, but could be expected to demonstrate specific facts that are direct consequences of the definitions and the properties of equivalence relations: they should be able to show that congruence to a polynomial modulus in $F[x]$ is an equivalence relation.

Students will be expected to know how to carry out long division of one polynomial in $F[x]$ into another — i.e. the Division Algorithm in $F[x]$, cf. [19, §4.1].

17.1.1 Congruence in $F[x]$, and Congruence Classes [19, §5.1, p. 119]

17.1.2 Congruence-Class Arithmetic [19, §5.2, p. 123]

17.1.3 The Structure of $F[x]/(p(x))$ when $p(x)$ is Irreducible [19, §5.3, p. 128]

Students should understand how to construct a finite field over $\mathbb{Z}_q$ where q is a prime and $p(x)$ is irreducible. They will not be expected to be familiar with the formal theorems in this section but should be able to demonstrate why, if a *reducible* polynomial $p(x)$ factorizes as $p(x) = a(x)b(x)$, where a and b both have positive degree, then the congruence classes $[a(x)]$ and $[b(x)]$ would have product $[0]$, so the resulting ring of congruence classes, $F[x]/(p(x))$, would not be a field.

Students should be able to use the Euclidean algorithm to determine the inverse of a given congruence class $[f(x)]$, and to carry out computations in "small" finite fields, including being able to construct addition and multiplication tables. (It was shown in class that, in the finite fields constructed using certain irreducible polynomials, all the non-zero classes can be expressed as powers of the class $[x]$; students are *not* expected to be able to identify which fields have this property.)

17.2 Chapter 6, Ideals and Quotient Rings

Omit this chapter entirely.

17.3 Chapter 7, Groups [19, p. 160]

17.3.1 Definitions and Examples of Groups [19, §7.1]

The *Dihedral* groups will be considered as automorphism groups of a polygon (graph) rather than as groups of geometric isometries.

17.3.2 Basic Properties of Groups [19, §7.2, p. 174]

17.3.3 Subgroups [19, §7.3, p. 181]

Omit *center* p. 183.

17.3.4 Isomorphisms and Homomorphisms [19, §7.4, p. 191]

Only isomorphisms will be studied, pp. 191–193.

17.3.5 Congruence and Lagrange's Theorem [19, §7.5, p. 199]

We have covered up to the end of Theorem 7.28; students should know the statements of Theorems 7.29, but need not know how to prove them.

Consequences of Theorem 7.28 have been discussed at the lectures. It was shown that, in a finite group of order k the order of every element divides k; hence the kth power of every element is equal to e. This was applied, in particular, to the multiplicative group U_n of *units* in $\mathbb{Z}_n$. It was shown in class on 22 March that the units are precisely the congruence classes $[a]_n$ such that $(a, n) = 1$. (The units form a group under the ring operation of multiplication.) The order of the group U_n is denoted by $\phi(n)$ or $\varphi(n)$, called the *Euler (totient) function* or *Euler phi-function* of n. It was proved in class that, if the prime decomposition of n is

$$n = \prod_{i=1}^{k} p_i^{r_i}$$

then

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)$$

(The proof given was by Inclusion-Exclusion; students are not expected to be able to prove this theorem; a proof can be found in [36, Exercise 5.6.23, p. 205].) The case of

$n = p$, a prime, should be clear, however, where $\varphi(p) = p - 1$. Here we know that, if $(a, p) = 1$, then $[a]_p^{p-1} = [1]_p$, or, equivalently, $a_{p-1} \equiv 1 \pmod{p}$, which result is known as *Fermat's "Little" Theorem*. Another proof can be found in the textbook [19, Theorem 12.2, p. 402].

17.3.6 Normal Subgroups [19, §7.6, p. 208]

Omit this section.

17.3.7 Quotient Groups [19, §7.7, p. 216]

Omit this section.

17.3.8 Quotient Groups and Homomorphisms [19, §7.8, p. 222]

Omit this section.

17.3.9 The Symmetric and Alternating Groups [19, §7.9]

The disjoint cycle notation for permutations of a finite set was studied prior to entering this section. Know the definitions of S_n and A_n. Be familiar with the results in the section up to Theorem 7.50, but you need not know how to prove them.

17.3.10 The Simplicity of A_n [19, §7.10, p. 239]

Omit this section.

17.4 Chapter 8, Topics in Group Theory [19, p. 245]

17.4.1 Direct Products [19, §8.1]

Only the definition of *direct product* on pages 244–246; omit all references to *normal* subgroups.

17.4.2 Finite Abelian Groups [19, §8.2, p. 252]

Students will be expected to understand the Fundamental Theorem of Finite Abelian Groups [19, Theorem 8.7, p. 256; alternative formulation, Theorem 8.10, p. 257], but not its proof.

17.4.3 The Sylow Theorems [19, §8.3, p. 282]

Omit this section.

17.4.4 Conjugacy and the Proof of the Sylow Theorems [19, §8.4, p. 267]

Omit this section.

17.4.5 The Structure of Finite Groups [19, §8.5, p. 275]

Students should read [19, pp. 277-281] to understand the nature of the groups of orders less than 16.

17.5 [19, Chapters 9 - 12]

Omit these chapters.

17.6 Chapter 13, The Chinese Remainder Theorem [19, p. 406]

17.6.1 Proof of the Chinese Remainder Theorem [19, §13.1]

Students will be expected to be able to solve — in a systematic way — systems of congruences satisfying the conditions of the theorem. The method of the textbook, entailing a recursive reduction in the number of congruences, may be used. Other methods will be discussed.

17.6.2 Applications of the Chinese Remainder Theorem [19, §13.2, p. 412]

Students should read this section, but it will not be examination material.

18 Fifth Problem Assignment

Mounted on the Web on Sunday, 17 March, 2002
Distributed in hard copy on Wednesday, 20th March, 2002
Solutions are to be submitted on Friday, April 5th, 2002

NOTE: Students must not assume that every topic on the syllabus has been covered by problems on the assignments. In particular, the Chinese Remainder Theorem ([19, Chapter 13]) will not be represented by problems on the assignments.

1. [19, part of Exercise 7.1.A4, p. 171] Determine whether the set G is a group under the operation $*$:

   (a) $G_1 = \{2, 4, 6, 8\}$ in $\mathbb{Z}_{10}$; $a * b = ab$.

   (b) $G_2 = \{2^x | x \in \mathbb{Q}\}$; $a * b = ab$.

   (c) $G_3 = \{x \in \mathbb{Z} | x \equiv 1 \pmod 5\}$; $a * b = ab$.

   (d) $G_4 = \{c + di \in \mathbb{C} | cd = 0 \wedge c + d \neq 0\}$; $a * b = ab$.

2. Consider the set $K = \{r \in \mathbb{R} | r \neq 0, r \neq 1\}$. Determine whether the following define functions from K to K, and whether the functions constitute a group of order 6 under function composition:

$$\begin{aligned} f_1(x) &= \frac{x-1}{x} \\ f_2(x) &= \frac{1}{x} \\ f_3(x) &= \frac{x}{1} \\ f_4(x) &= \frac{1-x}{1} \\ f_5(x) &= \frac{x}{x-1} \\ f_6(x) &= \frac{1}{1-x} \end{aligned}$$

   If they form a group, give its composition table.

3. [19, Exercise 7.2.A10] Find the order of every element in each of the following groups.
   (a) $\mathbb{Z}_4$.
   (b) $\mathbb{Z}_4 \times \mathbb{Z}_2$.
   (c) S_3.
   (d) The group D_4 of automorphisms of the undirected graph of edges of the square whose vertices are 1, 2, 3, 4, and whose edges are $\{1,2\}$, $\{2,3\}$, $\{3,4\}$, $\{4,1\}$.
   (e) $\mathbb{Z}$ (under addition).

4. [19, Exercise 7.2.12, p. 179] Determine whether or not the following statement is always true: *A group of order n must contain an element of order n.* If it is true, prove that fact. If it is false, give a counterexample that has the smallest possible order.

5. [19, Exercise 7.2.B22, p. 180] Suppose that a group G with operation $*$ has the property that $\forall a \forall b[a*b*a*b = a*a*b*b]$ (which we may write, using juxtaposition for the operation, as $\forall a \forall b[(ab)^2 = a^2b^2]$). Prove that G is abelian.

6. (cf. [19, Exercise 7.3.13, p. 188]) List all the elements of the subgroup of S_7 generated by
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 7 & 6 & 2 & 4 \end{pmatrix}$$

7. (a) [19, Exercise 7.3.A21(a), p. 188] Show that the additive group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.
   (b) [19, Exercise 7.3.A21(b), p. 188] Show that the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, but is generated by 2 elements.
   (c) Give an example of a group with 8 elements that is not cyclic, and is not generated by 2 elements either.

8. (a) (cf. [19, Exercise 8.2.A3, p. 260]) List all the abelian groups (up to isomorphism) of the given orders:
      i. 15.
      ii. 72.
   (b) Use a non-abelian group of order 8 studied in this course to construct a group of order 72 that is non-abelian.

9. Prove that no two of the groups $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9 \times \mathbb{Z}_3$, and $\mathbb{Z}_{27}$ are isomorphic.

10. (a) [19, Exercise 7.5.A2(c)] List the distinct right cosets of the subgroup

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle$$

in the group S_3.

(b) Repeat, this time determining the *left* cosets.

(c) The congruence classes modulo 12, $[a]_{12}$ in $\mathbb{Z}$ are cosets of a certain subgroup in the additive group $\mathbb{Z}$ of the integers. Explain what the subgroup is, and whether the cosets are right or left cosets.

11. (a) Can a group with infinite order contain an element of finite order (other than the identity)? Explain with examples.

(b) Can a group of order 12 contain an element of order 6? Must it contain such an element? Explain.

(c) Can a group of order 12 contain an element of order 9? Explain.

19 Solutions to Problems on the Class Test

which was administered on Wednesday, March 13th, 2002
(First draft – subject to correction.)

Distribution Date: Wednesday, March 20th, 2002

	Version 1	Version 2	Version 3	Version 4
First Question	1	11	7	4
Second Question	10	6	9	12
Third Question	5	2	3	8

All questions were worth 10 marks. The performance on Versions ##1, 2, 3 was similar; but students writing Version #4 appeared to find it more difficult. Grades for Version #4 were scaled up by a factor of about 15% in an attempt to equalize the four versions.

1. (a) Showing all your work, use the Euclidean Algorithm — no other method will be accepted — to determine integers a and b such that

$$(195, 187) = 195a + 187b\,.$$

(b) Use your results in (a) to find an integer n such that

$$[n]_{195}[187]_{195} = [1]_{195}\,.$$

Solution:

(a) We apply the Euclidean Algorithm:

$$\begin{aligned} 195 &= 187 \cdot 1 + 8 \\ 187 &= 8 \cdot 23 + 3 \\ 8 &= 3 \cdot 2 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ \Rightarrow (195, 187) &= 1 \end{aligned}$$

By back substitution we obtain

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (8 - 3 \cdot 2) \cdot 1 \\ &= 8 \cdot (-1) + 3 \cdot 3 = 8 \cdot (-1) + (187 - 8 \cdot 23) \cdot 3 \\ &= 187 \cdot 3 + 8 \cdot (-70) = 187 \cdot 3 + (195 - 187 \cdot 1) \cdot (-70) \\ &= 195 \cdot (-70) + 187 \cdot 73 \end{aligned}$$

(b) Since $73 \cdot 187 = 1 + 195 \cdot 70$,

$$73 \cdot 187 = 1 + 195 \cdot 70 \equiv 1 \pmod{195};$$

it follows that

$$[73]_{195} \cdot [187]_{195} = [73 \cdot 187]_{195} = [1]_{195}.$$

2. (a) Showing all your work, use the Euclidean Algorithm — no other method will be accepted — to determine integers a and b such that

$$(209, 182) = 209a + 182b.$$

(b) Use your results in (a) to find an integer n such that

$$[n]_{209}[182]_{209} = [1]_{209}.$$

Solution:

(a) We apply the Euclidean Algorithm:

$$\begin{aligned} 209 &= 182 \cdot 1 + 27 \\ 182 &= 27 \cdot 6 + 20 \\ 27 &= 20 \cdot 1 + 7 \\ 20 &= 7 \cdot 2 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 + 0 \\ \Rightarrow (195, 187) &= 1 \end{aligned}$$

By back substitution we obtain

$$\begin{aligned} 1 &= 7 - 6 \cdot 1 = 7 - (20 - 7 \cdot 2) \cdot 1 \\ &= 20 \cdot (-1) + 7 \cdot 3 = 20 \cdot (-1) + (27 - 20 \cdot 1) \cdot 3 \\ &= 27 \cdot 3 + 20 \cdot (-4) = 27 \cdot 3 + (182 - 27 \cdot 6) \cdot (-4) \\ &= 182 \cdot (-4) + 27 \cdot 27 = 182 \cdot (-4) + (209 - 182 \cdot 1) \cdot 27 \\ &= 209 \cdot 27 + 182 \cdot (-31) \end{aligned}$$

(b) Since $(-31) \cdot 182 = 1 - 209 \cdot (27)$,

$$(-31) \cdot 182 \equiv 1 \pmod{209};$$

it follows that

$$[-31]_{209} \cdot [182]_{209} = [(-31) \cdot 182]_{209} = [1]_{209}.$$

3. In the ring $\mathbb{Z}_2[y]$ the polynomials y^3+y+1 and y^3+y^2+1 are relatively prime. Use the Euclidean Algorithm — no other method will be accepted — to determine a polynomial $g(y) \in \mathbb{Z}_2[y]$ such that

$$(y^3+y+1)g(y) \equiv 1 \pmod{y^3+y^2+1}$$

in $\mathbb{Z}_2[y]$.

Solution:

$$\begin{aligned} y^3+y^2+1 &= (y^3+y+1)\cdot 1 + (y^2+y) \\ y^3+y+1 &= (y^2+y)\cdot(y+1)+1 \\ y^2+y &= 1\cdot(y^2+y)+0 \\ \Rightarrow 1 &= (y^3+y+1)+(y^2+y)\cdot(y+1) \\ &= (y^3+y+1)+((y^3+y^2+1)+(y^3+y+1)\cdot 1)\cdot(y+1) \\ &= (y^3+y+1)\cdot y + (y^3+y^2+1)\cdot 1 \end{aligned}$$

Since $(y^3+y+1)\cdot y$ differs from 1 by a multiple of the modulus, $(y^3+y+1)\cdot y \equiv 1 \pmod{y^3+y^2+1}$. Thus one polynomial $g(y)$ is y.

4. In the ring $\mathbb{Z}_2[x]$ the polynomials x^3+x^2+x and x^3+x+1 are relatively prime. Use the Euclidean Algorithm — no other method will be accepted — to determine a polynomial $f(x) \in \mathbb{Z}_2[x]$ such that

$$(x^3+x^2+x)f(x) \equiv 1 \pmod{x^3+x+1}$$

in $\mathbb{Z}_2[x]$.

Solution:

$$\begin{aligned} x^3+x+1 &= (x^3+x^2+x)\cdot 1 + (x^2+1) \\ x^3+x^2+x &= (x^2+1)\cdot(x+1)+1 \\ x^2+1 &= 1\cdot(x^2+1)+0 \\ \Rightarrow 1 &= (x^3+x^2+x)+(x^2+1)\cdot(x+1) \\ &= (x^3+x^2+x)+((x^3+x+1)+(x^3+x^2+x)\cdot 1)\cdot(x+1) \\ &= (x^3+x^2+x)\cdot x + (x^3+x+1)\cdot(x+1) \end{aligned}$$

Since $(x^3+x^2+x)\cdot x$ differs from 1 by a multiple of the modulus, $(x^3+x^2+x)\cdot x \equiv 1 \pmod{x^3+x+1}$. Thus one polynomial $f(x)$ is x.

5. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we

will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = ab^2$$

Solution: This operation is neither associative nor distributive over addition. In order to be associative, it would have to have the property that, for all real numbers a, b, c, $(a*b)*c = a*(b*c)$, i.e., that $ab^2c^2 = a(bc^2)^2 = ab^2c^4$. Thus we can obtain a counterexample by taking a, b, c to be non-zero real numbers such that $c^2 \neq 1$; for example, take $a = b = 1$, $c = 2$. Then

$$(a * b) * c = 4 \neq 16 = a * (b * c)$$

The operation also fails to satisfy the distributive law. Since $a*(b+c) = a(b+c)^2 = a(b^2 + 2bc + c^2)$, and $(a * b) + (a * c) = ab^2 + ac^2$, we need only take values of a, b, c such that $2abc \neq 0$, for example $a = b = c = 1$.

6. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition, and $-$ is the usual operation of subtraction).

$$a * b = a - b$$

Solution: This operation is neither associative nor distributive over addition. In order to be associative, it would have to have the property that, for all real numbers a, b, c, $(a-b)-c = a-(b-c)$, i.e., that $a-b-c = a-b+c$. Thus we can obtain a counterexample by taking a, b, c to have any real values and $c \neq 0$; for example, with $a = b = c = 1$,

$$(a * b) * c = -1 \neq 1 = a * (b * c)$$

The operation also fails to satisfy the distributive law. Since $a*(b+c) = a-(b+c) = a - b - c$, and $(a * b) + (a * c) = (a - b) + (a - c) = 2a - b - c$, we need only take values of a, b, c such that $a \neq 0$, for example $a = b = c = 1$.

7. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that

the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = a$$

Solution: This operation is not distributive over addition. Since $a * (b + c) = a$, and $(a * b) + (a * c) = a + a = 2a$, we need only take values of a, b, c such that $a \neq 0$, for example $a = b = c = 1$. Then

$$a * (b + c) = 1 \neq 1 + 1 = (a * b) + (a * c)$$

8. We wish to construct a ring whose underlying set is the set $\mathbb{R}$ of real numbers. The addition operation is to be taken to be the usual addition of real numbers, and we will use the usual symbol for it. Provide an explicit counterexample to show that the following definition of multiplication (denoted by $*$) does *not* satisfy all the axioms of a ring (where we denote the usual operation of multiplication in $\mathbb{R}$ by juxtaposition).

$$a * b = a + b$$

Solution: This operation is not distributive over addition. Since $a * (b + c) = a + (b + c)$, and $(a * b) + (a * c) = (a + b) + (a + c) = 2a + b + c$, we need only take values of a, b, c such that $a \neq 0$, for example $a = b = c = 1$. Then $a * (b + c) = a + (b + c) = 3 \neq 2 + 2 = (a + b) + (a + c) = (a * b) + (a * c)$

9. Give the addition and multiplication tables of the ring $\mathbb{Z}_3 \times \mathbb{Z}_2$.

Solution: We shall write the element $([a]_3, [b]_2) \in \mathbb{Z}_3 \times \mathbb{Z}_2$ simply as ab.

$+$	00	01	10	11	20	21
00	00	01	10	11	20	21
01	01	00	11	10	21	20
10	10	11	20	21	00	01
11	11	10	21	20	01	00
20	20	21	00	01	10	11
21	21	20	01	00	11	10

$\cdot$	00	01	10	11	20	21
00	00	00	00	00	00	00
01	00	01	00	01	00	01
10	00	00	10	10	20	20
11	00	01	10	11	20	21
20	00	00	20	20	10	10
21	00	01	20	21	10	11

10. List the elements of the ring $\mathbb{Z}_2[x]/(x^2 + 1)$ of congruence classes of polynomials in $\mathbb{Z}_2[x]$ modulo the polynomial $x^2 + 1$. Give the addition and multiplication tables of $\mathbb{Z}_2[x]/(x^2 + 1)$. In these tables you are expected to denote each element in only one way: that is, the same element may not appear in your tables with more than one representation.

Solution: The ring contains 4 elements, representable by the 4 possible remainders when a polynomial is divided by x^2+1, i.e. [0], [1], [x], [$1+x$]. In constructing the tables we shall suppress the square brackets.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0

11. Give your choice of three rows of the composition table of the group S_3.
Solution: Here is the entire table:

	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

12. Give the composition table of the group whose elements are $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$.
Solution:

	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$

20 Solutions, Fourth Problem Assignment

Distribution Date: Mounted on the Web on Thursday, April 11th, 2002
Solutions were to be submitted by Friday, March 15th, 2002
PLEASE NOTE: THIS IS A PRELIMINARY VERSION, AND IS SUBJECT TO CORRECTION.

1. (a) Prove that the polynomial $x^4 + x^3 + x^2 + x^1 + x^0$ is irreducible in $\mathbb{Z}_2[x]$ by assuming that it has a factorization, and deriving a contradiction. You will have to consider various types of possible factorizations. (You will see a different proof of this result in the solutions to Assignment 2.)

   (b) Using the Euclidean Algorithm, determine the inverse to the congruence class $[x^3 + x^2 + x^0]$ in the ring $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x^1 + x^0)$.

   (c) In each of the congruence classes $[x^1]$, $[x^3]$, $[x^5]$, $[x^9]$ of the ring $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x^1 + x^0)$ determine a member polynomial of degree less than 4.

   Solution:

   (a) If there exists a nontrivial factorization of this polynomial into polynomials of smaller degrees, then the degrees of the factors must be one of the following (with given multiplicities): $(3, 1)$, $(2, 2)$, $(2, 1, 1)$, $(1, 1, 1, 1)$. We can eliminate all but the second of these partitions by observing that $1^4+1^3+1^2+1^1+1^0 = 1 = 0^4 + 0^3 + 0^2 + 0^1 + 0^0$,[28] so neither of the elements of the field $\mathbb{Z}_2$ is a root. By the Factor Theorem, there can be no factor $x - a$ since that would correspond to a root a.

   Suppose that

$$x^4 + x^3 + x^2 + x^1 + x^0 = (x^2 + ax + b)(x^2 + cx + d)\,,$$

   where $a, b, c, d \in \mathbb{Z}_2$. We can take the two second-degree factors to be monic since all polynomials (except 0) in $\mathbb{Z}_2[x]$ are monic. Equating coefficients of corresponding powers of x yields

$$\begin{aligned} 1 &= 1 && (28)\\ 1 &= a + c && (29)\\ 1 &= b + d + ac && (30)\\ 1 &= ad + bc && (31)\\ 1 &= bd && (32) \end{aligned}$$

[28] Remember, $0^0 = 1$.

The only possible solution to (32) is

$$b = 1 = d\,. \tag{33}$$

Substituting in (30) we observe that the only possible solution of the resulting equation is

$$a = 1 = c\,. \tag{34}$$

But these four values are not compatible with either (29) or (31). We conclude that no factorization into quadratic factors exists. It follows that the given polynomial is irreducible over $\mathbb{Z}_2$. Of course, this polynomial is *reducible* over some other fields, e.g. $\mathbb{C}$, $\mathbb{Z}_5$.

(b)

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 &= (x^3 + x^2 + x)x + (x^2 + 1) \\ x^3 + x^2 + 1 &= (x^2 + 1)(x + 1) + x \\ x^2 + 1 &= x \cdot x + 1 \\ x &= 1 \cdot x + 0 \end{aligned}$$

$$\begin{aligned} 1 &= (x^2 + 1) - x \cdot x \\ &= (x^2 + 1) - ((x^3 + x^2 + 1) - (x^2 + 1)(x + 1))x \\ &= (x^3 + x^2 + 1)x + (x^2 + 1)(x^2 + x + 1) \\ &= (x^3 + x^2 + 1)x \\ &\qquad +((x^4 + x^3 + x^2 + x + 1) - (x^3 + x^2 + 1)x)(x^2 + x + 1) \\ &= (x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) + (x^3 + x^2 + 1)(x^3 + x^2) \end{aligned}$$

It follows that

$$(x^3 + x^2 + 1)(x^3 + x^2) \equiv 1 \pmod{()x^4 + x^3 + x^2 + x + 1}$$

in $\mathbb{Z}_2[x]$, and that $[x^3 + x^2 + 1]^{-1} = [x^3 + x^2]$ in $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$.

(c) For the congruence classes $[x^1]$ and $[x^3]$ the given representatives, i.e. x and x^3 are (the only) polynomial members whose degree is less than 4. Since

$$x^5 = (x^4 + x^3 + x^2 + x + 1)(x - 1) + 1$$

over any field,

$$x^5 \equiv 1 \pmod{x^4 + x^3 + x^2 + x + 1}$$

in $\mathbb{Z}_2$. Thus 1 is a member polynomial of $[x^5]$ of degree less than 4. (In fact, it is the *only* such member polynomial.)

$$\begin{aligned} x^9 &= x^5 \cdot x^4 \equiv 1 \cdot x^4 \pmod{x^4+x^3+x^2+x+1} \\ &= 1 \cdot ((x^4+x^3+x^2+x+1)1 + (x^3+x^2+x+1)) \\ &\equiv x^3+x^2+x+1 \pmod{x^4+x^3+x^2+x+1} \end{aligned}$$

so the representative of class $[x^9]$ having degree less than 4 is x^3+x^2+x+1.

2. [19, Exercise 5.2.A4] Show that, under congruence modulo x^3+2x+1 in $\mathbb{Z}_3[x]$, there are exactly 27 distinct congruence classes. Describe a system of representatives for these classes.

   Solution: Two polynomials are congruent — i.e. in the same congruence class — iff they yield the same remainder upon division by x^3+2x+1. The quotients upon division by this 3rd degree polynomial can be any of the polynomials of degree less than 3, including the 0 polynomial. The number of polynomials of these types is the number of ways of selecting coefficients $a_0, a_1, a_2 \in \mathbb{Z}_3$ for a polynomial $a_2x^2 + a_1x^1 + a_0x^0 \in \mathbb{Z}_3[x]$, i.e. $3^3 = 27$. Each of these polynomials may serve as the representative of the congruence class of which it is a member, and no 2 of them are congruent.

3. In the following problems each element of the given congruence class ring can be written in the form $[ax + b]$ (Why?). Determine the rules for addition and multiplication of congruence classes. (In other words, if the product $[ax+b]\cdot[cx+d]$ is the class $[rx + s]$, describe how to find r and s from a, b, c, d, and similarly for addition.)

   (a) [19, Exercise 5.2.B8] $\mathbb{Q}[x]/(x^2)$.

   (b) $\mathbb{Z}_3[x]/(x^2+1)$. Work out the multiplication table.

   (c) $\mathbb{R}[x]/(x^2+1)$. Show that this ring of polynomials is isomorphic to the field $\mathbb{C}$.

   Solution:

   (a) We are considering congruence classes in the ring of rational polynomials in an indeterminate x modulo the polynomial x^2. Since very polynomial is congruent to its remainder upon division by x^2, and since that remainder will have degree 1 at most, we may select, as the representative of a class $[a_0 + a_1x + a_2x^2 + ... + a_nx^n]$, the common remainder upon division by x^2, and this will be a linear polynomial of the form $ax + b$.

Modulo the polynomial x^2 over the field $\mathbb{Q}$,

$$\begin{aligned}[ax+b]+[cx+d] &= [(a+c)x+(b+d)]\\ [ax+b]\cdot[cx+d] &= [(ac)x^2+(ad+bc)x+(b+d)] = [(ad+bc)x+(b+d)]\,.\end{aligned}$$

(b) Modulo the 2nd-degree polynomial x^2+1 over the field $\mathbb{Z}_3$ $[ax+b]+[cx+d]$ is computed just as in the preceding case, with term by term addition of coefficients of like powers of x, and reductions modulo 3 as required; and

$$\begin{aligned}[ax+b]\cdot[cx+d] &= [(ac)x^2+(ad+bc)x+(b+d)]\\ &= [(ac)(x^2+1)+(ad+bc)x+(b+d-ac)]\\ &= [(ad+bc)x+(b+d+2ac)]\end{aligned}$$

where the coefficients of x^1 and x^0 are again reduced, this time modulo 3; we may also describe the aggregate reductions here as *modulīs*[29] 3 and x^2+1. The addition table is

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

The multiplication table is

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

[29] meaning, *to the modulī* (the plural of *modulus*)

(c) The only difference between this case and the preceding is that the calculation of $ad + bc + ad$ and $b + d$ are carried out in $\mathbb{R}$.

4. Find a polynomial in $\mathbb{R}[x]$ that satisfies the given conditions:

   (a) [19, Exercise 4.6.A2(a), p. 118] Monic of degree 3 with 2 and $3 + i$ as roots

   (b) [19, Exercise 4.6.A2(b), p. 118] Monic of least possible degree with $1 - i$ and $2i$ as roots

   (c) [19, Exercise 4.6.A2(c), p. 118] Monic of least possible degree with 3 and $4i - 1$ as roots.

   Solution:

   (a) Since the coefficients are real numbers [19, Lemma 4.28, p. 116] ensures that the conjugates of the two given complex numbers are also roots of the polynomial when it is considered over the field $\mathbb{C}$. This has no implications for 2, since $\overline{2} = 2$; however, $\overline{3 + i} = 3 - i$ must also be a root. The polynomial will be divisible by $(x - 2)(x - (3 + i))(x - (3 - i))$, i.e. by $(x - 2)((x - 3)^2 + 1)$, i.e. by $(x - 2)(x^2 - 6x + 10) = x^3 - 8x^2 + 22x - 20$. As this last mentioned polynomial is monic, it satisfies the given root conditions. As its degree is 3, it is the only polynomial with the desired properties.

   (b) The fact that each of the given roots is not on the real line in $\mathbb{C}$ implies that their conjugates, which are distinct from them, are also roots. Hence any real polynomial with these roots will be divisible by $(x - (1 - i))(x - 2i)(x - (1 + i))(x - (-2i))$, i.e. by $((x - 1)^2 + 1)(x^2 + 4) = x^4 - 2x^3 + 6x^2 - 8x + 8$. As this last polynomial is monic, it is the polynomial of least possible degree satisfying the given conditions.

   (c) The polynomial will be divisible by $(x - 3)(x - (4i - 1))(x - (-4i - 1)) = (x - 3)((x + 1)^2 + 16) = x^3 - x^2 + 11x - 51$.

5. [19, Exercise 4.6.B8, p. 118] Prove or disprove: Let a and b be real numbers. If $a + bi$ is a root of $x^3 - 3x^2 + 2ix + i - 1 \in \mathbb{C}[x]$, then $a - bi$ is also a root.[30]

   Solution: The theorem that states that the complex conjugate of a root is also a root requires that all coefficients of the polynomial be real. If the coefficients are not all on the real line in $\mathbb{C}$, then one cannot infer that the conjugates of roots must also be roots.

   In the given example, one root is i, since $i^3 - -3i^2 + 2i^2 + i - 1 = 0$. But $(-i)^3 - 3(-i)^2 + 2i(-i) + i - 1 = 2i + 4 \neq 0$, so $-i$ is not a root.

[30] We are using the familiar $x + iy$ notation for complex numbers [19, p. 47].

21 Solutions, Fifth Problem Assignment

Distribution Date: Mounted on the Web on Thursday, April 11th, 2002
Solutions were to be submitted on Friday, April 5th, 2002
PLEASE NOTE: THIS IS A PRELIMINARY VERSION, AND IS SUBJECT TO CORRECTION.

NOTE: Students must not assume that every topic on the syllabus has been covered by problems on the assignments. In particular, the Chinese Remainder Theorem ([19, Chapter 13]) will not be represented by problems on the assignments.

1. [19, part of Exercise 7.1.A4, p. 171] Determine whether the set G is a group under the operation $*$:

   (a) $G_1 = \{2, 4, 6, 8\}$ in $\mathbb{Z}_{10}$; $a * b = ab$.

   (b) $G_2 = \{2^x | x \in \mathbb{Q}\}$ $a * b = ab$.

   (c) $G_3 = \{x \in \mathbb{Z} | x \equiv 1 \pmod 5\}$; $a * b = ab$.

   (d) $G_4 = \{c + di \in \mathbb{C} | cd = 0 \wedge c + d \neq 0\}$; $a * b = ab$.

   Solution:

   (a) This is, indeed, a group: it is cyclic, of order 4, generated by the element 2. We observe that $2 * 2 = 4 \in G_1$; $2 * 4 = 8 \in G_1$, $2 * 8 = 16 = 6 \in G_1$, $2 \times 6 = 12 = 2$, so $2^4 = 16$ is the identity element. Note that $\mathbb{Z}_{10}$ is not a group, so we cannot solve this problem by appealing to [19, Theorem 7.10, p. 182]. (Some of the elements of $\mathbb{Z}_{10}$ do not have inverses under the operation of multiplication — e.g. 5 does not have an inverse under multiplication.) The multiplication table defined by $*$ is

$*$	$2^0 = 6$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$
2^0	2^0	2^1	2^2	2^3
2^1	2^1	2^2	2^3	2^0
2^2	2^2	2^3	2^0	2^1
2^3	2^3	2^0	2^1	2^2

   .

   This is a table we know to represent a cyclic group of order 4, e.g. the additive group of $\mathbb{Z}_4$, or the group of rotations of the 4-gon, generated by the permutation (1234).

   (b) We are working with a subset of the real numbers, using the usual definition of multiplication of real numbers. We have to prove that the set is

- non-empty
- closed under $*$
- closed under the taking of inverses

It is non-empty, since one member is 2^0, i.e. 1. If a and b are any two elements of G_2, they must be of the form $a = 2^\alpha$, $b = 2^\beta$, where α and β are rationals, say $\alpha = \frac{u}{v}$, $\beta = \frac{w}{x}$, where u, v, w, x are integers, and v and x are non-zero. Then $a * b$ is defined to be $2^{\alpha+\beta} = 2^{\frac{u}{v}+\frac{w}{x}} = 2^{\frac{ux+wv}{vx}}$ which is in G_2, since the exponent is again a rational number. Thus G_2 is closed under $*$.

The identity being $2^0 = 1$, the inverse of any element $2^{\frac{u}{v}}$ is $2^{\frac{-u}{v}} \in G_2$, so G_2 is closed under the taking of inverses. Hence G_2 is a subgroup.

(c) The product of two integers that are congruent to 1 will be congruent to $1 \times 1 = 1$, so G_3 is closed under $*$. But all that shows is that the operation $*$ is well defined. Since $\mathbb{Z}$ is not a group under multiplication, we cannot appeal to any subgroup theorems. There is an identity for this operation, namely $1 \in G_3$. However, not every element has an inverse. For example, there does not exist an integer $b \in G_3$ with the property that $6 * b = 1$. G_3 is not a group; it is only what we call a *monoid*.

(d) G_4 consists of those complex numbers for which either the real part or the "imaginary part" is 0, but not both; thus it consists of all numbers on the real and imaginary axes (x- and y-axes), except for 0, which lies at their intersection. This set is, indeed, closed under the taking of products and inverses (as $i^2 = -1$ and $i^{-1} = -i$), and so G_4 is a group under the usual multiplication of complex numbers, since it is a subgroup of the multiplicative group $\mathbb{C} - \{0\}$ of the field $\mathbb{C}$.

2. Consider the set $K = \{r \in \mathbb{R} | r \neq 0, r \neq 1\}$. Determine whether the following define functions from K to K, and whether the functions constitute a group of order 6 under function composition:

$$\begin{aligned} f_1(x) &= \frac{x-1}{x} \\ f_2(x) &= \frac{1}{x} \\ f_3(x) &= \frac{x}{1} \\ f_4(x) &= \frac{1-x}{1} \end{aligned}$$

$$f_5(x) = \frac{x}{x-1}$$

$$f_6(x) = \frac{1}{1-x}$$

If they form a group, give its composition table.

Solution: We observe that the denominators of the fractions are non-zero throughout the domain K, so the fractions are well defined; we also observe that the values of the fractions are never 0 or 1, so the values are all in K, and the 6 functions are well defined. Function composition has been shown in the lectures to be associative. We have to prove the other axioms. Function f_3 is the identity function. Let us compute all the compositions $f_i \circ f_j$ $(i, j = 1, 2, 3, 4, 5, 6)$. Remember that we are not multiplying fractions here. Thus it is not true that $f_1 \circ f_4$ is the identity, since, while $\frac{1}{1-x} \times (1-x) = 1$, $(f_1 \circ f_4)(x) = f_1(1-x) = \frac{1-(1-x)}{1-x} = \frac{x}{x-1} = f_5(x)$ for all $x \in K$, so $f_1 \circ f_4 = f_3$. Proceeding in this fashion we compute all entries in the composition table:

$\circ$	f_3	f_1	f_2	f_4	f_5	f_6
f_3	f_3	f_1	f_2	f_4	f_5	f_6
f_1	f_1	f_6	f_4	f_5	f_2	f_3
f_2	f_2	f_5	f_3	f_6	f_1	f_4
f_4	f_4	f_2	f_1	f_3	f_6	f_5
f_5	f_5	f_4	f_6	f_1	f_3	f_2
f_6	f_6	f_3	f_5	f_2	f_4	f_1

We can see from the table that f_3 is an identity element. Function composition is always associative [19, pp. 510-511]. For any element f_i the entry f^3 appears in the ith row and in the ith column of the table; the column (respectively, row) of the table containing this entry f_3 corresponds to the inverse of f_i $(i = 1, 2, 3, 4, 5, 6)$.

3. [19, Exercise 7.2.A10] Find the order of every element in each of the following groups.

   (a) $\mathbb{Z}_4$.

   (b) $\mathbb{Z}_4 \times \mathbb{Z}_2$.

   (c) S_3.

   (d) The group D_4 of automorphisms of the undirected graph of edges of the square whose vertices are 1, 2, 3, 4, and whose edges are $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, $\{4, 1\}$.

   (e) $\mathbb{Z}$ (under addition).

Solution:

(a) 1 and -1 (which is the same as 3) are both generators of the group: their order is 4. 2 has order 2, since $2 + 2 = 0$. 0 has order 1.

(b) The elements are ordered pairs, where the first coordinate is treated modulo 4, while the second is treated modulo 2. Elements $(1, x)$ and $(3, x)$ have order 4, for either of the possible values of x. Element $(2, x)$) has order 2 for either x; element $(0, 0)$ is the identity, and has order 1; element $(0, 1)$ has order 2.

(c) For convenience the elements will be expressed in disjoint cycle notation. The two 3-cycles (123) and (132) both have order 3; the 2-cycles — i.e. the elements expressible in the form $(\bullet\bullet)(\bullet)$ — all have order 2; the identity has order 1.

(d) This was discussed in the lecture of March 15th. The elements (1234) and (1432) have order 4; elements (13)(24), (12)(34), and (14)(23) have order 2; elements (13) and (24) have order 2 also; and the identity has order 1.

(e) All elements except 0 have infinite order; the order of the identity, 0, is 1.

4. [19, Exercise 7.2.12, p. 179] Determine whether or not the following statement is always true: *A group of order n must contain an element of order n.* If it is true, prove that fact. If it is false, give a counterexample that has the smallest possible order.

   Solution: The statement is false. The statement is equivalent to saying that every group is cyclic. For examples, S_3 has order 6, but the orders of its elements are 1, 2, 3; $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4, but the orders of its elements are 1 and 2 only. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the smallest counterexample, since groups of orders 1, 2, 3 are all cyclic.

5. [19, Exercise 7.2.B22, p. 180] Suppose that a group G with operation $*$ has the property that $\forall a \forall b[a*b*a*b = a*a*b*b]$ (which we may write, using juxtaposition for the operation, as $\forall a \forall b[(ab)^2 = a^2b^2]$). Prove that G is abelian.

   Solution: From $abab = aabb$ it follows that $a^{-1}(abab)(b^{-1} = a^{-1}(aabb)b^{-1}$, from which it follows (by the associativity property) that $ebae = eabe$, so $ba = ab$. As this is true for all a and all b, the group is abelian.

6. (cf. [19, Exercise 7.3.13, p. 188]) List all the elements of the subgroup of S_7 generated by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 7 & 6 & 2 & 4 \end{pmatrix}$$

   Solution: We shall express the elements in the disjoint cycle notation. The given element is (13)(47)(256). When we compose this element with itself, we find that

in even powers the two 2-cycles disappear; and, in powers divisible by 3, the 3-cycle disappears. Only when we take a power divisible by both 2 and 3 do we have the product equal to the identity. More precisely,

$$\begin{aligned}
((13)(47)(256))^1 &= (13)(47)(256) \\
((13)(47)(256))^2 &= (1)(3)(4)(7)(256)^2 = (265) \\
((13)(47)(256))^3 &= (13)(47)(2)(5)(6) = (13)(47) \\
((13)(47)(256))^4 &= (1)(3)(4)(7)(256) = (256) \\
((13)(47)(256))^5 &= (13)(47)(265) \\
((13)(47)(256))^6 &= (1)(3)(4)(7)(2)(5)(6) = e
\end{aligned}$$

7. (a) [19, Exercise 7.3.A21(a), p. 188] Show that the additive group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

   (b) [19, Exercise 7.3.A21(b), p. 188] Show that the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, but is generated by 2 elements.

   (c) Give an example of a group with 8 elements that is not cyclic, and is not generated by 2 elements either.

   Solution:

   (a) The group is generated by either of the elements $(1, 1)$ and $(1, 2)$. For example, $(1, 1) + (1, 1) = (2, 2) = (0, 2)$; $(1, 1) + (1, 1) + (1, 1) = (3, 3) = (1, 0)$, $(1, 1) + (1, 1) + (1, 1) + (1, 1) = (4, 4) = (0, 1)$, $(1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) = (5, 5) = (1, 2)$ and the sum of 6 copies is the identity element, $(0, 0)$; so we have expressed all the elements of the group as sums of copies of the single generator.

   (b) The orders of all elements are either 1 (for the identity), or 2 (for each of the other 3 elements, $(1, 0)$, $(0, 1)$, $(1, 1)$), so none of them can generate a subgroup containing for distinct elements. But any 2 of the non-zero elements add to give the 3rd, so the two of them generate the entire group, since any element plus itself gives the identity element (here the element $(0, 0)$.)

   (c) The group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ contains $2^3 = 8$ elements. All of its elements have order 2, except for the identity, which has order 1. It is not cyclic, since the largest cyclic subgroups have order 2. Any two distinct elements a, b, commute, and together generate a subgroup of order either 2 or 4: of order 2 if one of them is the identity, and otherwise of order 4 (with elements e, a, b, $a + b$, since $a + b$ will be distinct from both a and b.

8. (a) (cf. [19, Exercise 8.2.A3, p. 260]) List all the abelian groups (up to isomorphism) of the given orders:

i. 15.
ii. 72.

(b) Use a non-abelian group of order 8 studied in this course to construct a group of order 72 that is non-abelian.

Solution:

(a) i. $15 = 3^1 \times 5^1$. Since 3 and 5 are primes, the only abelian group of this order is (isomorphic to) $\mathbb{Z}_3 \times \mathbb{Z}_5$. This group is isomorphic to $\mathbb{Z}_{15}$. (It happens that this is the *only* group of order 15.)

ii. Since $72 = 2^3 \times 3^2$, we find, by considering the partitions of 3 and 2, that the groups of order 72 are the following:

$$\begin{gathered}\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \\ \mathbb{Z}_8 \times \mathbb{Z}_9\end{gathered}$$

(b) Let D_4 be the dihedral group of order 8, seen as the automorphism group of the graph of edges of a square with vertices 1, 2, 3, 4. Then $D_4 \times \mathbb{Z}_9$ will have order 72, but will not be abelian. For example, since the elements (12)(34) and (13)(2)(4) do not commute in D_4 — $(12)(34) \circ (13) = (1432)$, while $(13) \circ (12)(34) = (1234)$ — neither do the following elements in $D_4 \times \mathbb{Z}_9$: $((12)(34), 0)$ and $((13)(2)(4), 0)$.

9. Prove that no two of the groups $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9 \times \mathbb{Z}_3$, and $\mathbb{Z}_{27}$ are isomorphic.

Solution: In $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, the orders of the elements are either 1 (for the identity) or 3 (for all other elements); in $\mathbb{Z}_9 \times \mathbb{Z}_3$, the orders of all elements are either 1, 3, or 9 — and there are elements whose orders are different from those available in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, for example $([1]_9, [0]_3)$ has order 9. And, in $\mathbb{Z}_{27}$, there are elements (e.g. $[1]_{27}$) of order 27 — an order not available in either of the other two groups. The orders of elements must be preserved under isomorphism, so no two of the groups can be isomorphic.

10. (a) [19, Exercise 7.5.A2(c)] List the distinct right cosets of the subgroup

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle$$

in the group S_3.

(b) Repeat, this time determining the *left* cosets.

(c) The congruence classes modulo 12, $[a]_{12}$ in $\mathbb{Z}$ are cosets of a certain subgroup in the additive group $\mathbb{Z}$ of the integers. Explain what the subgroup is, and whether the cosets are right or left cosets.

Solution:

(a) The subgroup is a cyclic group of order 2, so its index in S^3 is $\frac{3!}{2} = 3$. The three right cosets are

$$\begin{aligned} < (23) > &= \{e, (23)\} \\ \{e, (23)\}(12) &= \{(12), (23)(12)\} = \{(12), (132)\} \\ \{e, (23)\}(13) &= \{(13), (23)(13)\} = \{(13), (123)\} \end{aligned}$$

(b) The three left cosets are

$$\begin{aligned} < (23) > &= \{e, (23)\} \\ (12)\{e, (23)\} &= \{(12), (12)(23)\} = \{(12), (123)\} \\ (13)\{e, (23)\} &= \{(13), (13)(23)\} = \{(13), (132)\} \end{aligned}$$

(c) The subgroup is the group $(12) = 12\mathbb{Z} = \{\ldots, -24, -12, 0, 12, 24, 36, \ldots\}$ of multiples of 12. Every left coset is a right coset, and vice versa, since the group $\mathbb{Z}$ is abelian.

11. (a) Can a group with infinite order contain an element of finite order (other than the identity)? Explain with examples. Explain.

(b) Can a group of order 12 contain an element of order 6? Must it contain such an element? Explain.

(c) Can a group of order 12 contain an element of order 9? Explain.

Solution:

(a) A group of infinite order can — but need not — contain elements of finite order. For example, the additive group $\mathbb{Z}$ contains, with the exception of the identity element, 0, only elements of infinite order. However, the infinite group $\mathbb{Z} \times \mathbb{Z}_2$ contains the element $(0, [1]_2)$ — which is not the identity — of order 2.

(b) A group of order 12 may contain an element of order 6, but it need not contain such an element either. The group $\mathbb{Z}_{12}$ contains the elements $[2]_{12}$ and $[10]_{12}$, both of order 6. However, the group A_4 of "even" permutations in S_4 has order

$\frac{4!}{2} = 12$, but the orders of its elements are only 1, 2, and 3.[31] The elements of A_4 are those elements of S_4 having disjoint cycle decompositions of forms $(\bullet)(\bullet)(\bullet)(\bullet)$, $(\bullet\bullet)(\bullet\bullet)$, $(\bullet\bullet\bullet)(\bullet)$; there are, respectively, 1 element of the first type (only the identity), $\frac{\binom{4}{2}}{2} = 3$ of the second type, and $\binom{4}{3} \cdot (3-1)! = 8$ of the third type.

(c) But a group of order 12 can contain only subgroups whose orders are divisors of 12, i.e. orders 1, 2, 3, 6, 12. As 9 does not divide 12, there will be no subgroups of order 9.

[31] It doesn't even contain a subgroup of order 6.

22 References

[1] N. L. Biggs, *Discrete Mathematics*. Clarendon Press, Oxford (1985). ISBN 0–19–853252–0; 0–19–853266–0 (Pbk).

[2] D. M. Bressoud, *Factorization and Primality Testing*. Springer-Verlag, New York (1989). ISBN 0–387–97040–1.

[3] W. Burnside, *Theory of Groups of Finite Order, (2nd Edition)*. Dover Books, New York (1955); reprint of original edition published by Cambridge University Press (1911).

[4] Lindsay N. Childs, *A Concrete Introduction to Higher Algebra, Second Edition*. Spinger-Verlag, New York, 1995 . ISBN 0-387-94484-2.

[5] H. Davenport, *The Higher Arithmetic: an Introduction to the Theory of Numbers*. Hutchison's University Library, London (1952); Harper Torchbooks, New York (1960); 5th edition, Cambridge University Press, Cambridge and New York (1982).

[6] L. E. Dickson, *History of the Theory of Numbers – I. Divisibility and Primality*. Chelsea Publishing Co., New York (1971) reprint of 1919–1923 edition (Carnegie Institute, Washington). ISBN 0–8284–0086–5.

[7] L. E. Dickson, *History of the Theory of Numbers – II. Diophantine Analysis*. Chelsea Publishing Co., New York (1971) reprint of 1919–1923 edition (Carnegie Institute, Washington). ISBN 0–8284–0086–5.

[8] J. R. Durbin, *Modern Algebra, An Introduction. Third Edition*, (J. Wiley & Sons, Inc., New York, &c, 1992); ISBN 0-471-51001-7.

[9] H. M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory.* Graduate Texts in Mathematics **50**. Springer-Verlag, New York (1977). ISBN 0–387–90230–9.

[10] Euclid, *Euclid's Elements*, translated with introduction and commentary by Sir Thomas L. Heath, Second Edition unabridged. Dover Publications, Inc., New York. ISBN 0–486–60088–2, –60089–0, –60090–4 (1956).

[11] L. Gårding and T. Tambour, *Algebra for Computer Science*. Springer-Verlag, New York, Berlin, etc.; ISBN 0–387–96780–X (1988).

[12] R. E. Greenwood and A. M. Gleason, *Combinatorial relations and chromatic graphs*. Canadian Journal of Mathematics, **7** (1955), pp. 1–7.

[13] Gary Haggard, John Schlipf, and Sue Whitesides, *Discrete Mathematical Structures for Computer Science*. Preliminary edition (February 26th, 1990), reproduced xerographically.

[14] H. S. Hall and S. R. Knight, *Higher Algebra, (Fourth Edition)*. London, MacMillan & Co. Ltd. (1891).

[15] M. Hall, Jr., *The Theory of Groups*. The Macmillan Company, New York (1959).

[16] P. Hall, *On representatives of subsets.* Journal of the London Mathematical Society, **10** (1935), 26-30.

[17] P. R. Halmos and H. E. Vaughan, *The marriage problem.* American Mathematical Monthly, **72** (1950), 214-215.

[18] A. J. Hoffman, R. R. Singleton, *On Moore graphs with diameters 2 and 3*. IBM Journal of Research and Development **4** (1960) pp. 497–504.

[19] Thomas W. Hungerford, *Abstract Algebra, An Introduction (Second Edition)*, Saunders College Publishing, Harcourt Brace College Publishers (1990). ISBN 0-03-010559-5 (hardbound).

[20] N. Jacobson, *Lectures in Abstract Algebra. I. Basic Concepts*. Springer-Verlag, New York. ISBN 0–387–90181-7.

[21] M. Ch. Klin, R. Pöschel, K. Rosenbaum, *Angewandte Algebra für Mathematiker und Informatiker*. Friedr. Vieweg u. Sohn, Braunschweig/Wiesbaden (1988). ISBN 3–528–08985–7.

[22] D. E. Knuth, *The Art of Computer Programming, Volume 1/Fundamental Algorithms*. Addison-Wesley Publishing Company, Reading, Mass., Don Mills, Ontario, etc. (1968).

[23] D. E. Knuth, *The Art of Computer Programming, Volume 2/Seminumerical Algorithms*. Addison-Wesley Publishing Company, Reading, Mass., Don Mills, Ontario, etc. (1969).

[24] N. Koblitz, *A Course in Number Theory and Cryptography. Graduate Texts in Mathematics* **114**. *Springer-Verlag, New York, (1987). ISBN 0–387–96576–9.*

[25] P. G. Lejeune-Dirichlet, *Abhandlungen der Akad. Wiss. Berlin* (1837), 45-81.

[26] C. L. Liu, *Introduction to Combinatorial Mathematics*. McGraw-Hill Book Company, New York, etc. (1968). PSEAL Library, QA164 L58.

[27] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, Amsterdam, etc. 1977. ISBN 0–444–85009–0, 0–444–85010–4.

[28] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers, 3rd edition*. John Wiley & Sons, Inc., New York, Toronto, etc., (1972) ISBN 0–471–64154–5.

[29] V. Pless, *Introduction to the Theory of Error-Correcting Codes.* Wiley-Interscience, New York (1982). ISBN 0–471–08684–3.

[30] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen*. Acta Mathematica **68** (1937), 145–254.

[31] A. M. Gleason, R. M. Greenwood, L. M. Kelly (editors) *The William Lowell Putnam Mathematical Competition, Problems and Solutions, 1938 –1964.* Mathematical Association of America (1980). ISBN 0-988385-428-7.

[32] G. Pólya and R. C. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*. Springer-Verlag, New York, (1987). ISBN 0–387–96413–4.

[33] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the Association for Computing Machinery **21** (1978), 120–126.

[34] K. R. Rosen, *Discrete Mathematics and its Applications. Third Edition*, (McGraw-Hill Inc., 1995); ISBN 0-07-053965-0.

[35] K. R. Rosen, *Discrete Mathematics and its Applications. Fourth Edition*, (McGraw-Hill Inc., 1999); ISBN 0-07-289905-0.

[36] K. H. Rosen *Student Solutions Guide for Discrete Mathematics and its Applications, 4th Edition*, (McGraw-Hill, Inc., 1999), ISBN 0–07-289906-9.

[37] K. R. Rosen, *Elementary Number Theory and its Applications. Third Edition*, (Addison-Wesley, 1993); ISBN 0-201-57889-1.

[38] J. J. Rotman, *An Introduction to the Theory of Groups, 3rd Edition.* Allyn and Bacon, Inc., Boston (1984). ISBN 0–205–07963–6.

[39] M. R. Schroeder, *Number Theory in Science and Communication* . Springer-Verlag, Berlin (1984). ISBN 3–540–12164–1.

[40] W. Sierpiński, *Elementary Theory of Numbers*. Polska Akademia Nauk, Monografie Matematyczne **42**, Warsaw (1964).

[41] W. Sierpiński, *250 Problems in Elementary Number Theory*. American Elsevier Publishing Company, Inc. (New York, 1970); and PWN — Polish Scientific Publishers (Warsaw, 1970). ISBN 444–00071–2.

[42] A. D. Thomas and G. V. Wood, *Group Tables*. Shiva Publishing Limited (1980). ISBN 0-906812-04-6.

[43] I. M. Vinogradov, *Elements of Number Theory*. (Translation of the 5th Revised Russian Edition (1949), by S. Kravetz.) Dover Publications, New York (1954).

[44] B. L. van der Waerden, *A History of Algebra*. Springer-Verlag, Berlin, New York, etc. (1985). ISBN 0–387–13610–X.

[45] J. H. van Lint, *Introduction to Coding Theory*. Springer-Verlag, New York (1982). ISBN 0–387–11284–7.

[46] J. H. M. Wedderburn, *A theorem on finite algebras*. Transactions of the American Mathematical Society **6** (1905), 349–352.

[47] R. D. Carmichael, *Introduction to the theory of groups of finite order*. Dover Publications, Inc. 1956 reprint of original 1937 edition.

[48] *Handbook of Student Rights and Responsibilities*. Located at the following URL (as of March 8th, 2002): http://ww2.mcgill.ca/students-handbook/index.html.

A Notes on Algebra

A.1 Theory of Numbers

A.1.1 Introduction

For computer science students this introduction to number theory serves multiple purposes:

- introduction to a corpus of mathematical techniques having immediate and pervasive applications in the design of computer algorithms and hardware
- motivational preparation for study, later in the course, of the theory of rings and fields; much of ring and field theory was originally investigated in an attempt to generalize and/or delimit phenomena encountered in $\mathbb{Z}$
- technical preparation for study, later in the course, of group, ring, and field theory, where specific number theoretical results may be required in proofs of theorems; as a specific application, the syllabus of this course includes applications of number theory to cryptography

The spirit of the ordering of topics is to introduce results as early as they can be proved with the tools available at that point, even if machinery introduced later will yield simpler proofs; concepts (like the "little Fermat Theorem") that are closely linked to elementary group theory, are mainly deferred to a later chapter.

Accessible introductory sources on number theory are [5], [43], [28].[301]

A.1.2 The number systems

1. **Notational conventions.** We adopt the following notation

$$\begin{array}{rcl} \mathbb{N} & = & \text{the set of } \mathbb{N}\text{atural numbers} \quad {}^{302} \\ \mathbb{Z} & = & \text{the set of integers } (\textit{ganzen } \mathbb{Z}\textit{ahlen}) \\ \mathbb{Q} & = & \text{the set of rationals } (\mathbb{Q}\text{uotients}) \\ \mathbb{R} & = & \text{the set of } \mathbb{R}\text{eal numbers} \\ \mathbb{C} & = & \text{the set of } \mathbb{C}\text{omplex numbers} \end{array}$$

[301] Concerning terminology: the word *elementary*, when used in a number theoretical context, does not necessarily mean *easy*; a proof is usually said to be *elementary* if it does not require the use of complex analysis; but some authors restrict the term *elementary* to that part of the theory that does not require the notion of limit.

[302] There are two schools of thought among mathematicians; some define the *natural numbers* to be only the strictly positive integers; others include 0 as a natural number. In these notes $0 \notin \mathbb{N}$.

In each case we will assume the usual algebraic structures (addition, multiplication, ordering, etc.). Where there is danger of confusion we may subscript an operation or relation symbol to indicate the context; for example, $<_{\mathbb{Z}}$ will denote the usual ordering of the integers.

2. **The "natural" numbers.** This set is denoted by $\mathbb{N}$. Note that we do not consider 0 to be a natural number.

   There are several algebraic "structures" which we normally associate with this set: addition ($+$), multiplication ($\times$ or written by juxtaposition) are both binary *operations*, which map $\mathbb{N}\times\mathbb{N}$ into $\mathbb{N}$; $\leq$, $\geq$, $<$ and $>$ are all binary *relations* defined on $\mathbb{N}$ — the first two are partial orderings (indeed, total orderings), while the last two are antisymmetric and transitive, but are not reflexive. We will not be defining these operations and relations formally at this time.

3. **The integers.** This set is denoted by $\mathbb{Z}$.

   It is obtained from $\mathbb{N}$ by adjoining 0, and by associating with each natural number n two integers, $+n$ and $-n$, with obvious properties; we think of $\mathbb{N}$ as being a subset of $\mathbb{Z}$, under the mapping $n \mapsto +n$; the preceding mapping is called an *embedding* because it is an injection.

   The operations of $+$ and $\times$ defined on $\mathbb{N}$ may be *extended* to be meaningful over the enlarged set. It is also possible to define an "inverse" relation to $+$, subtraction ($-$) with obvious properties. Here 0 acts as the "identity" for addition, in the sense that $x+0 = x = 0+x$ for all $x \in \mathbb{Z}$; and 1 acts as the "identity" for multiplication. But, while there is an inverse for addition (in the sense that there exists, for any $x \in \mathbb{Z}$ an element y such that $x + y = 0 = y + x$ (that element y is precisely $-x$), there is not (except for the elements $x = 1$ and $x = -1$) an inverse for x under the operation of multiplication. Here again, we will make no attempt to formalize these definitions at this time.

4. **The rationals.** This set is denoted by $\mathbb{Q}$. Here we wish to enlarge the set $\mathbb{Z}$ so that multiplication also has an inverse (except for multiplication by 0). The construction may appear, at first, to be complicated. Remember that the construction is not as simple as the transition from natural numbers to integers; and that we have to be able to cope with the situation where the same rational number can be represented in different ways; for example, that $\frac{2}{1}$, $\frac{18}{9}$, and $\frac{-64}{-32}$ are all to be the rational number which is identified with the natural number 2. This construction can be accomplished by beginning with the set $\mathbb{Z}\times\mathbb{Z}$ of ordered pairs of integers, where the first element of the pair represents the numerator, and the second represents the denominator. More precisely, we begin with the set

$$S = \mathbb{Z} \times (\mathbb{Z} - \{0\}),$$

where we exclude the possibility that a denominator may be zero. On this set we will define an equivalence relation; the equivalence classes will become the rational numbers, and we will define an *embedding* of $\mathbb{Z}$ into $\mathbb{Q}$ in such a way that the operations defined on $\mathbb{Z}$ extend to operations on $\mathbb{Q}$ in the way we expect. (This use of an equivalence relation is the usual way in which mathematicians deal with situations where an object admits more than one representation.) Students are not expected to work through all the details at this time, but a brief description of the process is as follows:

(a) Define a binary relation $\sim$ on S, by $(a, b) \sim (c, d)$ iff $ad = bc$.

(b) Prove that $\sim$ is an equivalence relation.

(c) $\mathbb{Q}$ is defined to be the set of equivalence classes, each of which is called a *rational number*.

(d) Embed $\mathbb{Z}$ in $\mathbb{Q}$ by the mapping $x \mapsto (x, 1)$.

(e) Define addition $\oplus$ and multiplication $\odot$ of rationals by $(a, b) \oplus (c, d) = (ad + bc, bd)$, $(a, b) \odot (c, d) = (ac, bd)$.

(f) Show that $\oplus$ and $\odot$, when applied to embedded integers, give the same results as $+$ and $\times$; thus they are *extensions* of the operations defined on the integers. This justifies the use of the same symbols, as there is no danger of confusion: so we now write $+$ and $\times$ (or juxtaposition) instead of $\oplus$ and $\odot$.

(g) The additive identity is not the element $(0, 1)$ that resulted from the embedding of the integer 0; rather, it is the equivalence class of S containing the element $(0, 1)$ (which can be seen to be the set $\{(0, y) : y \in \mathbb{Z} - \{0\}\}$). Define the *multiplicative inverse* of a non-zero element $[(a, b)]$ to be the rational number $[(b, a)]$.

We are unable to define division by 0: that is, there is no way to do this without causing massive breakdown of the properties of the operations we have been defining.

5. **The set of real numbers.** The set $\mathbb{Q}$ can be further enlarged to form the set of *real* numbers, denoted by $\mathbb{R}$. One reason for doing this is to arrange that every monotonely increasing bounded sequence of rational numbers should converge to a limit. For example, the sequence of partial sums of the series $\sum_{n=0}^{\infty} \frac{1}{n!}$ is increasing, yet can be shown to converge to a sum less than 3, which is not a rational number. The set of real numbers "completes" the rationals so that all bounded monotone sequences of rationals converge to a limit in the set. This new construct has the property that it is "closed" under the same operation: all bounded monotone sequences of real numbers can be shown to converge to a real number.

6. **The set of "complex" numbers.** The complex numbers can also be defined in terms of a "completion". Without considering that property at this time, we can simply define a complex number (x, y) to be an ordered pair of real numbers. Thus, until we define a *structure* on $\mathbb{C}$, it is the same as $\mathbb{R} \times \mathbb{R}$. The structure is defined through two operations: addition is simply the usual definition of addition of vectors, wherein $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$; we really should use different symbols for these two additions, until we have proved that addition in $\mathbb{C}$ "extends" addition in $\mathbb{R}$. The definition of multiplication in $\mathbb{C}$ requires motivation that will not be given here at this time; it is $(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$. The embedding of $\mathbb{R}$ in $\mathbb{C}$ is given by $x \mapsto (x, 0)$.

A.1.3 Other notational conventions

For any set $\mathfrak{A}$, we define $\mathfrak{A}^n$ recursively by $\mathfrak{A}^1 = \mathfrak{A}$; $\mathfrak{A}^n = \mathfrak{A}^{n-1} \times \mathfrak{A}$ $(n > 0)$. We will assume that students have already been exposed to such formalities as showing that sets $(\mathfrak{A} \times \mathfrak{B}) \times \mathfrak{C}$ and $\mathfrak{A} \times (\mathfrak{B} \times \mathfrak{C})$ are equivalent, and we may denote elements of either set in such a context by an ordered triple (a, b, c) without internal parentheses.

We normally compose functions *on the left*. That is, given $f : \mathfrak{A} \longrightarrow \mathfrak{B}$, and $g : \mathfrak{B} \longrightarrow \mathfrak{C}$, the composition which acts as $a \longmapsto g(f(a))$ will be denoted by $g \circ f$, or possibly even by gf. With this convention it is usually convenient to denote points in $\mathbb{R}^n$ by a *column* matrix, as $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, so that matrices of linear transformations operate on the *left* of a vector. These conventions will usually coincide with the student's background, and should require no adjustment. We mention them only because the opposite conventions are in use by some algebraists, and may be encountered in some textbooks.

The end of a proof may be indicated by the symbol $\square$.

A.1.4 Divisibility of integers

A.1.4.1 DEFINITION. Let $a, b \in \mathbb{Z}$. We write $a \mid b$, and say that *a divides b*, or *a is a divisor of b*, or *b is a multiple of a* if there exists $c \in \mathbb{Z}$ such that $b = ac$. The negation of $a \mid b$ is written $a \nmid b$.

A.1.4.2 THEOREM. *1. Divisibility is a partial ordering on* $\mathbb{N}$.[303]

2. If a, b, c are integers, then $a \mid b \Longrightarrow a \mid bc$.

[303] We cannot make this claim for $\mathbb{Z}$ since we have, for any a, $a \mid -a$ and $-a \mid a$, so that $\mid$ is not antisymmetric on $\mathbb{Z}$.

3. If a, b, c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (b+c)$.

A.1.4.3 Exercise. Prove Theorem A.1.4.2.

A.1.4.4 Definition. Let m be a *fixed* integer. We write

$$a \equiv b \pmod{m} \tag{301}$$

(read *a is congruent to b modulo m*) if $m \mid (a-b)$. Statement (301) is called a *congruence*; m is the *modulus*[304].

A.1.4.5 Theorem. *1. $\equiv$ is an equivalence relation on $\mathbb{Z}$.*

2. If $a \equiv b \pmod{m}$ and $c \in \mathbb{Z}$, then $ca \equiv cb \pmod{m}$.

3. $\left.\begin{array}{rcll} a & \equiv & b & \pmod{m} \\ c & \equiv & d & \pmod{m} \end{array}\right\}$ *together imply* $\left\{\begin{array}{rcll} a+c & \equiv & b+d & \pmod{m} \\ ac & \equiv & bd & \pmod{m} \end{array}\right.$.

4. Let $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$ be a polynomial with integer coefficients, Then

$$a \equiv b \pmod{m} \quad \Rightarrow \quad f(a) \equiv f(b) \pmod{m}$$

A.1.4.6 Exercise. Prove Theorem A.1.4.5.

Solution:

4. Suppose $a \equiv b \pmod{m}$. Then, by part 3, $a^i \equiv b^i \pmod{m}$, hence, by part 2, $f_i a^i \equiv f_i b^i \pmod{m}$, $(i = 0, 1, 2, ..., n)$; summing these congruences yields the desired congruence.

A.1.4.7 Definition. The equivalence classes under congruence *modulo m* are called *residue classes*. The residue class containing a may be denoted by $[a]_m$, or briefly by $[a]$.

A.1.5 The Division "Algorithm". Bases of Notation.

Let a and b be integers, $b > 0$. Then there exist integers q (the *quotient*) and r (the *remainder*) such that

$$\begin{array}{c} a = q \cdot b + r \\ 0 \le r \le b - 1 \end{array} \tag{302}$$

[304]The plural is *modulī*. Thus *modulō* is Latin for *to the modulus*.

In some algebraic contexts this theorem is called the *Division algorithm*[305] [306].

Suppose that a and b are positive integers. We may apply (302), to obtain

$$a = q_1 \cdot b + r_0 \,,$$

and repeat the process,

$$q_1 = q_2 \cdot b + r_1 \,,$$

$$q_2 = q_3 \cdot b + r_2 \,,$$

progressively reducing the quotient, until ultimately we obtain

$$q_k = q_{k+1} \cdot b + r_k$$

where $q_{k+1} = 0$. Thus a admits a decomposition in the form

$$a = r_k b^k + r_{k-1} b^{k-1} + ... + r_1 b + r_0 \,,$$

which may be denoted briefly by

$$a = (r_k r_{k-1} ... r_1 r_0)_b$$

and designated as *the b-ary expansion of a*; the 10-ary expansion is the familiar *decimal* expansion; 2-ary, 3-ary, 8-ary, 12-ary, 16-ary expansions are known as *binary*, *ternary*, *octal*, *duodecimal*, and *hexadecimal* expansions, respectively. We call b the *radix* or *base* of the expansion.

Where no parentheses or subscripted radix are shown, a representation of an integer is to be understood to be in decimal notation.

A.1.5.1 Exercise. Show that, for fixed integers a and b, $(b \neq 0)$, integers q and r satisfying (301) are unique.

[305] This terminology derives from the analogous statement to (302) which holds for *polynomials*. One can describe an algorithm for determining, for two given polynomials $a(x)$ and $b(x)$, polynomials $q(x)$ and $r(x)$, where $r(x)$ has degree less than the degree of $b(x)$, such that $a(x) = q(x) \cdot b(x) + r(x)$. When, in a later section, we introduce the concept of a *ring* we may define a *Euclidean ring* to be a *ring* $\mathcal{R}$ for which there is defined a function $d : \mathcal{R} - \{0\} \longrightarrow \mathbb{N}$ such that

1. $\mathcal{R}$ is an integral domain
2. $d(a) \leq d(ab)$ $\forall a, b \in \mathcal{R}$, not both zero
3. For nonzero $a, b \in \mathcal{R}$, there exist $q, r \in \mathcal{R}$ such that $a = q \cdot b + r$, where $r = 0$ or $d(r) \leq d(b) - 1$.

[306] A proof of the division algorithm would have to be based on the axiomatic construction of $\mathbb{Z}$. One approach would be to consider the non-empty set $\{a - q \cdot b : q \in \mathbb{Z}\}$ and to define r to be the smallest non-negative element.

Solution: If $q_1 \cdot b + r_1 = a = q_2 \cdot b + r_2$ for $0 \le r_1 \le b-1$, $0 \le r_2 \le b-1$, $r_1 \ge r_2$, then $0 \le r_1 - r_2 = (q_2 - q_1) \cdot b$; the only nonnegative multiple of b less than b is 0, so $q_1 = q_2$, implying that $r_1 = r_2$.

A.1.5.2 EXERCISE. 1. Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 2 iff a_0 is divisible by 2.

2. Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 4 iff $10a_1 + a_0$ is divisible by 4.

3. Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 8 iff $100a_2 + 10a_1 + a_0$ is divisible by 8.

4. Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 3 iff $a_k + a_{k-1} + ... + a_1 + a_0$ is divisible by 3.

5. ("Casting out nines") Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 9 iff $a_k + a_{k-1} + ... + a_1 + a_0$ is divisible by 9.

6. Prove that any integer $a = (a_k a_{k-1} ... a_1 a_0)_{10}$ is divisible by 11 iff $(a_0 + a_2 + a_4 + ... + a_{2k} + ...) - (a_1 + a_3 + ... + a_{2k+1} + ...)$ is divisible by 11.

Solution:

1. $a = \sum_{i=0}^{k} a_i 10^i \equiv a_0 + \sum_{i=1}^{k} a_i 0^i \pmod 2$.

2. Since $10^i \equiv 0 \pmod 4$ for $i > 1$,

$$a = \sum_{i=0}^{k} a_i 10^i \equiv a_0 + 10a_1 + \sum_{i=2}^{k} a_i 0^i \pmod 2$$

3. Since $10^i \equiv 0 \pmod 8$ for $i > 2$,

$$a = \sum_{i=0}^{k} a_i 10^i \equiv a_0 + 10a_1 + 100a_2 + \sum_{i=3}^{k} a_i 0^i \pmod 2$$

4. Since $10 \equiv 1 \pmod 3$, $10^i \equiv 1 \pmod 3$ for all i, so

$$a = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i 1^i \pmod 3$$

5. Since $10 \equiv 1 \pmod 9$, $10^i \equiv 1 \pmod 9$ for all i, so

$$a = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i 1^i \pmod 9$$

6. Since $10 \equiv -1 \pmod{11}$, $10^i \equiv (-1)^i \pmod{11}$, so

$$a = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i (-1)^i \pmod{11}$$

A.1.5.3 EXERCISE. Show that the number of digits in the b-ary expansion of a positive integer a is

$$\lfloor \log_b a \rfloor + 1\,, \quad \text{i.e.} \quad \left\lfloor \frac{\log a}{\log b} \right\rfloor + 1\,;$$

(in the latter ratio these logarithms may be taken to base e, or to any other convenient base.)

Solution: Suppose that $a = (r_k r_{k-1} ... r_1 r_0)_b$, where $r_k > 0$. Then

$$\begin{aligned} a &= r_k b^k + r_{k-1} b^{k-1} + \ldots + r_1 b^1 + r_0 b^0 \\ &< r_k b^k + b^k \\ &\leq (b-1) b^k + b^k = b^{k+1} \end{aligned}$$

so $b^k \leq a < b^{k+1}$. Taking logarithms to base b gives $k \leq \log_b a < k+1$; hence[307] $\lfloor \log_b a \rfloor = k$, one less than the number of digits.

A.1.5.4 EXERCISE. 1. Multiply $(23420)_8$ by $(11610)_8$, working within the 8-ary (*octal*) system.

2. Divide 1000 by 35, working within the 3-ary system.

3. Express $(1.2)_{10}$ in binary notation.

Solution:

[307] The logarithm, being a monotonely increasing function, preserves inequalities.

1.

$$\begin{array}{ccccccccc}
 & & & & 2 & 3 & 4 & 2 & 0 \\
 & & & & 1 & 1 & 6 & 1 & 0 \\
\hline
 & & & & 0 & 0 & 0 & 0 & 0 \\
 & & & 2 & 3 & 4 & 2 & 0 & \\
 & 1 & 6 & 5 & 1 & 4 & & & \\
 & 2 & 3 & 4 & 2 & & & & \\
2 & 3 & 4 & 2 & & & & & \\
\hline
2 & 7 & 6 & 5 & 7 & 0 & 2 & 0 & 0
\end{array}$$

To verify, observe that $(23420)_8 = 2 \cdot 8 + 4 \cdot 64 + 3 \cdot 512 + 2 \cdot 4096 = (10000)_{10}$; that, similarly, $(11610)_8 = 5000$; and that $(276570200)_8 = (500000000)_{10}$.

2.

$$\begin{array}{rcl}
1000 & = & 333 \cdot 3 + 1 \\
333 & = & 111 \cdot 3 + 0 \\
111 & = & 37 \cdot 3 + 0 \\
37 & = & 12 \cdot 3 + 1 \\
12 & = & 4 \cdot 3 + 0 \\
4 & = & 1 \cdot 3 + 1 \\
1 & = & 0 \cdot 3 + 1
\end{array} \quad \Rightarrow 1000 = (1101001)_3$$

$$\begin{array}{rcl}
35 & = & 11 \cdot 3 + 2 \\
11 & = & 3 \cdot 3 + 2 \\
3 & = & 1 \cdot 3 + 0 \\
1 & = & 0 \cdot 3 + 1
\end{array} \quad \Rightarrow 35 = (1022)_3$$

$$\begin{array}{cccc|cccccc}
 & & & & & & 1 & 0 & 0 & 1 \\
\cline{5-10}
1 & 0 & 2 & 2 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
 & & & & 1 & 0 & 2 & 2 & & & \\
\cline{5-8}
 & & & & & & 2 & 0 & 0 & 1 \\
 & & & & & & 1 & 0 & 2 & 2 \\
\cline{7-10}
 & & & & & & & 2 & 0 & 2
\end{array}$$

where $(202)_3 = 20$.

3. We have to deal with the integer and fractional parts separately. The integer part is trivial, as $(1)_{10} = 1 = (1)_2$. Suppose that

$$0.2 = \frac{a_1}{2^1} + \frac{a_2}{2^2} + \frac{a_3}{2^3} + \ldots + \frac{a_i}{2^i} + \ldots \tag{303}$$

The binary digits a_1, a_2, ..., can be determined by multiplying (303) by the radix — here 2 — and taking the integer part (floor) of both sides, subtracting the integer

part from both sides and repeating the process until either the remainder is finally zero or a periodicity is detected. We have

$$\begin{aligned}
0.4 &= a_1 + \frac{a_2}{2^1} + \frac{a_3}{2^2} + \frac{a_4}{2^3} + \ldots + \frac{a_i}{2^{i-1}} + \ldots \\
&\Rightarrow a_1 = \lfloor 0.4 \rfloor = 0 \\
0.8 &= a_2 + \frac{a_3}{2^1} + \frac{a_4}{2^2} + \frac{a_5}{2^3} + \ldots + \frac{a_i}{2^{i-2}} + \ldots \\
&\Rightarrow a_2 = \lfloor 0.8 \rfloor = 0 \\
1.6 &= a_3 + \frac{a_4}{2^1} + \frac{a_5}{2^2} + \frac{a_6}{2^3} + \ldots + \frac{a_i}{2^{i-3}} + \ldots \\
&\Rightarrow a_3 = \lfloor 1.6 \rfloor = 1 \\
1.2 &= a_4 + \frac{a_5}{2^1} + \frac{a_6}{2^2} + \frac{a_7}{2^3} + \ldots + \frac{a_i}{2^{i-4}} + \ldots \\
&\Rightarrow a_4 = \lfloor 1.2 \rfloor = 1 \\
0.4 &= a_5 + \frac{a_6}{2^1} + \frac{a_7}{2^2} + \frac{a_8}{2^3} + \ldots + \frac{a_i}{2^{i-5}} + \ldots \\
&\Rightarrow a_5 = \lfloor 0.4 \rfloor = 0 \\
0.8 &= a_6 + \frac{a_7}{2^1} + \frac{a_8}{2^2} + \frac{a_9}{2^3} + \ldots + \frac{a_i}{2^{i-6}} + \ldots \\
&\Rightarrow a_6 = \lfloor 0.8 \rfloor = 0 \quad \text{etc.}
\end{aligned}$$

We have shown that

$$\begin{aligned}
0.2 &= \left(\frac{0}{2^1} + \frac{0}{2^2} + \frac{1}{2^3} + \frac{1}{2^4}\right)\left(1 + \frac{1}{2^4} + \frac{1}{2^8} + \frac{1}{2^{12}} + \ldots\right) \\
&= (0.0011001100110011...)_2 \,,
\end{aligned}$$

which is a repeating binary expansion; thus $(1.2)_{10} = (1.0011001100110011...)_2$. We can verify the validity of these computations by observing that $\frac{0}{2^1}+\frac{0}{2^2}+\frac{1}{2^3}+\frac{1}{2^4} = \frac{3}{16}$, while $1 + \frac{1}{2^4} + \frac{1}{2^8} + \frac{1}{2^12} + \ldots = \frac{\frac{3}{16}}{1-\frac{1}{16}} = \frac{3}{15} = \frac{1}{5} = 0.2$. A faster solution to this problem could have been achieved by converting first to the *hexadecimal* scale.

$$\begin{aligned}
0.2 &= \frac{a_1}{16^1} + \frac{a_2}{16^2} + \frac{a_3}{16^3} + + \ldots + \frac{a_i}{16^i} + \ldots \\
\Rightarrow 3.2 &= a_1 + \frac{a_2}{16^1} + \frac{a_3}{16^2} + + \ldots + \frac{a_i}{16^{i-1}} + \ldots \\
&\Rightarrow a_1 = \lfloor 3.2 \rfloor = 3 \\
\Rightarrow 0.2 &= \frac{a_2}{16^1} + \frac{a_3}{16^2} + \frac{a_4}{16^2} + + \ldots + \frac{a_i}{16^{i-2}} + \ldots \\
&\Rightarrow 3 = a_2 = a_3 = a_4 = \ldots
\end{aligned}$$

So $(1.2)_{10} = (1.333333...)_{16}$, which is no surprise, since $(1.333333...)_{16} = 1 + \frac{\frac{3}{16}}{1-\frac{1}{16}} =$

$1 + \frac{3}{15}$, and each of the hexadecimal digits 3 corresponds to a string of 4 binary digits 0011.

A.1.6 Greatest Common Divisor

If a and b are integers, not both zero, there will be only a finite number of positive integers which simultaneously divide both of them. Thus the set

$$\{c \in \mathbb{N} : c \mid a \text{ and } c \mid b\} \tag{304}$$

is finite and non-empty (since it contains 1). Moreover, it is partially ordered by the relation $|$.

A.1.6.1 DEFINITION. Let a, b be integers, not both zero. It is easily proved by induction or otherwise [13, §2.7.3, Theorem 3(a)] that there will exist a unique $|$-*maximal* element in (304), i.e. a positive integer n such that

$$\left.\begin{array}{l} m \mid a \\ m \mid b \end{array}\right\} \Rightarrow \begin{array}{l} n \mid a \\ n \mid b \end{array} \quad \Rightarrow \quad m \mid n \tag{305}$$

This maximal element is called the *greatest common divisor* of a and b and may be denoted by g.c.d.(a, b), or simply (a, b) (not to be confused with the notation for points in $\mathbb{Z}^2$.)

A.1.6.2 EXERCISE. As in much of the terminology of mathematics, the actual English words used in a term should not be assumed apriori to carry any particular meaning. While we have proved that the greatest common divisor is indeed a *common divisor* of the two given integers, is it the *greatest*? Indeed it is: prove that

$$\left.\begin{array}{l} m \in \mathbb{N} \\ m \mid a \\ m \mid b \end{array}\right\} \Rightarrow m \leq (a, b)$$

Solution: By (305), $m \mid (a, b)$, i.e. there exists an integer $k > 0$ such that $(a, b) = km \geq m$.

A.1.6.3 EXERCISE. Show that, for any non-zero integer a, $(a, 0) = (0, a) = |a|$.

The following algorithm appears in Euclid's Elements [10, Book VII, Proposition 2].

A.1.6.4 THEOREM (EUCLIDEAN ALGORITHM). *Let a and b be integers, $b > 0$. First, divide b into a:*

$$a = q_0 \cdot b + r_0 \qquad (0 \leq r_0 \leq b - 1)$$

Then divide r_0 into b:

$$b = q_1 \cdot r_0 + r_1 \qquad (0 \leq r_1 \leq r_0 - 1)$$

and repeat the process

$$\begin{aligned} r_0 &= q_2 \cdot r_1 + r_2 \qquad (0 \leq r_2 \leq r_1 - 1) \\ &\cdots \\ r_{k-1} &= q_{k+1} \cdot r_k \end{aligned}$$

until the remainder is zero. (As the remainders are strictly decreasing, the algorithm terminates.) Then the last non-zero remainder, i.e. r_k, is the g.c.d.

Proof: To see this we work upwards through the equations. From the last equation, $r_k \mid r_{k-1}$; in the preceding equation r_k divides both summands on the right side, so, by Theorem A.1.4.2, r_k divides the left member, viz. r_{k-2}. Proceeding upwards we find, by induction, that $r_k \mid b$ and $r_k \mid a$ — i.e. that r_k is a *common* divisor of a and b. Then, proceeding *downwards* through the equations, we can argue that if $m \mid a$ and $m \mid b$, then $m \mid r_0$, hence m divides $b - q_1 \cdot r_0 = r_1$, ..., and finally m divides r_k. Thus the *Euclidean algorithm* yields the greatest common divisor in its penultimate step. □

Working upwards from the penultimate equation we can actually express $r_k = (a, b)$ as a linear combination of a and b; that is, we can compute integers k and ℓ such that

$$(a, b) = ka + \ell b \tag{306}$$

This *essentially* proves the following theorem.

A.1.6.5 THEOREM. *For integers a and b, not both zero, there exist integers k and ℓ such that (306) holds.*

Proof: The argument provided above applies to the first of the following cases. We shall show how the proof can be broken down into three cases, of which the second may be trivially derived from the first.

1. Case 1: $b > 0$.
2. Case 2: $b < 0$. Case 1 applied with $b := -b$ yields k' and ℓ' such that $(a, -b) = k'a + \ell'(-b)$, so[308]
$$(a, b) = (a, -b) = k'a + (-\ell')b$$
and we may take $k = k'$, $\ell = -\ell'$.

[308] The property $(a, b) = (a, -b)$ is to be proved in Exercise A.1.6.8.1 below.

3. Case 3: $b = 0$, $a \neq 0$. By Exercise A.1.6.3, $(a, b) = |a|$. We may take $k = \frac{a}{|a|}$, $\ell = 0$.

□

There exist more elegant methods for determining k and ℓ. Students may be interested in the following elegant extension of the Euclidean algorithm, in which k and ℓ (here called x and y) are output at the same time as (a, b), with minimal use of storage. [22, p. 14]:

> "EXTENDED EUCLID'S ALGORITHM. *Given two positive integers a and b, we compute (a, b) and two integers x and y such that $ax + by = (a, b)$.*
>
> **"Initialize.** *Set $x' \leftarrow y \leftarrow 1$, $x \leftarrow y' \leftarrow 0$, $c \leftarrow a$, $d \leftarrow b$.*
>
> **"Divide.** *Let q, r be the quotient and remainder, respectively, of c divided by d. (We have $c = qd + r$, $0 \leq r < d$.)*
>
> **"Remainder zero?** *If $r = 0$, the algorithm terminates; we have in this case $ax + by = d = (a, b)$ as desired.*
>
> **"Recycle.** *Set $c \leftarrow d$, $d \leftarrow r$, $t \leftarrow x'$, $x' \leftarrow x$, $x \leftarrow t - qx$, $t \leftarrow y'$, $y' \leftarrow y$, $y \leftarrow t - qy$, and go back to [Divide]."*

A.1.6.6 EXERCISE. In discussing the remainders, it is convenient to define $r_{-1} = b$, $r_{-2} = a$, so that

$$r_{i-2} = q_i r_{i-1} + r_i \quad (0 \leq i \leq k) \tag{307}$$

We can prove bounds for the remainders r_i:

1. Prove that $r_i < \frac{1}{2} r_{i-2}$ $(i = 2, 3, ..., k)$.

2. Let F_i denote the ith Fibonacci number, defined by $F_0 = F_1 = 1$, $F_{i+2} = F_{i+1} + F_i$ $(i \geq 0)$. Prove that

$$r_i \geq F_{k-i} \tag{308}$$

for $(-2 \leq i \leq k)$.

Solution:

1. [24, p. 13] If $r_{i-1} \leq \frac{1}{2} r_{i-2}$, then $r_i < r_{i-1} \leq \frac{1}{2} r_{i-2}$, Otherwise it follows from $r_{i-1} > \frac{1}{2} r_{i-2}$ that $q_{i+1} = 1$, $r_i = r_{i-2} - r_{i-1} < r_{i-2} - \frac{1}{2} r_{i-2}$.

2. Since r_k and r_{k-1} are positive integers, $r_k \geq 1 = F_0$ and $r_{k-1} \geq 1 = F_1$. Suppose (308) is true for $i = k, k-1, \ldots, j$. Then

$$\begin{aligned} r_{j-1} &= q_{j+1} r_j + r_{j+1} \\ &\geq q_{j+1} F_{k-j} + F_{k-j-1} \quad \text{by the induction hypothesis} \\ &\geq F_{k-j} + F_{k-j-1} = F_{k-(j-1)} \end{aligned}$$

so, by induction, (308) holds for $-2 \leq i \leq k$. From the case $a = r_{-2} \geq F_{k+2}$, and known estimates for the Fibonacci numbers, one can determine a bound for k.

A.1.6.7 DEFINITION. When $(a, b) = 1$ we say that a and b are *relatively prime*.

A.1.6.8 EXERCISE. 1. Prove that for any nonzero integers a, b, c,

$$(a, b) = (b, a) = (|a|, |b|) = (a - b, b)\,,$$
$$(ac, bc) = (a, b)c\,.$$

2. Prove the validity of the following algorithm, due to Josef Stein (1967). This algorithm, "is extremely fast, especially in machine language" [2, pp. 11–12] and may be more efficient than the Euclidean algorithm, provided that one is not interested in expressing the g.c.d. as a linear combination. For *positive* integers a and b, it proceeds by progressively reducing the larger of a and b in the computation of (a, b), after factoring out the maximum power of 2.

   (a) If $a = b$, $(a, b) = a$.
   (b) If a and b are both even, $(a, b) = 2\left(\frac{a}{2}, \frac{b}{2}\right)$.
   (c) If just one — say b — is even, $(a, b) = \left(a, \frac{b}{2}\right)$.
   (d) If neither a nor b is even, and $a > b$, $(a, b) = (a - b, b)$.

3. You are given $n + 1$ distinct integers in the set $\{1, 2, ..., 2n - 1, 2n\}$. Show that among them are two that are pairwise coprime.

4. Let a and b be any non-negative integers. Then
$$\left(2^a - 1, 2^b - 1\right) = 2^{(a,b)} - 1$$

5. Apply the Euclidean algorithm and the Stein algorithm to determine the greatest common divisor of 43732 and 15863.

6. Apply the Euclidean algorithm to determine an integer a such that $2 \cdot a \equiv 1 \pmod 9$. Could the same algorithm be used to determine an integer b such that $3 \cdot b \equiv 1 \pmod 9$?

Solution:

1.

2.

3. Let the given integers be arranged in increasing order: $1 \leq x_1 < x_2 < ... < x_{n+1} \leq 2n$. Consider the differences $y_i = x_{i+1} - x_i$ $(i = 1, 2, ..., n)$. These n differences sum to $x_{n+1} - 1 \leq 2n - 1$. As their average value is less than 2, at least one of them[309]

[309] by the "Pigeonhole Principle"

must assume a positive integer value less than 2, i.e. must equal 1. Thus there will be 2 consecutive integers, say m, $m+1$. But $(m, m+1) = (m, 1) = 1$ for all m.

This result is "best possible, in the sense that it fails for a subset of n points: take the even integers.

4. Suppose that $a = q_0 \cdot b + r_0$, $a \geq b$. Then $(2^a - 1, 2^b - 1) = (2^a - 2^b, 2^b - 1) = (2^b(2^{a-b} - 1), 2^b - 1) = (2^{a-b} - 1, 2^b - 1) = ... = (2^{r_0} - 1, 2^b - 1)$. We see, using the notation of Theorem A.1.6.4, that ultimately $(2^a - 1, 2^b - 1) = (2^{r_k} - 1, 2^{r_{k-1}} - 1) = (2^{r_k} - 1, 0) = (2^{(a,b)} - 1, 0) = 2^{(a,b)} - 1$.

5.

6.

A.1.6.9 LEMMA. *1. If $d = k \cdot a + \ell \cdot b$, then $(a, b) \mid d$. In particular, if $1 = k \cdot a + \ell \cdot b$, then $(a, b) = 1$.*

2. Let a and b be non-zero integers. Then

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1 \, .$$

3. (cf. Theorem A.1.4.2, part 2.) Let a, b d be non-zero integers such that $(d, a) = 1$ and $d \mid ab$. Then $d \mid b$.

4. Suppose that a, b, k, ℓ satisfy (306) and that

$$(a, b) = k'a + \ell' b \, . \tag{309}$$

Then there exists an integer t such that

$$k' = k + t\frac{b}{(a,b)} \tag{310}$$

$$\ell' = \ell - t\frac{a}{(a,b)} \tag{311}$$

Conversely, for any integer t, k', ℓ' satisfying (310), (311) will be a solution of (306).

Proof:

1. Any common divisor of k and ℓ must divide any linear combination of k and ℓ.

2. Dividing a, b, and (a,b) by (a,b) in (306), we obtain
$$1 = k\frac{a}{(a,b)} + \ell\frac{b}{(a,b)}\,.$$

3. Since $(d,a) = 1$, there exist integers k and ℓ such that $(d,a) = 1 = kd + \ell a$; since $d \mid ab$, d divides the sum $d(kb) + \ell(ab)$, i.e. $d \mid b$.

4. From (309) and (306) it follows that
$$(k-k')\frac{a}{(a,b)} = -(\ell-\ell')\frac{b}{(a,b)}\,.$$
By part 2, $\frac{a}{(a,b)} \,\Big|\, (-\ell+\ell')$, hence there exists an integer t such that $k' = k + t\frac{b}{(a,b)}$, $\ell' = \ell - t\frac{a}{(a,b)}$, etc.

□

A.1.6.10 Definition. The *least common multiple* of two non-zero integers a, b, is defined as the unique $|$-minimal element in the set
$$\{c \in \mathbb{N} : a \mid c \text{ and } b \mid c\}\,, \tag{312}$$
It may be denoted by l.c.m.(a,b), or by $[a,b]$.

The remaining exercises in this subsection may be proved using the machinery already provided. However, as can be seen, proofs tend to be surprisingly cumbersome. Students are advised to return to these results after reading §A.1.8 to write short proofs based on the Fundamental Theorem of Arithmetic. The reluctance of mathematicians to use stronger tools than are required is due not only to efforts to demonstrate virtuosity (not unlike the 19th century concert violinist that would intentionally break a high string on his violin before playing a showpiece); a result that can be proved with fewer tools may admit generalization to a broader class. In the present case, the following results will hold even in number fields where the Fundamental Theorem fails to hold.

A.1.6.11 Exercise. (cf. Exercise A.1.6.2) Prove that $[a,b]$ is indeed the *least* common multiple of a and b; i.e. that
$$\left.\begin{array}{c} m \in \mathbb{N} \\ a \mid m \\ b \mid m \end{array}\right\} \Rightarrow [a,b] \leq m$$

A.1.6.12 Lemma. *If $a_1 \mid b$ and $a_2 \mid b$, then $[a_1,a_2] \mid b$.*

Proof: The hypotheses imply that b is a common multiple of a_1 and a_2, i.e. an element of set (312). Dividing $[m_1, m_2]$ into b yields $b = q[m_1, m_2] + r$, where $0 \leq r \leq [m_1, m_2] - 1$. Both m_1 and m_2 divide 2 terms of this equation, so they both divide r; i.e. r is also a nonnegative common multiple, and is strictly less than $[m_1, m_2]$. It follows that $r = 0$, i.e. that $[m_1, m_2] \mid b$. $\square$

A.1.6.13 Exercise. Prove that for any nonzero integers a, b, c,

$$[a, b] = [b, a] = [|a|, |b|]\,,$$

$$[ac, bc] = [a, b]c\,.$$

But show that it is not true in general that $[a, b] = [a - b, b]$ (cf. Exercise A.1.6.8).

Solution: (part) Since $c \mid ac$ and $c \mid bc$, $c \mid [ac, bc]$; let $c = \frac{[ac,bc]}{d}$.

$$ac \mid [ac, bc] \Leftrightarrow ac \mid cd \Rightarrow a \mid d$$

$$bc \mid [ac, bc] \Leftrightarrow bc \mid cd \Rightarrow b \mid d$$

It follows that $[a, b] \mid d$.

But

$$a \mid [a, b] \Rightarrow ac \mid [a, b]c$$

$$b \mid [a, b] \Rightarrow bc \mid [a, b]c$$

Hence $[ac, bc] \mid [a, b]c$, i.e. $dc \mid [a, b]c$, hence $d \mid [a, b]$. By the antisymmetry of $\mid$ on $\mathbb{N}$, $d = [a, b]$, i.e. $[ac, bc] = [a, b]c$.

A.1.6.14 Exercise. For positive integers a, and b, prove that $ab = (a, b)[a, b]$.

Solution: First let us consider the special case where $(a, b) = 1$. Since $a \mid [a, b]$, there exists an integer d such that $[a, b] = ad$. But $b \mid [a, b]$; since $(b, a) = 1$, we conclude by Lemma A.1.6.9 that $b \mid d$; thus $ab \mid [a, b]$. But ab is a common multiple of a and b, so it must be divisible by $[a, b]$. Two positive integers which divide each other must coincide.

We consider the general case now.

$$\left\{ \begin{array}{l} (a, b) \mid b \\ (a, b) \mid a \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} a(a, b) \mid ab \\ b(a, b) \mid ab \end{array} \right\} \Rightarrow [(a, b)a, (a, b)b] \mid ab \Leftrightarrow (a, b)[a, b] \mid ab\,.$$

Conversely, by Lemma A.1.6.9, $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. Hence $\left[\frac{a}{(a,b)}, \frac{b}{(a,b)}\right] = \frac{a}{(a,b)}\frac{b}{(a,b)}$. By Exercise A.1.6.13,

$$(a, b)[a, b] = (a, b)^2 \left[\frac{a}{(a, b)}, \frac{b}{(a, b)}\right] = (a, b)^2 \frac{a}{(a, b)}\frac{b}{(a, b)} = ab$$

A.1.7 Algebraic operations on sets of integers

We will find it useful to extend the binary operations of addition and multiplication, hitherto defined for pairs of integers, to pairs of *sets* of integers. For this purpose we shall begin by *temporarily* introducing new symbols, $\boxplus$ and $\boxdot$ to represent addition and multiplication.

A.1.7.1 DEFINITION. Let $\mathfrak{A} \subseteq \mathbb{Z}$ and $\mathfrak{B} \subseteq \mathbb{Z}$. We define[310]

$$\begin{aligned} \mathfrak{A} \boxplus \mathfrak{B} &= \{a + b : a \in \mathfrak{A},\, b \in \mathfrak{B}\} \\ \mathfrak{A} \boxdot \mathfrak{B} &= \{ab : a \in \mathfrak{A},\, b \in \mathfrak{B}\} \end{aligned}$$

Where either of these sets consists of a single integer we may suppress braces, writing, for example, $a \boxplus \mathfrak{B}$ for $\{a\} \boxplus \mathfrak{B}$ and $a \boxdot \mathfrak{B}$ for $\{a\} \boxdot \mathfrak{B}$.

Basic properties of these operations are established in the following exercise.

A.1.7.2 EXERCISE. 1. Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ be sets of integers. Prove that

(a) $(\mathfrak{A} \boxplus \mathfrak{B}) \boxplus \mathfrak{C} = \mathfrak{A} \boxplus (\mathfrak{B} \boxplus \mathfrak{C})$

(b) $(\mathfrak{A} \boxdot \mathfrak{B}) \boxdot \mathfrak{C} = \mathfrak{A} \boxdot (\mathfrak{B} \boxdot \mathfrak{C})$

(c) $\mathfrak{A} \boxplus \mathfrak{B} = \mathfrak{B} \boxplus \mathfrak{A}$

(d) $\mathfrak{A} \boxdot \mathfrak{B} = \mathfrak{B} \boxdot \mathfrak{A}$

(e) $\mathfrak{A} \boxplus \varnothing = \mathfrak{A}$

(f) $\mathfrak{A} \boxdot \varnothing = \varnothing$

(g) $\mathfrak{A} \boxdot 0 = \begin{cases} 0 & \mathfrak{A} \neq \varnothing \\ \varnothing & \mathfrak{A} = \varnothing \end{cases}$

(h) $\mathfrak{A} \boxdot 1 = \mathfrak{A}$

(i) For integers m and n, $m \boxplus n = m + n$, $m \boxdot n = m \cdot n$.

(j) For any integer m,

$$m \boxdot (\mathfrak{A} \boxplus \mathfrak{B}) = (m \boxdot \mathfrak{A}) \boxplus (m \boxdot \mathfrak{B})$$

2. Prove by counterexample that the distributive law does not hold in general: exhibit sets $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ such that $\mathfrak{A} \boxdot (\mathfrak{B} \boxplus \mathfrak{C}) \neq (\mathfrak{A} \boxdot \mathfrak{B}) \boxplus (\mathfrak{A} \boxdot \mathfrak{C})$.

[310] Once we have established that these operations have properties sufficiently similar to addition and multiplication in $\mathbb{Z}$, we shall replace $\boxplus$ by $+$, and write $\mathfrak{A} + \mathfrak{B}$ in place of $\mathfrak{A} \boxplus \mathfrak{B}$; and replace $\boxdot$ by either $\cdot$, writing $\mathfrak{A} \cdot \mathfrak{B}$ for $\mathfrak{A} \boxdot \mathfrak{B}$, or even suppress the operation symbol entirely, writing multiplication by juxtaposition, as $\mathfrak{A}B$.

Solution:

1.

2.

□

The only application we will make of ⊡ will be where one of the factors is a set consiting of a single integer. For such applications there is no harm in now suppressing the symbol and writing the operation by juxtaposition: it has the properties we normally associate with multiplication. In the same way, we will simply write + where we wish to consider the set of all sums of elements of two sets; this again we have shown to be without risk.

A.1.7.3 Definition. Let $m \in \mathbb{Z}$. We define

$$(m) = m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$$

i.e., $m\mathbb{Z}$ consists of all multiples of m. We call[311] (m) the *ideal generated by* m; it may also be called a *modul* or *module*.[312]

We have shown in (306) that the greatest common divisor of two integers a and b is expressible as a linear combination of a and b. It follows that all multiples of (a, b) are also expressible as such linear combinations.

A.1.7.4 Theorem. *Let a and b be integers, not both zero. Then*

$$\begin{aligned}(a,b)\mathbb{Z} &= \{k \cdot a + \ell \cdot b : k \in \mathbb{Z}, \ell \in \mathbb{Z}\} \\ &= a\mathbb{Z} + b\mathbb{Z} \\ ((a,b)) &= (a) + (b)\end{aligned}$$

Proof: By (306), $(a, b) \in (a) + (b)$. Conversely, since (a, b) is a common divisor of a and b, it divides all sums $ka + \ell b$. □

A.1.7.5 Definition. 1. The *cosets* of an ideal (m) in $\mathbb{Z}$ are defined to be the sets $a + (m)$, defined by Definition A.1.7.1 to be

$$a + (m) = \{a + mn : n \in \mathbb{Z}\}$$

as a ranges over all integers.

[311] This adds one more use that we will make of round parentheses. Some uses will be distinguishable by commas and other separators inside the parentheses. But the reader will often have to face ambiguities that can only be resolved from the context. The present notation for "principal ideals" is a time-honoured one.

[312] Students are, however, discouraged from using the term *module*, as this word now usually has a more general sense.

2. Any element of a coset may be chosen as the *representative* of that coset; when we write $a + (m)$ we are taking a to be that representative.

3. A set containing exactly one representative from each coset of (m) in $\mathbb{Z}$ is called a *complete system of representatives modulo* m.[313].

A.1.7.6 THEOREM. *Let m be a fixed non-zero integer.*

1. *For all integers a and m, $a + (m) = [a]_m$.*[314]

2. *No two of the integers 0, 1, ..., $m - 1$ can be contained in the same coset.*

3. *Every complete system of representatives modulo m contains one integer congruent to each of 0, 1, ..., $m - 1$.*

4. *$\{0, 1, ..., m - 1\}$ is a complete system of representatives modulo m.*

Proof: □

By Theorem A.1.4.5 sums and products of cosets are full cosets. More precisely, we have the following theorem:

A.1.7.7 COROLLARY (TO THEOREM A.1.4.5). *Let a, b, m be integers, $m \neq 0$. Then*

$$a + (m) \ + \ b + (m) \ = \ a + b + (m) \tag{313}$$

$$a + (m) \ \cdot \ b + (m) \ \subseteq \ ab + (m) \tag{314}$$

Proof[315]: We first observe, as a special case of (313), that $(m) + (m) = (m)$. The first property then follows from the associativity and commutativity of addition of subsets, proved in Exercise (A.1.7.2): $a + (m) + b + (m) = a + b + (m) + (m) = a + b + (m)$.

[313] More generally, if we are considering a family $\mathcal{F}$ of subsets of a set $\mathfrak{A}$, a complete system of representatives is a function $r : \mathcal{F} \to \mathfrak{A}$ that associates each of the subsets with one of its elements, i.e. such that $(\forall F \in \mathcal{F})[r(F) \in \mathcal{F}]$. In the present context the subsets under consideration are disjoint, as they constitute a partition of $\mathfrak{A}$; hence the representatives of the subsets must be distinct. A famous theorem of Philip Hall [16] characterizes families of subsets $\mathcal{F}$ such that the representatives will be distinct: it is both necessary and sufficient that, for any k subsets of $\mathcal{F}$ the union contain at least k elements. A short proof can be found in [17].

[314] $[a]_m$ was defined in Definition A.1.4.7.

[315] In (313) and (314) we should have included parentheses to indicate the order of operations, writing

$$\begin{aligned} (a + (m)) + (b + (m)) \ &= \ a + b + (m)\,, \\ (a + (m)) \cdot (b + (m)) \ &\subseteq \ ab + (m)\,. \end{aligned}$$

or by using the alternative notation,

$$\begin{aligned} [a]_m \ + \ [b]_m \ &= \ [a + b]_m \\ [a]_m \ \cdot \ [b]_m \ &\subseteq \ [ab]_m \end{aligned}$$

To prove (314), we observe that, for any integers s and t, $(a+ms)(b+mt)-ab \equiv 0 \pmod{m}$, so $a+(m)\ \cdot\ b+(m) \subseteq ab+(m)$.

A.1.7.8 Exercise. Construct a counterexample to show that the opposite inclusion need not hold in (314).

We have shown that the sum (respectively, product) of two cosets is contained entirely in a coset that may be determined by adding (respectively, multiplying) any representatives taken from the two cosets. The set of these cosets may be variously denoted by $\mathbb{Z}_m$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/(m)$. In defining operations of addition and multiplication on $\mathbb{Z}_m$ we will give this set the structure of what we call a *commutative ring*. The definition of addition will be that given in (313), and the definition of multiplication will be *based on*[316] that given in (314). We shall return to this concept later in the course.

A.1.8 Primes

A.1.8.1 Definition. An integer p is *prime* if $|p| \neq 1$ and if its only positive divisors are p and 1.

An integer distinct from 1 and -1 which is not prime is said to be *composite*. Note that 1 and -1 are neither prime nor composite. In the context of $\mathbb{Z}$ we often tacitly confine the term *prime* to *positive* primes. Where different (positive) primes appear in a discussion, we may denote them by symbols like[317] p_1, p_2, p_k, ...

A.1.8.2 Lemma. *Let p be a prime, and a any integer. If $p \nmid a$ then $(p,a)=1$.*

Proof: (p,a) is, by definition, a positive divisor of p; hence its only possible values are p, 1. Of these only $1 \mid a$. □

A.1.8.3 Lemma. *Let n be a integer, not a prime, and assume that $n>1$. Then there exists a divisor $d \mid n$ such that $1<d\leq\sqrt{n}$.*

Proof: By definition, n admits a factorization in the form $n=d_1d_2$, where $1<d_1<n$, $1<d_2<n$. If both $\sqrt{n}<d_1$, and $\sqrt{n}<d_2$, then $n<d_1d_2=n$. We conclude that one of d_1 and d_2 does not exceed $\sqrt{n}$. □

[316] In the case of addition we can simply reinterpret (313) as *defining* what we mean by the *sum* of two cosets. However, in the case of multiplication, (314) does not involve an equality. We will have to argue, based on the fact that residue classes, being equivalence classes, are disjoint; thus we can, without any ambiguity, determine the unique class that contains the product of one representative from each class: that is the class we will *define* to be the product of the given classes. In the end we will casually use various symbols for multiplication indiscrimately, confident that there will be no danger of confusion, as the meaning will be clear from the context.

[317] Some authors, however, use these subscripted symbols to denote specific primes. For them $p_1=2$, $p_2=3$, $p_{5761455}=99999989$.

A.1.8.4 LEMMA. *Let n be a integer, not a prime, and assume that $n > 1$. Then there exists a prime p which divides n, such that*

$$1 < p \leq \sqrt{n}\,. \tag{315}$$

Proof: Once we have proved the existence of a prime divisor p, inequality (315) will follow by Lemma A.1.8.3. The first nonprime is 4, which is divisible by 2. Suppose the result proved for all integers less than n, $n > 4$, and suppose that n is not prime. Then there exists a positive integer d such that $n = dd_1 > d > 1$. Without restricting generality, assume that d is the smaller of d and d_1, so $d \leq \sqrt{n}$. By the induction hypothesis, either d is a prime, or there exists a prime p such that $p \mid d$ and $d \mid n$, from which we may infer by transitivity that $p \mid n$. □

The following result is remarkable, in that it was known to the ancient Greeks in a geometric form (in terms of lengths of line segments):

A.1.8.5 THEOREM (EUCLID). *[10, Book IX, Prop. 20] There exist infinitely many primes.*

Proof: Suppose that there are only finitely many primes, p_1, p_2, ..., p_n. Consider the integer $N = p_1 p_2 ... p_n + 1$. By Lemma A.1.8.4 N has a prime factor. But $N \equiv 0 + 1 \pmod{p_i}$ $(i = 1, 2, ..., n)$, so none of p_1 ..., p_n divides N, which is a contradiction. We conclude that the hypothesis that there are only n primes is invalid.

A.1.8.6 EXERCISE. Adapt Euclid's proof of the infinity of primes to show that there exist infinitely many primes of the form $4m - 1$.

Solution: Suppose there are only n such primes other than 3: p_1, p_2, ..., p_n, and define $N = \prod_{i=1}^{n} p_i$; let $4N + 3$ have prime decomposition $4N + 3 = \prod_{j=1}^{s} q_i$, where q_1, q_2, ..., q_s are primes, not necessarily distinct. Were $q_i = 2$ for some i, the product would also be congruent to 0 or 2 mod 4; hence all q_i are odd. It cannot happen that $q_i \equiv 1 \bmod 4$ $(i = 1, 2, ..., s)$, for then the product would also be congruent to 1, a contradiction. Hence for some i_0, $1 \leq i_0 \leq s$, $q_{i_0} \equiv 3 \bmod 4$, i.e. $q_{i_0} = 3$ or q_{i_0} is one of the primes p_1, ..., p_n. If $q_{i_0} = 3$, it follows from $3|(4N + 3)$ and $3|3$ that $3|4N$, hence $3|N$, a contradiction; hence q_{i_0} is one of the primes p_1, ..., p_n. Since q_{i_0} divides both N and $4N + 3$, it must divide 3, again a contradiction. From these contradictions we may conclude that the number of primes of this type is infinite.[318] □

A.1.8.7 EXERCISE. 1. *The Sieve of Eratosthenes* is an algorithm based on Lemma A.1.8.3. It proceeds by "sifting" out from the list of integers 2, 3, 4, 5, ..., n

[318] Dirichlet's Theorem, proved in 1837 [25], states that $(a, b) = 1 \Rightarrow \exists$ infinitely many primes of the form $ak + b$.

those which cannot be prime, until all surviving members are prime, and are all the primes not exceeding n. At the ith repetition of the algorithm the first i such primes will have been determined, and all of their multiples (except these primes themselves) will have been deleted. In the next repetition the next survivor in the list is declared prime, and all of its non-trivial multiples are deleted. The algorithm is repeated until, other than the integers found to be prime, there are no survivors less than $\sqrt{n}$. Try writing code in your favourite programming language to compile a list of the primes less than n. Using your code, or by hand, determine the primes less than 100.

2. By inspection of the list of primes you have compiled, determine examples of prime pairs (i.e. ordered pairs of natural numbers $(p, p+2)$ where both p and $p+2$ are prime) not exceeding 100.[319]

Solution:

1. We begin by listing the integers from 2 to 100:

$$\begin{array}{cccccccccc}
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\
22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \\
42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 \\
52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 & 61 \\
62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 & 71 \\
72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 & 81 \\
82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 & 91 \\
92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100 &
\end{array}
\longrightarrow
\begin{array}{cccccc}
2 & 3 & 5 & 7 & 9 & 11 \\
 & 13 & 15 & 17 & 19 & 21 \\
 & 23 & 25 & 27 & 29 & 31 \\
 & 43 & 45 & 47 & 49 & 51 \\
 & 53 & 55 & 57 & 59 & 61 \\
 & 63 & 65 & 67 & 69 & 71 \\
 & 73 & 75 & 77 & 79 & 81 \\
 & 83 & 85 & 87 & 89 & 91 \\
 & 93 & 95 & 97 & 99 &
\end{array}$$

[319] The problem of twin primes alluded to above is concerned with resolving whether or not there exist infinitely many such pairs. It is known that, even if there do exist infinitely many such pairs, their distribution is "sparse" in the following sense: while it was proved by Euler that the series $\sum_{p \text{ prime}} \frac{1}{p}$ of sums of reciprocals of the primes is divergent, the series $\sum_{p,p+2 \text{ both prime}} \frac{1}{p}$ is *con*vergent. This latter result was proved in 1919 by the Danish mathematician Viggo Brun, using a combinatorial argument.

$$\longrightarrow \begin{array}{cccccc} 2 & 3 & 5 & 7 & & 11 \\ 13 & & 17 & 19 & & \\ 23 & 25 & & 29 & 31 & \\ 43 & & 47 & 49 & & \\ 53 & 55 & & 59 & 61 & \\ & 65 & 67 & & 71 & \\ 73 & & 77 & 79 & & \\ 83 & 85 & & 89 & 91 & \\ & 95 & 97 & & & \end{array} \longrightarrow \begin{array}{cccccc} 2 & 3 & 5 & 7 & & 11 \\ 13 & & & 17 & 19 & \\ 23 & & & & 29 & 31 \\ 43 & & & 47 & & \\ 53 & & & & 59 & 61 \\ & & & 67 & & 71 \\ 73 & & & & 79 & \\ 83 & & & & 89 & \\ & & & 97 & & \end{array}$$

$$\longrightarrow \begin{array}{cccccc} 2 & 3 & 5 & 7 & & 11 \\ 13 & & & 17 & 19 & \\ 23 & & & & 29 & 31 \\ 43 & & & 47 & & \\ 53 & & & & 59 & 61 \\ & & & 67 & & 71 \\ 73 & & & & 79 & \\ 83 & & & & 89 & \\ & & & 97 & & \end{array}$$

Since we have already eliminated all integers having at least one divisor less than 11, all surviving integers in our list are primes.

2. (3,5), (5,7), (11,13), (17,19), (29,31), (59,61), (71,73)

A.1.8.8 Exercise. 1. For any natural number n, show that $2^n + 1$ cannot be prime unless n is a power of 2. (To solve this problem, recall that if m is odd, $x^m + y^m$ admits a factorization $(x + y)(x^{m-1} - x^{m-2}y + x^{m-3}y^2 + ... + y^{m-1})$.) Note that the statement does not claim that every integer of the form $2^n + 1$ is prime; there exists a counterexample, i.e. a composite natural number of the form $2^{2^r} + 1$: $825753601|(2^{65536} + 1)$.

2. Show that if $2^n - 1$ is prime, then n is prime. (Such an integer $2^n - 1$ is called a *Mersenne* prime.)

Solution:

1. Suppose that $n = pm$, where $p > 1$ is odd. Then $2^n + 1 = (2^m)^p + 1^p = (2^m + 1)\left((2^m)^{p-1} - ... + 1^{p-1}\right)$; hence $(2^m + 1)|(2^n + 1)$, so $2^n + 1$ is composite (since $m < n$). It follows that all prime divisors of n are even, i.e. are 2.

2. Suppose that $n = ab$, where a and b are integers greater than 1. Then $2^{ab} - 1 = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + ... + 1\right)$; since $1 < a < ab$, $2^n - 1$ is composite.

A.1.8.9 THEOREM. *1. Let $n \in \mathbb{Z}$, $n > 1$.*[320] *Then there exist primes p_1, p_2, ..., p_r, possibly not all distinct, such that*

$$n = p_1 p_2 ... p_r \tag{316}$$

2. [**Fundamental Theorem of Arithmetic**] *The factorization (316) of a positive integer n into primes is unique up to order.*

Proof:

1. Our proof is by induction on n. It is evidently true for $n = 2$, since 2 is a prime. Suppose it has been proved for all positive integers distinct from 1 and less than n. If n is prime, the decomposition is $n = n$. Otherwise, n admits a decomposition $n = d_1 d_2$, where $1 < d_1 < n$, $1 < d_2 < n$. By the induction hypothesis, there exist decompositions $d_1 = p_1 p_2 ... p_r$, $d_2 = p_{r+1} p_{r+2} ... p_{r+s}$. Hence $n = d_1 d_2 = p_1 p_2 ... p_r p_{r+1} p_{r+2} ... p_{r+s}$.

2.

□

Where we are working with factorizations of several integers, it may be convenient to generalize (316) to admit the presence of some primes with exponent 0. In this way we can prove the following

A.1.8.10 EXERCISE. 1. Let $a = p_1^{u_1} p_2^{u_2} ... p_n^{u_n}$, $b = p_1^{v_1} p_2^{v_2} ... p_n^{v_n}$, where $u_i \geq 0$, $v_i \geq 0$, $(i = 1, 2, ..., n)$. Then

$$(a, b) = p_1^{\min(u_1, v_1)} p_2^{\min(u_2, v_2)} ... p_n^{\min(u_n, v_n)} \tag{317}$$

$$[a, b] = p_1^{\max(u_1, v_1)} p_2^{\max(u_2, v_2)} ... p_n^{\max(u_n, v_n)}$$

2. Use the preceding to reprove that $ab = (a, b)[a, b]$, (cf. Exercise A.1.6.14).

[320] The restriction to $n > 1$ may appear artificial. We can extend the theorem to the case $n = 1$ by defining an "empty" product of integers to equal 1. The case of *negative* n creates no difficulty, since p is prime iff $-p$ is prime. However, the theorem does not hold for $n = 0$.

A.1.8.11 Exercise. Determine representatives for the cosets (= congruence classes) of all squares modulo each of 5, 7, 11, 13, 17, 19. Based on this experimental evidence, formulate a conjecture (guess) on

1. the number of such squares (the non-zero squares are called *quadratic* residues)
2. whether or not 1, -1 are squares.

A.1.8.12 Exercise. Prove that all cubes are congurent modulo 13 to 0, 1, 5, 8, or 12.

A.1.9 Congruences

We have seen, in Theorem A.1.4.5 that congruences to a fixed modulus have similar algebraic properties to equations: they may be multiplied and added in the obvious way. We should like to be able to solve congruence analogues of problems we regard as routine when stated in terms of equations. In particular, we shall consider

- the solution of a linear congruence of the form $ax \equiv b \pmod{m}$
- the solution of *systems* of linear congruences, of the form

$$\begin{array}{rcll} a_1x & \equiv & b_1 & (\text{mod } m_1) \\ a_2x & \equiv & b_2 & (\text{mod } m_2) \\ \cdots & \equiv & \cdots & (\text{mod } \cdots) \\ a_kx & \equiv & b_k & (\text{mod } m_k) \end{array} \tag{318}$$

There are, of course, other analogues that come to mind, some of which may be considered in the exercises; for example

- the solution of polynomial congruences, of the form

$$a_nx^n + a_{n-1}x^{n-1} + ... + a_0 \equiv 0 \pmod{m}$$

- the solution in integers of a linear congruence in more than one variable

$$a_1x_1 + a_2x_2 + ... + a_nx_n \equiv b \pmod{m}$$

(called a *diophantine*[321] *equation of the first degree*)

[321] after Διόφαντός of Alexandria

The main theorem in this subsection is the so called "Chinese Remainder Theorem", which concerns the solution set of a system of linear congruences (322) subject to (323). We shall devote considerable effort to showing that any system (318) which has a solution is "equivalent" to a system of this type. Computer Science students will see applications of "Chinese Remaindering" in algorithms for high-speed integer arithmetic.

The similarity between equations and congruences ends when we consider division, however. The best we can prove is the following:

A.1.9.1 LEMMA. $ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$

Proof:
$\Leftarrow$:

$$\begin{aligned} a \equiv b \pmod{\frac{m}{(m,c)}} &\Rightarrow \frac{m}{(m,c)} \mid (a-b) \Leftrightarrow m \mid (a-b)(m,c) \\ &\Rightarrow m \mid (a-b)(m,c)\frac{c}{(m,c)} \Rightarrow m \mid (a-b)c\,. \end{aligned}$$

$\Rightarrow$: $ac \equiv bc \pmod{m} \Rightarrow \exists d \in \mathbb{Z}$ such that $md = (a-b)c \Rightarrow \frac{m}{(m,c)}d = (a-b)\frac{c}{(m,c)} \Rightarrow \frac{m}{(m,c)} \mid (a-b)\frac{c}{(m,c)}$. By Lemma A.1.6.9, $\frac{m}{(m,c)} \mid (a-b)$, i.e. $a \equiv b \pmod{\frac{m}{(m,c)}}$. □

We see, in particular, that we *can* divide both sides of a congruence by the same integer c, *provided c is relatively prime to the modulus!*

The relationship between congruences between the same pair of integers to different moduli is given by the following:

A.1.9.2 LEMMA.

$$\left.\begin{array}{ll} a \equiv b & \pmod{m_1} \\ a \equiv b & \pmod{m_2} \end{array}\right\} \Leftrightarrow a \equiv b \pmod{[m_1, m_2]}$$

Proof:
$\Rightarrow$: By Lemma A.1.6.12 $\left.\begin{array}{ll} a \equiv b & \pmod{m_1} \\ a \equiv b & \pmod{m_2} \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} m_1 \mid (a-b) \\ m_2 \mid (a-b) \end{array}\right\} \Rightarrow [m_1, m_2] \mid (a-b) \Rightarrow a \equiv b \pmod{[m_1, m_2]}$
$\Leftarrow$: By the transitivity of $|$,

$$\begin{aligned} a \equiv b \pmod{[m_1, m_2]} &\Rightarrow [m_1, m_2] \mid (a-b) \\ &\Rightarrow \left\{\begin{array}{l} m_1 \mid (a-b) \\ m_2 \mid (a-b) \end{array}\right\} \Leftrightarrow \left\{\begin{array}{ll} a \equiv b & \pmod{m_1} \\ a \equiv b & \pmod{m_2} \end{array}\right\} \end{aligned}$$

□

A.1.9.3 EXERCISE. 1. Prove that the decimal expansion of the square of any integer n must have, as its units digit (i.e. the coefficient of 10^0 in the decimal expansion) one of 0, 1, 4, 5, 6 or 9.

2. Prove that the decimal expansion of the 4th power of any integer n must have, as its units digit (i.e. the coefficient of 10^0 in the decimal expansion) one of 0, 1, 5 or 6.

A *linear congruence* of the form

$$ax \equiv b \pmod{m} \tag{319}$$

will have a solution iff b admits a decomposition of the form

$$b = x \cdot a + \ell \cdot m\,;$$

i.e. iff $(a, m) \mid b$, i.e. iff

$$b \in a\mathbb{Z} + m\mathbb{Z} = (a) + (m)\,.$$

Then if we define

$$a' = \frac{a}{(a,m)},\ b' = \frac{b}{(a,m)},\ m' = \frac{m}{(a,m)}$$

(319) is equivalent to the congruence

$$a'x \equiv b' \pmod{m'} \tag{320}$$

with the added condition that

$$(a', m') = 1 \tag{321}$$

We have proved the following

A.1.9.4 THEOREM. *Congruence (319) has solutions iff* $(a, m) \mid b$.

One special case of (319) requires special attention:

$$ax \equiv 1 \pmod{m}$$

By Theorem A.1.9.4, this congruence is solvable precisely when $(a, m) \mid 1$, i.e. when $(a, m) = 1$.

A.1.9.5 DEFINITION. Let m be a non-zero integer, and $(a, m) = 1$. An *inverse*[322] of a modulo m is an integer x such that $ax \equiv 1 \pmod{m}$; a is *invertible* if it possesses an inverse.

[322]Since the term *inverse* is normally associated with an operation — in this case multiplication — we may wish to speak of the *inverse under multiplication* or *multiplicative inverse*, to distinguish the $x + (m)$ from the *inverse under addition* or *additive inverse*, which is $-a + (m)$.

Let x be an inverse of a modulo m. Since the solutions to a congruence constitute a coset, *all* integers in $x+(m)$ will then be inverses of a — indeed, of *all* integers in $a+(m)$. We may then speak of the coset $x+(m)$ as being the *inverse* of the coset $a+(m)$ in $\mathbb{Z}_m$. It is sometimes convenient to denote x by a^{-1}, remembering that this is a generic symbol for any element of the coset $x+(m)$.

A.1.9.6 Definition. Let m be a positive integer.

1. A coset $a+(m)$ is said to be *invertible* when one of its representatives (i.e. members) is invertible.

2. A set of integers containing one representative from each *invertible* coset of (m) in $\mathbb{Z}$ is called a *reduced system of representatives modulo* m.

One way in which the inverse of a modulo m can be computed is via the Euclidean algorithm: from an equation

$$1 = k \cdot a + \ell \cdot m$$

we deduce the congruence

$$1 \equiv ka \pmod{m}$$

i.e. that k is an inverse. We have thus proved the following

A.1.9.7 Theorem. *Let a and m be non-zero integers, and $(a,m)=1$. Then a has an inverse modulo m. All inverses of a are contained in the same coset modulo m.*

A.1.9.8 Corollary (to Theorem A.1.9.4). *Congruence (319) has solutions iff*

$$(a,m) \mid b\,;$$

the set of solutions, in that case, is the coset

$$\left\{\frac{a}{(a,m)}\right\}^{-1}\frac{b}{(a,m)} + \left(\frac{m}{(a,m)}\right) = \left\{\frac{a}{(a,m)}\right\}^{-1}\frac{b}{(a,m)} + \frac{m}{(a,m)}\mathbb{Z}$$

of $\left(\frac{m}{(a,m)}\right)$.

We shall return to the problem of determining inverses in §A.5.A.5.1.

When we pass to considering systems of type (318), there is thus no limitation of generality to confine our attention to cases where $a_1 = a_2 = \ldots = a_k = 1$:

$$\begin{array}{rcll} x & \equiv & b_1 & \pmod{m_1} \\ x & \equiv & b_2 & \pmod{m_2} \\ \cdots & \equiv & \cdots & \pmod{\cdots} \\ x & \equiv & b_k & \pmod{m_k} \end{array} \tag{322}$$

We shall see that further restrictions may be made without limiting generality. By Lemma A.1.9.2, two congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}$$

are equivalent to

$$\begin{aligned} x &\equiv b_1 \quad \left(\text{mod } (m_1, m_2)\frac{m_1}{(m_1, m_2)}\right) \\ x &\equiv b_2 \quad \left(\text{mod } (m_1, m_2)\frac{m_2}{(m_1, m_2)}\right) \end{aligned}$$

i.e. to

$$\begin{aligned} x &\equiv b_1 \pmod{(m_1, m_2)} \\ x &\equiv b_1 \quad \left(\text{mod } \frac{m_1}{(m_1, m_2)}\right) \\ x &\equiv b_2 \pmod{(m_1, m_2)} \\ x &\equiv b_2 \quad \left(\text{mod } \frac{m_2}{(m_1, m_2)}\right) \end{aligned}$$

There cannot exist a solution unless $b_1 \equiv b_2 \pmod{(m_1, m_2)}$, and analogous congruences corresponding to other pairs. Where there does exist a solution, the system can be converted to one of form (322) wherein

$$(m_i, m_j) = 1 \quad (i \neq j; i = 1, ..., k; j = 1, ..., k) \tag{323}$$

This explains the apparently restricted class of system considered in the following theorem; (it isn't restricted — any solvable system can be transformed into this form).

A.1.9.9 Theorem (Chinese Remainder Theorem). *A system (322) of linear congruences to relatively prime moduli m_1, m_2, ..., m_k has as its solutions all members of a coset $u + (m_1 m_2 ... m_k)$ where a representative u may be determined as follows: Let d_i be an inverse of $m_1 m_2 ... m_{i-1} m_{i+1} ... m_k$ modulo m_i $(i = 1, 2, ..., k)$. Then u may be taken to be*

$$\sum_{i=1}^{k} m_1 m_2 ... m_{i-1} d_i m_{i+1} ... m_k \cdot b_i$$

In other words, if we define $M = m_1 m_2 ... m_k$, and $M_i = \dfrac{M}{m_1}$, and take d_i to be an inverse of M_i mod m_i, then the solution set is the coset

$$\sum_{i=1}^{k} M_i d_i b_i \ + \ (M) \tag{324}$$

Proof: Taking residues modulo m_i, we see that every integer in (324) is a solution to the system of congruences ($i = 1, 2, ..., k$). But any two solutions must differ by a multiple of M, hence, by Theorem A.1.7.6, there exists a unique solution to (322) lying between 0 and $M - 1$ (inclusive). □

Algorithms for high-speed arithmetic involving integers of bounded magnitude may be based upon the one-to-one correspondence that Theorem A.1.9.9 proves exists between integers in the interval 0, 1, ..., $M - 1$ and points in the Cartesian product $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ...\mathbb{Z}_{m_k}$ (cf. [23].) One convenient set of moduli is integers of the form $2^{u_i} - 1$, where u_1, u_2, ..., u_k are relatively prime. As seen in Exercise A.1.6.8, the integers $2^{u_1} - 1$, $2^{u_2} - 1$, ..., $2^{u_k} - 1$ are relatively prime.

The Chinese Remainder Theorem may be viewed as analogous to the *Lagrange interpolation formula* for polynomials:

A.1.9.10 Theorem (Lagrange Interpolation Theorem). *Let α_i and β_i be elements of any field $\mathbb{F}$. Then there exists just one polynomial $f(x)$ of degree n, with coefficients taken from $\mathbb{F}$, such that $f(\alpha_i) = \beta_i$;*

$$f(x) = \sum_{i=0}^{n} \frac{(x-\alpha_0)(x-\alpha_1)...(x-\alpha_{i-1})(x-\alpha_{i+1})...(x-\alpha_n)}{(\alpha_i-\alpha_0)(\alpha_i-\alpha_1)...(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})...(\alpha_i-\alpha_n)}\beta_i$$

Proof: [23, §4.6.4, p. 430] □

For a history of the Chinese Remainder Theorem, cf. [7, pp. 57–64].

In practical applications algorithms may be designed which are more efficient than the naïve techniques suggested by the statement of the theorem. At the other extreme, the system may be solved recursively by proceeding through successive recurrences, in each case refining the set of solutions.

A.1.9.11 Exercise. 1. (a) By factorizing both integers, explain why 7 must have an inverse modulo 15.

(b) Determine the inverse of 7 modulo 15

i. by computing the products of 7 with each of 1, 2, 3, ...

ii. by using the Euclidean algorithm.

(c) Use your computed value of 7^{-1} to determine inverses of powers of 7.

(d) Find the smallest positive integer n — if any — whose powers, together with an element of the ideal $15\mathbb{Z}$, yield a complete set of representatives modulo 15. Repeat with 15 replaced by 17.

2. Solve the congruence $98n \equiv 1 \pmod{139}$.

3. (Sun Tsu, 1st century a.d.) Determine an integer having remainders 2, 3, 2 when divided by 3, 5, 7 respectively. (Solve this problem in two ways: first recursively, finding the form of integers satisfying the first congruence, and subjecting this to the constraint of the second congruence, etc.; then by determining inverses and applying the formula of Theorem A.1.9.9.)

4. (Leonardo Pisano, *Liber Abbaci*, 1228) Find the smallest integer N, divisible by 7, which gives the remainder 1 when divided by 2, 3, 4, 5, 6. (Hint: Translate the word problem into congruences, then transform them into a set of congruences to relatively prime moduli. You may wish to use Lemma A.1.9.2.)

Solution:

1. (a) As the factorizations $7 = 7^1$; $15 = 3^1 5^1$ involve disjoint sets of prime factors,

$$(7, 15) = 3^{\min(0,1)} 5^{\min(0,1)} 7^{\min(1,0)} = 1$$

By Theorem A.1.9.7, 7 is invertible modulo 15.

(b) i. As instructed, we begin to compute the products of 7 with each of 1, 2, 3, ...:

$$\begin{aligned} 7 \cdot 1 &= 1 \\ 7 \cdot 2 &= 14 \\ 7 \cdot 3 &= 21 \equiv 6 \pmod{15} \\ 7 \cdot 4 &= 28 \equiv 13 \pmod{15} \\ 7 \cdot 5 &= 35 \equiv 5 \pmod{15} \\ 7 \cdot 6 &= 42 \equiv 12 \pmod{15} \\ \ldots &= \ldots \end{aligned}$$

But the information we need is actually contained in the 2nd equation:

$$7 \cdot 2 = 14 \equiv -1 \pmod{15}$$

for we may infer from it that

$$7 \cdot (-2) \equiv 1 \pmod{15};$$

thus -2 is an inverse; another inverse is $-2 + 15 = 13$, which would have appeared if we had persisted in computing all products earlier.

ii. By the Euclidean algorithm,

$$15 = 2 \cdot 7 + 1\,,$$

hence

$$1 = 1 \cdot 15 + (-2) \cdot 7 \equiv -2 \cdot 7 \pmod{15}$$

(c)

$$\begin{aligned} 7^1 \cdot (-2) &\equiv 1 \pmod{15} \\ \Rightarrow 7^2 \cdot 4 &\equiv 1^2 \equiv 1 \pmod{15} \\ \Rightarrow 7^3 \cdot (-8) &\equiv 1 \pmod{15} \\ \Rightarrow 7^4 \cdot (16) &\equiv 1 \pmod{15} \\ \text{i.e.} \quad 7^4 &\equiv 1 \pmod{15} \end{aligned}$$

Hence, for any power 7^n, the inverse can be found by reducing the exponent n modulo 4, then raising 7 to the complement of that reduced exponent (in 4).

(d) For moduli 1, 2, 4, and for moduli of the form p^a, $2p^a$ (p an odd prime, ($a \in \mathbb{N}$) it is possible to find a *primitive root* — i.e. an integer n whose powers form a set of representatives of all residue classes which are prime to the modulus; 17 is of this form, and $n = 3$ is the smallest integer whose powers, together with 0, form a complete set of representatives. (The set of powers of 1 — modulo 17 — is simply $\{1\}$; the set of powers of 2 modulo 17 is $\{2, 4, 8, 16, 15, 13, 9, 1\}$.] When the modulus is 15, we can immediately exclude integers not prime to 15 — i.e. 3, 5, 6, 9, 10, 12, as their powers cannot, after reduction modulo 15, include 1. This leaves as candidates 1, 2, 4, 7, 8, 11, 13, 14. 1 obviously yields only itself as a power; 14, which is congruent to -1, can yield only -1 and 1. The powers of 2 are 2, 4, 8, 1; of 4 are 4 and 1. We can elminate -2, i.e. 13, and -4, i.e. 11 in the same way. Finally, we find the powers of 7 to be 7, $49 \equiv 4$, ...; we can stop here, since we know there are only 2 distinct powers of 4, so there will be only 4 distinct powers of 7. And 8 will behave in the same way: 8, $8^2 \equiv 4$, $8^3 \equiv 2$, $8^4 \equiv 1$.

2. By the Euclidean algorithm we find that

$$\begin{aligned} 139 &= 1 \cdot 98 + 41 \\ 98 &= 2 \cdot 41 + 16 \\ 41 &= 2 \cdot 16 + 9 \\ 16 &= 1 \cdot 9 + 7 \end{aligned}$$

$$\begin{aligned} 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

from which it follows that

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 &&= 7 - 3(9 - 1 \cdot 7) \\ &= -3 \cdot 9 + 4 \cdot 7 &&= -3 \cdot 9 + 4(16 - 1 \cdot 9) \\ &= 4 \cdot 16 - 7 \cdot 9 &&= 4 \cdot 16 - 7(41 - 2 \cdot 16) \\ &= -7 \cdot 41 + 18 \cdot 16 &&= -7 \cdot 41 + 18(98 - 2 \cdot 41) \\ &= 18 \cdot 98 - 43 \cdot 41 &&= 18 \cdot 98 - 43(139 - 1 \cdot 98) \\ &= -43 \cdot 139 + 61 \cdot 98 \end{aligned}$$

Reducing both members of the equation

$$(-43)(139) + (61)(98) = 1\,,$$

modulo 139, we find that $(98)^{-1} \equiv 61 \pmod{139}$. Hence $n \equiv 61$, i.e. $n = 61 + 139t$, $t \in \mathbb{Z}$.

3. To solve the system

$$x \equiv 2 \pmod 3 \tag{325}$$
$$x \equiv 3 \pmod 5 \tag{326}$$
$$x \equiv 2 \pmod 7 \tag{327}$$

(a) $M = 3 \cdot 5 \cdot 7 = 105$; $M_1 = 35$, $M_2 = 21$, $M_3 = 15$.

$$d_1 \equiv 35^{-1} \pmod 3 \equiv 2^{-1} \pmod 3 = 2$$

$$d_2 = 21^{-1} \pmod 5 = 1^{-1} \pmod 5 = 1$$
$$d_3 = 15^{-1} \pmod 7 = 1^{-1} \pmod 7 = 1$$

where the inverses were computed by trial, although the Euclidean algorithm could have been used. One solution is therefore the sum

$$35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 \equiv 23 \pmod{105}$$

so the set of all solutions is the coset $23 + (105)$.

(b) From congruence (325), there exists an integer a such that $x = 3a + 2$; substituting in congruence (326), we find that

$$3a \equiv 1 \pmod 5,$$

which we solve by multiplying by the modulo 5 inverse of 3, 2, to obtain

$$a \equiv 2 \pmod 5$$

which implies the existence of an integer b such that $a = 5b+2$, so $x = 15b+8$. This we substitute into congruence (327), to deduce that

$$15b \equiv 1 \pmod 7,$$

i.e. $1 \cdot b \equiv 1 \pmod 7$, so $b = 1 + 7c$ for some integer c, and $x = 23 + 105c$; conversely, for any c, any such integer is a solution to the system of congruences.

4. We are considering the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod 2 && (328)\\ x &\equiv 1 \pmod 3 && (329)\\ x &\equiv 1 \pmod 4 && (330)\\ x &\equiv 1 \pmod 5 &&\\ x &\equiv 1 \pmod 6 && (331)\\ x &\equiv 0 \pmod 7 &&\end{aligned}$$

Now, (330)⇒(328). Also, (331) implies (328) and (329). So the system reduces to

$$\begin{aligned} x &\equiv 1 \pmod 4\\ x &\equiv 1 \pmod 3\\ x &\equiv 1 \pmod 5\\ x &\equiv 0 \pmod 7\end{aligned}$$

which we solve in the usual way: $M_1 = 105$, $M_2 = 140$, $M_3 = 84$, $M_4 = 60$. Modulo 4, $105^{-1} \equiv 1^{-1} \equiv 1$; the other inverses can be determined by trial or otherwise, to yield as solution the coset represented by

$$105 \cdot 1 \cdot 1 + 140 \cdot 2 \cdot 1 + 84 \cdot 4 \cdot 1 + 60 \cdot 2 \cdot 0 = 721 \equiv 301 \pmod{420}$$

A.1.9.12 EXERCISE. 1. An integer is *square-free* if the only integers whose squares divide it are $+1$ and -1. Prove that the largest number k of consecutive integers *all of which* are square-free is at most 3. Then show that there do exist 3 consecutive integers which are square free.

2. Prove that for any $k \in \mathbb{N}$ there exist k consecutive integers x, $x+1$, ..., $x+k-1$ *none of which* is square-free.

3. Give a proof based on congruences that the product of any 3 consecutive integers is divisible by 3.

Solution:

1. Since consecutive multiples of 4 are spaced 4 apart, any 4 consecutive integers contain one that is such a multiple; a square-free integer cannot be divisible by 2^2. Hence no more than 3 consecutive integers can be square-free. Examples: $\{1,2,3\}$, $\{5,6,7\}$.

2. We solve a system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{m_1} \\ x &\equiv -1 \pmod{m_2} \\ ... &\equiv ... \pmod{.}.. \\ x &\equiv -k+1 \pmod{m_k} \end{aligned}$$

with a judiciously chosen set of relatively prime moduli. In this problem we would want these moduli to be divisible by squares > 1. For example, we could take $m_i = p_i^2$ $(i = 1, 2, ..., k)$, where p_1, ..., p_k are any distinct primes.

3. Since x, $x+1$, $x+2$ differ by 1, or 2 — never by a multiple of 3 — no two of them can be contained in the same congruence class (coset) modulo 3. But there are precisely three distinct congruence classes modulo 3: $3\mathbb{Z}$, $1+3\mathbb{Z}$, $2+3\mathbb{Z}$; so one of the three integers considered must be in the class $3\mathbb{Z}$ — i.e. divisible by 3. (This fact may also be proved combinatorially: the number of 3-element subsets of a set of $n+2$ elements is $\binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}$, so $6 \mid (n(n+1)(n+2))$.)

A.2 Functions etc.

A.2.1 Set Theory

We assume students are familiar with the concepts, terminology, and notation of elementary set theory. In particular, for the purposes of standardization, we make the following definitions:

A.2.1.1 DEFINITION. 1. Let $\mathfrak{A}$ and $\mathfrak{B}$ be sets. We write $\mathfrak{A} = \mathfrak{B}$, and say that the sets are *equal* iff both of the conditions $\mathfrak{A} \subseteq \mathfrak{B}$ and $\mathfrak{A} \supseteq \mathfrak{B}$ hold.

2. The *power set* of a set $\mathfrak{A}$ is the set $\{B|\mathfrak{B} \subseteq \mathfrak{A}\}$, and is denoted by either $P(\mathfrak{A})$ or by $2^{\mathfrak{A}}$.

3. The *cardinality* of a set $\mathfrak{A}$ is denoted by $|\mathfrak{A}|$; intuitively this is the *number* of elements in $\mathfrak{B}$. When $|\mathfrak{A}| \in \mathbb{N} \cup \{0\}$, $\mathfrak{A}$ is *finite*, otherwise it is *infinite*.

A.2.2 Basic Definitions

Recall that a *(binary) relation* from a set $\mathfrak{A}$ to a set $\mathfrak{B}$ is a subset of the *Cartesian product* $\mathfrak{A} \times \mathfrak{B}$. Any such subset is a relation — ranging from the *empty* relation $\varnothing$ to the entire set $\mathfrak{A} \times \mathfrak{B}$.

A.2.2.1 DEFINITION. A *function f from $\mathfrak{A}$ to $\mathfrak{B}$* is a relation $f \subseteq \mathfrak{A} \times \mathfrak{B}$ such that

1. $(\forall a \in \mathfrak{A})(\exists b \in \mathfrak{B})[(a, b) \in f]$

2. $\forall a[((a, b) \in f) \wedge ((a, c) \in f) \Rightarrow (b = c)]$.

In addition to denoting such a function by its name f, we may also employ such symbols as $f : \mathfrak{A} \to \mathfrak{B}$ and $\mathfrak{A} \xrightarrow{f} \mathfrak{B}$.[323] We call $\mathfrak{A}$ and $\mathfrak{B}$ respectively the *domain* and *codomain*[324] of the function.[325]

A.2.2.2 REMARK. Condition 2 of Definition A.2.2.1 asserts that no point of $\mathfrak{A}$ is associated with more than one point of $\mathfrak{B}$; as to the existence of such points, that is ensured by condition 1; thus the two conditions together assert the existence of a *unique* point of $\mathfrak{B}$ associated with each point of $\mathfrak{A}$.

[323] In *commutative diagrams* one may orient the arrows at slopes other than horizontal.

[324] But avoid using the word *range* as this word has also been used to denote the *image* $f(\mathfrak{A})$.

[325] Some authors use the term *partial function* for a relation f satisfying condition 2, but possibly not condition 1.

A.2.2.3 DEFINITION. 1. For a function $f : \mathfrak{A} \to \mathfrak{B}$ the unique point $b \in \mathfrak{B}$ such that $(a, b) \in f$ is called the *image* of a under f. In these notes we shall usually denote that image by $f(a)$.[326] We may also write $a \mapsto b$, and say that a *is mapped (on)to* b. For a subset $\mathfrak{A}' \subseteq \mathfrak{A}$ we may also use the word *image*, this time to denote the set

$$f(\mathfrak{A}') = \{f(a)|a \in \mathfrak{A}'\}.$$

In particular, $f(\mathfrak{A})$ is called the *image*[327] of f.

2. Any point $a \in \mathfrak{A}$ such that $f(a) = b$ is called a *preimage of* b *under* f. More generally, if $\mathfrak{B}' \subseteq \mathfrak{B}$, the *preimage*[328] of $\mathfrak{B}'$ is defined to be the set $\{a|f(a) \in \mathfrak{B}'\}$.[329]

3. In the specification of a function $f : \mathfrak{A} \to \mathfrak{B}$ both the domain and codomain are fixed. Should we wish to alter these, we obtain different functions, for which we have a precise terminology, where it is required. When we wish to *restrict* the domain to a subset $\mathfrak{A}'$ of $\mathfrak{A}$, we speak of the *restriction* of f to $\mathfrak{A}'$, and denote it by

$$f_{|\mathfrak{A}'} : \mathfrak{A}' \to \mathfrak{B}$$

and define it to be the set $\{(a, f(a))|a \in \mathfrak{A}'\}$. We also have a terminology when we wish to *extend* the domain of a function f. If $\mathfrak{A}'' \supseteq \mathfrak{A}$, a function $g : \mathfrak{A}'' \to \mathfrak{B}$ is said to be an *extension* of $f : \mathfrak{A} \to \mathfrak{B}$ if $f = g_{|\mathfrak{A}}$. In practice one often uses the same symbol for a restriction where there is no danger of confusion.

A.2.2.4 EXERCISE. Let $f : \mathfrak{A} \to \mathfrak{B}$ and $g : \mathfrak{C} \to \mathfrak{D}$ be given functions.

1. Prove that, if $\mathfrak{A}' \subseteq \mathfrak{A}$, then

$$(f(\mathfrak{A}') = \varnothing) \Rightarrow \mathfrak{A}' = \varnothing$$

2. Prove that, if $a \in \mathfrak{A}$, then $f(\{a\}) = \{f(a)\}$.

[326] This notation is familiar to students from the calculus; however, there are often advantages in algebraic contexts in denoting it also by a^f, where the function name is written in a location usually reserved for an exponent; or by $(a)f$ or, even more simply, by af.

[327] Some authors call this set the *range* of f. Use of this word should be avoided because of the ambiguity of use described in a preceding footnote.

[328] also called the *inverse image*

[329] This set may be denoted by $f^{-1}(\mathfrak{B})$. This is yet another situation where a notation is used for more than one purpose. Here the inverse function notation defined later in this section is applied to a slightly different purpose. Whereas the inverse function $f^{-1} : \mathfrak{B} \to \mathfrak{A}$ does not always exist, the function we are defining here maps the *power set* of $\mathfrak{B}$ to the power set of $\mathfrak{A}$. So, for a given point b in the codomain of f, we may not be giving any meaning to $f^{-1}(b)$ — there will always be a meaning defined for $f^{-1}(\{b\})$ — it is the set of all preimages of b.

3. Prove that f and g are the same function — written $f = g$ — iff the following three conditions hold:

   (a) $\mathfrak{A} = \mathfrak{C}$

   (b) $\mathfrak{B} = \mathfrak{D}$

   (c) $(\forall a \in \mathfrak{A})[f(a) = g(a)]$

A.2.2.5 DEFINITION. Let $\mathfrak{A}$ and $\mathfrak{B}$ be given sets.

1. The function defined by $(\forall a)[a \mapsto a]$ is called the *identity* function on $\mathfrak{A}$. We shall denote it by $\iota_{\mathfrak{A}}$; the subscript may be omitted where there is no ambiguity.

2. For any fixed element $b \in \mathfrak{B}$, the function defined by $\forall a[a \mapsto b]$ is called a *constant* function; we may sometimes denote it simply by b.

A.2.2.6 DEFINITION. Let $f : \mathfrak{A} \to \mathfrak{B}$ be a given function.

1. f is *injective* or *one-to-one* if

$$\forall a_1 \forall a_2[(f(a_1) = f(a_2)) \Rightarrow (a_1 = a_2)]$$

2. f is *surjective* or *onto* if $\quad \forall b \exists a[f(a) = b]$.

3. f is *bijective* or *a one-to-one correspondence* if it is both injective and surjective.

An *injection* is an *inject*ive func*tion*. *Surjection*s and *bijection*s are defined analogously.

A.2.2.7 EXERCISE. 1. Prove that $\iota_{\mathfrak{A}}$ is a bijection.

2. Determine conditions on the domain and codomain under which constant functions are respectively injective, surjective, bijective.

A.2.3 Function Composition

A.2.3.1 DEFINITION. Let $f : \mathfrak{A} \to \mathfrak{B}$ and $g : \mathfrak{B} \to \mathfrak{C}$ be given functions. The *composition* $g \circ f : \mathfrak{A} \to \mathfrak{C}$ is the function defined by $\forall a[a \mapsto g(f(a))]$.

Note that the order of the functions in the symbol $b \circ f$ is the reverse of the order in which the functions f and g are usually written when the arrow notations are concatenated, as

$$\mathfrak{A} \xrightarrow{f} \mathfrak{B} \xrightarrow{g} \mathfrak{C}$$

A.2.3.2 Exercise. Given functions

$$\mathfrak{A} \xrightarrow{f} \mathfrak{B} \xrightarrow{g} \mathfrak{C} \xrightarrow{h} \mathfrak{D}$$

prove that

1. $h \circ (g \circ f) = (h \circ g) \circ f$ (i.e. that $\circ$ is *associative*.)
2. $f \circ \iota_{\mathfrak{A}} = f = \iota_{\mathfrak{B}} \circ f$ (i.e. that the respective identity functions are right and left identities for f).
3. If f and g are both injective, then $g \circ f$ is injective.
4. If f and g are both surjective, then $g \circ f$ is surjective.

A.2.3.3 Exercise. Given functions

$$\mathfrak{A} \xrightarrow{f} \mathfrak{B} \xrightarrow{g} \mathfrak{C}$$

construct "small" examples to prove that

1. If f is injective and g is surjective, then $g \circ f$ need not be injective.
2. If f is injective and g is surjective, then $g \circ f$ need not be surjective.
3. If f is surjective and g is injective, then $g \circ f$ need not be injective.
4. If f is surjective and g is injective, then $g \circ f$ need not be surjective.

A.2.3.4 Definition. Let

$$\mathfrak{A} \xrightarrow{f} \mathfrak{B} \xrightarrow{g} \mathfrak{A}$$

1. If $g \circ f = \iota_{\mathfrak{A}}$, we say that g is a *left inverse* of f, and also that f is a *right inverse* if g.
2. If g is both a left inverse and a right inverse of f, we say that g is a *two-sided inverse* or simply an *inverse* of f.
3. A function that possesses an inverse is said to be *invertible*.

A.2.3.5 Theorem. *Let*

$$\mathfrak{A} \xrightarrow{f} \mathfrak{B} \xrightarrow{g} \mathfrak{A}$$

1. *If g is a left inverse of f, then f is injective.*
2. *If g is a right inverse of f, then f is surjective.*
3. *If g is an inverse of f, then f is bijective.*
4. *If g is an inverse of f, then f is an inverse of g.*

A.2.3.6 COROLLARY. 1. *If $g : \mathfrak{B} \to \mathfrak{A}$ and $h : \mathfrak{B} \to \mathfrak{A}$ are both inverses of $f : \mathfrak{A} \to \mathfrak{B}$, then $g = h$; i.e. an inverse, if it exists, is unique.*

2. *Let $f : \mathfrak{A} \to \mathfrak{B}$, $g : \mathfrak{B} \to \mathfrak{A}$, and $h : \mathfrak{B} \to \mathfrak{A}$ have the properties that $g \circ f = \iota_{\mathfrak{A}}$ and $f \circ h = \iota_{\mathfrak{B}}$. Then $g = h$.*

Proof: Evidently part 2 implies part 1; we prove only 2.

$$\begin{aligned} g &= g \circ \iota_{\mathfrak{B}} \\ &= g \circ (f \circ h) \\ &= (g \circ f) \circ h \\ &= \iota_A \circ h \\ &= h \quad \square \end{aligned}$$

A.2.3.7 DEFINITION. The inverse of f, if it exists, is denoted by f^{-1}.

A.2.3.8 THEOREM (CONVERSE OF THEOREM A.2.3.5). 1. *If $f : \mathfrak{A} \to \mathfrak{B}$ is injective, it has a left inverse.*

2. *If $f : \mathfrak{A} \to \mathfrak{B}$ is surjective, it has a right inverse.*

3. *If $f : \mathfrak{A} \to \mathfrak{B}$ is bijective, it has an inverse.*

Proof:

1. We can define a left-inverse $g : \mathfrak{B} \to \mathfrak{A}$ as follows: Let $b \in f(\mathfrak{A})$. Since f is injective there exists exactly one point $a \in \mathfrak{A}$ such that $f(a) = b$; *define* $g(b) = a$. As for the points $b \in \mathfrak{B}$ which are *not* in the image of f, let $f(b)$ have any convenient value. Then, for any $a \in \mathfrak{A}$,

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \quad \text{by definition of } \circ \\ &= a \quad \text{by definition of } g \\ &= \iota_{\mathfrak{A}}(a) \quad \text{by definition of } \iota_{\mathfrak{A}}\,. \end{aligned}$$

Thus $g \circ f$ and $\iota_{\mathfrak{A}}$ are functions with the same domain — $\mathfrak{A}$, the same codomain — $\mathfrak{B}$ and with the same *action* on all points of the domain. By virtue of Exercise A.2.2.4.3, $g \circ f = \iota_{\mathfrak{A}}$.

2. We define a right inverse $g : \mathfrak{B} \to \mathfrak{A}$ by mapping each point $b \in \mathfrak{B}$ on to any one of its preimages; since f is surjective, we know that such preimages always exist. Then, for any such b,

$$\begin{aligned}(f \circ g)(b) &= f(g(b)) \quad \text{by definition of } \circ \\ &= b \quad \text{by definition of } g \\ &= \iota_{\mathfrak{B}}(b) \quad \text{by definition of } \iota_{\mathfrak{B}}\end{aligned}$$

The functions $f \circ g$ and $\iota_{\mathfrak{B}}$ have the same domain, the same codomain, and the same action on all points of their common domain, so $f \circ g = \iota_{\mathfrak{B}}$.

3. Part 3 is a consequence of parts 1 and 2. □

A.2.3.9 REMARK. 1. By virtue of the uniqueness of the inverse, where one exists, we may now change the article we associate with the word: instead of speaking of *an* inverse, we may now speak of *the*. The notation f^{-1} could be open to question, however: by placing the symbol -1 in a location normally used for an exponent, are we suggesting that the operation of taking the inverse behaves like exponentiation? Indeed, we are! For example, it follows from Theorem A.2.3.5.4 that $(f^{-1})^{-1} = f$.

2. Other properties of the exponent also hold, where these are meaningful. We now have to restrict ourselves to functions whose domain and codomain are the same set, in order that we may compose a function with itself. Let $f : \mathfrak{A} \to \mathfrak{B}$ be given. We can define f^n to be the composition of n copies of f when n is a positive integer; to be the composition of $-n$ copies of f^{-1} when n is a negative integer; and to be $\iota_{\mathfrak{A}}$ when $n = 0$. It can be shown that all the properties we expect to hold do actually hold.

We have not presented a formal definition of the notion of "finiteness", relying instead on students' intuition. Had we been more formal in this concept — and also in definitions of such concepts as the natural numbers, cardinality, etc./ we could prove the following result, which will be required in the next section.

A.2.3.10 THEOREM. *1. A set $\mathfrak{A}$ is finite iff there exists no function $f : \mathfrak{A} \to \mathfrak{A}$ such that f is injective, but not surjective.*

2. A set $\mathfrak{A}$ is finite iff there exists no function $f : \mathfrak{A} \to \mathfrak{A}$ such that f is surjective, but not injective.

A.3 Permutation Groups

A.3.1 Permutations

A.3.1.1 DEFINITION. A *permutation* of a set $\mathfrak{A}$ is a one-to-one correspondence (= bijection = one-to-one onto function = injective surjection = surjective injection) $f : \mathfrak{A} \longrightarrow \mathfrak{A}$.

By Theorem A.2.3.10, where $\mathfrak{A}$ is *finite*, every one-to-one function $f : \mathfrak{A} \longrightarrow \mathfrak{A}$ is onto, and every onto function $f : \mathfrak{A} \longrightarrow \mathfrak{A}$ is one-to-one.

Students may already have encountered the word *permutation* in combinatorics, where a *permutation* of a set $\mathfrak{A} = \{a_1, a_2, ..., a_n\}$ traditionally has meant a "word" or arrangement $a_{i_1}a_{i_2}...a_{i_n}$ in which each of the letters a_1, ..., a_n appears exactly once. Such a word can be interpreted as representing a bijection by defining $f : \mathfrak{A} \longrightarrow \mathfrak{A}$ by $a_1 \mapsto a_{i_1}$, $a_2 \mapsto a_{i_2}$, ..., $a_n \mapsto a_{i_n}$, i.e. $f(a_j) = a_{i_j}$ $(j = 1, 2, ..., n)$. The action of a permutation is often described by a 2-line matrix:

$$f = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_{i_1} & a_{i_2} & ... & a_{i_n} \end{pmatrix}.$$

A.3.1.2 EXAMPLE. There are precisely $3! = 6$ permutations of the set $\{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

If, for a fixed set $\mathfrak{A}$, we always list the points in the same order in the upper row, the two-row notation is redundant. We could chosen to suppress that row entirely, and simply write the arrangement which is the second row; but that would be risky if there was no "obvious" order for the elements of $\mathfrak{A}$. Instead, we usually represent a permutation by another type of symbol, written on one line, which consists of one or more sequences of set elements, each sequence surrounded by parentheses. This notation, called *disjoint cycle notation* describes the successive set elements that are images of a fixed element under repeated applications of the permutation. We present an example of the notation first, and then a general definition.

A.3.1.3 EXAMPLE. For the set $\{1, 2, 3\}$ the disjoint cycle representations of all of its permutations are shown below:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &= (1)(2)(3) = (1)(3)(2) = (2)(1)(3) = (2)(3)(1) = (3)(1)(2) = (3)(2)(1) \\ &= I \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} &= (1)(23) = (1)(32) = (23)(1) = (32)(1) = (23) = (32) \end{aligned}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (3)(12) = (3)(21) = (12)(3) = (21)(3) = (12) = (21)$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) = (231) = (312)$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (213) = (321)$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (2)(13) = (2)(31) = (13)(2) = (31)(2) = (13) = (31)$$

A.3.1.4 DEFINITION. A *disjoint cycle symbol* for a set $\mathfrak{A} = \{a_1\, a_2 \ldots a_n\}$ is a listing of some or all of the elements of the set, together with left and right parentheses; or of the single symbol[330] I with the following properties:

1. No element of the set is listed more than once.
2. Where no elements of the set are listed, I is the only disjoint cycle symbol.
3. Except for the case of I, the symbol begins on the left with a left parenthesis (.
4. A left parenthesis (is always followed by an element of $\mathfrak{A}$.
5. An element of $\mathfrak{A}$ is always followed by either another element of $\mathfrak{A}$, or by a right parenthesis).
6. A right parenthesis) is either the end of the symbol, or is followed immediately by a left parenthesis.

We shall interpret the symbol I as representing the *identity* permutation — the function $\iota_{\mathfrak{A}} : \mathfrak{A} \longrightarrow \mathfrak{A}$ defined by $a \mapsto a\ \forall a \in \mathfrak{A}$.

The symbol

$$(u_1\, u_2 \ldots u_r)(v_1\, v_2 \ldots v_s)\ldots(w_1\, w_2 \ldots w_t) \tag{332}$$

represents the permutation which has the following action:

$$u_i \longmapsto u_{i+1} \quad (i = 1, 2, \ldots, r-1) \tag{333}$$
$$u_r \longmapsto u_1 \tag{334}$$
$$v_j \longmapsto v_{j+1} \quad (j = 1, 2, \ldots, s-1) \tag{335}$$
$$v_s \longmapsto v_1 \tag{336}$$
$$\cdots \tag{337}$$
$$w_k \longmapsto w_{k+1} \quad (k = 1, 2, \ldots, t-1) \tag{338}$$
$$w_t \longmapsto w_1 \tag{339}$$

[330] Called the *identity*, and sometimes denoted by such other symbols as e, or 1

(Statements (333) and (334) may be combined into one:

$$u_i \longmapsto u_{i+1} \quad (i = 1, 2, ..., r)$$

under the convention that subscripts are taken *modulo* r — i.e. that u_i is identified with u_{i+kr} for any integer k. Similarly, statements (335) through (339) are equivalent to

$$v_j \longmapsto v_{j+1} \quad (j = 1, 2, ..., s)$$

$$w_k \longmapsto w_{k+1} \quad (k = 1, 2, ..., t)\,.)$$

A.3.1.5 DEFINITION. In the disjoint cycle symbol (332), the subsequences $(u_1\, u_2 \,...\, u_r)$, $(v_1\, v_2 \,...\, v_s)$, $(w_1\, w_2 \,...\, w_t)$ are called *cycles*, respectively of *lengths* r, s, ..., t. A cycle of length i may be called an *i-cycle*. A cycle of length 2 is called a *transposition*. A cycle of length 1 may — by abuse of language — be called a *fixed point*. The *set* of points in any one cycle is called an *orbit* of the permutation.[331]

Note that the sets of points named in the various cycles which constitute a disjoint cycle symbol are *disjoint*, whence the name.

A.3.1.6 DEFINITION. The term *cycle* is also applied to a permutation corresponding to a disjoint cycle symbol having at most one cycle of length greater than 1.

Two distinct permutations f and g which are cycles are said to be *disjoint* if the intersection of any orbit of f with any orbit of g is empty, unless at least one of those orbits consists of just one point.

Evidently the same permutation may be represented by more than one symbol in disjoint cycle notation. The following operations (and repeated applications of them) applied to a disjoint cycle symbol do not alter the permutation to which the symbol corresponds:

- rearrangement of the cycles
- cyclic rearrangement of the points within any one cycle: specifically, the replacement of $(u_1\, u_2 \,...\, u_{r-1}\, u_r)$ by $(u_2\, u_3 \,...\, u_r\, u_1)$

A.3.1.7 EXERCISE. For the set $\{1, 2, 3, 4, 5, 6\}$ determine the number of permutations having disjoint cycle representations having each of the following lengths of cycles. (Be careful, remembering that certain changes in order of symbols in the disjoint cycle notation do not affect the permutation represented.)

[331] This term will be generalized below (cf. Definition A.3.4.1).

1. 1 cycle of length 6
2. 2 cycles, both of length 3
3. 2 cycles, one of length 4, one of length 2
4. 3 cycles, all of length 2.

Solution:

1. This is the familiar problem of arranging 6 symbols "around a table". While there are 6! sequences consisting of a linear arrangement of the symbols between parentheses, two symbols represent the same permutation iff one can be transformed into the other "cyclically". There are 5! such arrangements.
2. There are $\binom{6}{3} = 20$ ways of dividing 6 objects into two sets of 3, *where the sets are labelled*. Here the objects are to be divided into two sets, which will be permuted separately; the order of the 2 3-cycles in the symbol is not relevant. Thus the number of partitions of the elements into two sets of 3 is $\frac{1}{2!}\binom{6}{3} = 10$. Each of the sets of 3 can be arranged in $(3-1)! = 2$ ways; in all we have $10 \times 2! \times 2! = 40$ distinct permutations of this type.
3. Unlike the preceding case, because the two orbits have different size, there is no need to compensate for the permutability of the cycles, which are distinguishable by their sizes. The total number of permutations of this type is $\binom{6}{2} \times (2-1)! \times (4-1)! = 90$.
4. The number of partitions into 3 *distinguishable* subsets of 2 each is $\binom{6}{2}\binom{6-2}{2} = \frac{6!}{2!2!2!} = 90$; however, 3 indistinguishable orbits of the same size could be labelled to render them distinguishable in $3! = 6$ ways; hence the number of partitions into *indistinguishable* sets of 2 is $\frac{90}{3!} = 15$. The points within each orbit may be arranged cyclically in $(2-1)! = 1! = 1$ way.

We follow the convention that some or all 1-cycles may be suppressed from the symbol. Thus, in Example A.3.1.3, we have abbreviated (12)(3) to simply (12).

A.3.1.8 Exercise. Let the vertices of a pentagon be labelled with the symbols 1, 2, 3, 4, 5. Considering this as a graph C_5 with edges 12, 23, 34, 45, 51, determine those permutations f of the set $\{1,2,3,4,5\}$ which are isomorphisms of C_5 — i.e. such that $f(i)$ is adjacent to $f(j)$ iff i is adjacent to j in the graph C_5; in the case of the present graph, f is an isomorphism iff $f(i)$ is adjacent to $f(i+1)$ for all[332] i. Write each of those permutations in 3 ways:

[332] arguments modulo 5

- in the 2-line matrix notation;
- in the disjoint cycle notation;
- in the *reduced* disjoint cycle notation, with fixed points suppressed.

For each permutation, indicate which permutation is its inverse.

Solution: Suppose that the point 1 is mapped on to the point i. Its neighbours, 5 and 2 must therefore be mapped on to the points $i \pm 1$ in either of two ways; in the former case we obtain the permutation (1)(25)(34), and, in the latter case, (1)(2)(3)(4)(5). This permutation has one fixed point, and interchanges the other four vertices in pairs; geometrically, it may be viewed as a *reflection* in a mirror through the vertex 1. Evidently there will be 4 other reflections, in mirrors through the other four vertices, respectively: (2)(31)(45), (3)(42)(51), (4)(53)(12), (5)(14)(23).

Another type of isomorphism not yet listed is the rotations. Evidently (12345) is a rotation through one vertex; its powers will also be isomorphisms:

$$\begin{aligned} (12345)^2 &= (13524) \\ (12345)^3 &= (14253) \\ (12345)^4 &= (15432) \\ (12345)^5 &= (1)(2)(3)(4)(5) \qquad \text{(already listed).} \end{aligned}$$

Can we be sure that we have found all isomorphisms of the pentagon? Suppose that f is any isomorphism. We have already argued for uniqueness when $f(1) = 1$. Suppose that $f(1) = i$. There exists some power of (12345) which maps i on to 1 — namely the $(6-i)$th power. Then the product

$$(12345)^{6-i} f$$

is an isomorphism of the pentagon which fixes 1; hence it coincides with either I or (25)(34); it follows that f is equal to either $(12345)^{-6+i}$ or to $(12345)^{-6+i}(25)(34)$; the first possibility is one of the rotations; the second can be shown to be the reflection in the mirror through $2i - 1$ (all vertices are taken modulo 5).

$$\begin{aligned} \begin{pmatrix} 12345 \\ 12345 \end{pmatrix} &= (1)(2)(3)(4)(5) = I = I^{-1} \\ \begin{pmatrix} 12345 \\ 15432 \end{pmatrix} &= (1)(25)(34) = (25)(34) = \begin{pmatrix} 12345 \\ 15432 \end{pmatrix}^{-1} \\ \begin{pmatrix} 12345 \\ 51234 \end{pmatrix} &= (15432) = \begin{pmatrix} 12345 \\ 23451 \end{pmatrix}^{-1} \end{aligned}$$

$$\begin{array}{rcl}
\left(\begin{array}{c} 12345 \\ 21543 \end{array}\right) & = & (12)(35)(4) = (12)(35) = \left(\begin{array}{c} 12345 \\ 21543 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 45123 \end{array}\right) & = & (14253) = \left(\begin{array}{c} 12345 \\ 34512 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 32154 \end{array}\right) & = & (13)(2)(45) = (13)(45) = \left(\begin{array}{c} 12345 \\ 32154 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 34512 \end{array}\right) & = & (13524) = \left(\begin{array}{c} 12345 \\ 45123 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 43215 \end{array}\right) & = & (14)(23)(5) = (14)(23) = \left(\begin{array}{c} 12345 \\ 43215 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 23451 \end{array}\right) & = & (12345) = \left(\begin{array}{c} 12345 \\ 51234 \end{array}\right)^{-1} \\
\left(\begin{array}{c} 12345 \\ 54321 \end{array}\right) & = & (15)(24)(3) = \left(\begin{array}{c} 12345 \\ 54321 \end{array}\right)^{-1}
\end{array}$$

A.3.2 Multiplication (Composition) of Permutations

A.3.2.1 DEFINITION. Let $f : \mathfrak{A} \longrightarrow \mathfrak{A}$ and $g : \mathfrak{A} \longrightarrow \mathfrak{A}$ be permutations. We define the *product* fg to be the composition $f \circ g : \mathfrak{A} \longrightarrow \mathfrak{A}$, i.e. $fg(x) = f(g(x)) \forall x \in \mathfrak{A}$, i.e. g followed by f. (Warning! Many algebraists define fg to be the composition $g \circ f$, i.e. f *followed by* g. That convention can be justified in several ways, including the fact that English is written from left to right; we are adhering to the "right-to-left" convention[333] to remain consistent with the text-book used by students in 189-240A.)

To evaluate a product

$$\left(\begin{array}{cccc} a_1 & a_2 & ... & a_n \\ a_{j_1} & a_{j_2} & ... & a_{j_n} \end{array}\right)\left(\begin{array}{cccc} a_1 & a_2 & ... & a_n \\ a_{i_1} & a_{i_2} & ... & a_{i_n} \end{array}\right) = \left(\begin{array}{cccc} a_1 & a_2 & ... & a_n \\ & & ... & \end{array}\right).$$

we follow each element through the first i.e. rightmost array, then the left array; a_1 is mapped on to a_{i_1} by the first function; we then scan the *upper* row of the left array until we find a_{i_1}, then look below it to find the ultimate image of a_1 under the composition of the two functions: this is what is written under a_1 in the product.

Where the factors are written in disjoint cycle notation, we begin by writing a left parenthesis (; then we select an arbitary element — say 1 — of the set of point and

[333]Note that the convention we are using in connection with individual cycles is "left-to-right", in that we are interpreting a cycle $(\ldots ij \ldots)$ as stating that $i \mapsto j$.

follow it through successive mappings until its image — call it i — is determined, then write that image after i: $(1\,i\,....$ We continue this process, next determining the image of i, until we reach a point whose image is a point whose name is already written in our product; here we close with a right parenthesis); if not all points have been accounted for, we open a new left parenthesis, (, and continue. The process terminates when all points have been accounted for; of course, 1-cycles may be suppressed.

A.3.2.2 EXAMPLE.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & \downarrow & & & \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & & & & & \\ 3 & 1 & 4 & 6 & 5 & 2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & & & & & \end{pmatrix}$$

$$(1)(\underline{\underline{23}})(4)(56) \cdot (1\underline{3}462)(5) = (12...$$

A.3.2.3 EXERCISE. Fill in the following table (called the *Cayley table*) to show all products of permutations f and g of the set $\{1, 2, 3\}$.

f \ g	I	(12)	(23)	(13)	(123)	(132)
I						
(12)						
(23)						
(13)						
(123)						
(132)						

A.3.2.4 EXERCISE. 1. Construct a Cayley table for products of all powers of the permutation (12345).

2. Construct a Cayley table for products of all powers of the permutation (123456).

3. For each of the preceding 2 cases, list the types of disjoint cycle decompositions that appear, and the number of permutations of each type. (For example, $(123456)^3$ has disjoint cycle decomposition of the form $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)$.)

4. Construct a Cayley table for the group of symmetries of a square with vertices labelled 1, 2, 3, 4, writing all group elements in disjoint cycle notation.

Solution:

1.

f \ g	I	(12345)	(13524)	(14253)	(15432)
I	I	(12345)	(13524)	(14253)	(15432)
(12345)	(12345)	(13524)	(14253)	(15432)	I
(13524)	(13524)	(14253)	(15432)	I	(12345)
(14253)	(14253)	(15432)	I	(12345)	(13524)
(15432)	(15432)	I	(12345)	(13524)	(14253)

2.

f \ g	I	(123456)	(135)(246)	(14)(25)(36)	(153)(264)	(165432)
I	I	(123456)	(135)(246)	(14)(25)(36)	(153)(264)	(165432)
(123456)	(123456)	(135)(246)	(14)(25)(36)	(153)(264)	(165432)	I
(135)(246)	(135)(246)	(14)(25)(36)	(153)(264)	(165432)	I	(123456)
(14)(25)(35)	(14)(25)(36)	(153)(264)	(165432)	I	(123456)	(135)(246)
(153)(264)	(153)(264)	(165432)	I	(123456)	(135)(246)	(14)(25)(35)
(165432)	(165432)	I	(123456)	(135)(246)	(14)(25)(35)	(153)(264)

3. The group consisting of all powers of (12345) contains, beside the identity, of disjoint cycle decomposition type $(\cdot)(\cdot)(\cdot)(\cdot)(\cdot)$, 4 permutations all of type $(\cdot\cdot\cdot\cdot\cdot)$.

   The group consisting of all powers of (123456) contains

   - the identity, of type $(\cdot)(\cdot)(\cdot)(\cdot)(\cdot)(\cdot)$,
   - two permutations of type $(\cdot\cdot\cdot\cdot\cdot\cdot)$,
   - two permutations of type $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)$,
   - one permutation of type $(\cdot\cdot\cdot)(\cdot\cdot\cdot)$.

4.

	e	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(23)	(24)
e	e	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(23)	(24)
(1234)	(1234)	(13)(24)	(1432)	e	(13)	(14)(23)	(24)	(12)(34)
(13)(24)	(13)(24)	(1432)	e	(1234)	(14)(23)	(24)	(12)(34)	(13)
(1432)	(1432)	e	(1234)	(13)(24)	(24)	(12)(34)	(13)	(14)(23)
(12)(34)	(12)(34)	(24)	(14)(23)	(13)	e	(1432)	(13)(24)	(1234)
(13)	(13)	(12)(34)	(24)	(14)(23)	(1234)	e	(1432)	(13)(24)
(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(13)(24)	(1234)	e	(1432)
(24)	(24)	(14)(23)	(13)	(12)(34)	(1432)	(13)(24)	(1234)	e

We may interpret a product (332) as being a product of cycles in the broader sense, i.e. of permutations having at most one orbit containing more than one point, namely as a product fgh, where

$$\begin{aligned} f &= (u_1\, u_2 \ldots u_r)(v_1)(v_2)\ldots(v_s)\ldots(w_1)(w_2)\ldots(w_t) \\ g &= (u_1)(u_2)\ldots(u_r)(v_1\, v_2 \ldots v_s)\ldots(w_1)(w_2)\ldots(w_t) \\ h &= (u_1)(u_2)\ldots(u_r)(v_1)(v_2)\ldots(v_s)\ldots(w_1\, w_2 \ldots w_t) \end{aligned}$$

This proves

A.3.2.5 THEOREM. *Every permutation is expressible as a product of disjoint cycles.*

Any permutation may also be expressed as a product of *non-disjoint* permutations, in infinitely many ways. Such representations are occasionally of interest, if we wish to show that a certain set of permutations *generate*[334] a larger set.

A.3.2.6 EXERCISE. 1. Show that every cycle involving only symbols from the set $\{1, 2, ..., n\}$ is expressible as a product of transpositions of the form $(1k)$, where $k \in \{2, ..., n\}$

2. Show that every cycle involving only symbols from $\{1, 2, ..., n\}$ is expressible as a product of transpositions of the form $(k\ k+1)$, where $k \in \{1, 2, ..., n-1\}$.

3. (More difficult) Show that every cycle involving only an odd number of symbols from $\{1, 2, ..., n\}$ is expressible as a product of cycles of length 3. (Hint: Use one of the preceding decompositions, grouping successive pairs of transpositions. We shall see later that this type of decomposition is impossible for cycles of even length.)

4. By appealing to Theorem A.3.2.5, show that every permutation of the set $\{1, 2, ..., n\}$ is expressible as a product of transpositions of the form $(1k)$ and also as a product of transpositions of the form $(k\,k+1)$.

5. Show that every permutation of $\{1, 2, ..., n\}$ is expressible as a product of the two permutations (12) and (123...n) (unlimited repetitions permitted). Using a term that is to be defined later, you are to prove that the two permutations (12) and (123...n) *generate* the symmetric group.

Solution

1. Generalize from $(123...m) = (1m)(1 \quad m-1)(1 \quad m-2)...(13)(12)$; $(23...m) = (1m)(1 \quad m-1)(1 \quad m-2)...(13)(12)(1m)$.

2. First observe that $(13) = (23)(12)(23)$, then that $(14) = (34)(23)(12)(23)(34)$. For any n,
$$(1n) = (n-1 \quad n)(1 \quad n-1)(n-1 \quad n)\,.$$
Hence, by induction, every transposition $(1n)$ is expressible as a product of transpositions of the form $(k\ k+1)$. Such products, when substituted into the decomposition of the preceding part, yield an expression of any cycle as a product of this type of transpositions.

3. It suffices to observe that the product of two transpositions whose 2-cycles overlap in one point is a 3-cycle: $(12)(23) = (123)$. The argument of the preceding part can be refined to show that successive transpositions in the factorization

[334]This term will be defined precisely later.

have this property. However, that isn't necessary: if we ever meet two successive transpositions without this property, like (12)(34), we can replace this by (12)(23)(23)(34) without changing the *parity* of the number of transpositions.[335] Hence (12)(34) = (123)(234), a product of 3-cycles.

4. We have proved that cycles admit the desired decompositions. But every permutation is a product of cycles, hence a product of transpositions.

5. $$(12...n)(12)(12...n)^{-1} = (12...n)(12)(1\ n\ n-1\ ...\ 2) = (23)\,.$$

   Hence
   $$(12...n)^{r-1}(12)\left((12...n)^{-1}\right)^{r-1} = (r\ r+1)\,.$$

   for $r = 1, 2, ..., n-1$. (We have not yet formalized the concept of exponentiation. Here the intention is, for the first factor, the product of $r-1$ copies of the cycle $(12...n)$. For the last factor we intend the product of the same number of copies of the inverse permutation, i.e. of $(12...n)^{n-1}$ or $(1\ n\ n-1\ ...\ 1)$. The properties of exponentiation will be studied following Definition A.4.2.13.)

A.3.3 Groups of permutations

Examination of the Cayley table of Exercise A.3.2.3 shows a number of interesting structural features:

- No symbol is repeated in any one row, nor in any one column.
- The symbols appearing in any row or column are precisely those which index the rows and columns — i.e. every product of permutations in the set under consideration is again in the set.
- For every permutation f considered, there exists some permutation — *possibly* f *itself* such that $fg = I$, and some permutation h such that $hf = I$.

These properties, together with one which derives from the associativity of composition of functions, define the algebraic structure we call a *permutation group*

A.3.3.1 Definition. Let $\mathcal{G}$ be a set of permutations of a set $\mathfrak{A}$ with the following properties:

1. The identity permutation is contained in $\mathcal{G}$.

[335] *Parity* means "evenness" or "oddness". More precisely, an integer m has *even parity* if it is divisible by 2, otherwise it has *odd parity*.

2. If $f \in \mathcal{G}$, then $f^{-1} \in \mathcal{G}$.[336]

3. If $f \in \mathcal{G}$ and $g \in \mathcal{G}$, then $fg \in \mathcal{G}$.

Then $\mathcal{G}$ is called a *permutation group* acting on $\mathfrak{A}$.

When we come to generalize the preceding definition, we shall describe the second property as *Closure under Inverses*, and the third as *Closure under Composition*.

A.3.3.2 THEOREM. *Let $\mathfrak{A}$ be a given set.*

1. *The set of all permutations of $\mathfrak{A}$ is a permutation group.*

2. *The set consisting of only the identity function is a permutation group.*

A.3.3.3 EXERCISE. Prove Theorem A.3.3.2.

A.3.3.4 DEFINITION. The group of all permutations of $\mathfrak{A}$ is called the *symmetric group*, and denoted by $\mathcal{S}_{\mathfrak{A}}$. Where $\mathfrak{A} = \{1, 2, ..., n\}$, the group is often denoted by $\mathcal{S}_n$, and may be called the *symmetric group on n letters*.

A.3.3.5 EXERCISE. 1. Where a subset of a permutation group is also a permutation group, we call it a *(permutation) subgroup*. Determine all subgroups of the group $\mathcal{S}_3$, whose elements were determined in Example A.3.1.3

2. Determine all subgroups of the group of symmetries of the pentagon graph, C_5, considered in Exercise A.3.1.8. (The symmetry group of the pentagon is called the *dihedral* group, and usually denoted by[337] $\mathcal{D}_5$.)

3. Determine as many subgroups of the group $\mathcal{D}_6$ of symmetries of the hexagon graph, C_6, as you can. (At this point you may lack the machinery to solve this problem exhaustively.)

Solution:

1. Every subgroup contains the identity. By Theorem A.3.3.2 the identity is a subgroup.

   The transpositions are each their own inverse. Hence each of the three transpositions forms, with the identity, a subgroup, said to be *of order 2*.

[336] Since f is a bijection, it has a unique inverse mapping.
[337] But some authors denote this group by $\mathcal{D}_{10}$.

Suppose that a subgroup contains two 2-cycles, say — without limiting generality — (12) and (23). Then it also contains (12)(23)(12) = (13), also (12)(23) = (123) and (23)(12) = (132), i.e. it is all of $\mathcal{S}_3$. The same holds where a subgroup contains one transposition and one 3-cycle.

Finally, can a subgroup (different from the "trivial" subgroup) contain no transpositions? The square of each of the 3-cycles is the other 3-cycle; any subgroup containing one must therefore contain the other. These — with the identity — form a subgroup *of order 3*.

2. (to be completed)

3. (to be completed)

A.3.3.6 EXERCISE. It is not necessary to check all of the conditions of Definition A.3.3.1 for a subset $\mathcal{H}$ of a permutation group $\mathcal{G}$ to determine whether $\mathcal{H}$ is a permutation subgroup. Prove that if

1'. $\mathcal{H}$ is not empty

and $\mathcal{H}$ satisfies conditions 2 and 3, then it will also satisfy condition 1[338].

Solution: Suppose that $g \in \mathcal{G}$. By condition 2, $g^{-1} \in \mathcal{G}$. Then, by condition 3, $gg^{-1} \in \mathcal{G}$, i.e. condition 1 is satisfied.

A.3.3.7 EXERCISE. Let $\mathfrak{A}$ be the set of points on the unit circle in $\mathbb{R}^2$, i.e. $\{(\cos\theta, \sin\theta) : 0 \leq \theta < 2\pi\}$, For any real numbers α, β, define functions f_α and g_β respectively by

$$f_\alpha(\cos\theta, \sin\theta) = (\cos(\theta + \alpha), \sin(\theta + \alpha))$$

$$g_\beta(\cos\theta, \sin\theta) = (\cos(2\beta - \theta), \sin(2\beta - \theta))$$

The first function acts geometrically as a rotation counterclockwise through an angle of α; the second acts as a reflection in a mirror inclined at an angle of β to the positive x-axis.

1. Before considering the following questions you should convince yourself that these functions are *well defined*, by showing that every point on the unit circle has just one associated argument θ in the interval $0 \leq \theta < 2\pi$.

2. Show that $f_\alpha g_\beta = g_\beta f_{-\alpha}$.

3. Show that $f_\alpha f_\beta = f_{\alpha+\beta}$.

[338] We shall prove a stronger result below for *finite* $\mathcal{H}$. In that case conditions 1' and 3 will be sufficient!

4. Determine a real number α such that $g_{\beta_1} g_{\beta_2} = f_\alpha$.

5. Show that $g_{\beta_1} g_{\beta_2} \neq g_{\beta_2} g_{\beta_1}$ unless $\beta_1 - \beta_2$ is an integer multiple of $\frac{\pi}{2}$.

A.3.3.8 DEFINITION. Let $\mathcal{G}$ be a permutation group acting on a set $\mathfrak{A}$. Let $a_1 \in \mathfrak{A}$, $a_2 \in \mathfrak{A}$. We say that a_1 *is* $\mathcal{G}$*-equivalent to* a_2 iff there exists $f \in \mathcal{G}$ such that $f(a_1) = a_2$.

A.3.3.9 THEOREM. *$\mathcal{G}$-equivalence is an equivalence relation.*

A.3.3.10 EXERCISE. Prove Theorem A.3.3.9.

A.3.3.11 EXAMPLE. For any fixed integer $a \in \mathbb{Z}$, define the function $\phi_a : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $n \longmapsto n + a$; thus ϕ is a *translation* to the right by a. Then ϕ_a is a bijection: its inverse is ϕ_{-a}. (Note that we are working here with an infinite set; it is not sufficient to prove only that ϕ_a is one-to-one, or only that ϕ_a is onto. By exhibiting the inverse we show that ϕ_a is bijective: since $\phi_{-a}\phi_a = 1$, ϕ_a is one-to-one; since $\phi_a\phi_{-a} = 1$, ϕ_a is onto.) For any $b \in \mathbb{Z}$, $\phi_a\phi_b = \phi_{a+b}$. The set of all positive *and negative* powers of ϕ_a and the identity mapping $\iota_{\mathbb{Z}} = \phi_0 : \mathbb{Z} \longrightarrow \mathbb{Z}$ form a permutation group. If two integers n_1 and n_2 are equivalent under the action of this group, we say that they are *congruent modulo* a, and write

$$n_1 \equiv n_2 \pmod{a}.$$

Thus two integers are congruent modulo a iff they differ by a multiple of a.

A.3.4 Invariance under a Permutation Group

Think of a group $\mathcal{G}$ of permutations of a set $\mathfrak{A}$ as "moving" the elements of $\mathfrak{A}$ about. This explains the term *fixed point* defined in Definition A.3.1.5: a fixed point of a permutation f is a point that is not moved by f.

A.3.4.1 DEFINITION. Let $\mathcal{G}$ be a permutation group acting on $\mathfrak{A}$, and let $\mathfrak{B} \subseteq \mathfrak{A}$.

1. If no element of $\mathcal{G}$ moves any element of $\mathfrak{B}$ outside of $\mathfrak{B}$ — i.e. if

$$\left.\begin{array}{c} g \in \mathcal{G} \\ b \in \mathfrak{B} \end{array}\right\} \Rightarrow g(b) \in \mathfrak{B},$$

   we say that $\mathfrak{B}$ is *invariant under (the action of)* $\mathcal{G}$.

2. A point $a \in \mathfrak{A}$ is a *fixed point* of $\mathcal{G}$ if $\{a\}$ is invariant under $\mathcal{G}$. We may also say that the functions in $\mathcal{G}$ *fix* a.

3. Let $a \in \mathfrak{A}$. The set of points $\{g(a) : g \in \mathcal{G}\}$ is called the *orbit* of $\mathcal{G}$ containing a, and may be denoted by[339] $a^{\mathcal{G}}$ or $\mathcal{G}(a)$ (not to be confused with $\mathcal{G}_a$, which is a group.)

4. Where $\mathcal{G}$ has only one orbit, the group is said to be *transitive*.

A.3.4.2 EXERCISE. 1. Prove that the orbits of $\mathcal{G}$ are the equivalence classes of the $\mathcal{G}$-equivalence relation.

2. Prove that a point is a fixed point iff its orbit contains no points other than itself.

3. Prove that a subset is invariant iff it is a union of orbits.

A.3.4.3 EXERCISE. 1. Let $\mathbb{R}^n$ be the vector space of ordered real n-tuples, written as column matrices $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Prove that the set of non-singular linear transformations of $\mathbb{R}^n$ constitute a permutation group. Show that the zero vector is a fixed point of this permutation group. Assuming the theorem that any set of independent vectors can be extended to a basis of the vector space, show that there is only one other orbit of this group. The group is known as the *general linear group*. Once a coordinate system $\vec{e}_1$, $\vec{e}_2$, ..., $\vec{e}_n$ has been fixed, every linear transformation $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ can be represented by an $n \times n$ non-singular matrix $[T]_{\vec{e}_1,\vec{e}_2,...,\vec{e}_n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$, whose columns are the coordinate vectors of the images of the basis vectors $\vec{e}_1$, $\vec{e}_2$, ..., $\vec{e}_n$; the action is given by

$$T \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} .$$

This group, when represented by the set of non-singular $n \times n$ real matrices, is often denoted by $GL(n, \mathbb{R})$.

[339] This notation is consistent with composition of functions "on the right", and with writing functions as exponents; since we are composing "on the left", the notation $\mathcal{G}(a)$ may be preferable here.

2. Show that the set of $n \times n$ real matrices having determinant ± 1 form a subgroup of $GL(n, \mathbb{R})$.

3. Show that the set of $n \times n$ real matrices having determinant 1 form a subgroup of $GL(n, \mathbb{R})$. This group is called the *special linear group*, and may be denoted by $SL(n, \mathbb{R})$. Determine the orbits of $\mathbb{R}^1$ under the action of $SL(1, \mathbb{R})$.

4. (More difficult) Determine the orbits of $\mathbb{R}^2$ under the action of $SL(2, \mathbb{R})$.

Solution:

1. For any real $n \times n$ matrix A, and $\vec{0} \in \mathbb{R}^n$, $A\vec{0} = \vec{0}$. Thus $\vec{0}$ is a fixed point of $\mathbb{R}^n$ under the action of $GL(n, \mathbb{R})$.

   Now let *non-zero* vectors $\vec{b_1} = \begin{pmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{pmatrix}$, $\vec{c_1} = \begin{pmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{n1} \end{pmatrix}$ be given. Extend $\vec{b_1}$ to a basis $\{\vec{b_1}, \vec{b_2}, ..., \vec{b_n}\}$, and extend $\vec{c_1}$ to a basis $\{\vec{c_1}, \vec{c_2}, ..., \vec{c_n}\}$. Then the nonsingular matrices

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}, \qquad C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$$

   represent permutations of $\mathbb{R}^n$. The matrix CB^{-1} then represents the permutation mapping $\vec{b_1}$ onto[340] $\vec{c_1}$. It follows that all non-zero vectors in $\mathbb{R}^n$ constitute a second orbit of $GL(n, \mathbb{R})$.

2. If a matrix has determinant ± 1, it is invertible, and its inverse has the same property; hence the set is closed under the taking of inverses. As the product of two matrices of determinant ± 1 has determinant[341] ± 1, the set is closed under composition. Finally, the identity matrix has determinant 1, so it is a member.

[340] Purists claim that the word *onto* does not exist in the English language; mathematicians are accustomed to introducing extensions whenever they are expedient, and have admitted *onto* both as a preposition and as an adjective! Another example of extended mathematical English (French) is the word *iff* (*ssi*).

[341] We are violating a convention here, which is that where the $\pm$ sign is used more than once in a discussion, the reader is to interpret the signs as being always the upper sign, or always the lower; for that purpose the symbol $\mp$ is available where signs are reversed. Here our intention is only that the product of the determinants is in the set $\{-1, 1\}$.

3. The same reasoning as in the previous part shows that these matrices form a subgroup of $GL(n,\mathbb{R})$.

   $SL(1,\mathbb{R})$ consists of 1×1 matrices of determinant 1, i.e. only of the matrix $(\ 1\ )$. Under this permutation every vector in $\mathbb{R}^1$ is fixed, i.e. forms its own orbit.

4. The zero vector again is a fixed point.

   We shall show that every non-zero vector $\vec{c}=\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ is equivalent to the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$; hence all non-zero vectors consistute a second orbit. We need only observe that, if $c_1 \neq 0$,

   $$\begin{pmatrix} c_1 & 0 \\ c_2 & c_1^{-1} \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \end{pmatrix};$$

   while, if $c_2 \neq 0$,

   $$\begin{pmatrix} c_1 & -c_2^{-1} \\ c_2 & 0 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

   In both cases the 2×2 matrix has determinant 1.

Suppose that f and g are both permutations of $\mathfrak{A}$ that *fix* a point $a\in\mathfrak{A}$ (i.e. for which a is a fixed point). Then $fg(a)=f(g(a))=f(a)=a$. Also, if ι is the identity mapping on $\mathfrak{A}$, then

$$a=\iota(a)=(f^{-1}f)(a)=f^{-1}(f(a))=f^{-1}(a)\,,$$

so f^{-1} also fixes a. It follows that the set of permutations which fix a is "closed under composition" and "closed under the taking of inverses". Since $1:\mathfrak{A}\longrightarrow\mathfrak{A}$ also fixes a, we have proved

A.3.4.4 THEOREM. *Let $\mathcal{G}$ be any group of permutations of $\mathfrak{A}$. Then the permutations in $\mathcal{G}$ which fix an element $a\in\mathfrak{A}$ form a subgroup of $\mathcal{G}$.*

A.3.4.5 DEFINITION. The subgroup of a permutation group $\mathcal{G}$ acting on $\mathfrak{A}$, consisting of those permutations which fix $a\in\mathfrak{A}$, is called the *stabilizer* of a, and will be denoted by $\mathcal{G}_a$.

A.3.4.6 THEOREM. *Let $\mathcal{G}$ be a permutation group acting on a set $\mathfrak{A}$. Suppose that $g\in\mathcal{G}$, $a\in\mathfrak{A}$. Then the mapping*

$$f\longmapsto gfg^{-1} \tag{340}$$

of $\mathcal{G}$ induces a bijection between $\mathcal{G}_a$ and $\mathcal{G}_{g(a)}$. Thus elements of $\mathfrak{A}$ lying in the same orbit of $\mathcal{G}$ have stabilizers containing the same numbers of elements.[342]

Proof: $f \in \mathcal{G}_{g(a)} \Leftrightarrow f(g(a)) = g(a) \Leftrightarrow g^{-1}fg(a) = a \Leftrightarrow g^{-1}fg \in \mathcal{G}_a$. Thus the mapping (340) is a bijection. The proof that it is a homomorphism is left to the student. □

A.3.4.7 Exercise. Determine the following stabilizers:

1. in $GL(2,\mathbb{R})$, the stabilizer of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$;
2. in $\mathcal{D}_6$ (the dihedral group of symmetries of the hexagon), the stabilizer of any vertex.
3. in $GL(3,\mathbb{R})$, the stabilizer of the point $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, and the stabilizer of the point $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.
4. in $\mathcal{D}_8$ (the dihedral group of symmetries of the octagon), the stabilizer of each vertex.

Solution:

1. $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ iff
$$a_{11} + a_{12} = 1 = a_{21} + a_{22}\,.$$
The stabilizer therefore consists of all matrices $\begin{pmatrix} \alpha & 1-\alpha \\ 1-\beta & \beta \end{pmatrix}$ such that $\alpha+\beta \neq 1$.
2. If vertex 1 is fixed, vertex 2 is mapped either on to 6 or on to 2; in the latter case the permutation is I; in the former case it is (1)(26)(35)(4), briefly (26)(35). These two permutations constitute the stabilizer of 1.

[342]Indeed, these groups can be shown to have the same structure, not merely in the sense of abstract groups, to be defined below §A.5, but even in the stronger sense that one can be obtained from the other by a relabelling of the elements of $\mathfrak{A}$; in particular, corresponding elements (under the bijection described above) have the same cycle structure.

3. (a)
$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a_{11} \\ a_{21} \\ a_{23} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$
Thus the stabilizer of $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ consists of all real matrices of the form
$$\begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}.$$

   (b) The zero vector is mapped on to itself by any linear transformation. Conversely, a non-singular transformation has only the zero vector in its kernel (null space), so the stabilizer of zero consists of all elements of $GL(3, \mathbb{R})$.

4. Without limiting generality, we determine the stabilizer of the point 1. The rotations — powers of (12345678) all move this point, except for the identity rotation, which fixes it. As for the reflections, only the reflection (1)(5)(28)(37)(46) fixes this point. Thus the stabilizer of 1 consists of the group of order 2 generated by (1)(5)(28)(37)(46). In general, the stabilizer of a vertex consists of the reflection whose "mirror" passes through that point, and the identity.

A.3.4.8 Exercise. For a single point $a \in \mathfrak{A}$, a is invariant under the action of a group $\mathcal{G}$ of permutations iff a is a fixed point for $\mathcal{G}$. However, for larger subsets, the concept of invariance is weaker than that of being "pointwise fixed".

1. For example, in the proof above that the permutations fixing a point form a subgroup, we proved that the inverse of a permutation fixing a point also fixes that point. Consider the set $\mathbb{R}$ and the function $x \longmapsto \dfrac{x}{2}$ to construct a permutation $f : \mathbb{R} \longrightarrow \mathbb{R}$ and a subset $\mathfrak{B} \subset \mathbb{R}$ which is invariant under f but not under f^{-1}.

2. But show that if f and g are permutations of $\mathfrak{A}$, and $\mathfrak{B} \subseteq \mathfrak{A}$, then
$$\left.\begin{array}{l} f(\mathfrak{B}) \subseteq \mathfrak{B} \\ g(\mathfrak{B}) \subseteq \mathfrak{B} \end{array}\right\} \Rightarrow fg(\mathfrak{B}) \subseteq \mathfrak{B}\,,$$

3. Show that a 1-dimensional subspace of $\mathbb{R}^2$ which is invariant under a subgroup of $GL(2, \mathbb{R})$ consists (in addition to the zero vector) of vectors which are each eigenvectors of all matrices in the subgroup. In particular, show that the matrices under which the x-axis is invariant constitute the group of upper triangular matrices, of the form $\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}$.

Solution:

1. Let $\mathfrak{B} = [-1, 1]$, $f(x) = \frac{x}{2}$. Then $f(\mathfrak{B}) = \left[-\frac{1}{2}, \frac{1}{2}\right] \subset \mathfrak{B}$. But $f^{-1}(\mathfrak{B}) = [-2, 2] \not\subseteq \mathfrak{B}$.

2. $fg(\mathfrak{B}) = f(g(\mathfrak{B})) \subseteq f(\mathfrak{B}) \subseteq \mathfrak{B}$.

3. Suppose that the 1-dimensional subspace B generated by a vector $\vec{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ is invariant under a subgroup $\mathcal{G}$. Then a matrix $A \in \mathcal{G}$ maps $\vec{b}$ on to $A\vec{b} \in B$, i.e. $A\vec{b}$ is a scalar multiple of $\vec{b}$, i.e. $\vec{b}$ is an eigenvector of A.
   The $x-axis$ is invariant under $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ iff the product $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is of the form $\begin{pmatrix} \lambda \\ 0 \end{pmatrix}$, i.e. iff $a_{21} = 0$. These *upper triangular* matrices form a subgroup. (Check for closure under inversion and under multiplication.)

A.3.5 Conjugacy classes of permutations

Let a cycle $(a_1a_2...a_r)$ be given, and consider the product $(b_1b_2)(a_1a_2...a_r)(b_1b_2)^{-1}$. If neither b_1 nor b_2 is a member of $\{a_1, a_2, ..., a_r\}$, it is obvious that $(b_1b_2)(a_1a_2...a_r)(b_1b_2)^{-1} = (a_1a_2...a_r)$. When precisely one of b_1, b_2 is in $\{a_1, a_2, ..., a_r\}$, say — without limiting generality — that $a_1 = b_1$, the product is equal to $(b_2a_2...a_r)$; finally, if both b_1 and b_2 are in $\{a_1, a_2, ..., a_r\}$, we can show that again, the effect of premultiplying by (b_1b_2) and then postmultiplying by the same transposition is to interchange the positions of b_1 and b_2 in $(a_1a_2...a_r)$ — which describes the result in the other cases as well! In every case, the result of this pair of operations is a cycle of the same length. More generally, by Exercise A.3.2.6, since every permutation is expressible as a product of transpositions, we have sketched a proof of the following result:

A.3.5.1 THEOREM. *Let f, g be permutations of the finite set $\mathfrak{A}$. Then gfg^{-1} is a permutation with the same cycle structure as f, obtainable by applying the permutation g to each of the points in the disjoint cycle symbol for f.*

A.3.5.2 EXERCISE. Prove the following corollary to Theorem A.3.5.1: Let f, h be permutations of a finite set $\mathfrak{A}$, having the same cycle structure. Then there exists a permutation $g \in \mathcal{S}_{\mathfrak{A}}$ such that $h = gfg^{-1}$.

Solution: To simply the exposition, let us assume that the elements of $\mathfrak{A}$ have been labelled 1, 2, ..., n. If permutations f and h have the same cycle structure, we may —

possibly in many ways — describe a permutation $g \in \mathcal{S}_{\mathfrak{A}}$ such that

$$\begin{aligned} f &= (a_{11}\ a_{12}\ ...\ a_{1r_1})(a_{21}\ a_{22}\ ...\ a_{2r_2})...(a_{k1}\ a_{k2}\ ...\ a_{kr_k}) \\ h &= (b_{11}\ b_{12}\ ...\ b_{1r_1})(b_{21}\ b_{22}\ ...\ b_{2r_2})...(b_{k1}\ b_{k2}\ ...\ b_{kr_k}) \\ g &= \begin{pmatrix} a_{11} & a_{12} & ... & a_{1r_1} & a_{21} & a_{22} & ... & a_{2r_2} & ... & a_{k1} & a_{k2} & ... & a_{kr_k} \\ b_{11} & b_{12} & ... & b_{1r_1} & b_{21} & b_{22} & ... & b_{2r_2} & ... & b_{k1} & b_{k2} & ... & b_{kr_k} \end{pmatrix} \end{aligned}$$

Then $gfg^{-1} = h$. $\square$

A.3.5.3 EXERCISE. 1. Let $\mathcal{G}$ be a permutation group acting on $\{1, 2, ..., n\}$, i.e. a subgroup of $\mathcal{S}_n$. Let f be any permutation in $\mathcal{S}_n$, *not necessarily in* $\mathcal{G}$. Show that $\{fgf^{-1} : g \in \mathcal{G}\}$ is a subgroup of $\mathcal{S}_n$. We say that this subgroup is *conjugate to* $\mathcal{G}$ (in $\mathcal{S}_n$)[343].

2. For the subgroups of the group S_3, studied in Exercise A.3.3.5, determine which pairs of subgroups are conjugate, and which elements effect this relationship.

3. For the subgroups of the group of symmetries of the pentagon graph, determined in Exercise A.3.3.5, determine which pairs of subgroups are conjugate, and which elements effect this relationship.

4. Show that the relation of conjugacy of subgroups is an equivalence relation.

5. Within any permutation group $\mathcal{G}$, we say that f is *conjugate* to g whenever there exists h such that $f = hgh^{-1}$. Show that conjugacy is an equivalence relation. The equivalence classes are called *conjugacy classes*.

6. (More difficult) Within the group $\mathcal{S}_4$ determine the conjugacy classes. (Hint: Use Theorem A.3.5.1.)

Solution:

1. (a) The permutation $fef^{-1} = e$ is contained in the set, so it is not empty.
   (b) $fg_1f^{-1}fg_2f^{-1} = f(g_1g_2)f^{-1}$, which is again a conjugate. Thus the set of conjugates by f is closed under composition.
   (c) $(fgf^{-1})^{-1} = fg^{-1}f^{-1}$, which is again a conjugate. Thus the set of conjugates is closed under the taking of inverses.

   These three properties ensure that the set of conjugates by a fixed permutation f form a subgroup.

[343] In these notes we will consider conjugacy of permutation groups only with reference to the full symmetric group.

2. Under conjugation by a fixed element f, any subgroup is transformed into a subgroup having the same order — indeed, permutations are transformed into permutations having the same cycle structure. Since there is only one subgroup of each of the orders 1 and 6, we know that each of the subgroups $\{e\}$ and $\mathcal{S}_3$ is "self"-conjugate.

   The remaining subgroups all have order 2. Define $\mathcal{G}_1 = \{e, (23)\}$, $\mathcal{G}_2 = \{e, (31)\}$, $\mathcal{G}_3 = \{e, (12)\}$. Then conjugation permutes these subgroups: for example,

$$\begin{aligned} (12)\mathcal{G}_3(12) &= \mathcal{G}_3 \\ (13)\mathcal{G}_3(13) &= \mathcal{G}_1 \\ (23)\mathcal{G}_3(23) &= \mathcal{G}_2 \\ (123)\mathcal{G}_3(132) &= \mathcal{G}_1 \\ (132)\mathcal{G}_3(123) &= \mathcal{G}_2 \end{aligned}$$

3. The subgroups of $\mathcal{D}_5$ are $\{e\}$, $\mathcal{C}_5$ (the group of rotations, generated by (12345)), 5 groups consisting of e and one reflection, and the whole group $\mathcal{D}_5$. As in the preceding problem, the subgroups $\{e\}$, $\mathcal{C}_5$, $\mathcal{D}_5$ (which are not *proper*) are all *self*-conjugate. The groups generated by one reflection are all mutually conjugate.

4. (a) If $\mathcal{G}_1$ consists of the conjugates of all elements of a subgroup $\mathcal{G}$ by a fixed element f, then $\mathcal{G}$ consists of all conjugates of elements of $\mathcal{G}_1$ by the fixed element f^{-1}. Thus conjugacy is a *symmetric* relation.

   (b) Conjugation by the fixed element e transforms a subgroup into itself; thus conjugacy is a *reflexive* relation.

   (c) Suppose that $\mathcal{G}_1$ consists of all conjugates of elements of $\mathcal{G}_0$ by a fixed element f_1, and that $\mathcal{G}_2$ consists of all conjugates of elements of $\mathcal{G}_1$ by a fixed element f_2. Then $\mathcal{G}_2$ consists of all conjugates of elements of $\mathcal{G}_0$ by the fixed element $f_2 f_1$, since $f_2(f_1 g f_1^{-1}) f_2^{-1} = (f_2 f_1) g (f_2 f_1)^{-1}$. Thus conjugacy is a *transitive* relation.

5. **Reflexivity:** For any element $f \in \mathcal{G}$, $f = efe^{-1}$.

   Symmetry: Suppose that $f = hgh^{-1}$. Then $g = (h^{-1})\, h\, (h^{-1})^{-1}$.

   Transitivity: Suppose that $f = hgh^{-1}$ and $g = k\ell k^{-1}$. Then $f = (hk)\ell(hk)^{-1}$.

6. The intention of this problem was to determine the conjugacy classes *of elements* of $\mathcal{S}_4$. By Theorem A.3.5.1these classes consist in each case of all permutations having the same cycle index. Thus the conjugacy classes are

$$\{(1)(2)(3)(4)\}$$

$$\{(1)(2)(34), (1)(3)(24), (1)(4)(23), (2)(3)(14), (2)(4)(13), (3)(4)(12)\}$$
$$\{(12)(34), (13)(24), (14)(23)\}$$
$$\{(1)(234), (1)(243), (2)(134), (2)(143), (3)(124), (3)(142), (4)(123), (4)(132)\}$$
$$\{(1234), (1243), (1324), (1342), (1423), (1432)\}$$

(Note that the situation would be more complicated if we did not have all elements of $\mathcal{S}_4$ available for conjugation purposes: then the partition into conjugacy classes could be a refinement of the above.)

A.3.6 Even and Odd Permutations. The Alternating Group.

We proved in Theorem A.3.2.5 that every permutation is expressible as a product of transpositions. While there are infinitely many ways in which this can be done, it can be shown that the *parity*[344] of the number of transposition factors is always the same.

A.3.6.1 THEOREM. *1. Let $a_{i,j} \in \mathfrak{A}$, $b_{i,k} \in \mathfrak{A}$, $(i = 1, 2)$, where $a_{1,j} \neq a_{2,j}$, $b_{1,k} \neq b_{2,k}$, $(j = 1, 2, ..., m)$, $(k = 1, 2, ..., n)$, and suppose that a certain permutation f of $\mathfrak{A}$ admits two factorizations as a product of transpositions:*

$$(a_{11}\, a_{12})(a_{21}\, a_{22})...(a_{m1}\, a_{m2}) = f = (b_{11}\, b_{12})(b_{21}\, b_{22})...(b_{n1}\, b_{n2})\,.$$

Then $m - n \equiv 0 \pmod 2$.

2. In any permutation group $\mathcal{G}$, the set of permutations expressible as products of an even number of transpositions constitutes a subgroup.

Proof: cf. [34, pp. 37–38], [1, §5.6] □

A.3.6.2 DEFINITION. 1. A permutation expressible as a product of an even number of transpositions is said to be *even*; a permutation which is not even is *odd*.

2. The subgroup of $\mathcal{S}_n$ consisting of the even permutations is called the *alternating group*, and denoted by $\mathcal{A}_n$.

Note that a cycle $(a_1 a_2 ... a_{2r})$ is odd, while a cycle $(a_1 a_2 ... a_{2r+1})$ is even!

[344] cf. Footnote 335

A.3.7 The Cycle Index of a Permutation Group

We shall require the following definitions in future applications to enumeration problems.

A.3.7.1 DEFINITION. Let $\mathcal{G}$ be a permutation group acting on a finite set $\mathfrak{A}$. Let x_1, x_2, ...x_n be n distinct *commuting*[345] "indeterminates"[346]. If an element $f \in \mathcal{G}$ admits a decomposition as a disjoint product

$$f = (\cdot)^{j_1}(\cdot\cdot)^{j_2}(\cdot\,\cdot\,\cdot)^{j_3}...(\cdot\,\cdot\,\cdot\,\cdot\,\cdot)^{j_n}$$

of j_1 1-cycles, j_2 2-cycles, ..., j_n n-cycles, we say that f has *cycle type*

$$z(f) = x_1^{j_1}x_2^{j_2}...x_n^{j_n}$$

The *cycle index* of $\mathcal{G}$ is defined to be the polynomial

$$Z(\mathcal{G}) = \frac{1}{|\mathcal{G}|}\sum_{\substack{f \\ f\in\mathcal{G}}} z(f)$$

(where $|\mathcal{G}|$ denotes the number of elements[347] in $\mathcal{G}$.)

Note that if $|\mathfrak{A}| = n$, the exponents in cycle type $x_1^{j_1}x_2^{j_2}...x_n^{j_n}$ have the property that

$$1 \cdot j_1 + 2 \cdot j_2 + ... + n \cdot j_n = n \tag{341}$$

A.3.7.2 EXERCISE. Determine the cycle index of each of the following permutation groups: $\mathcal{S}_n$ $(n = 1, 2, 3, 4, 5)$; $\mathcal{A}_n$ $(n = 1, 2, 3, 4, 5)$; $\mathcal{D}_n$ $(n = 3, 4, 5, 6)$

Solution:

1. $\mathcal{S}_1$: $\frac{1}{1!}x_1^1$
   $\mathcal{S}_2$: $\frac{1}{2!}\left(z(e) + z((12))\right) = \frac{1}{2!}\left(x_1^2 + x_2^1\right)$
   $\mathcal{S}_3$: $\frac{1}{3!}\left(z(e) + 3z((12)(3)) + 2z((123))\right) = \frac{1}{3!}\left(x_1^3 + 3x_2^1x_1^1 + 2x_3^2\right)$
   $\mathcal{S}_4$: $\frac{1}{4!}\left(x_1^4 + 3x_2^2 + 6x_2^1x_1^2 + 8x_3^1x_1^1 + 6x_4^1\right)$
   $\mathcal{S}_5$: $\frac{1}{5!}\left(x_1^5 + 10x_2x_1^3 + 15x_2^2x_1^1 + 20x_3^1x_2^1 + 20x_3^1x_1^2 + 30x_4^1x_1^1 + 24x_5^1\right)$

[345] i.e. Any product of these indeterminates may be rewritten as a product of powers of x_1, x_2, ... We may standardize our notation so that all products are of the form $x_1^{j_1}x_2^{j_2}...x_n^{j_n}$, where all exponents are non-negative. Moreover, in any sum of products, we may collect together all terms with the same respective exponents, and thereby obtain a polynomial with integer coefficients.

[346] Although the context is algebraic, there is no harm in thinking of these are distinct real variables.

[347] also called the *order* of $\mathcal{G}$

2. $\mathcal{A}_1$: $\frac{1}{1!}x_1^1$
   $\mathcal{A}_2$: $\frac{2}{2!}\left(z(e)\right) = \frac{2}{2!}x_1^2$
   $\mathcal{A}_3$: $\frac{2}{3!}\{z(e) + 2z((123))\} = \frac{2}{3!}\left(x_1^3 + 2x_3^1\right)$
   $\mathcal{A}_4$: $\frac{2}{4!}\left(x_1^4 + 3x_2^2 + 8x_3^1x_1^1\right)$
   $\mathcal{A}_5$: $\frac{2}{5!}\left(x_1^5 + 15x_2^2x_1^1 + 20x_3^1x_1^2 + 24x_5^1\right)$
3. $\mathcal{D}_3$: $\frac{1}{6}\left(z(e) + 3z((12)(3)) + 2z((123))\right) = \frac{1}{3!}\left(x_1^3 + 3x_2^1x_1^1 + 2x_3^2\right)$
   $\mathcal{D}_4$: $\frac{1}{8}\left(x_1^4 + 3x_2^2 + 2x_2^1x_1^2 + 2x_4^1\right)$
   $\mathcal{D}_5$: $\frac{1}{10}\left(x_1^5 + 4x_5^1 + 5x_2^2x_1^1\right)$
   $\mathcal{D}_6$: $\frac{1}{12}\left(x_1^6 + 2x_6^1 + 3x_2^2x_1^2 + 3x_2^3 + 2x_3^2 + 1x_2^3\right)$

A.3.7.3 THEOREM (CAUCHY-FROBENIUS-BURNSIDE). [348] *The total number of orbits of a permutation group $\mathcal{G}$ operating on a set $\mathfrak{A}$ is*

$$\frac{1}{|\mathcal{G}|}\sum_{\substack{f\\ f\in\mathcal{G}}}\left|\{a : f(a) = a\}\right|$$

Proof: We use a standard combinatorial device to solve this counting problem — we count the elements of a set in two different ways, equate the results, and solve for the number ω of orbits. The set whose elements we count is

$$\{(a, f) \in \mathfrak{A} \times \mathcal{G} : f(a) = a\}$$

the number of instances in which some point is fixed by some permutation. (In effect, we are reversing the order of summation in a finite sum.) From the point of view of the elements of $\mathcal{G}$, the number of such points is

$$\sum_{\substack{f\\ f\in\mathcal{G}}}\sum_{\substack{a\\ a\in\mathfrak{A}}} 1 = \sum_{\substack{f\\ f\in\mathcal{G}}}\left|\{a : f(a) = a\}\right|.$$

From the point of view of the points of $\mathfrak{A}$, the number of such ordered pairs is

$$\sum_{\substack{a\\ a\in\mathfrak{A}}}\sum_{\substack{f\\ f\in\mathcal{G}}} 1 = \sum_{\substack{a\\ a\in\mathfrak{A}}}\left|\mathfrak{G}_a\right|;$$

we thus have proved

$$\sum_{\substack{f\\ f\in\mathcal{G}}}\left|\{a : f(a) = a\}\right| = \sum_{\substack{a\\ a\in\mathfrak{A}}}\left|\mathfrak{G}_a\right|$$

[348] This theorem has been traditionally known as "Burnside's Lemma"; having been found in the earlier writings of Cauchy and Frobenius, it is now often styled the "Cauchy-Frobenius Lemma".

Let a_1, a_2, ..., a_N be a set of representatives of the orbits of $\mathcal{G}$ — i.e. one point selected from each of the orbits, and let n_1, n_2, ..., n_N be the numbers of points in each of those orbits. Then, by Theorem A.3.4.6, this last sum may be expressed as

$$\sum_{i=1}^{N} n_i \, |\mathcal{G}_{a_i}|$$

To complete the proof we need to appeal to Theorem A.5.4.18 (part 3), a consequence of "Lagrange's Theorem", which will be proved in the sequel. According to that result, each of the summands $\sum_{i=1}^{N} n_i \, |\mathcal{G}_{a_i}|$ is equal to $|\mathcal{G}|$.

A.3.7.4 Example. 1. Let $\mathcal{G} = \mathcal{D}_6$. We count the numbers of fixed points:

(a) (1)(2)(3)(4)(5)(6) fixes 6 points.

(b) Neither the rotation (135)(246), nor its inverse (=square) (153)(264) fixes any points.

(c) Neither of the rotations (123456), (165432) (its inverse = 5th power) fixes any points.

(d) One half-turn (14)(25)(36) fixes no points.

(e) Three "edge-centred" reflections like (14)(23)(56) each fix no points.

(f) Three "vertex-centred" reflections like (1)(26)(35)(4) each fix 2 points: total contribution $= 3 \times 2 = 6$.

In all, the number of orbits will be $\frac{1}{12}[1 \cdot 6 + 2 \cdot 0 + 2 \cdot 0 + 1 \cdot 0 + 3 \cdot 0 + 3 \cdot 2] = 1$. This is no surprise, as we know this group is transitive.

2. Analogously to the preceding example, the number of orbits of $\mathcal{C}_6$ is $\frac{1}{6}[1 \cdot 6 + 2 \cdot 0 + 2 \cdot 0 + 1 \cdot 0] = 1$, again, no surprise.

A.3.7.5 Example. A circular table has 6 seats, numbered in counterclockwise order 1, 2, 3, 4, 5, 6. A waiter is to serve 6 bowls of soup, 3 bouillons (B), 3 potages (P). You are to determine the number of distinct ways in which the soups may be served, if only the relative positions are significant, i.e. up to rotational symmetries.

Intuitively, we appear to be working with the cyclic group $\mathcal{C}_6$, which consists of the 6 powers of (123456). This is not quite correct, however: the group of rotational symmetries indeed has the structure of $\mathcal{C}_6$, but the set on which it is acting is not the symbols 1, 2, ..., 6. Rather, let us designate as $\mathfrak{A}$ the set of all possible assignments of soups to numbered positions. There are thus $\binom{6}{3} = 20$ elements in $\mathfrak{A}$; we may represent an element by a symbol $[x_1, x_2, ..., x_6]$, where x_i denotes the type of soup at position i on

the table, and is either a B or a P ($i = 1, 2, 3, 4, 5, 6$). We may still denote the elements of the group of symmetries by the familiar symbols, like (123456). The action is given by

$$(123456)[x_1x_2x_3x_4x_5x_6] = [x_6x_1x_2x_3x_4x_5]$$

(as though the assignment is turned through $\pi/3$, keeping the table fixed).[349] The symmetries we are considering are all powers of the symmetry we have denoted by[350] (123456). For example, the orbit containing $[BBBPPP]$ consists of

$$[BBBPPP],\ [PBBBPP],\ [PPBBBP],\ [PPPBBB],\ [BPPPBB],\ [BBPPPB]$$

To apply Theorem A.3.7.3 we enumerate the fixed assignments under the various permutations, i.e. under the powers of the symmetry we have denoted by (123456):

under I: all 20 assignments

under (123456)**:** No assignments have this symmetry, as it would entail that every position has the same soup as its neighbours.

under $(123456)^2 = (135)(246)$ The soups at positions 1, 3, 5 must be the same, similarly those at positions 2, 4, 6. There are two possible assignments of $3 + 3$ soups: $[BPBPBP]$, $[PBPBPB]$.

under $(123456)^3 = (14)(25)(36)$**:** The soups at positions 1 and 4 must be the same; also those at positions 2 and 5; also those at positions 3 and 6. But the number of soups of type B is odd. This case cannot occur.

under $(123456)^4 = (153)(264)$**:** same as for $(135)(246)$

under $(123456)^5 = (165432)$**:** impossible for $3B + 3P$.

[349] We could equally well have defined the action to be given by

$$(123456)[x_1x_2x_3x_4x_5x_6] = [x_2x_3x_4x_5x_6x_1]$$

(as though the table is turned through $\pi/3$, keeping the assignment fixed). Since invariance under a symmetry is equivalent to invariance under its inverse, both definitions will lead to the same counts of fixed points.

[350] To avoid confusion we should use some other symbol for this symmetry; it is not (123456), but, rather, the permutation *induced* by (123456) on the set of 20 assignments.

In all we have

$$\frac{1}{6}(20+0+2+0+2+0)=4$$

assignments up to rotational symmetry. These are represented by (i.e. a list of representatives of the equivalence classes [=orbits] is)

$$[BBBPPP],\ [BBPBPP],\ [BBPPBP],\ [BPBPBP]$$

A.3.7.6 EXAMPLE. For the same symmetry group as in Example A.3.7.5 determine the total number of assignments of soups of two kinds (B and P) with no limitation as to numbers.

For each of the symmetries, the number of distinct assignments which are fixed will be precisely 2 raised to the number of cycles in the symmetry. We tabulate these numbers:

Symmetry	Cycle Type	Number of Fixed Points
(1)(2)(3)(4)(5)(6)	x_1^6	64
(123456)	x_6^1	2
(135)(246)	x_3^2	4
(14)(25)(36)	x_2^3	8
(153)(264)	x_3^2	4
(165432)	x_6^1	2
	Total:	84

Hence the number of orbits is $\frac{84}{6}=14$.

To further verify, we tabulate the numbers of fixed points for each of the six possible partitions of 6 into a number of B's and a number of P's:

	$0+6$	$1+5$	$2+4$	$3+3$	$4+2$	$5+1$	$6+0$
(1)(2)(3)(4)(5)(6)	$\binom{6}{0}=1$	$\binom{6}{1}=6$	$\binom{6}{2}=15$	$\binom{6}{3}=20$	$\binom{6}{4}=15$	$\binom{6}{5}=6$	$\binom{6}{6}=1$
(123456)	1	0	0	0	0	0	1
(165432)	1	0	0	0	0	0	1
(135)(246)	1	0	0	2	0	0	1
(153)(264)	1	0	0	2	0	0	1
(14)(25)(36)	1	0	3	0	3	0	1
TOTALS:	1×6	1×6	3×6	4×6	3×6	1×6	1×6

We see that, in counting *all* assignments, the corresponding term in the numerator is obtained by replacing each of the indeterminates in the cycle types by a factor 2. More generally, if we had replaced x_i by the polynomial $1+t^i$ and then expanded all products, we would have obtained from the cycle index

$$\frac{1}{6}\left(x_1^6+2x_6^1+2x_3^2+x_2^3\right)$$

the polynomial

$$\frac{1}{6}\left((1+t)^6+2(1+t^6)^1+2(1+t^3)^2+(1+t^2)^3\right)$$
$$=1+1t+3t^2+4t^3+3t^4+1t^5+1t^6$$

This is the *generating function* for such arrangements.

A.3.7.7 Exercise. Determine the number of circular binary sequences of 8 binary digits up to the symmetries in $\mathcal{D}_8$. Repeat the calculations for the symmetries in $\mathcal{C}_8$.

Solution:

1. Dihedral Group:

Symmetry	Cycle Type	Number of Fixed Points
(1)(2)(3)(4)(5)(6)(7)(8)	x_1^8	2^8
(12345678)	x_8^1	2^1
(14725836)	x_8^1	2^1
(16385274)	x_8^1	2^1
(18765432)	x_8^1	2^1
(1357)(2468)	x_4^2	2^2
(15)(26)(37)(48)	x_2^4	2^4
(1753)(2864)	x_4^2	2^2
(18)(27)(36)(45)	x_2^4	2^4
(21)(38)(47)(56)	x_2^4	2^4
(32)(41)(58)(67)	x_2^4	2^4
(43)(52)(61)(78)	x_2^4	2^4
(28)(37)(46)(1)(5)	$x_1^2x_2^3$	2^5
(31)(48)(57)(2)(6)	$x_1^2x_2^3$	2^5
(42)(51)(68)(3)(7)	$x_1^2x_2^3$	2^5
(53)(62)(71)(4)(8)	$x_1^2x_2^3$	2^5
	Total:	480

The total number of distinct sequences is therefore $\frac{480}{16}=30$. To verify, we may substitute in the cycle index

$$\frac{1}{16}\left(x_1^8+4x_8^1+2x_4^2+5x_2^4+4x_2^3x_1^2\right)$$

(replacing x_1 by $1+t$, x_2 by $1+t^2$, etc.) to obtain the polynomial

$$1t^0+1t^1+4t^2+5t^3+8t^4+5t^5+4t^6+1t^7+1t^8$$

2. Rotations only:

Symmetry	Cycle Type	Number of Fixed Points
(1)(2)(3)(4)(5)(6)(7)(8)	x_1^8	2^8
(12345678)	x_8^1	2^1
(14725836)	x_8^1	2^1
(16385274)	x_8^1	2^1
(18765432)	x_8^1	2^1
(1357)(2468)	x_4^2	2^2
(15)(26)(37)(48)	x_2^4	2^4
(1753)(2864)	x_4^2	2^2
	Total:	288

The total number of distinct sequences is therefore $\frac{288}{8} = 36$. To verify, we may substitute in the cycle index

$$\frac{1}{8}\left(x_1^8 + 4x_8^1 + 2x_4^2 + 1x_2^4 + 0x_2^3x_1^2\right)$$

(replacing x_1 by $1 + t$, x_2 by $1 + t^2$, etc.) to obtain the polynomial

$$1t^0 + 1t^1 + 4t^2 + 7t^3 + 10t^4 + 7t^5 + 4t^6 + 1t^7 + 1t^8$$

The syllabus item, "Pólya enumeration", will not be discussed further in the lectures this year. For the history, and a full translation of Pólya's original 1937 paper [30], cf. [32]; cf. also [1, §20.6], [34, pp. 53–55], [26, Chapter 5]. Some of Pólya's innovations were discovered independently earlier by J. H. Redfield, in 1927.)

A.3.8 The "Graph Isomorphism Problem"

The problem is to design algorithms which, given two graphs G, H, — possibly of a specific type — can decide whether or not they are *isomorphic*, i.e. whether or not there exists a permutation of the rows and columns of the *adjacency matrix* of G which will yield the adjacency matrix of H. We may consider this problem at the end of the course.

A.4 Binary Operations; Semigroups and Monoids

A.4.1 Introduction

Among the properties of permutation *groups* which we have considered in §A.3, some derive from the specific character of the objects, namely, bijections. But many of the properties we have studied could be inferred from the properties of associativity (deriving, in the case of permutation groups, from the fact that the objects we consider are functions), of the identity, and of the inverse which exists for each group element. We now proceed to abstract from the structure of permutation groups properties which permit us to prove highly non-trivial theorems. The objects we work with will be called *groups*; the term, *permutation group*, that we have been using in §A.3, will be justified by the fact that a permutation group will be a group.

There are various equivalent ways in which a group can be defined. We shall present a set of defining axioms in §A.5. Our axioms will not be the most economical possible, but may appear to be weaker than those you see in some text-books, in order to convey the flavour of economy with which mathematicians often try to minimize assumptions. Mathematicians often try to demonstrate their virtuosity in this fashion. Once the "performance" is over, we shall indicate a less economical but more symmetric form of the axioms.

However, before introducing axioms for groups we shall work with some "weaker" algebraic structures, which have some non-trivial applications. These weaker structures are also interesting in that any theorems we can prove for them will surely apply to groups, which have all the structure assumed, and more.

A.4.2 Semigroups

The structures we are defining in this subsection and the next will all involve an operation of "multiplication", which we shall write in various ways — like $a*b$, $a\star b$, etc., eventually often suppressing the symbol entirely and simply *juxtaposing* the symbols, as ab. The term "composition" which is often applied is reminiscent of such examples as permutation groups, where the operation derives from the composition of functions. But remember, the words *composition*, *multiplication*, etc. are simply terms that mathematicians choose to use at some particular time; the meaning of the word in the English language may suggest the actual properties, but occasionally does not.

A.4.2.1 Definition. A *(binary) law of composition* or *(binary) operation* or *multiplication* on a set $\mathfrak{A}$ is a function

$$f : \mathfrak{A} \times \mathfrak{A} \longrightarrow \mathfrak{A}\,.$$

We shall often denote such a function by a symbol such as $*$ which is written between the elements of the ordered pair in $\mathfrak{A} \times \mathfrak{A}$, writing $a_1 * a_2$ for $f(a_1, a_2)$.

A.4.2.2 EXAMPLE. 1. Composition of permutations of a set $\mathfrak{A}$ is a composition. More generally, composition of *any* functions on $\mathfrak{A}$ — not necessarily bijections — is a *composition*.

2. Addition, subtraction, multiplication all are compositions defined on the set $\mathbb{R}$. Division, however, is not a composition on $\mathbb{R}$ since there exist certain ordered pairs for which it is not defined; division is, however, a composition on the set $\mathbb{R} - \{0\}$.

3. The *cross product* is a binary composition defined on the set $\mathbb{R}^3$.

4.

All the algebraic structures we shall be studying in the sequel will have the property of *associativity*:

A.4.2.3 DEFINITION. A composition $*$ defined on $\mathfrak{A}$ is said to be *associative* if, for all a_1, a_2, a_3 in $\mathfrak{A}$,

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)\,. \tag{342}$$

A.4.2.4 EXERCISE. Show that the following operations are *not* associative:

1. $(a, b) \longmapsto a - b$, defined on $\mathbb{Z}$;

2. $(x, y) \longmapsto x/y$, defined on $\mathbb{R} - \{0\}$;

3. $(\vec{v}, \vec{w}) \longmapsto \vec{v} \times \vec{w}$, defined on $\mathbb{R}^3$.

A.4.2.5 EXERCISE. (Difficult) Follow the instructions to prove by induction that condition (342) implies that a generalized associativity law holds.

For any positive integer n, and any sequence a_1, a_2, ..., a_n of elements of $\mathfrak{A}$ (not necessarily distinct), we define recurively a set $A_n(a_1, a_2, ..., a_n)$. For $n = 1$ we define $A_1(a_1) = \{a_1\}$. Suppose that A_r has been defined for all r such that $1 \leq r < n$. We define $A_n(a_1, a_2, ..., a_n) =$

$$\{u * v : u \in A_i(a_1, a_2, ..., a_i),\ v \in A_{n-i}(a_{i+1}, a_{i+2}, ..., a_n); i = 1, 2, ..., n-1\}$$

i.e., $A_n(a_1, a_2, ..., a_n)$ consists of all possible interpretations of $a_1 * a_2 * ... * a_n$ as the result of $n - 1$ binary compositions under $*$. The exercise is to prove that

$$|A_n(a_1, a_2, ..., a_n)| = 1 \tag{343}$$

for all n and all sequences a_1, a_2, ..., a_n.

Solution: For $n = 1$ a set $A_1(a_1)$ is defined to contain only a_1, so its cardinality is evidently 1. For $n = 2$ the definition again admits in $A_2(a_1, a_2)$ only the point $a_1 * a_2$ — again the cardinality is 1. Suppose now that (343) holds for all r such that $2 \leq r < n$; i.e. that $A_r(a_1, a_2, ..., a_r)$ consists uniquely of the element $a_1 * (a_2 * (a_3 * ...))$. In any product uv with $u \in A_i(a_1, a_2, ..., a_i)$, $v \in A_{n-i}(a_{i+1}, a_{i+2}, ..., a_n)$, either $i > 2$ or $n - i > 2$. In the first case, $u = a_i * w$, where $w \in A_{i-1}(a_2, ..., a_i)$, the associative law ensures that $u*v{=}a_1*(w*v)$; but $w*v \in A_{n-1}(a_2, a_3, ..., a_n)$, a set known to contain just one element; the case where $n - i > 2$ may be proved analogously.

Students should not assume that *non-associative* compositions are not of mathematical interest. Rather, these often lead to more complex structures than we shall be considering in this course.

A.4.2.6 DEFINITION. 1. A *semigroup* $(\mathfrak{A}, *)$ consists of a set $\mathfrak{A}$, and an associative binary composition, $(a_1, a_2) \longmapsto a_1 * a_2$. Where there is no danger of confusion, we may simply denote the semigroup by $\mathfrak{A}$.

2. The *order*[351] of $(\mathfrak{A}, *)$ is defined to be the cardinality $|\mathfrak{A}|$.

A.4.2.7 EXAMPLE. 1. Every permutation group is a semigroup, with composition of permutations as the law of multiplication.

2. Let $\mathfrak{A}$ be any set, and $\mathfrak{A}^{\mathfrak{A}}$ the set of functions having this set as domain and codomain. Again with composition of functions as the law of multiplication, these functions form a semigroup.

3. The set of $n \times n$ matrices with entries in $\mathbb{N}$ form a semigroup, with matrix multiplication as multiplication.

4. Let a_0 be some fixed element of a set $\mathfrak{A}$, and define $a_1 * a_2 = a_0$ $\forall a_1, a_2 \in \mathfrak{A}$. Then $(\mathfrak{A}, *)$ is a semigroup; (we may call it the *trivial* semigroup on $\mathfrak{A}$.)

5. Let $\mathfrak{A}$ be any set, and define $a_1 * a_2 = a_1$. Then $(\mathfrak{A}, *)$ is a semigroup.

6. For any real numbers r_1, r_2, define $r_1 * r_2 = \max(r_1, r_2)$. Then $(\mathbb{R}, *)$ is a semigroup.

[351] This term should not be confused with additional structure of a partial or total order*ing* which may be present on a semigroup. For example, the semigroup $(\mathbb{R}, +)$ is endowed with an order relation $<$ which is, in a sense, consistent with the semigroup composition: $a < b \Leftrightarrow a + c < b + c$.

There are also other senses in which the word *order* may appear in algebraic contexts. The present use, *order=cardinality* is standard in the literature, and little would be gained by avoiding it. However, a traditional related use of the word *order* in connection with individual elements of a group is now often replaced by the word *period*, (cf. §A.5.6).

7. Let $\mathfrak{A}$ be any set, and consider the finite sequences of 1 or more elements of $\mathfrak{A}$, written as "words" $a_1a_2...a_r$. We can define a composition by juxtaposition:

$$a_1a_2...a_r \cdot b_1b_2...b_s = a_1a_2...a_rb_1b_2...b_s\,.$$

   We call the semigroup $(\mathfrak{A}^+, \cdot)$ so formed the *free semigroup on* $\mathfrak{A}$.

8. In the sequel we shall define what is meant by a *monoid*. Any monoid is a semigroup.

How can we describe a semigroup? As in the preceding examples, the composition rule can be described in terms of some previously defined function. Alternatively, for a finite semigroup, the rule can be described using a *Cayley table*, i.e. a matrix whose rows and columns are indexed by the elements of the *underlying set*. Normally one indexes rows and columns in the same order, so that the resulting matrix is *symmetric*.

We formalize the concept of two semigroups having the same structure up to a relabelling of points:

A.4.2.8 DEFINITION. Let $(\mathfrak{A}, *)$ and $(\mathfrak{B}, \star)$ be semigroups. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is an *isomorphism* if

1. ϕ is a bijection
2. $\phi(a_1 * a_2) = \phi(a_1) \star \phi(a_2)\ \forall a_1 \in \mathfrak{A}, \forall a_2 \in \mathfrak{A}$.

We may then speak of an *isomorphism* $\phi : (\mathfrak{A}, *) \longrightarrow (\mathfrak{B}, \star)$, and say that the semigroups are *isomorphic*.

A.4.2.9 EXERCISE. If $\phi : (\mathfrak{A}, *) \longrightarrow (\mathfrak{B}, \star)$ is an isomorphism show that ϕ^{-1} is also an isomorphism.

Solution: Let $b_1.b_2 \in \mathfrak{B}$. Then

$$\begin{aligned}
\phi^{-1}(b_1 \star b_2) &= \phi^{-1}\left(\phi(\phi^{-1}(b_1)) \star \phi(\phi^{-1}(b_2))\right) \\
&= \phi^{-1}\phi\left(\phi^{-1}(b_1) * \phi^{-1}(b_2)\right) \\
&\quad \text{since } \phi \text{ is an isomorphism} \\
&= \phi^{-1}(b_1) * \phi^{-1}(b_2) \\
&\quad \text{since} \quad \phi^{-1}\phi(a) = a \forall a \in \mathfrak{A}
\end{aligned}$$

□

For isomorphic finite semigroups, an isomorphism provides a recipe for relabelling the elements of rows and columns of the Cayley table of one so that it becomes the Cayley

table of the other. More precisely, the Cayley table of a semigroup is not uniquely determined, but depends upon the order that is chosen for the labelling of rows and columns. The *isomorphism problem for semigroups* is to design an algorithm that can decide, given two semigroups, whether or not they are isomorphic.

A.4.2.10 Exercise. Show that the following table fails to define a semigroup:

g / f	1	2	3	4
1	1	2	3	4
2	1	2	3	4
3	3	1	4	2
4	4	3	2	1

.

Solution: The composition fails to be associative. For example,

$$(4 * 2) * 4 = 3 * 4 = 2 \neq 1 = 4 * 4 = 4 * (2 * 4)$$

A.4.2.11 Exercise. Determine (using Cayley tables) all semigroups on sets with 0, 1, or 2 elements. (The intention is to determine semigroups *up to isomorphism*[352].)

Solution:

0 elements: There exists a unique function mapping $\emptyset \times \emptyset$ to $\emptyset$. Since there exist no ordered triples of set elements, this composition is vacuously associative. The Cayley table is empty.

1 element: Let $\mathfrak{A} = \{a\}$. There exists a unique mapping from $\mathfrak{A} \times \mathfrak{A}$ to $\mathfrak{A}$, with Cayley table $\begin{array}{c|c} * & a \\ \hline a & a \end{array}$. Observing that $a * a = a$, we check for associativity:

$$(a * a) * a = a * a = a * (a * a)$$

and conclude that this is indeed the Cayley table of a semigroup.

2 elements: Let $\mathfrak{A} = \{a, b\}$, $a \neq b$. There are $2^4 = 16$ ways in which a 2×2 table can be completed:

1. $\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ b & a & a \end{array}$ Since all products equal a, the associative law must hold. This is the Cayley table of the "trivial" semigroup.

[352] i.e. without listing Cayley tables for 2 isomorphic semigroups

2. $\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ b & a & b \end{array}$ The only product of two elements which is equal to b is $b*b$. A product of 3 elements, in either order, will be a unless all 3 factors are b's. But then $(b*b)*b = b*b = b*(b*b)$. Thus associativity holds, and this is the Cayley table of a semigroup.

3. $\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ b & b & a \end{array}$ Since $(b*a)*b = b*b = a \neq a = b*a \neq b*(a*b)$, this composition is not associative.

4. $\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ b & b & b \end{array}$ Any product $x*y$ takes the value of the left factor y; hence $(x*y)*z = x*z = x = x*(y*z)$, and this composition is associative.

5. $\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & a & a \end{array}$ Since $(b*a)*b = a*b = b \neq a = b*b = b*(ab)$, this composition is not associative.

6. $\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & a & b \end{array}$ Analogously to case 4, any product here takes the value of the right factor; hence $(x*y)*z = y*z = z = y*z = z*(y*z)$, and the composition is associative.

7. $\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & b & a \end{array}$ This case could be solved "by brute force", checking all possible triples for associativity. Eventually we shall be able to dispose of this case in another way, by deferring it to the last, and showing that it is the only table not excluded which corresponds to a *group*. We shall see below that this is the addition table of the group $\mathbb{Z}_2$, (up to isomorphism, the only group with 2 elements.)

8. $\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & b & b \end{array}$ This case is isomorphic to case 2.

9. $\begin{array}{c|cc} * & a & b \\ \hline a & b & a \\ b & a & a \end{array}$ Since $(a*a)*b = b*b = a \neq b = a*a = a*(a*b)$, this case is not associative.

10. $\begin{array}{c|cc} * & a & b \\ \hline a & b & a \\ b & a & b \end{array}$ This case is isomorphic to case 7.

11. $\begin{array}{c|cc} * & a & b \\ \hline a & b & a \\ b & b & a \end{array}$ Since $(a*a)*a = b*a = b \neq a = a*b = a*(a*a)$, this case is not associative.

12. $\begin{array}{c|cc} * & a & b \\ \hline a & b & a \\ b & b & b \end{array}$ This case is isomorphic to case 3.

13. $\begin{array}{c|cc} * & a & b \\ \hline a & b & b \\ b & a & a \end{array}$ Since $(a*a)*a = b*a = a \neq b = a*b = a*(a*a)$, this case is not associative.

14. $\begin{array}{c|cc} * & a & b \\ \hline a & b & b \\ b & a & b \end{array}$ This case is isomorphic to case 5.

15. $\begin{array}{c|cc} * & a & b \\ \hline a & b & b \\ b & b & a \end{array}$ This case is isomorphic to case 9.

16. $\begin{array}{c|cc} * & a & b \\ \hline a & b & b \\ b & b & b \end{array}$ This case is isomorphic to case 1.

To summarize, we have found that, up to isomorphism, there are 5 semigroups on 2 points:

$$\begin{array}{c|cc} \text{trivial} & a & b \\ \hline a & a & a \\ b & a & a \end{array}$$

$$\begin{array}{c|cc} \text{left absorption} & a & b \\ \hline a & a & a \\ b & b & b \end{array}, \quad \begin{array}{c|cc} \text{right absorption} & a & b \\ \hline a & a & b \\ b & a & b \end{array}$$

$$\begin{array}{c|cc} (\mathbb{Z}_2, \times, 1) & a & b \\ \hline a & a & a \\ b & a & b \end{array}, \quad \begin{array}{c|cc} (\mathbb{Z}_2, +, 0) & a & b \\ \hline a & a & b \\ b & b & a \end{array}.$$

A.4.2.12 Exercise. We have suggested above that the checking of associativity of a composition on a set of n elements requires n^3 different comparisons. Show that if there is an identity[353], the triples (a_1, e, a_3) do not have to be checked, i.e. that $(a_1 * e) * a_3 = a_1 * (e * a_3)$.

In the context of groups we shall often have occasion to consider iterated products of an element with itself — i.e. powers or exponentials. From our experience with the real numbers, we expect exponentials to have certain properties; we prove that the rules we expect to hold for exponentials do hold in fact.

A.4.2.13 Definition. Let a be an element of a semigroup $(\mathfrak{A}, *)$, and let n be any positive integer. The exponential a^n is defined *recursively* as follows:

1. $a^1 = a$.
2. For $n > 1$, $a^n = a^{n-1} * a$.

A.4.2.14 Theorem. *Let $(\mathfrak{A}, *)$ be a semigroup, $a \in \mathfrak{A}$, and m and n any positive integers. Then*

1. $a^m * a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn} = (a^n)^m$.

Proof:

1. We prove this part by induction on n.

$$\begin{aligned} a^m * a^1 &= a^m * a \quad \text{by definition of } a^1 \\ &= a^{m+1} \quad \text{by definition of } a^{m+1}. \end{aligned}$$

Suppose that $a^m * a^{n-1} = a^{m+(n-1)}$. Then

$$\begin{aligned} a^m * a^n &= a^m * (a^{n-1} * a) \quad \text{by definition of } a^n \\ &= (a^m * a^{n-1}) * a \quad \text{by associativity} \\ &= a^{m+n-1} * a \quad \text{by the induction hypothesis} \\ &= a^{m+n} \quad \text{by definition of } a^{m+n} \end{aligned}$$

[353] cf. Definition A.4.3.1

2. This case also we prove by induction on n.

$$\begin{aligned}(a^m)^1 &= a^m \quad \text{by definition of exponent 1}\\ &= a^{m\cdot 1}\end{aligned}$$

Suppose that $n > 1$, and $(a^m)^{n-1} = a^{m(n-1)}$. Then

$$\begin{aligned}(a^m)^n &= (a^m)^{n-1} * a^m \quad \text{by definition of } n\text{th power}\\ &= a^{m(n-1)} * a^m \quad \text{by the induction hypothesis}\\ &= a^{m(n-1)+m} \quad \text{by the preceding result}\\ &= a^{mn}\end{aligned}$$

Similarly we may show that $(a^n)^m = a^{nm}$. But the exponents are elements of $\mathbb{Z}, \times$, where multiplication is commutative. □

A.4.3 Monoids

We continue our study of semigroups by investigating those with a specialized "neutral" element.

A.4.3.1 Definition. A *monoid* $(\mathfrak{A}, *, e)$ is a semigroup $(\mathfrak{A}, *)$, for which there exists one distinguished element, $e \in \mathfrak{A}$, such that

$$e * a = a \quad \forall a \in \mathfrak{A} \tag{344}$$
$$a * e = a \quad \forall a \in \mathfrak{A} \tag{345}$$

Where an element e has property (344), e is called a *left identity*; where it has property (345) it is called a *right identity*; where it has both properties it is called a *two-sided identity*, or simply an *identity*.

The distinction between the terms *semigroup* and *monoid* is not universally accepted; there are still some authors who use them interchangeably for either of the cases, and at least one case [11, p. 184] of authors who use them in the reverse convention from that given above.

A.4.3.2 Example. 1.

2. In Example A.4.2.7 we defined the *free semigroup* on an alphabet $\mathfrak{A}$. If we adjoin the "empty" word — i.e. an object that may be denoted by, for example, 1, with the obvious definitions of compositions: $1 \cdot 1 = 1$, $a_1a_2...a_r \cdot 1 = a_1a_2...a_r$, $1 \cdot a_1a_2...a_r = a_1a_2...a_r$, we obtain the *free monoid on* $\mathfrak{A}$, sometimes denoted by $\mathfrak{A}^*$.

3. Let $\mathfrak{A}$ be any set. For two (binary) relations ρ, σ on $\mathfrak{A}$, we may define the composition
$$\sigma \star \rho = \{(a_1, a_2) \in \mathfrak{A}^2 : \exists b \in \mathfrak{A} \text{ such that } a_1 \rho b \text{ and } b \sigma a_2\}.$$
Then, with the equality relation as identity, $(P(\mathfrak{A}^2), \star, =)$ is a monoid.

4. In the sequel we shall define what is meant by a *group*. Any group is a monoid.

When a semigroup has an identity element e that element is unique.

A.4.3.3 THEOREM. *Let e and f be identity elements for a semigroup $(\mathfrak{A}, *)$. Then $e = f$.*

Proof:

$$\begin{aligned} e &= e * f \quad \text{since } f \text{ is a right identity} \\ &= f \quad \text{since } e \text{ is a left identity} \end{aligned}$$

Of course, there exist semigroups that do not possess an identity. □

A.4.3.4 EXAMPLE. The semigroup $(2\mathbb{Z}, \times)$, with composition defined by $(m, n) \longmapsto m \times n$ has no identity element.

Historically, the concept of a *semigroup* was introduced first. However, there is little to be gained in studying one concept rather than the other, since the following theorem can be proved:

A.4.3.5 THEOREM. *Let $(\mathfrak{A}, *)$ be a semigroup. There exists a set $\mathfrak{B}$ consisting of $\mathfrak{A}$ and one other element u, $u \notin \mathfrak{A}$ to which we can* extend *the composition rule of $(\mathfrak{A}, *)$ such that $(\mathfrak{B}, *)$ is a monoid.*

Proof: (By *extend* we mean that a function can be defined mapping $\mathfrak{B} \times \mathfrak{B}$ to $\mathfrak{B}$ such that its *restriction* to $\mathfrak{A} \times \mathfrak{A}$ has the same action as $*$. It's not quite correct to say that the restriction is the same function, since the restriction will still have $\mathfrak{B}$ as its codomain, even though the *image* of the restriction will be confined to $\mathfrak{A}$. A function is specified by its *domain*, by its action on points of that domain, and by its *codomain*!) In order to prove this theorem we must define the action of $*$ on the extended domain which includes, in addition to points in $\mathfrak{A} \times \mathfrak{A}$, ordered pairs of the type (u, a) and (a, u), where a ranges over $\mathfrak{A}$; also the pair (u, u). The definition we make is the obvious one: that $u * a = a = a * u$ for all $a \in \mathfrak{A}$, and that $u * u = u$. We must prove associativity, since the identity properties are now obvious.

There are 2^3 different types of triples on which we need to prove associativity:

1. Triples of the form $a_1 * (a_2 * a_3)$, where $a_1, a_2, a_3 \in \mathfrak{A}$, are covered by the hypothesized associativity of the restricted $*$.

2. $$\begin{array}{rcll} a_1 * (a_2 * u) & = & a_1 * a_2 & \text{by definition of } a_2 * u \\ & = & (a_1 * a_2) * u & \text{by definition of } (a_1 * a_2) * u \end{array}$$

3. $a_1 * (u * a_3) = a_1 * a_3 = (a_1 * u) * a_3$

4. $a_1 * (u * u) = a_1 * u = (a_1 * u) * u$

5. $u * (a_2 * a_3) = a_2 * a_3 = (u * a_2) * a_3$

6. $u * (a_2 * u) = a_2 * u = (u * a_2) * u$

7. $u * (u * a_3) = u * a_3 = (u * u) * a_3$

8. $u * (u * u) = u * u = (u * u) * u$

Could there be a problem in this proof because of Theorem A.4.3.3? If we apply this construction to a monoid $(\mathfrak{A}, *, e)$, will it not produce 2 identities? No. The newly constructed identity will be the only identity on the enlarged set; the element e will not be an identity for the enlarged set, since $e * u = e$, by construction, not $= u$. □

As we progressively "enrich" the structures we study, we correspondingly adjust Definition A.4.2.8.

A.4.3.6 Definition. Let $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ be monoids. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is an *isomorphism* if

1. ϕ is a bijection

2. $\phi(a_1 * a_2) = \phi(a_1) \star \phi(a_2)$ $\forall a_1 \in \mathfrak{A}$, $\forall a_2 \in \mathfrak{A}$.[354]

3. $\phi(e) = f$.

We may then speak of an *isomorphism* $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$, and say that the monoids are *isomorphic*.

In short, an isomorphism of monoids is an isomorphism of semigroups which preserves the identity.

A.4.3.7 Example. Consider the following Cayley table for a binary operation on the set $\{0, 1, 2, 3\}$:

[354] It can be shown that this condition is superfluous; that is, if tahe preceding conditions are satisfied, then this condition is a consequence.

f \ g				
	0	2	3	1
	3	1	0	2
	1	3	2	0
	2	0	1	3

Note that the rows and columns have not been labelled yet. We will assume that the labelling is to be in the same order for rows and columns.

1. Can this be the Cayley table of a monoid? What, then, would be the identity element? It will be an element e such that $e * e = e$. If 0 were the identity, then the labelling of the rows and columns could be inferred from the row and column having a 0 in the diagonal position, i.e. from row #1 and column #1:

f \ g	0	2	3	1
0	0	2	3	1
3	3	1	0	2
1	1	3	2	0
2	2	0	1	3

   .

   But this would imply different orders of labelling of rows and columns.

   The same difficulty arises if we assume 1,2, or 3 is the identity. We conclude that this cannot be the Cayley table of a monoid.

2. Could it be the Cayley table of a *semigroup*? We will have to check the associativity condition. After the labelling of rows and columns has been fixed — there are 4! ways in which this can be done — there are $4^3 = 64$ that triples that have to be checked.

3. Notice that this matrix is as unsymmetric as it can be: no off-diagonal element is equal to the element in the mirror-image position. Thus, if $x \neq y$, it will never happen that $x*y = y*x$. But we know from associativity that $a*(a*a) = (a*a)*a$. Thus, if this is the table of a semigroup, then $a * a = a$ for $a = 0, 1, 2, 3$. We may then read off from the diagonal elements what must be the labelling of the rows and columns:

f \ g	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

   .

It is now necessary, either to prove that associativity holds for all triples; or to exhibit a triple for which it fails. We find by trial and error that

$$0 * (1 * 2) = 0 * 0 = 0 \neq 2 = 2 * 2 = (0 * 1) * 2 \,.$$

We conclude that the given matrix cannot be the Cayley table of a semigroup. (This example is interesting since the matrix has all of the properties enumerated in §A.3.3. We call this type of matrix a *Latin square* – it is of particular interest in combinatorics and in the construction of statistical designs. Every group will have a Cayley table which is a Latin square, but here we have a Latin square which does not correspond even to a semigroup!)

A.4.3.8 Exercise. Show that the operation defined by the following multiplication table is not associative:

	0	1
0	1	0
1	0	0

, but that the operation defined by

	1	0
1	1	0
0	0	0

defines a monoid. What is its identity element? Can you describe in general how to identify the identity element from the multipication table?

Solution:

1. $$(11)0 = 00 = 1 \neq 0 = 10 = 1(10)$$

2. The identity element will correspond to a row and column whose entries coincide with the row and column labels. Only the first row contains all possible labels, so it must be associated with the identity, i.e. 1 must be the identity (if this is to be a monoid). That this element is an identity is evident. To check for associativity we would expect to have to consider 2^3 ordered triples; however, by Exercise A.4.2.12, only at most 4 are required in this case. Had the table been larger, the saving would not have been significant, however.

   There is another way to attack this problem. That is to demonstrate that this table is the composition table of a semigroup of functions, since we know that composition of functions is associative. Here we can interpret 1 as the identity function on a set $\iota_{\mathfrak{A}} = \iota_{\{a,b\}}$, and 0 as the function that maps all elements of that set on to a fixed element, say on to a. Then $0 \circ 1 = 0 = 1 \circ 0$ etc. Once we have shown that this set of 2 functions is closed under composition, we can deduce associativity from that property for function composition.

   This device resembles a proof that students may have seen in their linear algebra studies, that matrix multiplication is associative — based on exhibiting a correspondence between matrices and linear transformations.

A.4.3.9 EXERCISE. Determine (using Cayley tables) all monoids on sets with 0, 1, or 2 elements. (The intention is to determine monoids *up to isomorphism*.)

Solution: There cannot exist an empty monoid, since there must be an identity element.

Referring to the soluton to Exercise A.4.2.11, we observe that the unique (trivial) semigroup on one point is a monoid, (indeed, it is a *group*.)

Among the Cayley tables for semigroups with 2 elements we find only two that have a column (corresponding to the identity) that contains the labels of the rows; and the same property for the corresponding row: $\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ b & a & b \end{array}$, $\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & b & a \end{array}$. The first is isomorphic to $(\mathbb{Z}_2, \times, 1)$ — multiplication of residue classes modulo 2; the second is isomorphic to the monoid $(\mathbb{Z}_2, +, 0)$.

We can extend the results of Theorem A.4.2.14 to monoids, after generalizing Definition A.4.2.13 to permit the zero exponent.

A.4.3.10 DEFINITION. Let a be an element of a monoid $(\mathfrak{A}, *, e)$, and let n be any nonnegative integer. The exponential a^n is defined *recursively* as follows:

1. $a^0 = e$.
2. For $n > 0$, $a^n = a^{n-1} * a$.

A.4.3.11 THEOREM. *Let $(\mathfrak{A}, *, e)$ be a monoid, $a \in \mathfrak{A}$, and m and n any nonnegative integers. Then*

1. $a^m * a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

A.4.3.12 EXERCISE. Prove Theorem A.4.3.11.

As we proceed to the "richer" structure of *groups*, it will be enlightening to inquire, from time to time, whether the theorems we prove would be valid in the context of monoids or semigroups. One essential difference holds in the transition from monoids to groups: whereas the passage from semigroups to monoids was, a trivial one, in the sense that any semigroup may be embedded in a monoid, an analogous theorem to Theorem A.4.3.5 does not hold for the monoids in groups: there exist monoids which cannot be embedded in a group.

A.4.4 Subsemigroups, Submonoids, Generators

The algebraic structures we are studying in this course mostly involve an "underlying set", together with certain functions and relations defined on that set or on related sets. In such situations we often have occasion to consider a subset of the underlying set, and ask whether that subset is an object of the same type. For example, given a permutation group, we have investigated when a subset of its elements is also a permutation group (cf. Exercises A.3.3.5, A.3.3.6). Students who have studied linear algebra have also encountered the concept of a *subspace* of a vector space, usually defined as a non-empty subset closed under the operations of vector addition and multiplication by a scalar. We can usually prove, in these situations, a theorem that enables us to determine whether or not the subobject is of the desired type without checking all the criteria that would have to be checked for the "parent" object. For example, a subset of a semigroup will always have the property that, for any condition (342) (associativity) holds. Hence, given a semigroup $(\mathfrak{A}, *)$, and a subset $\mathfrak{B} \subseteq \mathfrak{A}$, the composition $*$ will always "induce" a composition on $\mathfrak{B}$, *provided the function* $*$ *maps the points in* $\mathfrak{B}\times\mathfrak{B}$ *into* $\mathfrak{B}$, i.e. provided that $\mathfrak{B}$ is *closed under the composition* $*$. If that is the case, we may speak, in an "abuse of language" of the semigroup $(\mathfrak{B}, *)$. The "abuse" here is that the function $*$ does not have domain $\mathfrak{B} \times \mathfrak{B}$ nor codomain $\mathfrak{B}$. As for the domain, we could speak instead of the *restriction of* $*$ *to* $\mathfrak{B} \times \mathfrak{B}$. Still, the formal definition of a restriction involves a change in domain, but not in the codomain. So, if we wish to be pedantic, we should introduce a new name for the function, for example $*_{\mathfrak{B}}$, defined by

$$b_1 *_{\mathfrak{B}} b_2 = b_1 * b_2$$

In practice there is no danger of confusion by recycling the symbol $*$ without the subscript, and we shall usually do so.

A.4.4.1 DEFINITION. Let $(\mathfrak{A}, *)$ be a semigroup, and suppose that $\mathfrak{B} \subseteq \mathfrak{A}$. If $\mathfrak{B}$ is closed under $*$, i.e. $\left.\begin{matrix} b_1 \in \mathfrak{B} \\ b_1 \in \mathfrak{B} \end{matrix}\right\} \Rightarrow b_1 * b_2 \in \mathfrak{B}$; and we say that $(\mathfrak{B}, *)$ is a subsemigroup of $(\mathfrak{A}, *)$

A.4.4.2 EXAMPLE. 1. $(k\mathbb{Z}, +)$ is a subsemigroup of $(\ell\mathbb{Z}, +)$ iff $\ell \mid k$.

2. $(k\mathbb{Z}, \times)$ is a subsemigroup of $(\ell\mathbb{Z}, \times)$ iff $\ell \mid k$.

3. Whenever $\mathfrak{B} \subseteq \mathfrak{A}$, the free semigroup $(\mathfrak{A}^+, \cdot)$ contains $(\mathfrak{B}^+, \cdot)$ as a subsemigroup.

The reader may have noticed that we have not defined the concept of *submonoid*. There is a natural way to do this, but it involves one additional condition. More precisely,

A.4.4.3 DEFINITION. Let $(\mathfrak{A}, *, e)$ be a monoid, and suppose that $\mathfrak{B} \subseteq \mathfrak{A}$. If

1. $\mathfrak{B}$ is closed under $*$, i.e. $\left.\begin{array}{l} b_1 \in \mathfrak{B} \\ b_1 \in \mathfrak{B} \end{array}\right\} \Rightarrow b_1 * b_2 \in \mathfrak{B}$; and
2. $e \in \mathfrak{B}$

we say that $(\mathfrak{B}, *, e)$ is a submonoid of $(\mathfrak{A}, *, e)$

This definition involves the same "abuse of language" we encountered in connection with subsemigroups. But there is also an additional condition 2. Thus we will not permit a submonoid to have an identity element different from the identity element of the "parent". (We have not required the subsemigroup to be non-empty, since condition 2 implies that.) This apparently arbitrary condition is one that we will not need to make when we come to the analogous stage in the development of *groups*. There we will be able to prove that closure under composition *and under the taking of inverses* will imply that the identity is present in a nonempty subset.

A.4.4.4 EXERCISE. TO BE SUPPLIED

Suppose that $(\mathfrak{A}, *)$ is a semigroup, and that $\mathfrak{B} \subseteq \mathfrak{A}$. As we did in defining the *free* semigroup, we can still consider finite sequences of 1 or more elements of $\mathfrak{B}$, written as "words" $b_1 * b_2 * ... * b_r$. (We don't need parentheses, by virtue of the associativity of $*$.) Here, however, every word is equal to some element of $\mathfrak{A}$ under the composition $*$. The set of words

$$\{b_1 * b_2 * ... * b_r : b_i \in \mathfrak{B}, r = 1, 2, ...\}$$

is still closed under composition, i.e. is a subsemigroup.

A.4.4.5 DEFINITION. 1. If $\mathfrak{B} \subseteq \mathfrak{A}$ and $(\mathfrak{A}, *)$ is a semigroup, we define

$$\langle \mathfrak{B} \rangle = (\{b_1 * b_2 * ... * b_r : b_i \in \mathfrak{B}; i = 1, 2, ...; r = 1, 2, ...\}, *) .$$

We call $\langle \mathfrak{B} \rangle$ the subsemigroup of $(\mathfrak{A}, *)$ *generated* by $\mathfrak{B}$; the elements of $\mathfrak{B}$ are called the *generators* of $\langle \mathfrak{B} \rangle$.

2. When $\mathfrak{B}$ consists of a single element a, we normally write $\langle a \rangle$, rather than $\langle \{a\} \rangle$.
3. A semigroup $(\mathfrak{A}, *)$ which contains an element a such that $(\mathfrak{A}, *) = \langle a \rangle$ is said to be *cyclic*.

Where $(\mathfrak{A}, *, e)$ is a *monoid*, and $\mathfrak{B} \subseteq \mathfrak{A}$, $\langle \mathfrak{B} \rangle$ may not be a monoid; however, $\langle \mathfrak{B} \rangle \cup \{e\}$ will be a monoid, and could be called the *submonoid generated by* $\mathfrak{B}$. In other words, the *submonoid generated by* $\mathfrak{B}$ consists of the *subsemigroup generated by* $\mathfrak{B}$, to which is adjoined (if it is not already present in the generated semigroup) the identity element.

A.4.4.6 EXAMPLE. 1. For any semigroup $(\mathfrak{A}, *)$, $(\mathfrak{A}, *) = \langle \mathfrak{A} \rangle$.

2. $(\mathcal{S}_n, *, I) = \langle (12), (12...n) \rangle$

3. $(\mathbb{N}, +, 0) = \langle 1 \rangle$. This is a *cyclic* monoid.

4. $(\mathbb{Z}, +, 0) = \langle 1, -1 \rangle$. When we come to consider the analogous concept for groups we shall admit the possibility of taking the inverse of any generator. We do not do so in the context of semigroups and monoids — for one thing, inverses do not always exist. This explains the listing of the inverse of 1. As a monoid — without the possibility of inversion, this cannot be generated by a single element. It is, accordingly, *not* cyclic. When we come to consider the same set, with the same operation, as a *group* it *will* be cyclic!

5. (A GEOMETRIC EXAMPLE)

A.4.5 Commutative Semigroups and Monoids

A.4.5.1 DEFINITION. A semigroup $(\mathfrak{A}, *)$ is *commutative* or *abelian* or *Abelian*[355] if $a_1 * a_2 = a_2 * a_1$ for all $a_1, a_2 \in \mathfrak{A}$.

The Cayley table of a commutative monoid is a *symmetric* matrix.

A.4.5.2 EXERCISE. Suppose that we changed equation (342) in Definition A.4.2.3 to read

$$(a_1 * a_2) * a_3 = a_1 * (a_3 * a_2) \quad \forall a_1, a_2, a_3 \in \mathfrak{A}\,. \tag{346}$$

Show that a monoid $(\mathfrak{A}, *, e)$ with this property is *commutative* i.e. $a_1 * a_2 = a_2 * a_1$ $\forall a_1, a_2 \in \mathfrak{A}$. More generally, show that a composition with this property is *both associative and commutative*.
Solution: Take $a_1 = e$. Then (346) implies that

$$a_2 * a_3 = (e * a_2) * a_3 = e * (a_3 * a_2) = a_3 * a_2$$

for all a_2, a_3 in $\mathfrak{A}$. Moreover, (346) then implies (342).

A.4.5.3 EXAMPLE. 1. $(\mathbb{N}, \times, 1)$, $(\mathbb{R}, \times, 1)$ are commutative monoids.

2. $(\mathcal{S}_n, \circ, I)$ is a non-commutative monoid for $n > 2$.

3. $(\mathcal{D}_n, \circ, I)$ is a non-commutative monoid for $n > 2$, but is commutative for $n = 2$.

4. $(k\mathbb{Z}, +, 0)$ is a commutative monoid.

[355] in deference to the work of N. H. Abel (1802–1829)

5. $(\mathbb{Z}[x], +, 0)$ is the additive monoid of polynomials with integer coefficients.

A.4.5.4 EXAMPLE. Let m be a positive integer. By Theorem A.1.7.6 the set $\{a+(m) : a \in \mathbb{Z}\}$ contains exactly m cosets, represented by 0, 1, ..., $m-1$. Let a, b be two integers. By the Corollary to Theorem A.1.4.5, the sum (and, analogously, the product) of an element from $a+(m)$ and an element from $b+(m)$ are always the same, no matter which representative elements we choose; we may thus define the sum $a+(m) \ + \ b+(m)$ and product $a+(m) \ \times \ b+(m)$ of cosets to be the sum and product of representatives chosen one from each coset. (Without the property we have mentioned, these operations would not be "well defined".) The operations we have defined can be shown to be associative and commutative. Indeed, we can prove that $(\mathbb{Z}_m, +, 0+(m))$ and $(\mathbb{Z}_m, \times, 1+(m))$ are both commutative monoids.

A.4.5.5 EXERCISE. 1. Prove that $(\mathbb{Z}_m, +, 0+(m))$ is a commutative monoid.

2. Prove that $(\mathbb{Z}_m, \times, 1+(m))$ is a commutative monoid.

A.4.6 Direct products

Given sets $\mathfrak{A}$ and $\mathfrak{B}$ each bearing an algebraic structure, it is natural to investigate whether these structures induce one on the cartesian product

$$\mathfrak{A} \times \mathfrak{B} = \{(a, b) : a \in \mathfrak{A},\ b \in \mathfrak{B}\}$$

Given compositions $*$ and $\star$ on $\mathfrak{A}$ and $\mathfrak{B}$ respectively, we define a composition $* \times \star$ on $\mathfrak{A} \times \mathfrak{B}$ by

$$((a_1, b_1), (a_2, b_2)) \longmapsto (a_1 * a_2, b_1 \star b_2) \tag{347}$$

A.4.6.1 THEOREM. *1. If $(\mathfrak{A}, *)$ and $(\mathfrak{B}, \star)$ are semigroups, the composition $* \times \star$ defined by (347) is associative; thus $(\mathfrak{A} \times \mathfrak{B}, * \times \star)$ is a semigroup.*

2. If $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ are monoids, the element (e, f) is an identity element for the semigroup $(\mathfrak{A} \times \mathfrak{B}, * \times \star)$. Hence $(\mathfrak{A} \times \mathfrak{B}, * \times \star, (e, f))$ is a monoid.

Proof: □

A.4.6.2 EXERCISE. Let $(\mathfrak{A}, *)$ and $(\mathfrak{B}, \star)$ be monoids. Let $a \in \mathfrak{A}$, $b \in \mathfrak{B}$, $n \in \mathbb{N}$. Prove that $(a, b)^n = (a^n, b^n)$.

A.4.7 Naming conventions

In practice the notations $(\mathfrak{A}, *)$ for a semigroup, or $(\mathfrak{A}, *, e)$ for a monoid are unnecessarily cumbersome. We normally denote such objects by a single symbol. The most convenient notation is to use the same letter for the semigroup or monoid as for the underlying set of objects, and to write the composition by juxtaposition. Thus, we may speak of the *direct product* $\mathfrak{A} \times \mathfrak{B}$. We may also use the same symbol for the identity element in all monoids.

A.5 Groups

A.5.1 Inverses

While every permutation group is a monoid, the structure of monoids, developed in §A.4, is not adequate to model the essential algebraic properties of permutation groups. This situation can be remedied by imposing just one additional axiom — more precisely one *family* of axioms, in the same sense as the associative law is a family which must hold *for all* triples.

A.5.1.1 Definition. Let $(\mathfrak{A}, *, e)$ be a monoid.

1. A *left inverse* of an element $a \in \mathfrak{A}$ is an element $\ell \in \mathfrak{A}$ such that $\ell * a = e$.
2. A *right inverse* of an element $a \in \mathfrak{A}$ is an element r such that $e = a * r$.
3. An *inverse* of an element $a \in \mathfrak{A}$ is an element which is both a left inverse and a right inverse of a. An element possessing an inverse is said to be *invertible*.
4. $(\mathfrak{A}, *, e)$ is a *group* if every element $a \in \mathfrak{A}$ possesses a left inverse and a right inverse.
5. A group $(\mathfrak{A}, *, e)$ is said to be *commutative* or *abelian* or *Abelian* if the semigroup $(\mathfrak{A}, *)$ is commutative. Abelian groups are often "written additively", i.e. with the group operation denoted by $+$, and the identity by 0.
6. A group which is not abelian may be said to be *non-abelian*.

A.5.1.2 Exercise. Prove that if ℓ and r are respectively a left inverse and a right inverse of an element a of a monoid $(\mathfrak{A}, *, e)$, then $\ell = r$.

Solution:

$$\ell = \ell * e = \ell * (a * r) = (\ell * a) * r = e * r = r$$

By virtue of Exercise A.5.1.2, no element of a monoid can have more than one inverse. Following Burnside [3] we introduce the following *temporary* notation:

A.5.1.3 Definition. (Temporary). If an element a of a monoid possesses an inverse, that inverse may be denoted by a_{-1}.

A.5.1.4 Exercise.
1. Prove that if a and b are invertible, then ab is invertible, and $(a * b)_{-1} = b_{-1} * a_{-1}$.
2. Prove that if a is invertible, then a_{-1} is also invertible, and $(a_{-1})_{-1} = a$.
3. Prove that e is invertible, and that $e_{-1} = e$.

4. Suppose that a is invertible. Prove, for any nonnegative integer n, that

$$(a^n)_{-1} = (a_{-1})^n \tag{348}$$

5. Suppose that a is invertible. Let m and n be any nonnegative integers. Then

$$((a^m)_{-1})^n = (a_{-1})^{mn}$$

$$((a^m)^n)_{-1} = (a^{mn})_{-1}$$

If $n \geq m$,

$$(a^m)_{-1} * a^n = a^{n-m}$$

If $n < m$,

$$(a^m)_{-1} * a^n = \left(a^{m-n}\right)_{-1}$$

Solution:

1. By hypothesis, elements a_{-1} and b_{-1} exist. Then

$$\begin{aligned}(a*b)*(b_{-1}*a_{-1}) &= a*(b*(b_{-1}*a_{-1})) = a*((b*b_{-1})*a_{-1}) \\ &= a*(e*a_{-1}) = a*a_{-1} = e\end{aligned}$$

$$\begin{aligned}(b_{-1}*a_{-1})*(a*b) &= ((b_{-1}*a_{-1})*a)*b = (b_{-1}*(a_{-1}*a))*b \\ &= (b_{-1}*e))*b = b_{-1}*b = e\end{aligned}$$

Thus $b_{-1} * a_{-1}$ is a left inverse and right inverse of $a * b$.

2. The same two equations that describe a_{-1} as left and right inverse of a also describe a as right and left inverse respectively of a_{-1}.

3. Since $e * e = e$, e serves as both left and right inverse of e.

4. For $n = 0$, $(a^0)_{-1} = e_{-1} = e = (a_{-1})^0$ for any a.

   Suppose that (348) has been proved for $n = N - 1$ for some invertible a.

$$\begin{aligned}a^N * (a_{-1})^N &= \left(a^{N-1}*a\right)*\left(a_{-1}*(a_{-1})^{N-1}\right) \\ &= \left(\left(a^{N-1}\right)*(a*a_{-1})\right)*(a_{-1})^{N-1} \\ &= \left(a^{N-1}*e\right)*(a_{-1})^{N-1} = \left(a^{N-1}\right)*(a_{-1})^{N-1} = e\end{aligned}$$

   by the induction hypothesis.

5. $((a^m)_{-1})^n = ((a_{-1})^m)^n = (a_{-1})^{mn}$
   $((a^m)^n)_{-1} = \big((a^m)_{-1}\big)^n = ((a_{-1})^m)^n = (a_{-1})^{mn} = (a^{mn})_{-1}$
   If $n \geq m$, $(a^m)_{-1} * a^n = (a^m)_{-1} * (a^m * a^{n-m}) = \big((a^m)_{-1}\big) * a^m * a^{n-m} = e * a^{n-m} = a^{n-m}$.
   If $n < m$, $(a^m)_{-1} * a^n = (a^n * a^{m-n})_{-1} * a^n = \big((a^{m-n})_{-1} * (a^n)_{-1}\big) * a^n = (a^{m-n})_{-1} * \big((a^n)_{-1} * a^n\big) = (a^{m-n})_{-1}$

If we now *define* negative exponents by

A.5.1.5 Definition. (replacing Definition A.5.1.3). Let a be an invertible element of the monoid $(\mathfrak{A}, *, e)$, and let n be a positive integer. We define $a^{-n} = (a_{-1})^n$. In particular, the inverse of a will be denoted by a^{-1}, replacing the "temporary" symbol a_{-1}.

We have proved in the preceding exercise that the exponent laws we proved to hold for nonnegative exponents can now be extended to all integer exponents. The notation a_{-1} is no longer required.

A.5.1.6 Definition. In the "additive notation" for abelian groups it is customary to denote the inverse of a by $-a$, and to define

$$a - b = a + (-b)$$

The composition of n copies of n is then denoted by na. This notation appears to be interpreting the integers as being elements of the abelian group. More precisely, we are defining an action of the integers on the abelian group. That is, we can interpret each integer n (positive, negative, or zero) as a *function* that maps the abelian group onto itself, given by

$$a \longmapsto \begin{cases} na & \text{if } n \text{ is positive} \\ 0 & \text{if } n = 0 \\ n(-a) & \text{if } n \text{ is negative} \end{cases}$$

Here we are interpreting the abelian group as a *left $\mathbb{Z}$-module*[356] [357].

A.5.1.7 Exercise. Let $(\mathfrak{A}, +, 0)$ be an abelian group, let $a, b \in \mathfrak{A}$, $m, n \in \mathbb{Z}$.

1. Prove that $-(a + b) = (-a) + (-b)$.

[356] The concepts of *left module* and *right module* may be defined for any *ring*. As the ring of integers is *commutative* — i.e. as multiplication in the monoid $(\mathbb{Z}, \times, 1)$ is commutative, the concepts of *left* and *right* module coincide; the *left* attribute appears only in the notation, that we write the ring element to the left of the module element.

[357] cf. Exercise A.5.2.11

2. Prove that $-(-a) = a$.
3. Prove that $(m + n)a = ma + na$.
4. Prove that $m(a + b) = ma + mb$.
5. Prove that $m(-a) = (-m)a = -(ma)$.
6. Prove that $m(na) = n(ma)$.

Solution:

1.
2.
3.
4.
5.
6.

A.5.1.8 EXAMPLE. 1. Every permutation group $\mathcal{G}$ on a set $\mathfrak{A}$ is a group $(\mathcal{G}, \circ, I)$.[358] While every permutation group is a group, is every group a permutation group? We shall see that any group may be interpreted as a group of permutations of a set. On the other hand, the passage from permutation groups to groups is one in which certain information is lost. That is, we *abstract* from the concept of a permutation group certain structure that enables us to prove theorems, while ignoring some other information. The result is that the same *group* may appear as the structure of quite different permutation groups — sometimes even acting on the same set. We will defer further investigation of this topic until we have introduced the concept of *isomorphism*.

2. Every real vector space $\mathcal{V}$ is a group $(\mathcal{V}, +, \vec{0})$.
3. $(\mathbb{Z}, +, 0)$ is a group.
4. For any positive integer n, $(\mathbb{Z}_n, +, (n))$ is a group, where addition is defined as in Definition A.1.7.1 and (313).

[358] This justifies the use of the same English word *group* simultaneously in both definitions. (We are not attempting to justify the particular English word that is used.)

5. Let $\mathbb{F}$ be any one of $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$. Then $(\mathbb{F}-\{0\},\times,1)$ is an abelian group. More generally, any *field* (to be defined in a later section) yields — with 0 deleted — a group under the operation of multiplication.

6. But $(\mathbb{Z}-\{0\},\times,1)$ is not a group, since only 2 elements have inverses.

7. The matrices $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a,b\in\mathbb{R}; a^2+b^2>0\right\}$ form a commutative subgroup of $GL(2,\mathbb{R})$.

8. $\mathcal{C}_n$, the group of rotations of the n-gon, is an abelian subgroup of $\mathcal{D}_n$, the group of all symmetries of the n-gon, (which is not commutative when $n\geq 3$).

A.5.1.9 Example. In Definition A.1.9.5 we defined what was meant, for a non-zero integer m, by the *inverse* of an integer a modulo m. We subsequently observed that if a^{-1} is an inverse of a, then all elements of the coset $a^{-1}+(m)$ are inverses of all elements of the coset $a+(m)$. In the monoid $(\mathbb{Z}_m,\times,1+(m))$ defined in Example A.4.5.4, $a+(m)$ will be invertible iff a is invertible modulo m; then $(a+(m))^{-1}=a^{-1}+(m)$.

Let us denote the set of invertible cosets in $\mathbb{Z}_m$ by[359] $\mathbb{Z}_m^\times$.

A.5.1.10 Exercise. 1. Prove that $a+(m)\in\mathbb{Z}_m^\times \Leftrightarrow (a,m)=1$.

2. Prove that $(\mathbb{Z}_m^\times,\times,1+(m))$ is an abelian group. (Note that this abelian group is not written additively.)

3. Prove that $|\mathbb{Z}_m^\times|=m-1\Leftrightarrow m$ is prime.

4. Determine Cayley tables for the groups $(\mathbb{Z}_m^\times,\times,1+(m))$, $m=2,3,4,5,10$.

Solution:

1. This follows immediately from Theorem A.1.9.7 and Corollary A.1.9.8.

2. By Exercise A.5.1.4.1 the set $\mathbb{Z}_m^\times$ is closed under $\times$. Multiplication was proved to be associative in Exercise A.1.7.2.1b. Evidently $1+(m)$ is the multiplicative identity. And, by definition, all elements are invertible. Thus all group postulates are satisfied.

3. Suppose that $m=ab$, where $1<a<m$, $1<b<m$. Then a (i.e. the product of cosets $a+(m)\cdot b+(m)$) is not invertible, since, if it were,

$$b\equiv 1b\equiv a^{-1}ab\equiv a^{-1}0\equiv 0$$

[359] Another common notation is $\mathbb{Z}_m^*$.

contradicting the hypothesis that $1 < b < m$. Thus $|\mathbb{Z}_m| \leq m - 2$.

Every coset $a + (m)$ contains a(n unique) representative between 0 and $m - 1$ inclusive; assume a is such a representative. Then, if m is prime, $m \nmid a$, so a is invertible; thus all cosets in $\mathbb{Z}_m - \{(m)\}$ are invertible, so $|\mathbb{Z}_m^\times| = m - 1$.

4.

$\mathbb{Z}_2^\times$	1
1	1

$\mathbb{Z}_3^\times$	1	2
1	1	2
2	2	1

$\mathbb{Z}_4^\times$	1	3
1	1	3
3	3	1

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_{10}^\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

A.5.1.11 EXAMPLE. Let $a, b, c, d \in \mathbb{R}$, with $ac \neq 0$. Define a function $f_{a,b;c,d} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ by $\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} ax + b \\ cy + d \end{pmatrix}$. Show that these functions form a subgroup of $\mathcal{S}_{\mathbb{R}^2}$. Determine conditions on a and c that will make this group abelian.

A.5.1.12 THEOREM. *Let $(\mathfrak{A}_1, *, e)$ and $(\mathfrak{A}_2, \star, f)$ be groups. Then the direct product $\mathfrak{A}_1 \times \mathfrak{A}_2$ is a group.*

Proof: By Theorem A.4.6.1, we need only prove the existence of inverses. We claim that $(a_1, a_2)^{-1} = \left(a_1^{-1}, a_2^{-1}\right)$. To do this we simply compute the products:

$$(a_1, a_2)\left(a_1^{-1}, a_2^{-1}\right) = \left(a_1\left(a_1^{-1}\right), a_2\left(a_2^{-1}\right)\right) = (e, f)$$

etc. □

A.5.1.13 DEFINITION. In the "additive" notation for abelian groups it is customary also to denote direct products additively. If $(\mathfrak{A}, +, 0)$ and $(\mathfrak{B}, +, 0)$ are abelian groups, we define the *direct sum*, usually denoted by $(\mathfrak{A}, +, 0) \oplus (\mathfrak{B}, +, 0)$, or simply by $\mathfrak{A} \oplus \mathfrak{B}$ to be the direct product $(\mathfrak{A} \times \mathfrak{B}, +, (0, 0))$ with the "coordinate-wise" definition for addition.

A.5.1.14 EXERCISE. Show that the direct sum of two abelian groups is abelian.

Solution: Suppose that $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ are abelian groups. THe direct sum is the group whose elements are the points of the cartesian product $\mathfrak{A} \times \mathfrak{B}$, with the group operation defined by $(a, b) \circ (a', b') = (a * a', b \star b')$. By the preceding theorem, this defines a group structure. We need only prove that the operation is commutative.

$$\begin{aligned} (a, b) \circ (a', b') &= (a * a', b \star b') \\ &= (a' * a, b' \star b) \qquad \text{since } * \text{ and } \star \text{ are commutative} \\ &= (a', b') \circ (a, b) \end{aligned}$$

A.5.1.15 Exercise. The complex plane can be "completed" by adjoining a single point at infinity, denoted by ∞. We then *define*

$$\frac{1}{\infty} = 0\,;$$

$$z + \infty = \infty + z = \infty\,,$$

$$z \cdot \infty = \infty \cdot z = \infty$$

for $z \neq 0$. Provided we avoid operating on certain pairs which cannot be assigned a meaningful value (like $\frac{0}{0}$, $\frac{\infty}{\infty}$, $0 \cdot \infty$) we can extend the algebraic operations defined in $\mathbb{C}$ to this larger plane, which we visualize as a plane "closed up" into a sphere. On this *extended complex plane* we may define functions $z \longmapsto \frac{az+b}{cz+d}$, where the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is nonsingular. Show that these functions form a permutation group acting on the extended complex plane, under function composition. Determine the inverse function to the function $z \longmapsto \frac{az+b}{cz+d}$. This group is called the *linear fractional group*, or the *Möbius*[360] *group*. Show that the set of functions

$$\left\{ z, \frac{1}{z}, \frac{1}{1-z}, 1-z, 1-\frac{1}{z}, \frac{z}{z-1} \right\}$$

form a subgroup. Is it abelian?

A.5.2 Objects and Morphisms

The functions of interest in the *category* of groups are called *homomorphisms*. In the language of *category theory* (a branch of algebra concerned with the abstract properties of composition of functions), homomorphisms are the *morphisms* of the category of groups. Let us return first to the category of *semigroups* to define a *semigroup homomorphism*; and generalize this through *monoid homomorphisms* in the category of monoids, to *group homomorphisms* in the category of groups. In practice only the word *homomorphism* is used, as the category can usually be determined from the context.

A.5.2.1 Definition. 1. Let $(\mathfrak{A}, *)$ and $(\mathfrak{B}, \star)$ be semigroups. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is a *(semigroup) homomorphism* if $\phi(a_1 * a_2) = \phi(a_1) \star \phi(a_2)$ $\forall a_1 \in \mathfrak{A}$, $\forall a_2 \in \mathfrak{A}$. We may then speak of a *homomorphism* $\phi : (\mathfrak{A}, *) \longrightarrow (\mathfrak{B}, \star)$.

2. Let $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ be monoids. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is a *(monoid) homomorphism* if

   (a) ϕ is a semigroup homomorphism

[360] A. N. Möbius (1790–1868)

(b) $\phi(e) = f$.

We may then speak of a *homomorphism* $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$.

3. Let $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ be groups. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is a *(group) homomorphism* if ϕ is a semigroup homomorphism. (There are no additional requirements.) We may then speak of a *homomorphism* $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$.

A homomorphism is a generalization of an *isomorphism*, introduced for semigroups in A.4.2.8. We showed that the inverse of an isomorphism is also an isomorphism. We can prove the converse:

A.5.2.2 Exercise. Let $\phi : (\mathfrak{A}, *) \longrightarrow (\mathfrak{B}, \star)$ and $\psi : (\mathfrak{B}, \star) \longrightarrow (\mathfrak{A}, *)$ be semigroup homomorphisms such that

$$\phi(\psi(b)) = b \quad \text{and} \quad \psi(\phi(a)) = a \quad \forall a \in \mathfrak{A} \quad \forall b \in \mathfrak{B}\,. \tag{349}$$

Then ϕ and ψ are isomorphisms.

Solution: Since ϕ and ψ are homomorphisms, we need only prove that they are bijective. It suffices to prove that one of the pair, say ϕ, is bijective; that ψ is bijective will then follow by symmetry.

$$\begin{aligned} \phi(a_1) = \phi(a_2) \quad &\Rightarrow \quad \psi(\phi(a_1)) = \psi(\phi(a_2)) \\ &\Leftrightarrow \quad a_1 = a_2 \end{aligned}$$

Thus ϕ is injective (one-to-one).

$b \in \mathfrak{B} \Rightarrow b = \phi(\psi(b))$. Thus b is the image of a point $\psi(b) \in \mathfrak{A}$. We have proved that ϕ is surjective (onto). □

For a more elegant rendition of the last result, let us involve the *identity function* (cf. Definition A.2.2.5.

A.5.2.3 Exercise. 1. Let $(\mathfrak{A}, *)$ be a semigroup. Prove that $\iota_{\mathfrak{A}}$ is a semigroup homomorphism. (Indeed, you may prove that it is an *iso*morphism.)

2. Let $(\mathfrak{A}, *, e)$ be a monoid. Prove that $\iota_{\mathfrak{A}}$ is a monoid homomorphism.

3. Let $(\mathfrak{A}, *, e)$ be a group. Prove that $\iota_{\mathfrak{A}}$ is a group homomorphism.

Solution:

1.

$$\iota(a * b) = a * b = \iota(a) * \iota(b)$$

2. We need only check that the mapping carries the identity element on to the identity element (i.e. onto itself, since the domain and codomain coincide). But *every* element is carried on to itself.

3. This follows from part 1 above.

We can now rewrite (349):

$$\phi \circ \psi = \iota_{\mathfrak{A}} \quad \text{and} \quad \psi \circ \phi = \iota_{\mathfrak{B}} \,. \tag{350}$$

This motivates the following definitions:

A.5.2.4 DEFINITION. 1. Let $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ be monoids. A homomorphism $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ is defined to be a *(monoid) isomorphism* if there exists a homomorphism $\psi(\mathfrak{B}, \star, f) \longrightarrow (\mathfrak{A}, *, e)$ such that (349) holds.

2. Let $(\mathfrak{A}, *, e)$ and $(\mathfrak{B}, \star, f)$ be groups. A homomorphism $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ is defined to be a *(group) isomorphism* if ϕ is a monoid isomorphism.

Remember that equations (349) are *functional equations*: two functions are equal iff

- their domains are identical
- their codomains are identical
- they act identically on each point of their common domain

Students may have found puzzling the extensions of the preceding definitions from semigroups to groups. It would have appeared "natural" to extend the definition of a *monoid homomorphism* to groups by some additional requirements that would ensure that a homomorphism preserve the group structure; yet we have failed to impose any constraint on the action of a homomorphism on the identity, as we *did* for monoids (condition 2b of Definition A.5.2.1). Also, don't we want to require that a homomorphism map inverses on to inverses? Indeed we do. Fortunately, these properties are "free": they require no additional assumptions, and follow as consequences of the properties of the inverse. More precisely, we have the following:

A.5.2.5 THEOREM. *Let $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ be a group homomorphism. Then*

1. *$\phi(e) = f$.*
2. *$\phi(g)$ is invertible, and $\phi\left(g^{-1}\right) = (\phi(g))^{-1}$.*

Proof:

1. $\phi(g) = \phi(g * e) = \phi(g) \star \phi(e) \Rightarrow f = (\phi(g))^{-1} \star \phi(g) = (\phi(g))^{-1} \star \phi(g) \star \phi(e) = f \star \phi(e) = \phi(e)$.

2. By hypothesis,
$$g * g^{-1} = e = g^{-1} * g$$
Applying ϕ to all three members of this pair of equations yields
$$\phi(g) \star \phi\left(g^{-1}\right) = \phi(e) = \phi\left(g^{-1}\right) \star \phi(g) \tag{351}$$
Since $\phi(e) = f$, (351) implies that $\phi(g)$ is the inverse of $\phi\left(g^{-1}\right)$.

A.5.2.6 Exercise. Definition A.5.2.4 could actually have been weakened! It is not necessary to assume that ψ is a homomorphism; all that is required is that ψ composes with ϕ in the manner indicated, i.e. that ψ is the inverse *function*. More precisely, we can prove the following: *Let* $(\mathfrak{A}, *, e)$ *and* $(\mathfrak{B}, \star, f)$ *be monoids. A homomorphism* $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ *is a* (monoid) isomorphism *iff there exists a function* $\psi : \mathfrak{B} \longrightarrow \mathfrak{A}$ *such that* $\psi \circ \phi = \iota_{\mathfrak{A}}$ *and* $\phi \circ \psi = \iota_{\mathfrak{B}}$.

Proof: We need only to prove that ψ is a monoid homomorphism. Let $b_1 \in \mathfrak{B}$ and $b_2 \in \mathfrak{B}$. Then $\psi(b_1 \star b_2) = \psi(\iota_{\mathfrak{B}}(b_1) \star \iota_{\mathfrak{B}}(b_2)) = \psi(\phi(\psi(b_1))) \star \phi(\psi((b_2))) = \psi(\phi(\psi(b_1) * \psi(b_2))) = \iota_{\mathfrak{A}}(\psi(b_1) * \psi(b_2)) = \psi(b_1) * \psi(b_2)$.[361]

In A.4.4.3 we defined the concept of submonoid. To extend this concept to groups we shall need to require closure under the operation of taking the inverse. However, condition 2 of Definition A.4.4.3 will no longer be required, as it can be shown (cf. Exercise A.5.2.8 below) to follow as a consequence of condition 1; we must, however require that the subset be non-empty.

A.5.2.7 Definition. Let $(\mathfrak{A}, *, e)$ be a group, and suppose that $\mathfrak{B} \subseteq \mathfrak{A}$. If

1. $\mathfrak{B}$ is closed under $*$, i.e. $\left.\begin{array}{l} b_1 \in \mathfrak{B} \\ b_2 \in \mathfrak{B} \end{array}\right\} \Rightarrow b_1 * b_2 \in \mathfrak{B}$; and

2. $\mathfrak{B}$ is closed under the taking of inverses, i.e. $b \in \mathfrak{B} \Rightarrow b^{-1} \in \mathfrak{B}$.

3. $\mathfrak{B} \neq \emptyset$

we say that $(\mathfrak{B}, *, e)$ is a *subgroup* of $(\mathfrak{A}, *, e)$ and write $(\mathfrak{B}, *, e) \leq (\mathfrak{A}, *, e)$, or simply $\mathfrak{B} \leq \mathfrak{A}$.

[361] This fortunate situation — that the inverse function inherits the algebraic properties of the homomorphism — is not one that can be expected to hold in all mathematical contexts. For example, in the analogous situation in the category of topological spaces, with continuous functions as the morphisms, the inverse function of a bijective continuous function need not always be continuous!

A.5.2.8 EXERCISE. Let $(\mathfrak{A}, *, e)$ be a group, and suppose that $\mathfrak{B} \subseteq \mathfrak{A}$.

1. Prove that a conditions 1 and 2 of Definition A.5.2.7 are equivalent to the single condition

   $$1'. \quad \left.\begin{array}{l} b_1 \in \mathfrak{B} \\ b_2 \in \mathfrak{B} \end{array}\right\} \Rightarrow b_1 * b_2^{-1} \in \mathfrak{B}.$$

2. Prove the claim made earlier: If $(\mathfrak{A}, *, e)$ is a group, $\emptyset \neq \mathfrak{B} \subset \mathfrak{A}$, and $\mathfrak{B}$ is closed under $*$ and the taking of inverses, then $e \in \mathfrak{B}$.

A.5.2.9 EXAMPLE. 1. (cf. Example A.5.1.8.2) Let n, m be any nonnegative integers. Any linear operator $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ is a homomorphism. T is an isomorphism iff T is non-singular, i.e. invertible.

2. For any positive integer n, the function $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $x \longmapsto x + (n)$ is a surjective homomorphism, by (313).[362]

3. The function $z \longmapsto |z|$ is a homomorphism from $(\mathbb{C} - \{0\}, \times, 1)$ to $(\mathbb{R} - \{0\}, \times, 1)$.

4. The function $A \longmapsto \det A$ is a homomorphism from $(GL(n, \mathbb{R}), \circ, I)$ to $(\mathbb{R} - \{0\}, \times, 1)$.

A.5.2.10 EXERCISE. Certain pairs of the following groups are isomorphic. Where that is so, give an isomorphism. Where that is false, prove it.

1. $(\mathbb{Z}_5^\times, \times, 1 + (5))$ and $(\mathbb{Z}_{10}^\times, \times, 1 + (10))$.

2. $(\mathbb{Z}_6, +, (6))$ and $(\mathbb{Z}_7^\times, \times, 1 + (7))$.

3. $(\mathbb{Z}_6, +, (6))$ and $\mathcal{S}_3$.

4.

A.5.2.11 EXERCISE. When $(\mathfrak{B}, *, e)$ is a *non*-abelian group, the function $a \longmapsto a^n$ is still well defined for every integer n; thus $\mathbb{Z}$ still *operates* on $(\mathfrak{B}, *, e)$. But there the function is not a homomorphism. Prove that the mapping $a \longmapsto a^2$ is a homomorphism iff the group is abelian!

A.5.2.12 EXERCISE. Let $(\mathfrak{A}, *, e)$ be a group, and $\mathfrak{B}$ a *finite* subset of $\mathfrak{A}$.

1. Prove that $(\mathfrak{B}, *, E)$ is a subgroup iff the following two conditions are satisfied:

[362] A surjective homomorphism is also known as an *epimorphism*.

(a) $\mathfrak{B} \neq \emptyset$

(b) $\mathfrak{B}$ is closed under $*$

2. Give a counterexample to show that this result need not hold when $\mathfrak{B}$ is not finite.

Solution:

1. Let $|\mathfrak{B}| = n$. Since $\mathfrak{B}$ is not empty, there exists $b_1 \in \mathfrak{B}$. Consider the products $b_1 b$ as b ranges over the n elements of $\mathfrak{B}$. These products must all be different (prove this); as $\mathfrak{B}$ is closed under composition, all of the products are in $\mathfrak{B}$. Thus they must collectively be all the elements of $\mathfrak{B}$. Thus one of them must be b_1; i.e. for some $b \in \mathfrak{B}$, $b_1 b = b_1$. Interpreting this equation in the group $\mathfrak{A}$, we may multiply on the left by $(b_1)^{-1}$, to obtain $b = e$. We have thus shown that $e \in \mathfrak{B}$.

   Again we examine the set $\{b_1 b : b \in \mathfrak{B}\}$. One of the products must be equal to $e \in \mathfrak{B}$; solving $b_1 b = e$ yields $b = b_1^{-1}$; that is, we have shown that the inverse of b_1 is in $\mathfrak{B}$. We have now proved that all the conditions of Definition A.5.2.7 are satisfied, so $\mathfrak{B} \leq \mathfrak{A}$. $\square$

2. The nonempty subset $\mathbb{N}$ of $\mathbb{Z}$ is closed under $+$, but does not constitute a subgroup of $(\mathbb{Z}, +, 0)$, since none of its elements has an additive inverse in the set.

A.5.3 Kernel and image of a homomorphism.

A.5.3.1 DEFINITION. Let Let $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ be a homomorphism of groups. We define

$$\text{Image}(\phi) = \phi(\mathfrak{A}) = \{\phi(a) : a \in \mathfrak{A}\}$$

$$\text{Kernel of } \phi = \ker(\phi) = \{a : a \in \mathfrak{A}, \phi(a) = f\}$$

A.5.3.2 THEOREM. *Let $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{B}, \star, f)$ be a homomorphism of groups.*

1. *The image of ϕ is a subgroup of $(\mathfrak{B}, \star, f)$.*
2. *The kernel of ϕ is a subgroup of $(\mathfrak{A}, *, e)$.*
3. *ϕ is one-to-one*[363] *iff* $\ker(\phi) = \{e\}$.

Proof:

[363] An injective homomorphism is also known as a *monomorphism*.

1. Since ϕ is a homomorphism, $\phi(e) = f$. Suppose that b_1 and b_2 are points in the image. Then there exist points $a_1, a_2 \in \mathfrak{A}$ such that $\phi(a_i) = b_i$ $(i = 1, 2)$. Thus $\phi(a_1) \star \phi(a_2) = \phi(a_1 * a_2) \in \text{Image}(\phi)$.

   Also, let $b \in \text{Image}(\phi)$. Then there exists $a \in \mathfrak{A}$ such that $b = \phi(a)$. But $(\phi(a))^{-1} = \phi(a^{-1}) \in \text{Image}(\phi)$.

2. Since $\phi(e) = f$, e is in the kernel. Suppose that a_1 and a_2 are points in the kernel, i.e. that $\phi(a_i) = f$ $(i = 1, 2)$. Then $\phi(a_1 * a_2) = \phi(a_1) \star \phi(a_2) = f \star f = f$, so $a_1 * a_2$ is also contained in the kernel.

   If a is in the kernel, $\phi(a) = f$. Then $\phi(a^{-1}) = (\phi(a))^{-1} = f^{-1} = f$, so a^{-1} is also in the kernel.

3. Suppose that ϕ is one-to-one, and that $a \in \ker(\phi)$. Then $\phi(a) = f$. But, by hypothesis, $\phi(e) = f$. We conclude that $a = e$.

   Conversely, suppose that the kernel contains only e,and that $\phi(a_1) = \phi(a_2)$. Then $\phi(a_1 * a_2^{-1}) = \phi(a_1) \star \phi(a_2^{-1}) = \phi(a_1) \star (\phi(a_2))^{-1} = \phi(a_2) \star (\phi(a_2))^{-1} = f$, so $a_1 * a_2^{-1} \in \ker(\phi) = \{e\}$. Thus $a_1 * a_2^{-1} = e$, and $a_1 = a_2$.

A.5.3.3 Exercise. 1. (cf. Example A.5.2.9.1) Determine the kernel and the image of the linear transformation $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ given by

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} 3x - y + z \\ x + 4y + z \\ 4x + 3y + 2z \\ 0 \end{pmatrix}$$

2. (cf. Example A.5.2.9.2) Determine the kernel and the image of the homomorphism[364] $\pi : \mathbb{Z} \to \mathbb{Z}_5$ defined by $x \longmapsto x + (5)$

3. (cf. Example A.5.2.9.3) Determine the kernel and the image of the homomorphism from $(\mathbb{C} - \{0\}, \times, 1)$ to $(\mathbb{R} - \{0\}, \times, 1)$ given by $z \longmapsto |z|$.

4. (cf. Example A.5.2.9.4) Determine the kernel and the image of the homomorphism from $(GL(2, \mathbb{R}), \circ, I)$ to $(\mathbb{R} - \{0\}, \times, 1)$ given by $A \longmapsto \det A$.

Solution:

[364] π here is the name of a function, not the constant 3.141592653589793238... This is a symbol frequently used for a projection on to a quotient group (to be defined below).

1. The matrix of T is $[T] = \begin{pmatrix} 3 & -1 & 1 \\ 1 & 4 & 1 \\ 4 & 3 & 2 \\ 0 & 0 & 0 \end{pmatrix}$, i.e. the action of T is given by $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto [T] \begin{pmatrix} x \\ y \\ z \end{pmatrix}$. By row reduction we may determine the kernel (= *null space*) to be

$$\left\{ t \begin{pmatrix} -5 \\ -2 \\ 13 \end{pmatrix} : t \in \mathbb{R} \right\} .$$

The image is generated by the images of basis vectors, whose coordinates in the *standard basis* are the columns of the matrix $[T]$. *Column* reducing the matrix yields $\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & 1 & 0 \\ \frac{4}{3} & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (Gaussian reduction), eventually to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (Gauss-Jordan reduction). Thus the image is generated (spanned) by the vectors $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$.

2. The kernel is (5); π is onto.

3. The kernel is the *unit circle* about the origin in $\mathbb{C}$, i.e. $\{\cos\theta + i\sin\theta : 0 \leq \theta < 2\pi\}$ — the function is not one-to-one: every point the image, which is

$$(\{r \in \mathbb{R} : r > 0\}, \times, 1) ,$$

is the image of a circle in $\mathbb{C}$.

4. The kernel is the set of matrices of determinant 1, i.e. $\ker(\det) = SL(2, \mathbb{R})$. The image is the set of values that a determinant can assume; for any real number $r \neq 0$, we can form a diagonal nonsingular matrix having r in the upper left hand corner, and 1's elsewhere along the main diagonal, having determinant r. Hence this homomorphism is onto: its image is all of $\mathbb{R} - \{0\}$.

Henceforth, in writing compositions in a group $(\mathfrak{A}, *, e)$, we shall usually suppress the symbol $*$, unless there is some specific reason for including it, and write compositions by *juxtaposition*. One specific context where the composition symbol will be retained is "additive" *abelian* groups $(\mathfrak{A}, +, e)$; it is customary to reserve the $+$ sign for abelian groups[365], and not to suppress it in writing products (there usually called *sums*).

[365] *Caveat lector!* There are some exceptions to this practice, where the $+$ sign is used in a nonabelian group (cf. [34, p. 144]). We shall not meet any such exceptions in this course, however.

A.5.4 Action of a group on itself

Hitherto in this section we have mentioned permutation groups only as examples of groups. We shall show in this subsection that *every* group is isomorphic to a permutation group. Indeed, we shall demonstrate this by interpreting the elements of a group $(\mathfrak{A}, *, e)$ as acting as permutations of the set $\mathfrak{A}$.

We introduce several different ways in which a group may be viewed as acting on itself. In each case the action involves multiplication by the group element associated with the action, or by its inverse, or by both.

The use of the terms *left* and *right* in the following definitions, and the ordering of factors in products, is not completely standard. Some authors reverse these terms and/or the orders of factors.

A.5.4.1 DEFINITION. Let $(\mathfrak{A}, *, e)$ be a group.

1. For any $a \in \mathfrak{A}$ we define a function $L_a : \mathfrak{A} \longrightarrow \mathfrak{A}$ by $L_a(x) = ax$.
2. For any $a \in \mathfrak{A}$ we define a function $R_a : \mathfrak{A} \longrightarrow \mathfrak{A}$ by $R_a(x) = xa^{-1}$.
3. For any $a \in \mathfrak{A}$ we define a function $G_a : \mathfrak{A} \longrightarrow \mathfrak{A}$ by $G_a(x) = axa^{-1}$.

The apparent anomaly in defining R_a in terms of multiplication by a^{-1} rather than by a is intentional; we can still speak of the function that multiplies by a on the right — it is $R_{a^{-1}}$.

A.5.4.2 THEOREM. *Let $(\mathfrak{A}, *, e)$ be a group.*

1. *For any $a \in \mathfrak{A}$, $L_a \in \mathcal{S}_{\mathfrak{A}}$.*
2. *For any $a \in \mathfrak{A}$, $R_a \in \mathcal{S}_{\mathfrak{A}}$.*
3. *For any $a \in \mathfrak{A}$, $G_a \in \mathcal{S}_{\mathfrak{A}}$.*
4. *For any $a, b \in \mathfrak{A}$, $L_{ab} = L_a \circ L_b$.*
5. *For any $a \in \mathfrak{A}$, $L_{a^{-1}} = (L_a)^{-1}$ (the inverse mapping of the permutation L_a).*
6. *For any $a, b \in \mathfrak{A}$, $R_{ab} = R_a \circ R_b$.*
7. *For any $a \in \mathfrak{A}$, $R_{a^{-1}} = (R_a)^{-1}$.*
8. *For any $a, b \in \mathfrak{A}$, $G_{ab} = G_a \circ G_b$.*
9. *For any $a \in \mathfrak{A}$, $G_{a^{-1}} = (G_a)^{-1}$.*

A.5.4.3 EXERCISE. Prove Theorem A.5.4.2.

Solution:

1.

2.

3.

4.

5.

6.

7.

8.

9. □

A.5.4.4 THEOREM. *Let* $\mathfrak{B} \leq \mathfrak{A}$.

1. $(\{L_b : b \in \mathfrak{B}\}, \circ, I)$ *is a subgroup of* $\mathcal{S}_{\mathfrak{A}}$.
2. $(\{R_b : b \in \mathfrak{B}\}, \circ, I)$ *is a subgroup of* $\mathcal{S}_{\mathfrak{A}}$.
3. $(\{G_b : b \in \mathfrak{B}\}, \circ, I)$ *is a subgroup of* $\mathcal{S}_{\mathfrak{A}}$.

Proof:

1.

2.

3.

□

A.5.4.5 DEFINITION. 1. We call the elements of $(\{L_a : a \in \mathfrak{A}\}, \circ, I)$ *left translations*; the function

$$L : (\mathfrak{A}, *, e) \longrightarrow (\{L_a : a \in \mathfrak{A}\}, \circ, I)$$

given by $a \longmapsto L_a$ is called the *left regular representation* of $(\mathfrak{A}, *, e)$.

2. We call the elements of $(\{R_a : a \in \mathfrak{A}\}, \circ, I)$ *right translations*; the function

$$R : (\mathfrak{A}, *, e) \longrightarrow (\{R_a : a \in \mathfrak{A}\}, \circ, I)$$

given by $a \longmapsto R_a$ is called the *right regular representation* of $(\mathfrak{A}, *, e)$.

3. We call the elements of $(\{G_a : a \in \mathfrak{A}\}, \circ, I)$ *inner automorphisms*.

The terms *representation* and *regular* will be defined later in the course. For the present, *left regular representation* and *right regular representation* should be thought of simply as long names.

We can now justify some of the heavy formalism introduced. We show that the functions L and R are homomorphisms; and, moreover, that they are one-to-one. Thus each of L and R *embeds* the group $(\mathfrak{A}, *, e)$ as a subgroup of the permutation group $\mathcal{S}_{\mathfrak{A}}$. If we are interested only in the structure of groups up to isomorphism, we do not limit ourselves by studying permutation groups; every group $(\mathfrak{A}, *, e)$ is isomorphic to a subgroup of a symmetric group![366]

A.5.4.6 THEOREM. *1. L is a one-to-one homomorphism.*

2. R is a one-to-one homomorphism.

Proof: □

A.5.4.7 EXERCISE. Suppose that we define, for any $a \in \mathfrak{A}$, $R'_a : \mathfrak{A} \longrightarrow \mathfrak{A}$ by $R'_a(x) = xa$. Show that the function

$$R' : (\mathfrak{A}, *, e) \longrightarrow (\{R'_a : a \in \mathfrak{A}\}, \circ, I)$$

given by $a \longmapsto R'_a$ need not be a homomorphism.[367]

Solution: We select a convenient non-abelian group — say $\mathcal{S}_3$, the smallest such group. Then we select two elements that do not commute, for example (12) and (123):

$$(12)(123) = (23) \neq (13) = (123)(12)\,.$$

$$R'_{(12)}R'_{(123)}(e) = e(123)(12) = (13) \neq (23) = e(23) = R'_{(12)(123)}(e)\,.$$

Thus $R'_{(12)}R'_{(123)}$ acts differently from $R'_{(12)(123)}$ on the element e, and so it is not true that $R'_{(12)}R'_{(123)} = R'_{(12)(123)}$.

[366] There is a cost to this theorem. If we begin with a permutation group acting on a set of n elements, the isomorphic copy we find in the symmetric group may act on as many as $n!$ elements.

[367] In fact, it is what is called an *antihomomorphism*.

A.5.4.8 EXERCISE. The group $\mathcal{D}_6$ of symmetries of the hexagon with vertices 1, 2, 3, 4, 5, 6 (in that order) contains a subgroup $\mathcal{H}$ of order 6 having $\{1,3,5\}$ and $\{2,4,6\}$ as orbits. Under the *left regular representation* $\phi : \mathcal{D}_6 \longrightarrow \mathcal{S}_{\mathcal{D}_6}$, each of the permutations in $\mathcal{H}$ is mapped on to a permutation of the 6 elements of $\mathcal{H}$.

1. Determine the disjoint cycle representation of each element in the image of ϕ. Remember, each of these will be a product of cycles which permute the 6 elements of $\mathcal{D}_6$. For example,

$$\phi(e) = (e)\ ((135)(246))\ ((153)(264))\ ((26)(35))\ ((15)(24))\ ((13)(46)).$$

[Hint: $\mathcal{D}_6$ has three subgroups of order 6:

$$\begin{aligned}\mathcal{H}_1 &= \langle(123456)\rangle \\ \mathcal{H}_2 &= \{e,(135)(246),(153)(264),(26)(35),(13)(46),(15)(24)\} \\ \mathcal{H}_3 &= \{e,(135)(246),(153)(264),(14)(23)(56),(12)(36)(45),(16)(25)(34)\}\,]\end{aligned}$$

2. Determine the orbits of the image of ϕ.

Solution:

1. $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ respectively have orbits

$$\{1,2,3,4,5,6\}$$

$$\{1,3,5\},\ \{2,4,6\}$$

$$\{1,2,3,4,5,6\}$$

Thus the group under consideration for this problem is $\mathcal{H}_2$.

$$\begin{aligned}\phi(e) &= (e)\ ((135)(246))\ ((153)(264))\ ((26)(35))\ ((15)(24)) \\ &\quad \cdot((13)(46)) \\ \phi((135)(246)) &= (e\ (135)(246)\ (135)^2(246)^2) \\ &\quad \cdot((26)(35)\ (135)(246)(26)(35)\ (135)^2(246)^2(26)(35)) \\ &= (e\ (135)(246)\ (152)(264))\ ((26)(35)\ (13)(46)\ (15)(24)) \\ \phi((153)(264)) &= (e\ (153)(264)\ (153)^2(264)^2) \\ &\quad \cdot((26)(35)\ (153)(264)(26)(35)\ (153)^2(264)^2(26)(35)) \\ &= (e\ (153)(264)\ (135)(246))\ ((26)(35)\ (15)(24)\ (13)(46)) \\ \phi((26)(35)) &= (e\ (26)(35))((135)(246)\ (15)(24))\ ((153)(264)\ (13)(46)) \\ \phi((15)(24)) &= (e\ (15)(24))((135)(246)\ (13)(46))\ ((153)(264)\ (26)(35)) \\ \phi((13)(46)) &= (e\ (13)(46))((135)(246)\ (26)(35))\ ((153)(264)\ (15)(24))\end{aligned}$$

2. Any left regular representation is transitive: if g_1 and g_2 are any elements of the group, the left representation of the group element $g_2 g_1^{-1}$ is a permutation which carries g_1 on to $g_2 g_1^{-1} \cdot g_1 = g_2$; thus all elements are in the same orbit.

A.5.4.9 DEFINITION. Let $(\mathfrak{B}, *, e) \leq (\mathfrak{A}, *, e)$.

1. Orbits of $(\mathfrak{A}, *, e)$ under the action of the group of left translations associated with elements of a subgroup $(\mathfrak{B}, *, e)$ are called *right*[368] *cosets* of $(\mathfrak{B}, *, e)$ in $(\mathfrak{A}, *, e)$. The right coset containing an element a may be denoted by $(\mathfrak{B}, *, e)a$, or simply by $\mathfrak{B}a$.

2. Orbits of a group $(\mathfrak{A}, *, e)$ under the action of the group of right translations associated with elements of a subgroup $(\mathfrak{B}, *, e)$ are called *left cosets* of $(\mathfrak{B}, *, e)$ in $(\mathfrak{A}, *, e)$. The left coset containing an element a may be denoted by $a(\mathfrak{B}, *, e)$, or simply by $a\mathfrak{B}$.

3. Orbits of a group under the action of the group of its inner automorphisms are called *conjugate classes* or *conjugacy classes*.

4. An element which is alone in its conjugate class — i.e. a fixed point of the inner automorphism group — is said to be *self-conjugate*.

A.5.4.10 EXERCISE. *Showing all of your work,* determine the conjugacy classes of the elements of each of the following groups:

1. $\mathcal{D}_6$
2. $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
3. $\mathcal{A}_5$
4. $\mathbb{Z}_3 \times \mathcal{S}_3$

Solution:

1. As always, the identity element is alone in its conjugacy class; $g_1 e g_1^{-1} = e$ always.

   We select any other element, and determine its conjugates; then repeat the process until we have exhausted all elements of the group. For example, beginning with (135)(246) we find that (26)(35) (135)(246) $((26)(35))^{-1}$ = (153)(264); (13)(46) (135)(246) (13)(46) = (153)(264), etc. Indeed, it can be shown that all conjugates in $\mathcal{S}_n$ have the same cycle structure. Thus the only candidate for a

[368] Remember, usage of the terms *right* and *left* is not standardized!

conjugate of (135)(264) (other than that element itself) is (153)(264). We have shown that these two elements are indeed conjugate. So one conjugacy class is $\{(135)(246),\ (153)(264)\}$.

We proceed to any remaining element, say (26)(35). One conjugate is

$$(135)(246)\ (26)(35)\ (153)(264) = (15)(24);$$

another is (153)(264) (26)(35) (135)(246) = (13)(46). We have exhausted all elements of this cycle structure, so the orbit is

$$\{(26)(35),\ (15)(24),\ (13)(46)\}.$$

There are 4 elements of cycle structure $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)$ in the group: the half-turn (14)(25)(36), and the three *edge-centred* reflections. The half turn is a power of (123456), so multiplying it on the left by a power of this rotation, and on the left by the inverse power, will leave it unchanged. We can also verify that

$$(12)(36)(45)\ (14)(25)(36)\ ((12)(36)(45))^{-1} = (14)(25)(36)$$

and

$$(13)(46)\ (14)(25)(36)\ ((13)(46))^{-1} = (14)(25)(36)\,;$$

by symmetry, conjugation by any reflection leaves this element invariant. Thus (14)(25)(36) is conjugate to no other elements of the group.

$$(135)(246)\ (12)(36)(45)\ (153)(264) = (16)(25)(34),$$

$$(153)(264)\ (12)(36)(45)\ (135)(246) = (14)(23)(56).$$

Thus the remaining three reflections are together in the conjugacy class

$$\{(12)(36)(45),\ (16)(25)(34),\ (14)(23)(56)\}.$$

We have now accounted for $1 + 2 + 3 + 1 + 3 = 10$ elements of the group; there remain the two cycles of length 6: (123456), and (165432). Since

$$(16)(25)(34) \cdot (123456) \cdot ((16)(25)(34))^{-1}\,,$$

these two elements constitute another orbit.

2. Where a group $\mathcal{G}$ is abelian, all products $g_1 g g_1^{-1}$ (or sums $g_1 + g - g_1$ if the group is being written additively) are equal to g. Thus the equivalence classes under conjugation each contain just one element!

3. We know that, in $\mathcal{S}_5$, all elements of the same cycle structure are conjugate. Some of these pairs will remain conjugate in $\mathcal{A}_5$. Indeed, conjugacy in $\mathcal{A}_5$ will be a *refinement* of the equivalence relation of conjugacy in $\mathcal{S}_5$ — i.e. the equivalence classes will each be fully contained in one of the conjugacy classes of $\mathcal{S}_5$. One class is evidently e. The elements of type $(\cdot\cdot)(\cdot\cdot)$ are easily seen to be conjugate in $\mathcal{A}_5$:

$$(13)(12)(34)(13)^{-1} = (14)(23) = (12)(13)(24)(12)^{-1}$$

From the equation $(34)(123)(34) = (124)$ we see that we may progressively move from any element of type $(\cdots)(\cdot)(\cdot)$ to any other element by a series of conjugations by a transposition; thus all such elements constitute one conjugacy class in $\mathcal{A}_5$.

The only remaining type of permutation to consider is $(\cdot\cdot\cdot\cdot\cdot)$. Students were not provided with machinery for a short proof that these do not constitute a single conjugacy class. By laborious computations it can be shown that, in fact, they constitute 2 classes. (A proof can be found in [34, p. 43, proof of Lemma 3.12], and may be discussed in the lectures.)

4. In the abelian group $\mathbb{Z}_3$ each element is conjugate only to itself; in the group $\mathcal{S}_3$ the conjugacy classes are the sets of elements having the same cycle index. Let $(a, f) \in \mathbb{Z}_3 \times \mathcal{S}_3$. Then for any $(b, g) \in \mathbb{Z}_3 \times \mathcal{S}_3$, $(b, g)(a, f)(b, g)^{-1} = (b, g)(a, f)(-b, g^{-1}) = (b + a - b, gfg^{-1}) = (a, gfg^{-1})$, since $\mathbb{Z}$ is abelian. And we know that gfg^{-1} has the same cycle index as f. Thus conjugate elements must coincide in their first argument, and all have — in their second argument — permutations having the same cycle index in $\mathcal{S}_3$. Conversely, suppose that (a, f), and (a, g) are elements of $\mathbb{Z}_3 \times \mathcal{S}_3$, where f and g have the same cycle structure in $\mathcal{S}_3$. Then there exists a permutation $h \in \mathcal{S}_3$ such that $hfh^{-1} = g$, so that $(0, h)(a, f)(0, h)^{-1} = (0 + a + 0, hfh^{-1}) = (a, g)$, and the two given elements are conjugate. Thus there are altogether 9 conjugate classes:

$$\{(0, e)\},\ \{(1, e)\},\ \{(2, e)\}\,;\ \{(0, (12)), (0, (23)), (0, (13))\},$$

$$\{(1, (12)), (1, (23)), (1, (13))\},\ \{(2, (12)), (2, (23)), (2, (13))\},$$

$$\{(0, (123)), (0, (132))\},\ \{(1, (123)), (1, (132))\},\ \{(2, (123)), (2, (132))\}\,.$$

A.5.4.11 THEOREM. *Let $(\mathfrak{A}, *, e)$ be a group, and $(\mathfrak{B}, *, e) \leq (\mathfrak{A}, *, e)$.*

1. (a) *$\mathfrak{B}a_1 \cap \mathfrak{B}a_2 \neq \emptyset \Leftrightarrow \mathfrak{B}a_1 = \mathfrak{B}a_2 \Leftrightarrow a_1$ and a_2 are equivalent under the group of left translations by an element of $\mathfrak{B}$.*
   (b) *$\mathfrak{B}a_1 = \mathfrak{B}a_2 \Leftrightarrow a_1 a_2^{-1} \in \mathfrak{B}$*
   (c) *$|\mathfrak{B}a| = |\mathfrak{B}|$ for all $a \in \mathfrak{A}$.*

(d) **(Theorem of Lagrange)** *If* $|\mathfrak{A}|$ *is finite, then* $|\mathfrak{B}| \mid |\mathfrak{A}|$. *In words, the order of a finite group is divisible by the order of any subgroup.*

2. The analogous properties hold for left cosets.

A.5.4.12 EXERCISE. Prove Theorem A.5.4.11.

Our earlier use of the word *coset* to describe subsets of $\mathbb{Z}$ of the form $a + (m)$ is consistent with the present use: the group and subgroup in that case are respectively $(\mathbb{Z}, +, 0)$ and $(m\mathbb{Z}, +, 0)$, the latter usually being denoted by (m). In that case there is also a *multiplicative* structure. Eventually we shall be defining *cosets of an ideal in a ring*, of which these are an example.

A.5.4.13 DEFINITION. Where $\mathfrak{A}$ is finite, and $\mathfrak{B} \leq \mathfrak{A}$ we often speak of the *left* and *right coset decompositions* as respectively the following partitions of $\mathfrak{A}$ into distinct cosets:

$$\mathfrak{A} = \ell_1\mathfrak{B} \cup \ell_2\mathfrak{B} \cup ... \cup \ell_k\mathfrak{B}$$

$$\mathfrak{A} = \mathfrak{B}r_1 \cup \mathfrak{B}r_2 \cup ... \cup \mathfrak{B}r_k$$

where ℓ_1, ℓ_2, ..., ℓ_k; r_1, r_2, ..., r_k are elements of $\mathfrak{A}$, called, respectively, *left coset representatives*, and *right coset representatives*. Usually we will take $\ell_1 = r_1 = e$. The common number of left and right cosets is called the *index* of $\mathfrak{B}$ in $\mathfrak{A}$, and denoted by $[\mathfrak{A} : \mathfrak{B}]$.

A.5.4.14 THEOREM. *Let* $\mathfrak{A}$ *be a finite group, and suppose that* $\mathfrak{A} \leq \mathfrak{B}$. *Then*

$$[\mathfrak{A} : \mathfrak{B}] = \frac{|\mathfrak{A}|}{|\mathfrak{B}|}$$

A.5.4.15 EXERCISE. Determine left and right coset decompositions of $\mathcal{D}_6$ with respect to the subgroup $\mathcal{L}$ generated by (135)(246).

Solution: The cosets will all contain 3 elements — the order of the subgroup. We describe them with a particular selection of *coset representatives* — i.e. of elements by which we multiply all elements of the subgroup, or, equivalently, of elements selected from the cosets. These selections are arbitrary: any element in a coset can be used as representative of that coset.

$$\begin{aligned}
\mathcal{L} &= \{e,\ (135)(246),\ (153)(264)\} \\
\mathcal{L}(123456) &= \{(123456),\ (135)(246)(123456),\ (153)(264)(123456)\} \\
&= \{(123456),\ (14)(25)(36),\ (165432)\} \\
\mathcal{L}(12)(36)(45) &= \{(12)(36)(45),\ (135)(246)(12)(36)(45), \\
&\quad (153)(264)(12)(36)(45)\} \\
&= \{(12)(36)(45),\ (14)(23)(56),\ (16)(25)(34)\} \\
\mathcal{L}(13)(46) &= \{(13)(46),\ (135)(246)(13)(46),\ (153)(264)(13)(46)\} \\
&= \{(13)(46),\ (15)(24),\ (26)(35)\};
\end{aligned}$$

$$\begin{aligned}
\mathcal{L} &= \{e,\ (135)(246),\ (153)(264)\} \\
(123456)\mathcal{L} &= \{(123456),\ (123456)(135)(246),\ (123456)(153)(264)\} \\
&= \{(123456),\ (14)(25)(36),\ (165432)\} \\
(12)(36)(45)\mathcal{L} &= \{(12)(36)(45),\ (12)(36)(45)(135)(246), \\
&\quad (12)(36)(45)(153)(264)\} \\
&= \{(12)(36)(45),\ (16)(25)(34),\ (14)(23)(56)\} \\
(13)(46)\mathcal{L} &= \{(13)(46),\ (13)(46)(135)(246),\ (13)(46)(153)(264)\} \\
&= \{(13)(46),\ (26)(35),\ (15)(24)\}.
\end{aligned}$$

We see that every left coset of this subgroup is a right coset, and vice versa; a coset with this property is said to be *normal*; properties of normality will be investigated in §A.5.5 below. Note that although we have written the elements of the cosets in different orders, that order is totally irrelevant.

A.5.4.16 Exercise. Determine left and right coset decompositions of $\mathcal{D}_6$ with respect to the subgroup $\mathcal{M} = \{e,\ (26)(35),\ (14)(23)(56),\ (14)(25)(36)\}$.

Solution:

$$\begin{aligned}
\mathcal{M} &= \{e,\ (26)(35),\ (14)(23)(56),\ (14)(25)(36)\} \\
\mathcal{M}(123456) &= \{(123456),\ (26)(35)(123456),\ (14)(23)(56)(123456), \\
&\quad (14)(25)(36)(123456)\} \\
&= \{(123456),\ (16)(25)(34),\ (13)(46),\ (153)(264)\} \\
\mathcal{M}(165432) &= \{(165432),\ (26)(35)(165432),\ (14)(23)(56)(165432), \\
&\quad (14)(25)(36)(165432)\} \\
&= \{(165432),\ (12)(36)(45),\ (15)(24),\ (135)(246)\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{M} &= \{e,\ (26)(35),\ (14)(23)(56),\ (14)(25)(36)\} \\
(123456)\mathcal{M} &= \{(123456),\ (123456)(26)(35),\ (123456)(14)(23)(56), \\
&\quad (123456)(14)(25)(36)\} \\
&= \{(123456),\ (12)(36)(45),\ (15)(24),\ (153)(264)\} \\
(165432)\mathcal{M} &= \{(165432),\ (165432)(26)(35),\ (165432)(14)(23)(56), \\
&\quad (165432)(14)(25)(36)\} \\
&= \{(165432),\ (16)(25)(34),\ (13)(46),\ (135)(246)\}.
\end{aligned}$$

Here the left cosets are not right cosets — the subgroup is not invariant. (Note that we have used the same representatives for left and right cosets. This is not necessary, but it can always be done.)

A.5.4.17 Exercise. Show that, for any n, $[\mathcal{S}_n : \mathcal{A}_n] = 2$.

Solution: □

A.5.4.18 Theorem. *Let $\mathcal{G}$ be a group of permutations of a set $\mathfrak{A}$, and let $\mathfrak{O}$ be the orbit of $\mathfrak{A}$ containing an element a.*

1. *Suppose that $g \in \mathcal{G}$. Then the inner automorphism (340) of $\mathcal{G}$ induces an isomorphism between $\mathcal{G}_a$ and $\mathcal{G}_{g(a)}$.*
2. *The elements of the left coset $g(a)\mathcal{G}_a$ are precisely those members of $\mathcal{G}$ which map a on to $g(a)$.*
3. $$|\mathfrak{O}| = [\mathcal{G} : \mathcal{G}_a]$$

Proof:

1. By Theorem A.3.4.6 mapping (340) induces a bijection; since it is now known to be an automorphism, that bijection is an isomorphism.
2. Evidently all elements of the left coset map a onto the same element $g(a)$. Conversely, if $f \in \mathcal{G}$ is such that $f(a) = g(a)$, then $g^{-1}f \in \mathcal{G}_a$, so $f \in g\mathcal{G}_a$.
3. By the preceding, each left coset of $\mathcal{G}_a$ in $\mathcal{G}$ corresponds to a distinct element of the orbit $\mathfrak{O}$. □

(Part 3 was applied in the proof of Theorem A.3.7.3.)

By Lagrange's theorem, the periods of all elements of a group divide the order of the group. The converse, however is not true: not every divisor of the order of a group need be realized as the period of an element.

A.5.5 Normal Subgroups. Quotient Groups

A.5.5.1 DEFINITION. A subgroup $\mathfrak{B} \leq \mathfrak{A}$ is said to be *normal* or *invariant* if it is invariant under the action of the group of inner automorphisms. We may then write $\mathfrak{B} \trianglelefteq \mathfrak{A}$.

A.5.5.2 EXERCISE. Let $\mathfrak{B} \leq \mathfrak{A}$. Prove that each of the following conditions is equivalent to $\mathfrak{B} \trianglelefteq \mathfrak{A}$:

1. $\left.\begin{array}{rcl} a & \in & \mathfrak{A} \\ b & \in & \mathfrak{B} \end{array}\right\} \Rightarrow aba^{-1} \in \mathfrak{B}$
2. $\left.\begin{array}{rcl} a & \in & \mathfrak{A} \\ b & \in & \mathfrak{B} \end{array}\right\} \Rightarrow a^{-1}ba \in \mathfrak{B}$
3. Every left coset of $\mathfrak{B}$ is also a right coset.
4. Every right coset of $\mathfrak{B}$ is also a left coset.
5. $a \in \mathfrak{A} \Rightarrow a\mathfrak{B}a^{-1} = \mathfrak{B}$.
6. $\mathfrak{B}$ is a union of conjugate classes of $\mathfrak{A}$

Solution:

1.
2.
3.
4.
5.
6.

□

A.5.5.3 EXERCISE. Show that every subgroup of an abelian group is normal.

Solution: When a subgroup is of index 2 all elements of the group not in the subgroup consistute the remaining coset — in the left and right cases. Thus they form a left coset, and also a right coset. Hence every left coset is also a right coset, and the subgroup is normal. □

A.5.5.4 Exercise. Show that a subgroup of index 2 is always normal. Conclude that any alternating group is invariant in the corresponding symmetric group.

Solution: □

A.5.5.5 Exercise. (cf. Exercise A.3.4.3) Prove that $SL(n,\mathbb{R}) \triangleleft GL(n,\mathbb{R})$.

A.5.5.6 Example. If $\mathcal{K} \trianglelefteq \mathcal{M} \trianglelefteq \mathcal{G}$ it need not follow that $\mathcal{K} \trianglelefteq \mathcal{G}$. For example, let $\mathcal{G} = \mathcal{D}_4$, $\mathcal{M} = \{e, (14)(23), (13)(24), (12)(34)\}$. The subgroup has index 2 in $\mathcal{D}_4$, so it must be normal. It is a group of 4 elements, the identity, and three elements of order 2, each of which is the product of the other two: i.e. it has the structure of the Klein 4-group; in particular, it is abelian, so any subgroup is normal. Select, for example, $\mathcal{K} = \{e, (12)(34)\}$; then $\mathcal{K} \triangleleft \mathcal{M} \triangleleft \mathcal{G}$. But $\mathcal{K}$ is transformed under certain conjugations to the subgroup $\{e, (14)(23)\}$, so $\mathcal{K} \not\triangleleft \mathcal{G}$.

A.5.5.7 Exercise. We know from the theorem of Lagrange that the order of every subgroup $\mathcal{H}$ of a finite group $\mathcal{G}$ is a divisor of $|\mathcal{G}|$. The following example shows that the converse is not generally true: there exist divisors d of $\mathcal{G}$ for which no subgroup $\mathcal{H}$ of $\mathcal{G}$ has order $|\mathcal{H}| = d$.

Let $\mathcal{G} = \mathcal{A}_4$, having order $4!/2 = 12$, and suppose that $\mathcal{H} \leq \mathcal{A}_4$, $|\mathcal{H}| = 6$.

1. Show that $\{g^2 : g \in \mathcal{G}\} \subseteq \mathcal{H}$.
2. Show that every cycle of length 3 in $\mathcal{A}_4$ is contained in $\mathcal{H}$.
3. Show that there are more than 5 3−cycles (ijk) in $\mathcal{A}_4$.
4. Conclude that no such $\mathcal{H}$ can exist.

Solution:

1. The alleged subgroup has index 2 in $\mathcal{G}$, so it must be normal. Consider an element $a \notin \mathcal{H}$ as representative of the coset distinct from $\mathcal{H}$. Then a^{-1} must be in the same coset (since it can't be in $\mathcal{H}$). The product of the coset with itself is therefore the coset $\mathcal{H}aa^{-1} = \mathcal{H}$; hence a^2, an element of that product, must be in $\mathcal{H}$. And, of course, the square of every element of $\mathcal{H}$ is surely in $\mathcal{H}$.
2. For any such cycle $\alpha = (ijk)$, $\alpha^3 = e$. Hence $\alpha = \alpha^{1+3} = (\alpha^2)^2$. Being a square, the element is in $\mathcal{H}$.
3. The number of subsets of 3 elements is $\begin{pmatrix} 4 \\ 3 \end{pmatrix} = 4$; each of these yields 2 3−cycles.

4. If it existed, the subgroup would contain all squares, hence all 3-cycles, hence — even before we count the identity — at least $8+1 > 6$ elements, a contradiction. □

Where a subgroup is normal, we may define a composition under which the set of cosets becomes a group. The necessary preliminaries are supplied by the following lemmas.

A.5.5.8 LEMMA. *Let $(\mathfrak{B}, *, e) \trianglelefteq (\mathfrak{A}, *, e)$, and let b_1 and b_2 be arbitary elements of $\mathfrak{B}$, and a_1 and a_2 be arbitary elements of $\mathfrak{A}$. Then*

$$a_1 b_1 a_2 b_2 \in a_1 a_2 \mathfrak{B}$$

Moreover, every element of $a_1 a_2 \mathfrak{B}$ is expressible as the product of an element of coset $a_1\mathfrak{B}$ followed by an element of coset $a_2\mathfrak{B}$.

Proof: $a_1 b_1 a_2 b_2 = a_1 a_2 (a_2^{-1} b_1 a_2) b_2$. By Exercise A.5.5.2, $a_2^{-1} b_1 a_2 \in \mathfrak{B}$, since $\mathfrak{B}$ is normal in $\mathfrak{A}$. By closure of $\mathfrak{B}$ under composition, $(a_2^{-1} b_1 a_2) b_2 \in \mathfrak{B}$, so $a_1 b_1 a_2 b_2 \in a_1 a_2 \mathfrak{B}$.

Since a_i is an element of $a_i\mathfrak{B}$, $(i = 1, 2)$, we have shown that the coset $(a_1 a_2)\mathfrak{B}$ coincides with the set of products of an element of $a_1\mathfrak{B}$ followed by an element of $a_2\mathfrak{B}$. □

We have thus shown that the composition operation in $\mathfrak{A}$ *induces* a composition in the set of cosets. More precisely, we may now define:

A.5.5.9 DEFINITION. Let $(\mathfrak{B}, *, e) \trianglelefteq (\mathfrak{A}, *, e)$. We denote the set of cosets of $\mathfrak{B}$ in $\mathfrak{A}$ by $\mathfrak{A}/\mathfrak{B}$. On this set we define a composition (usually denoted by juxtaposition or plus without confusion with the operation of the group $\mathfrak{A}$) by

$$(a_1\mathfrak{B}, a_2\mathfrak{B}) \longmapsto (a_1 a_2)\mathfrak{B} \tag{352}$$

A.5.5.10 LEMMA. *1. The composition defined in (352) is associative.*

2. The coset $e\mathfrak{B}$ is an identity of the semigroup structure which (352) defines on $\mathfrak{A}/\mathfrak{B}$.

3. For any element $a \in \mathfrak{A}$, the coset $a^{-1}\mathfrak{B}$ is the inverse of the coset $a\mathfrak{B}$.

4. The composition defined in (352) endows $\mathfrak{A}/\mathfrak{B}$ with a group structure.

A.5.5.11 EXERCISE. Prove Lemma A.5.5.10

A.5.5.12 DEFINITION. We call the group $\mathfrak{A}/\mathfrak{B}$ a *quotient group*. (This notation is used even when $\mathfrak{A}$ is written as an additive abelian group.)

A.5.5.13 EXAMPLE. For any natural number m, $(m\mathbb{Z}, +, 0) \triangleleft (\mathbb{Z}, +, 0)$, since the groups are abelian. We have already discussed the additive structure of $\mathbb{N}/m\mathbb{N}$ in §A.1.7; we shall impose a second structure — that of a multiplicative monoid — in the sequel.

A.5.5.14 Exercise. Suppose that $\mathfrak{B} \trianglelefteq \mathfrak{A}$. Define a mapping

$$\pi : \mathfrak{A} \longrightarrow \mathfrak{A}/\mathfrak{B}$$

by

$$a \longmapsto a\mathfrak{B}$$

1. Prove that π is a homomorphism.
2. Prove that π is onto.
3. Prove that the kernel of π is $\mathfrak{B}$.

A.5.5.15 Exercise. Let $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ be a homomorphism of groups.

1. Show that $\ker \phi \trianglelefteq \mathfrak{A}$.
2. Show that it need not be true that $\mathrm{Im}\ \phi \trianglelefteq \mathfrak{B}$.

Solution:

1.

2.

A.5.6 Generators and Relations. Cyclic Groups.

Continuing the discussion of §A.4.A.4.4, we extend Definition A.4.4.5 to groups. Let $(\mathfrak{A}, *, e)$ be a group, and let $\mathfrak{B} \subseteq \mathfrak{A}$. We have defined what we mean by $\langle \mathfrak{B} \rangle$, the submonoid generated by $\mathfrak{B}$. But our definition was tailored to the only operation we had on a monoid, the binary operation of composition. When we consider the monoid generated by a subset of a group, we may find that it is not a subgroup! For example, the submonoid of $(\mathbb{Z}, +, 0)$ generated by $\{1\}$ is $\mathbb{N}$, which is not a subgroup. We can remedy this deficiency by insisting that the monoid be generated by the elements in $\mathfrak{B}$ *and their inverses.* That is what is achieved by the following definition. As there is no practical likelihood of confusion, we use the same symbol for a generated subgroup as a generated submonoid.

A.5.6.1 Definition. Let $(\mathfrak{A}, *, e)$ be a group, and $\mathfrak{B} \subseteq \mathfrak{A}$. We define[369]

$$\langle \mathfrak{B} \rangle = \{e\} \cup \left(\{ b_1^{\epsilon_1} * b_2^{\epsilon_2} * ... * b_r^{\epsilon_r} : b_i \in \mathfrak{B}, \epsilon_i \in \{-1, 1\}; i = 1, 2, ..., r; r = 1, 2, ... \}, *, e \right).$$

[369]It is tempting to write this definition more compactly in terms of ± 1. But the usual convention for the use of this symbol (cf. Footnote 341) does not permit the use of this notation for several *independent* variables simultaneously.

A.5.6.2 EXERCISE. Let $(\mathfrak{A}, *, e)$ be a group, and $\mathfrak{B} \subseteq \mathfrak{A}$. Prove that $\langle \mathfrak{B} \rangle \leq (\mathfrak{A}, *, e)$.

Solution: We are considering the set of words — including the "empty word" e — generated by the set $\mathfrak{B} \cup \{b^{-1} : b \in \mathfrak{B}\}$. As this set of generated words is evidently closed under composition, we need only verify closure under the taking of inverses. But the inverse of a word $b_1^{\epsilon_1} * b_2^{\epsilon_2} * ... * b_r^{\epsilon_r}$ is $b_r^{-\epsilon_r} * b_{r-1}^{-\epsilon_{r-1}} * ... * b_1^{-\epsilon_1}$, also an element of $\langle \mathfrak{B} \rangle$. □

We also revise the meaning of the word *cyclic* when applied to groups. (This definition appears to be the same as for a cyclic monoid. The difference is in the meaning of a generating set.)

A.5.6.3 DEFINITION. A *cyclic* group is one that is generated by a single element.

A.5.6.4 EXAMPLE.

1. (cf. Example A.4.4.6.4) $(\mathbb{Z}, +, 0) = \langle 1 \rangle$. Note that we need not list -1 among the generators. As a *group* $(\mathbb{Z}, +, 0)$ is cyclic; but, as a *monoid*, it cannot be generated with fewer than 2 generators.

2. The group of rotations of an n-gon is a cyclic sugroup of the dihedral group $\mathcal{D}_n$, generated by the cycle $(12...n)$. This subgroup is often denoted by $\mathcal{C}_n$.

3. The group $(\mathbb{Z}/6\mathbb{Z}, +, 0 + (6))$ of residue classes (cosets) modulo 6 is cyclic, generated by $1+(6)$ or $5+(6)$. (The *number* of different elements that can each generate a cyclic group will be investigated below.)

4. Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$. Then $\langle a, b \rangle = \langle (a, b) \rangle$ by Theorem A.1.7.4.

5.

The subgroup $\langle a \rangle$ generated by a single element $a \in \mathfrak{A}$ is of particular interest.

A.5.6.5 DEFINITION. Let $\mathfrak{A}$ be a group.

1. The *period* or *order* of an element a of $\mathfrak{A}$, denoted by period(a), will be the order of the subgroup $\langle a \rangle$. Where $|\langle a \rangle|$ is finite, a is said to be *of finite period (order)*; otherwise *of infinite period (order)*.

2. a is said to *belong to exponent* n if $a^n = e$.

3. The *exponent* of $\mathfrak{A}$ is defined to be

$$\max\{\text{period}(a) : a \in \mathfrak{A}\}$$

where all elements of $\mathfrak{A}$ have finite period.

A.5.6.6 EXERCISE. 1. Show that a non-identity element has period 2 iff it is equal to its inverse.

2. Show that the period of an element is equal to the period of its inverse.

3. Let $\mathfrak{A}$ be a group of of even order, $2k$. Prove that $\mathfrak{A}$ must contain an element of period 2. (Hint: Prove that the number of elements of $\mathfrak{A}$ which have period 2 is odd.)

4. Give an example to show that the preceding result fails if the order of $\mathfrak{A}$ is odd.

5. Compute the composition table of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the *Klein 4-Group*) to show that a group whose order is divisible by 4 need not contain an element of period 4.

Solution:

1. $a^2 = e \Leftrightarrow a^2a^{-1} = a^{-1} \Leftrightarrow a = a^{-1}$

2. $a^k = e \Leftrightarrow a^ka^{-k} = ea^{-k} \Leftrightarrow e = a^{-k}$

3. A non-identity element has period different from 2 iff its inverse (also distinct from the identity) has period different from 2. Each is distinct from its inverse; the total number of elements in these pairs is even, leaving an even number of elements, one of which is the identity. The remaining odd number of elements are those of period 2.

4. $\mathbb{Z}_3$ contains the identity, of period 1, and two elements of period 2.

5. We represent the ordered pairs as 2-digit binary words:

	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

. As the main diagonal entries are all 00, every nonidentity element has order 2.

□

A.5.6.7 THEOREM. *Let a be an element of finite period in the group $\mathfrak{A}$.*

1. *If $a^n = e$ (i.e. if a belongs to exponent n), then period$(a) \mid n$.*

2. *period(a) is the smallest positive integer n such that $a^n = e$.*

3. *period(a) divides $|\mathfrak{A}|$.*

4. *The exponent of* $\mathfrak{A}$ *divides* $|\mathfrak{A}|$.

5. *If* $m \mid period(a)$, *then*

$$period\,(a^m) = \frac{period(a)}{m} \tag{353}$$

Proof: As the subgroup generated by a is finite, there exist distinct integers n_1 and n_2 such that $a^{n_1} = a^{n_2}$. Without limiting generality, assume $n_1 < n_2$. Then multiplying by the appropriate power of a^{-1} yields $a^{n_2-n_1} = e$. Thus the set $\{n \in \mathbb{N} : a^n = e\}$ is not empty. Let n_0 be the minimum element in this set.

Suppose that $a^n = e$. By the division algorithm there exist integers q, r such that $n = q \cdot n_0 + r$, where $0 \leq r \leq n_0 - 1$. Then $(a^{n_0})^q * a^r = e \Rightarrow e^q * a^r = e \Rightarrow a^r = e$. By the minimality of n_0 we may conclude that $r = 0$, i.e. that $n_0 \mid n$.

Consider now the elements of $\langle a \rangle$. These are all expressible as powers of a: ..., a^{-3}, a^{-2}, a^{-1}, $a^0 = e$, a, a^2, a^3, ... Since $a^{n_0} = e$, a^{-1} is expressible as a positive power of a. Thus the elements of $\langle a \rangle$ are all expressible as *positive* powers of a: a, a^2, a^3, ..., a^{n_0}. There can be no repetitions in this list, since that would imply that a smaller power of a is the identity. Hence $n_0 = \text{period}(a)$.

The exponent of $\mathfrak{A}$ is the maximum of a set of divisors of $|\mathfrak{A}|$.

Now suppose that $m \mid \text{period}(a)$. Then

$$(a^m)^{\frac{\text{period}_{(a)}}{m}} = a^{\text{period}_{(a)}} = e$$

so

$$\text{period}\,(a^m) \mid \frac{\text{period}(a)}{m}$$

But, from

$$a^{m\text{period}_{(a^m)}} = (a^m)^{\text{period}_{(a^m)}} = e$$

we deduce that $\text{period}(a) \mid m\text{period}\,(a^m)$; (353) follows. □

All cyclic groups of order n are isomorphic. When we wish to state a theorem about such groups we may specify one convenient *isomorph*, for example, $(\mathbb{Z}_n, +, 0)$, or $(\mathcal{C}_n, \circ, (1)(2)...(n))$.

A.5.6.8 Example. To appreciate why we did not introduce the concept of *period* when we studied monoids, consider the following example. Let $\mathfrak{B} = \{1, 2, 3, ..., 7\}$. Define the function $f : \mathfrak{B} \longrightarrow \mathfrak{B}$ by $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 5$, $5 \mapsto 6$, $6 \mapsto 7$, $7 \mapsto 4$. Define f^n recursively by $f^1 = f$, $f^{n+1} = f^n \circ f$ $(n = 1, 2, ...)$. Then $(\{\text{id}_{\mathfrak{B}}, f, f^2, f^3, ..., f^6\}, \circ, \iota_{\mathfrak{B}})$ is a monoid. The order of the subsemigroup generated by f is 6, but $f^7 = f^3$. (We don't have to check that this is indeed a monoid, since it is defined in terms of functions and their compositions, and we know that function composition is associative.)

A.5.6.9 THEOREM. *Let a and b be elements of an Abelian group $\mathfrak{A}$.*

1. *Let a belong to exponent m, and b belong to exponent n. Then ab belongs to exponent mn.*
2. *Let a have period m, and b have period n. Then, if $(m,n)=1$, ab has period mn.*
3. *Suppose that*
$$m = \mathit{period}(a) = \max\{\mathit{period}(c) : c \in \mathfrak{A}\}$$
and that b has period n. Then $n \mid m$.

Proof:

1.
$$\begin{aligned}(ab)^{mn} &= a^{mn}b^{mn} \quad \text{since multiplication is commutative}\\ &= (a^m)^n (b^n)^m\\ &= e^n e^m = e\end{aligned}$$

2. Denote the period of ab by ℓ.
$$\begin{aligned}e = e^n &= \left((ab)^\ell\right)^n = a^{n\ell}b^{n\ell}\\ &= a^{n\ell} \qquad \text{since } b \text{ has order } n\\ &\Rightarrow m \mid n\ell\end{aligned}$$
But, $(m,n)=1 \Rightarrow m \mid \ell$. We may prove in a similar fashion that $n \mid \ell$, hence (by Theorem A.5.6.7) $[m,n] \mid \ell$, i.e.
$$mn = \frac{mn}{(m,n)} \mid \ell$$
But, since ab belongs to exponent mn, $\ell \mid mn$. It follows that $\ell = mn$.

3. Let $m = p_1^{r_1}p_2^{r_2}...p_k^{r_k}$ and $n = p_1^{s_1}p_2^{s_2}...p_k^{s_k}$ be decompositions into powers of distinct primes, and suppose that $r_1 < s_1$. Then $a^{p_1^{r_1}}$ and $b^{np_1^{-s_1}}$ respectively have periods $mp_1^{-r_1}$ and $p_1^{s_1}$; these being relatively prime, the product $a^{p_1^{r_1}}b^{np_1^{-s_1}}$ has period $mp_1^{-r_1}p_1^{s_1} = mp_1^{s_1-r_1} > m$, contradicting the maximality of m. We conclude that the hypothesis that $r_1 < s_1$ was false; hence $r_i \geq s_i \quad (i = 1,2,...,k)$, and $n \mid m$. □

(Theorem A.5.6.9 may fail for a non-abelian group. For example, in $\mathcal{D}_5$, we can find elements of periods 2 and 5, but their product is not of order 10, since the group is not cyclic, and has no element whose period is equal to the order of the group.)

A.5.7 Group Presentations

Suppose that $\mathfrak{A}$ is a group generated by a subset $\mathfrak{B}$. Unless $\mathfrak{A}$ is freely generated by $\mathfrak{B}$, there must exist elements of $\mathfrak{A}$ that are expressible in more than one way as words in elements of $\mathfrak{B}$. Any equation between different words whose value is the same can be transformed into an equation of the form

$$b_1^{n_1} b_2^{n_2} ... b_k^{n_k} = e$$

where n_1, n_2, ..., n_k are integers, and $b_1, b_2, ..., b_k \in \mathfrak{B}$. We can describe the structure of the group by listing a set of generators and then listing all *relators* $b_1^{n_1} b_2^{n_2} ... b_k^{n_k}$. This description will be redundant, as some relators will imply others. For example, we could describe $\mathbb{Z}_2$ in the form

$$\left\{a : ..., a^{-4}, a^{-2}, a^2, a^4, a^6, ...\right\}$$

But it is sufficient to suppress any relators which are products of others or their inverses. A *presentation* is any such description, in the form

$$\{a_1, a_2, ... : R_1, R_2, ...\} \ ;$$

it is not assumed that the list of relators R_1, R_2, ... is minimal. Thus another presentation of $\mathbb{Z}_2$ is

$$\left\{a : a^2\right\}$$

Sometimes the notation is expanded to list *equations* or *relations* in place of *relators*, as

$$\left\{a : a^2 = e\right\}$$

The study of properties of group *presentations* is called *combinatorial* group theory. The *Word Problem* for a particular class of groups is to determine an algorithm for deciding whether any given word is equal to the identity.

A.5.7.1 Exercise. 1. Consider the group presented by

$$\{a, b : a^3, b^5, aba^{-1}b^{-1}\}$$

Show that this group is isomorphic to $\mathbb{Z}_{15}$.

2. Show that

$$\{a, b : a^2, b^5, (ab)^2\}$$

is isomorphic to $\mathcal{D}_5$.

3. Explain the difference between

$$\{a, b : a^2, b^2\}$$

and

$$\{a, b : a^2, b^2, abab\}$$

Solution:

1.

2.

3.

The *Cayley (colour) graph* of a presentation of a group is a *directed* graph whose vertices are the elements of the group, with an edge directed from vertex a to vertex b whenever there is a generator g in the presentation such that $ag = b$; this edge bears a label g; (originally the labels were colours). For each generator g there must be one directed edge bearing that label (colour) leaving each vertex and one entering that vertex. The directed graph will be *Eulerian* since the in-valency and out-valency are equal at every vertex and the graph is connected. (Why?) Every relator gives rise to a directed circuit — indeed, to a directed circuit at every vertex of the graph.

A.5.7.2 Exercise. Sketch a Cayley graph for each presentation studied in the preceding exercise.

A.5.8 The Quaternion Group

Define real matrices A and B as follows:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

It can be observed that $A^2 = B^2 = -I$. Moreover, the subgroup of $GL(4, \mathbb{R})$ generated by these two matrices can be seen to have order 8: Define

$$C = AB = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

Then it can be verified that $BA = -C$, $BC = A$, $CB = -A$, $CA = B$, $AC = -B$: the group has 1 element of order 1 (the identity, I), 1 element of order 2 ($-I = A^2 = B^2 = C^2$), and 6 elements of order 4 ($\pm A$, $\pm B$, $\pm C$).

The *quaternions* are the set of linear combinations of the form $x_0 + x_1 A + x_2 B + x_3 C$, where $x_i \in \mathbb{R}$, $(i = 0, 1, 2, 3)$. These matrices form a *skew field* or *division ring* or *sfield*: all axioms of a field are satisfied, except for commutativity of multiplication. (What we have constructed here is called the *group algebra* $\mathbb{R}Q$, where Q is the quaternion group: it is a vector space over the reals consisting of real linear combinations of the eight matrices in the group, with addition, scalar multiplication, and multiplication of vectors (here they are matrices) defined in the obvious ways, according to the distributive laws and the multiplication defined for elements of Q.) Note that the complex field can be embedded in the division ring of quaternions, in various ways.

Quaternions were apparently discovered by Sir William Rowan Hamilton, who described them in his notebook on October 16th, 1843. For a history cf. [44, pp. 179-188].

A.6 Abelian Groups

A.6.1 Direct Sums. The Fundamental Theorem.

A.6.1.1 LEMMA. *1. Let $\mathfrak{A}_1$ and $\mathfrak{A}_2$ be groups respectively generated by subsets $\mathfrak{B}_1 \subseteq \mathfrak{A}_1$, $\mathfrak{B}_2 \subseteq \mathfrak{A}_2$. Then the direct product $\mathfrak{A}_1 \times \mathfrak{A}_2$ is generated by the subset $\mathfrak{B}_1 \times \{f\} \quad \cup \quad \{e\} \times \mathfrak{B}_2$.*

2. Let m and n be positive integers. Then the group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic iff $(m, n) = 1$.

Proof:

1. see Exercise A.6.1.2.

2. For any m and n the direct summands are respectively generated by the cosets 1 and 1 (we use the abbreviated notation). Thus every element of the direct sum is generated by $\{(1, 0), (0, 1)\}$. If $(m, n) = 1$ there exist integers k and ℓ such that $1 = km + \ell n$. Then $\ell n(1, 1) = (\ell n, \ell n) = (1, 0) - k(m, 0) + \ell(0, n) = (1, 0) - (0, 0) + (0, 0) = (1, 0)$. Similarly, $km(1, 1) = (0, 1)$. Thus both generators are themselves powers (here, in the "additive" notation, multiples) of $(1, 1)$. It follows that $(1, 1)$ generates the direct sum, i.e. that the direct sum is cyclic.

   (Alternatively, we may, by Theorem A.5.6.9, deduce from $(m, n) = 1$ that the period of $(1, 1)$ is mn.)

   Conversely, suppose that the direct sum is cyclic, generated by (a, b). Since the period of a in $\mathbb{Z}_m$ is m, and of b in $\mathbb{Z}_n$ is n, the period of (a, b) divides $[m, n]$, i.e. (cf. A.1.6.14) divides $\frac{mn}{(m,n)}$. But, since (a, b) generates the cyclic group, its period is mn. It follows that $(m, n) = 1$. □

A.6.1.2 EXERCISE. Prove part 1 of Lemma A.6.1.1.

A group is *finitely generated* if it admits a presentation with a finite set of generators. For abelian groups (but not for groups in general) we can completely characterize groups which are finitely generated. This characterization is another result (cf. Theorem A.1.8.9) which has come to be known as "Fundamental":

A.6.1.3 THEOREM (FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS). *Let $(\mathfrak{A}, +, 0)$ be a finite abelian group. Then there exist elements a_1, a_2, ..., a_k in $\mathfrak{A}$ having orders o_i such that $o_1 \mid o_2 \mid ... \mid o_k$ and every element $a \in \mathfrak{A}$ is expressible uniquely in the form*

$$a = \sum_{m=1}^{k} r_m a_m$$

where $0 \leq r_i \leq o_i - 1$, $(i = 1, 2, ..., k)$.

More generally, we can characterize *finitely generated* abelian groups:

A.6.1.4 THEOREM (FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS). *Let $(\mathfrak{A}, +, 0)$ be a finitely generated abelian group. Then there exist elements a_1, a_2, ..., a_k in $\mathfrak{A}$ having orders o_i such that $o_1 \mid o_2 \mid ... \mid o_k$, and elements a_{k+1}, a_{k+2}, ..., $a_{k+\ell}$ in $\mathfrak{A}$ having infinite order such that every element $a \in \mathfrak{A}$ is expressible uniquely in the form*

$$a = \sum_{m=1}^{k} r_m a_m + \sum_{n=1}^{\ell} r_n a_{k+n}$$

where $0 \leq r_i \leq o_i - 1$, $(i = 1, 2, ..., k)$.

For proofs of these theorems cf. [15], [34].

A.6.2 Euler's "Totient" Function. Fermat's "Little" Theorem.

A.6.2.1 THEOREM. *An element $a + (n)$ generates $(\mathbb{Z}_n, +, 0)$ iff $(a, n) = 1$.*

Proof: Suppose that $(a, n) = 1$. Then there exist integers k and ℓ, such that $1 = k \cdot a + \ell \cdot n$. It follows that $1 + (n) = ka + (n) = k(a + (n))$, where the last expression is to be interpreted as the sum of k copies of $a + (n)$. We have shown that the element we usually denote by 1, i.e. the coset $1 + (n)$, is contained in the subgroup generated by the element we denote by a, i.e. the coset $a + (n)$. But 1 is a generator of $\mathbb{Z}_n$; hence a is also a generator.

Conversely, suppose that a generates $\mathbb{Z}_n$. Then every element of $\mathbb{Z}_n$ is expressible as a sum of copies of a; in particular, 1 is expressible as a sum, $1 \equiv k \cdot a$, i.e. $1 + (n) = k \cdot a + (n)$, i.e. $1 = k \cdot a + \ell \cdot n$ for some integer ℓ. But this implies (cf. Lemma A.1.6.9) that $(a, n) = 1$. □

A.6.2.2 COROLLARY (TO THEOREM A.6.2.1). *The elements of $\mathbb{Z}_n$ which can each serve as the sole generator of the cyclic group $(\mathbb{Z}_n, +, 0)$ are all the elements of the group $(\mathbb{Z}_n^\times, \times, 1)$.*

A.6.2.3 DEFINITION. The number of elements that can each alone generate a cyclic group of order n is denoted by $\varphi(n)$. φ is called the *Euler function*, or the *totient*[370] *function*.

A.6.2.4 COROLLARY (TO THEOREM A.6.2.1). *1.* $|(\mathbb{Z}_n^\times, \times, 1)| = \varphi(n)$

[370] i.e. the number of *totitives*.

2. **(Fermat's[371] "Little"[372] Theorem)** *Let p be a prime, and $a \in \mathbb{N}$. Then $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.*

3. **(Euler's Generalization of Fermat's "Little" Theorem).** *Let a and n be integers such that $(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}\,.$$

Proof:

1. This is a restatement of Corollary A.6.2.2 in terms of $\varphi(n)$, defined in Definition A.6.2.3.

2. This follows from the Euler generalization, proved next: set $n = p$.

3. The period of $a+(m)$ in the group $(\mathbb{Z}_m^\times, \times, 1+(m))$ divides the order of the group, $\varphi(m)$. Hence
$$1 + (m) = (a + (m))^{\varphi(m)} = a^{\varphi(m)} + (m)\,,$$
i.e. $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Every coset in $\mathbb{Z}_n$ has precisely one representative in the set $\{1, 2, 3, ..., n\}$. Thus $\varphi(n)$ may be interpreted as the number of positive integers less than and prime to n. Evidently $\varphi(p) = p - 1$ for any prime p. More generally, since the number of integers divisible by a prime p and lying between 1 and p^r is $\dfrac{p^r}{p} = p^{r-1}$,

$$\varphi(p^r) = p^r \left(1 - \frac{1}{p}\right) \quad \text{for any prime } p\,. \tag{354}$$

A.6.2.5 Theorem. *Let $m = p_1^{r_1} p_2^{r_2} ... p_n^{r_n}$ be a factorization of m into powers of distinct primes p_1, p_2, ..., p_n. Then*

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_n}\right)$$

A.6.2.6 Exercise. Prove Theorem A.6.2.5 using the Principle of Inclusion and Exclusion.

[371] Pierre S. de Fermat (1601–1665)

[372] As distinguished from the *Fermat conjecture*, also known as *Fermat's Last Theorem*, which states that the diophantine equation $a^n = b^n + c^n$ has an integer solution a, b, c only when $n \leq 2$. For a history of this problem cf. [9].

Solution: By Theorem A.6.2.1 we are counting those integers 1, 2, ..., m which are divisible by *none* of the primes p_1, p_2, ..., p_n. If we denote the set $\{a : 1 \leq a \leq m : p_i \mid a\}$ by $\mathfrak{S}_i$, then $|\mathfrak{S}_i| = \frac{m}{p_i}$. More generally, for distinct i_1, i_2, ..., i_j,

$$|\mathfrak{S}_{i_1}| \cap |\mathfrak{S}_{i_2}| \cap ... \cap \left|\mathfrak{S}_{i_j}\right| = \frac{n}{p_{i_1}p_{i_2}...p_{i_j}}$$

By the Principle of Inclusion and Exclusion, the number of integers in the given range which are in *none* of the sets $\mathfrak{S}_i$ $(i = 1, 2, ..., n)$ is the alternating sum

$$m - m\left(\frac{1}{p_1} + \frac{1}{p_2} + ... + \frac{1}{p_n}\right) + m\left(\frac{1}{p_1p_2} + \frac{1}{p_1p_3} + ... + \frac{1}{p_{n-1}p_n}\right) + ... + (-1)^n m\frac{1}{p_1p_2...p_n}$$

We recognize this to be the expansion of the product

$$m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_n}\right)$$

□

A.6.2.7 Exercise. 1. A function $f : \mathbb{N} \longrightarrow \mathbb{R}$ is said to be *multiplicative* if

$$(m, n) = 1 \Rightarrow f(mn) = f(m) \cdot f(n)$$

Prove that φ is multiplicative.

2. Prove that $\varphi : (\mathbb{N}, \times) \longrightarrow (\mathbb{R}, \times)$ is *not* a semigroup homomorphism.

A.6.2.8 Exercise. Prove the identity, $m = \sum_{d|m} \varphi(d)$.

Solution: Prove the result first for powers of a single prime: $\sum_{d|p^r} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + ... + \varphi(p^r) = 1 + (p-1) + p(p-1) + ... + p^{r-1}(p-1) = 1 + (p-1)\frac{p^r - 1}{p-1} = p^r$.

We can complete the proof by induction on the number k of distinct prime factors. Having proved it for $k = 0$ (i.e. $n = 1$, where it is obvious) and $k = 1$, assume it has been proved for $k = K$. Let $n = m \cdot p_{K+1}^{r_{K+1}}$, where m is of the form $p_1^{r_1}p_2^{r_2}...p_K^{r_K}$, all $r_i > 1$. The divisors d of n are all of the form d_1d_2 where $d_1|m$ and $d_2|p_{K+1}^{r_{K+1}}$. The sum of $\varphi(d)$ over all divisors is then the double sum $\sum_{d_1|m} \varphi(d_1) \sum_{d_2|p_{K+1}^{r_{K+1}}} \varphi(d_2)$ etc.

A.6.2.9 Exercise. 1. Determine all integers m for which $\varphi(m)$ is odd.

2. Determine all natural numbers m such that $\varphi(m) = 24$.

3. If n be a prime greater than 7, prove that $504|(n^6 - 1)$.

4. If $(a, 91) = 1 = (b, 91)$, show that $a^{12} - b^{12} \equiv 0 \pmod{91}$.

Solution:

1. Suppose $\varphi(m)$ is odd. If $p^2 \mid m$ then $p(p-1) \mid \varphi(m)$, so $\varphi(m)$ is even. It follows that m is a product of *distinct* primes. Even then, any odd prime factor p would produce an even factor $p - 1 \mid m$. Thus m can only be 2; $\varphi(2) = 1$. The only odd value assumed by the function φ is 1, and it is realised for $m = 1$ and $m = 2$.

2. Suppose $\varphi(m) = 24$. If $p \mid m$ then $(p-1) \mid 24$. The only positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24. Hence the only primes that can divide m are 2, 3, 5, 7, 13.

   Which primes can divide n to a power higher than the first? Considering the sequence $p(p-1)$ of products of primes and their predecessors, we find that the only such products dividing 24 are $2(2-1)$ and $3(3-1)$. Thus only 2 or 3 can appear as multiple powers in the factorization of 24. Thus $m = 2^{r_2}3^{r_3}5^{r_5}7^{r_7}13^{r_{13}}$, where the only possible non-zero values of the exponents are

Exponent			$\varphi(p^{r_i})$
r_2	$=$	1	1
	$=$	2	2
	$=$	3	4
	$=$	4	8
r_3	$=$	1	2
	$=$	2	6
r_5	$=$	1	4
r_7	$=$	1	6
r_{13}	$=$	1	12

   Any admissible factorization of 24 will have one factor divisible by 3. In our table only the φ-values of 3^2, 7, 13 contribute a needed divisor of 3 to 24; there are thus three cases to consider:

$$\begin{array}{rcll} m &=& 13k_1 & \varphi(k_1) = 24/\varphi(13) = 2 \quad (13 \nmid k_1) \\ m &=& 7k_2 & \varphi(k_2) = 24/\varphi(7) = 4 \quad (7 \nmid k_2) \\ m &=& 9k_3 & \varphi(k_3) = 24/\varphi(9) = 4 \quad (3 \nmid k_3) \end{array}$$

   $m = 13k_1$**:** We must factorize 2 into a product of distinct entries in the last column of the table: either $2 = 2$ or $2 = 2 \cdot 1$. The first corresponds to $k_1 = 4$ or to $k_1 = 3$; the second to $k_1 = 2 \cdot 3$.

$m = 7k_2$**:** We must factorize 4 into a product of distinct entries in the last column of the table: either $4 = 4$ or $4 = 4 \cdot 1$ or $4 = 2 \cdot 2$; (the case $4 = 2 \cdot 2 \cdot 1$ does not arise, since the divisor 1 of $\varphi(k_2)$ is associated only with the factor 2 of k_2, and one of the 2's would be associated with 2^2). These factorizations correspond to $k_2 = 8, 5, 5 \cdot 2, 4 \cdot 3$.

$m = 9k_3$**:** This case is as the preceding, except that we cannot have $3 \mid k_3$: $k_3 = 8, 5, 5 \cdot 2$.

In all there are 9 solutions: 35, 39, 45, 52, 56, 70, 72, 78, 84, 90.

3. Since $504 = 9 \cdot 8 \cdot 7$, the divisibility sought is equivalent to the simultaneous solution of the congruences $n^6 \equiv 1 \pmod 9$, $n^6 \equiv 1 \pmod 8$, $n^6 \equiv 1 \pmod 7$. The last of these follows from Fermat's little theorem, since n, being a prime greater than 7, must be relatively prime to 7. The first congruence follows from Euler's generalization of Fermat's theorem, for n being prime and greater than 3, it is surely relatively prime to 9: $n^{\varphi(9)} \equiv 1 \pmod 9$. To prove congruence modulo 8, we observe that n is odd, i.e. of the form $2\ell + 1$; its square is $4\ell(\ell + 1) + 1$. This last sum is congruent to 1 modulo 8, since $\ell(\ell + 1)$, being the product of two consecutive integers, must be even. Hence $n^6 \equiv (n^2)^3 \equiv 1^3 \equiv 1 \pmod 8$.

4. $91 = 7 \cdot 13$. This problem is equivalent to proving $a^{12} \equiv b^{12} \pmod 7$ and $a^{12} \equiv b^{12} \pmod{13}$. The first follows directly from Fermat's Little Theorem, applied separately to a and b modulo 13. Application of the same theorem to a and b modulo 7 yields $a^6 \equiv 1$ and $b^6 \equiv 1$, which respectively imply that $a^{12} \equiv 1$ and $b^{12} \equiv 1$, yielding the second congruence we seek.

A.6.2.10 Exercise. 1. Compute $3^{50,000}$ modulo 133.

2. Use the division algorithm to determine the binary expansion of 87. Then apply this expansion to evaluate 51^{87} modulo 101. [Hint: Express the exponential as $51^{a_n 2^n} 51^{a_{n-1} 2^{n-1}} 51^{a_{n-2} 2^{n-2}} ... 51^{a_1 2^1} 51^{a_0}$.]

Solution:

1. We discuss a solution "from first principles", and then several improvements.

   (a) $133 = 19 \cdot 7$. Since $(3, 133) = 1$, $3^{\varphi(133)} \equiv 1 \pmod{133}$.

   $$\varphi(133) = \varphi(19)\varphi(7) = 18 \cdot 6 = 108.$$

   A naive way of avoiding raising 3 to the power 50,000 would be to observe that $50000 = q \cdot 108 + 104$; thus we need only raise it to the 104th power. We could then compute 3^n by iteration, at each stage following a multiplication by reduction modulo 133. We can improve on this, however.

(b) We know that

$$3^{18} \equiv 1 \pmod{19}$$

and

$$3^{6} \equiv 1 \pmod{7}.$$

Hence $3^{18} \equiv 1 \pmod{7 \cdot 19}$ by Lemma A.1.9.2. Since $50000 = 2727 \cdot 18 + 14$, $3^{50000} \equiv 3^{14} \pmod{133}$. Thus, even if we adopt the "naïve" iterative approach proposed earlier, we may stop at a much smaller exponent. We have

$$\begin{aligned} 3^4 &= 81 \\ 3^5 &= 243 \equiv 110 \pmod{133} \\ 3^6 &\equiv 330 \equiv 64 \pmod{133} \\ 3^7 &\equiv 192 \equiv 59 \pmod{133} \end{aligned}$$

at which point it is obvious that we should consider squaring both sides of the last congruence,

$$3^{14} \equiv 59^2 \equiv 23 \pmod{133}$$

(c) The last "short cut" we took suggests a more efficient way to exponentiate to a given modulus. We can, by iteration, determine the smallest positive residues for 3 raised to powers of 2; then combine them.

$$\begin{aligned} 3^1 &\equiv 3 \pmod{133} \\ 3^2 &\equiv 3^2 \equiv 9 \pmod{133} \\ 3^4 &\equiv 9^2 \equiv 81 \pmod{133} \\ 3^8 &\equiv 81^2 \equiv 6561 \equiv 44 \pmod{133} \end{aligned}$$

Then we can express 3^{14} as a product of these powers by first determining the binary expansion of 14:

$$\begin{aligned} 14 &= 7 \cdot 2 + 0 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 2 + 1 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 14 = (1110)_2 \Rightarrow 3^{14} &= 3^{2^3+2^2+2^1} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} \\ &\equiv 44 \cdot 81 \cdot 9 \pmod{133} \\ &\equiv 3564 \cdot 9 \equiv 106 \cdot 9 \equiv 23 \pmod{133} \end{aligned}$$

(Could you write an algorithm to "automate" this procedure? It's not necessary to store all the powers of 3!)

(d) We could also have applied the Chinese Remainder Theorem to the following congruences to smaller moduli (which could be determined by any of the methods described above)

$$\begin{aligned} 3^{14} &\equiv 3^8 \cdot 3^4 \cdot 3^2 \equiv 6 \cdot 5 \cdot 9 \equiv 4 \pmod{19} \\ 3^{14} &\equiv 3^8 \cdot 3^4 \cdot 3^2 \equiv 2 \cdot 4 \cdot 2 \equiv 2 \pmod{7} \end{aligned}$$

Modulo 19, $7^{-1} \equiv 11$; modulo 7, $19^{-1} \equiv 5^{-1} \equiv 3$. We need only reduce

$$(4 \cdot 7 \cdot 11) + (2 \cdot 19 \cdot 3)$$

modulo 133.

2. Recursive application of the division algorithm, i.e. application of Euclid's algorithm, yields

$$\begin{aligned} 87 &= 43 \cdot 2 + 1 \\ 43 &= 21 \cdot 2 + 1 \\ 21 &= 10 \cdot 2 + 1 \\ 10 &= 5 \cdot 2 + 0 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

from which, reading the remainders upwards from the bottom, we obtain that $87 = 1010111_2$ (i.e. in the scale of 2).

We compute the needed powers of 51 recursively:

$$\begin{aligned} 51^2 &= 2601 \equiv 76 \\ 51^4 &\equiv 76^2 = 5776 \equiv 19 \\ 51^8 &\equiv 19^2 = 361 \equiv 58 \\ 51^{16} &\equiv 58^2 = 3364 \equiv 31 \\ 51^{32} &\equiv 31^2 = 961 \equiv 52 \\ 51^{64} &\equiv 52^2 = 2704 \equiv 78 \end{aligned}$$

from which we conclude that $51^{87} = 78 \cdot 31 \cdot 19 \cdot 76 \cdot 51 \equiv 95 \cdot 30 \cdot 51 \equiv (-6) \cdot 1530 \equiv (-6) \cdot 15 \equiv -90 \equiv 11 \pmod{101}$.

A.6.2.11 THEOREM (WILSON). *1. For any prime p,*

$$(p-1)! \equiv -1 \pmod{p}. \tag{355}$$

2. If

$$(n-1)! \equiv -1 \pmod{n}. \tag{356}$$

then n is prime.

Proof:

1. (a) To the modulus $p = 2$, $1 \equiv -1$.

   (b) Assume p is an odd prime. Then $\mathbb{Z}_p^\times$ has order $p-1$, which is even. Let $1 < a \leq p-1$.

   $$a^{-1} \equiv a \Leftrightarrow p \mid (a-1)(a+1) \Leftrightarrow p \mid (a-1) \quad \text{or} \quad p \mid (a+1)$$

   which implies that $a = p-1$. Thus, other than $1+(p)$, there is precisely one coset that coincides with its inverse, the coset $-1+(p)$. We conclude that the product of the elements in $\mathbb{Z}_p^\times$ is a product of an even number of elements paired with their (distinct) inverses, 1, and -1; in all the product is congruent to $1^{\frac{p-3}{2}} \cdot 1 \cdot (-1) \equiv -1 \pmod{p}$.

2. Suppose that n is composite. If $n = ab$, where $1 < a < b < n$, then $n \mid (n-1)!$, so (356) fails. The only way in which a composite n could not have a factorization of the desired type is where $n = p^2$ for some prime. Even then, if $p \geq 3$, then both p and $2p$ divide $(n-1)!$. Thus the only difficulty with this reasoning is where $n = 2^2$. But then $3! \not\equiv -1 \pmod{4}$. □

We have, in Wilson's Theorem, proved a *deterministic primality test*, i.e. a test which, when applied to a given integer n, can output whether or not n is a prime. For that purpose Wilson's Theorem is, unfortunately, of little *practical* value.

A.6.2.12 EXERCISE. Prove Leibniz's test for primality:

$$n \text{ is prime} \Leftrightarrow (n-2)! \equiv 1 \pmod{n}$$

A.6.2.13 EXERCISE. Show that for any odd prime p, $2(p-3)! + 1 \equiv 0 \pmod{p}$.

Solution: By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$; hence $(p-1)(p-2)\{(p-3)!\} \equiv -1$, i.e. $p(p-3)\{(p-3)!\} + 2(p-3)! \equiv -1 \pmod{p}$, which reduces to the desired congruence.

A.6.3 Public Key Cryptography: The RSA Cryptosystem

> *Cryptography is the study of methods of sending messages in disguised form, so that the intended recipients can remove the disguise and read the message.* [24, p. 53]

A "cryptosystem" may involve two separate alphabets — as in the transmission of English messages in Morse-type code, or the same alphabet — as in the "Cæsar cipher", in which the Latin alphabet is cyclically permuted so that A is enciphered as, say D, B as E, ..., Z as C. In this course we shall be considering only one instance of mathematical encryption.[373] [374] The example we study is intended as an indication of how mathematical results that were hitherto regarded as "abstract" can suddenly acquire immense practical significance. The actual application depends on the practical difficulty of factoring large integers. If new algorithms are discovered which reduce this difficulty, or if new hardware is produced which can implement existing algorithms more efficiently, this application may no longer be useful. It is a random algorithm, in the sense that the difficulty is predicated on the randomness of several parameters. Should it be known that certain parameters are chosen subject to constraints, the level of security could be compromised. For a convincing discussion of the RSA (Rivest-Shamir-Adleman) "Public Key" cryptosystem [33] we would have to investigate various questions concerning the difficulty of factorizing certain integers, and the densities of primes. We will not do this, but will simply confine ourselves to a description of the cryptosystem in its simplest form.

In cryptosystems like the Cæsar cipher the "key" is a letter or word which indicates the values of parameters: knowledge of the type of cryptosystem being used and of the values of the parameters allow both encoding and decoding. Partial knowledge may be complemented by algorithms to determine candidates for key values; for example, if we know that a Caesar-type cypher has been used, then frequency counts of single letters and sequences of 2 and 3 letters will indicate — based on knowledge of frequency counts in the "plaintext" language — likely candidates for keys. These can be tested to eliminate most or all extraneous values. In "public key" cryptosystems, values of certain of the

[373] For a discussion of other *number-theoretical* examples, cf. [24], [2, Chapter 4].

[374] Students should not confuse *cryptography* with *coding theory*, where the objective in *encoding* data is to minimize transmission errors due to noise and other factors; a non-trivial example of a *code* would be the *binary Hamming code of length 7*, which consists of the 16 7-digit binary words 0000000, 1111111, 1011000, 0101100, 0010110, 0001011, 1000101, 1100010, 0110001, 0100111, 1010011, 1101001, 1110100, 0111010, 0011101, 1001110. For example, each of the ASCII characters could be encoded by a *digraph* in this code — a sequence of two 7-digit words from the code. This code has the interesting feature that it is a *perfect single-error-correcting* code: if we know that at most one digit of any word is corrupted in transmission, we can both *detect* and *correct* the error, since any two of our code words differ in at least 3 digits. An encyclopædic discussion of many aspects of *algebraic coding theory* is to be found in [27]; cf. also [29], [45].

parameters are made public; others are concealed. Thus it may be possible to *encrypt* a message, but not to *decrypt* one; or to *decrypt* a message, but not to *encrypt*. We describe a variation where the public may encode, but — with a very high probability — only an individual in possession of the key may decode.

The RSA cryptosystem requires the "random" selection of several natural numbers. First one selects two very large *primes* p and q. (In practice this entails randomly selecting an integer, then submitting it to tests for primality. The student knows one "deterministic" test: Wilson's Theorem (Theorem A.6.2.11).[375]) Define $n = p \times q$, and make n public, (but not its factors). Then find an integer d which is relatively prime to $\varphi(n)$, i.e. to $(p-1)(q-1)$. This integer should be chosen "randomly". Again, this operation may be carried out by randomly choosing the integer, followed by primality testing. Since $(d, \varphi(n)) = 1$, d is invertible modulo $\varphi(n)$; call its inverse e, and publish e (but not d). Messages to be transmitted are first encoded as sequences of integers M such that

$$0 < M < n$$

and

$$(M, n) = 1\,.$$

Then an integer M is encoded by raising it to the eth power and reducing modulo n, so that the transmitted message is

$$E \equiv M^e \pmod{n}\,.$$

The message is decoded by an authorized reader by raising this remainder E to the dth power:

$$E^d \equiv M^{ed} \equiv M^{1+r\varphi(n)} \equiv M \pmod{n}$$

for some integer r by Corollary A.6.2.2.2 to Theorem A.6.2.1.

A.6.3.1 Example. cf. [24, pp. 92–93], [2, §4.2]

[375] Another test derives from Fermat's "Little" Theorem (Part 2 of Corollary A.6.2.4): if n is prime then $n \mid 2^n - 2$. Composite integers n satisfying this test, but which are not prime, are said to be *pseudoprime*. More generally, a composite integer n for which $a^n \equiv a \pmod{n}$ for *all* integers a may be said to be *absolutely pseudoprime*. Any composite integer n which is the product of distinct primes p_1, p_2, ..., p_k for which $(p_i - 1) \mid (n-1)$ $(i = 1, 2, ..., k)$ is absolutely pseudoprime [40, V, §7]. An example is $1729 = 7 \cdot 13 \cdot 19$. Any absolutely pseudoprime integer is *a fortiori* a *Carmichael number*:

$$(a, n) = 1 \Rightarrow n \mid \left(a^{n-1} - 1\right)$$

and n is composite. It can be shown that every Carmichael number is absolutely pseudoprime [24, V., §1].

A.6.4 Primitive Roots modulo n. The Discrete Logarithm

A.6.4.1 DEFINITION. 1. An element $a \in \mathbb{Z}_m^\times$ is said to be *primitive* (or, more completely, a *primitive root modulo* m) if $\mathbb{Z}_m^\times = \langle a \rangle$.

2. Relative to a fixed primitive root modulo m we may associate with every element $b \in \mathbb{Z}_m^\times$ an exponent or *index* or *discrete logarithm*, being any integer $k \in \mathbb{Z}$ such that $b \equiv a^k \pmod{m}$.

Since $|\mathbb{Z}_m^\times| = \varphi(m)$, $a^{\varphi(m)} \equiv 1 \pmod{m}$, hence $a^k \equiv a^{k+r\varphi(m)} \pmod{m}$ for all $r \in \mathbb{Z}$. We may thus interpret the index as a coset modulo $\varphi(m)$; normally, we shall represent this coset by its smallest positive member.

Unfortunately, primitive roots do not exist for most moduli:

A.6.4.2 THEOREM. *Unless m is 1, 2, or 4, or is of the form p^r or $2p^r$, where p is an* odd *prime and $r \in \mathbb{N}$, there exists no primitive root modulo m.*

Proof: Let a be a primitive root modulo m, where $m = 2^{r_0}p_1^{r_1}p_2^{r_2}...p_k^{r_k}$ is a factorization into powers of distinct primes.

1. Suppose that $r_i \geq 1$, $(i = 1, 2, ..., k \geq 2)$. By Exercise A.5.1.10.1, $(a, m) = 1$. Hence
$$(a, p_1^{r_1}) = 1 \qquad \text{and} \qquad \left(a, \frac{m}{p_1^{r_1}}\right) = 1$$
Applying Corollary A.6.2.2.2 to Theorem A.6.2.1, we obtain the congruences
$$\begin{aligned} a^{\varphi\left(p_1^{r_1}\right)} &\equiv 1 \pmod{p_1^{r_1}} \\ a^{\varphi\left(\frac{m}{p_1^{r_1}}\right)} &\equiv 1 \pmod{\frac{m}{p_1^{r_1}}} \end{aligned}$$
But, by Theorem A.6.2.5, $\varphi\left(p_1^{r_1}\right)$ and $\varphi\left(\frac{m}{p_1^{r_1}}\right)$ are both even. Hence $\varphi(m)$ is even, and
$$\begin{aligned} a^{\frac{\varphi(m)}{2}} &= \left(a^{\varphi\left(p_1^{r_1}\right)}\right)^{\frac{\varphi\left(\frac{m}{p_1^{r_1}}\right)}{2}} \equiv 1 \pmod{p_1^{r_1}} \\ a^{\frac{\varphi(m)}{2}} &= \left(a^{\varphi\left(\frac{m}{p_1^{r_1}}\right)}\right)^{\frac{\varphi\left(p_1^{r_1}\right)}{2}} \equiv 1 \pmod{\frac{m}{p_1^{r_1}}} \end{aligned}$$
implying, by Lemma A.1.9.2, that $a^{\frac{\varphi(m)}{2}} \equiv 1$ to the modulus $\left[p_1^{r_1}, \frac{m}{p_1^{r_1}}\right] = m$. From this contradiction we may deduce that a cannot generate a group of order $\varphi(m)$. Henceforth we may assume that $k \leq 1$.

2. Suppose that $k = 1$, $r_0 \geq 2$, $r_1 \geq 1$. Here again $\varphi\left(p_1^{r_1}\right)$ and $\varphi\left(\frac{m}{p_1^{r_1}}\right)$ are both even, and we may derive a contradiction as in the preceding case.

3. Suppose that $k = 0$ and $r_0 \geq 3$. Since a is a generator, $(a, 2^{r_0}) = 1$, so a has the form $a = 2n + 1$. It follows that $a^2 = 1 + 4n(n+1) \equiv 1 \pmod 8$, since $n(n+1)$ is always even. We may now prove by induction that

$$a^{2^s} \equiv 1 \pmod{2^{s+2}}$$

for $s \geq 1$. Hence, in particular, $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m$, so a has period less than $\varphi(m)$. $\square$

A.6.4.3 THEOREM. *For each of the cases $m = 1, 2, 4$ and $m = p^r, 2p^r$, where p is an odd prime, there exists a primitive root modulo m.*

In proving this theorem we shall require information concerning the number of integers modulo a prime where a specific polynomial can be congruent to zero.

A.6.4.4 LEMMA. *Let $f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$ be a polynomial with integer coefficients, $a_0 \not\equiv 0 \pmod p$. Then the number of solutions modulo p of the congruence*

$$f(x) \equiv 0 \pmod p \tag{357}$$

is at most n.[376]

Proof of Lemma A.6.4.4: Our proof is by induction on n. For $n = 1$ the result follows from the Chinese Remainder Theorem (Theorem 4:831). Suppose the result has been proved for all $n < N$, and take $n = N$. Suppose that x_1, x_2, ..., x_{N+1} are distinct solutions modulo p (i.e. that $x_i \not\equiv x_j$ whenever $i \neq j$). Then the polynomial

$$f(x) - a_0(x - x_1)(x - x_2)...(x - x_N)$$

has degree less than N, but more than $N - 1$ solutions; by the induction hypothesis, each of the coefficients of this polynomial is divisible by p; hence

$$f(x) \equiv (x - x_1)(x - x_2)...(x - x_N) \pmod p \tag{358}$$

for all x. Setting $x = x_{N+1}$ in (358) yields the contradiction

$$f(x_{N+1}) \equiv (x_{N+1} - x_1)(x_{N+1} - x_2)...(x_{N+1} - x_N) \pmod p$$

from which we conclude the truth of the statement for $n = N$. $\square$
Proof of Theorem A.6.4.3:

[376] If one member of a coset $a + (p)$ is a solution of (357), then all members are solutions. When we speak of "solutions modulo p", we are referring to such cosets.

1. $\mathbb{Z}_1^\times = \{1\} = \langle 1 \rangle$.

2. $\mathbb{Z}_2^\times = \{1\} = \langle 1 \rangle$.

3. $\mathbb{Z}_4^\times = \{1, 3\} = \langle 3 \rangle$.

4. Let h denote the exponent of $\mathbb{Z}_p^\times$. We have seen that h is a multiple of the periods of all elements of the group. Thus all elements of $\mathbb{Z}_p^\times$ satisfy the congruence

$$x^h \equiv 1 \pmod{p}$$

But this congruence cannot have more than h solutions; hence $h \geq \left|\mathbb{Z}_p^\times\right| = \varphi(p) = p - 1$. That is, there exists an element whose period is at least equal to the order of the group, so that element is a generator, i.e. a primitive element modulo p.

A construction for the case $m = p^r$ $(r > 1)$ can be found in text-books on number theory, for example [28, p. 48], [43, VI.]

5. Suppose that $m = 2p^r$. Let b be a primitive root modulo p^r, and define a to be the odd member of the set $\{p^r, b + p^r\}$. Then all powers of a are odd. Also, for every $k > 0$, the binomial exansion of $(b + p^r)k$ yields,

$$a^k \equiv b^k \pmod{p^r}$$

Thus

$$a^k \equiv 1 \pmod{m} \Leftrightarrow \left\{ \begin{array}{rcll} a^k & \equiv & 1 & \pmod{2} \\ b^k & \equiv & 1 & \pmod{p^r} \end{array} \right\} \Rightarrow \varphi(p^r) \mid k$$

But $\varphi(m) = \varphi(p^r)$. Thus a is a primitive root. □

A.6.4.5 Exercise. 1. Show, by tabulating indices modulo 29 in a table begun below, that 5 is a primitive root modulo 29.

	0	1	2	3	4	5	6	7	8	9
0									3	
1						1				
2						2				

2. Explaining your work, use the data in your completed table to determine all elements of $\mathbb{Z}_{29}^\times$ which are squares (called *quadratic residues*).

3. Explaining your work, use the data in your completed table to determine all elements of $\mathbb{Z}_{29}^\times$ which are cubes (called *cubic residues*).

A.6.5 Homomorphisms

A.6.5.1 Exercise. Define a function $f : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{R}^*$ by $(a, b) \longmapsto 2^b 5^a$. Show that f is a homomorphism from the abelian group $(\mathbb{Z} \oplus \mathbb{Z}, +, (0, 0))$ to the abelian group $(\mathbb{R}^*, \times, 1)$, and that it is one-to-one.

Solution:

$$\begin{array}{rcll} f((a,b)+(a',b')) & = & f(a+a', b+b') & \text{by definition of } + \text{ in the direct sum} \\ & = & 2^{b+b'}5^{a+a'} & \text{by definition of } f \\ & = & 2^b 2^{b'} 5^a 5^{a'} & \text{properties of exponentials} \\ & = & 2^b 5^a 2^{b'} 5^{a'} & \text{commutativity of multiplication in } \mathbb{R}^* \\ & = & f(a,b)f(a',b') & \text{by definition of } f \end{array}$$

Thus f is a homomorphism.

$f(a, b) = f(a', b') \Leftrightarrow 2^b 5^a = 2^{b'} 5^{a'} \Leftrightarrow 2^{b-b'} = 5^{a-a'}$. If $b \neq b'$, then 2 must divide the right side of this equation, whose only prime divisor is 5. From this contradiction we conclude that $b - b' = 0$ and, analogously, $a - a' = 0$. Thus $f(a, b) = f(a', b') \Leftrightarrow (a, b) = (a', b')$; it follows that f is one-to-one.

A.6.5.2 Exercise. In the abelian group $\mathcal{A} = \mathbb{Z}_{12} \oplus \mathbb{Z}_4$

1. Determine the subgroup $\mathcal{B}$ generated by $(3, 2)$.
2. List the cosets of $\mathcal{B}$ in $\mathcal{A}$, showing all members of each coset.
3. Set up an addition table for the group $\mathcal{A}/\mathcal{B}$. [Select one member of each coset to use as a representative, and form your table in terms of those representatives. Avoid the appearance of more than one representative of the same coset in the table.]
4. From your reading of this addition table, or otherwise, determine whether or not $\mathcal{A}/\mathcal{B}$ is cyclic. [If all else fails, you could, by iterated addition, compile a table showing the iterated sums of an element with itself, in order to determine the periods (orders) of all elements of the group.]
5. Define a function $f : \mathcal{A}/\mathcal{B} \longrightarrow \mathcal{A}/\mathcal{B}$ by $(a_1, a_2) + \mathcal{B} \longmapsto (2a_1, 2a_2) + \mathcal{B}$.
   (a) Show that f is well defined.
   (b) Show that f is a homomorphism.
   (c) Find the kernel and image of f.

Solution:

1. Adding $(3, 2)$ to itself repeatedly we obtain the set

$$\{(3, 2), (6, 0), (9, 2), (0, 0)\},$$

after which the sums repeat. This last is the subgroup generated by $(3, 2)$, having order 4.

2. There are $12 \times 4 = 48$ elements in the mother group, hence there will be $48/4 = 12$ cosets of any subgroup of order 4. These can be obtained by translating one element — for example the zero element — by elements judiciously chosen from $\mathcal{A}$; of course, if we are careless in choosing the elements by which to "translate", we may meet the same coset several times. At any time, the coset representative chosen should be an element which is not in the union of the cosets already considered.

Coset Representative				
(0,0)	(0,0)	(3,2)	(6,0)	(9,2)
(1,0)	(1,0)	(4,2)	(7,0)	(10,2)
(2,0)	(2,0)	(5,2)	(8,0)	(11,2)
(3,0)	(3,0)	(6,2)	(9,0)	(0,2)
(4,0)	(4,0)	(7,2)	(10,0)	(1,2)
(5,0)	(5,0)	(8,2)	(11,0)	(2,2)
(0,1)	(0,1)	(3,3)	(6,1)	(9,3)
(0,3)	(0,3)	(3,1)	(6,3)	(9,1)
(1,1)	(1,1)	(4,3)	(7,1)	(10,3)
(1,3)	(1,3)	(4,1)	(7,3)	(10,1)
(2,1)	(2,1)	(5,3)	(8,1)	(11,3)
(2,3)	(2,3)	(5,1)	(8,3)	(11,1)

3. In the following table we represent each coset by the representative chosen above.

+	(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)	(0,1)	(0,3)	(1,1)	(1,3)	(2,1)	(2,3)
(0,0)	(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)	(0,1)	(0,3)	(1,1)	(1,3)	(2,1)	(2,3)
(1,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)	(0,0)	(1,1)	(1,3)	(2,1)	(2,3)	(0,3)	(0,1)
(2,0)	(2,0)	(3,0)	(4,0)	(5,0)	(0,0)	(1,0)	(2,1)	(2,3)	(0,3)	(0,1)	(1,3)	(1,1)
(3,0)	(3,0)	(4,0)	(5,0)	(0,0)	(1,0)	(2,0)	(0,3)	(0,1)	(1,3)	(1,1)	(2,3)	(2,1)
(4,0)	(4,0)	(5,0)	(0,0)	(1,0)	(2,0)	(3,0)	(1,3)	(1,1)	(2,3)	(2,1)	(0,1)	(0,3)
(5,0)	(5,0)	(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(2,3)	(2,1)	(0,1)	(0,3)	(1,1)	(1,3)
(0,1)	(0,1)	(1,1)	(2,1)	(0,3)	(1,3)	(2,3)	(3,0)	(0,0)	(4,0)	(1,0)	(5,0)	(2,0)
(0,3)	(0,3)	(1,3)	(2,3)	(0,1)	(1,1)	(2,1)	(0,0)	(3,0)	(1,0)	(4,0)	(2,0)	(5,0)
(1,1)	(1,1)	(2,1)	(0,3)	(1,3)	(2,3)	(0,1)	(4,0)	(1,0)	(5,0)	(2,0)	(0,0)	(2,1)
(1,3)	(1,3)	(2,3)	(0,1)	(1,1)	(2,1)	(0,3)	(1,0)	(4,0)	(2,0)	(5,0)	(3,0)	(2,3)
(2,1)	(2,1)	(0,3)	(1,3)	(2,3)	(0,1)	(1,1)	(5,0)	(2,0)	(0,0)	(3,0)	(1,0)	(4,0)
(2,3)	(2,3)	(0,1)	(1,1)	(2,1)	(0,3)	(1,3)	(2,0)	(5,0)	(3,0)	(0,0)	(4,0)	(1,3)

4. We find the following elements all to have order 12: (1,1), (1,3), (2,1), (2,3). Each of these alone generates the group; their number is, of course, $\varphi(12)$. Only through rearrangement of the labels on the rows and columns of our Cayley table we could arrange for a cyclic table — i.e. for a circulant matrix. For example, we have

+	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)
(0,0)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)
(1,1)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)
(5,0)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)
(0,1)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)
(4,0)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)
(2,3)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)
(3,0)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)
(1,3)	(1,3)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)
(2,0)	(2,0)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)
(3,1)	(3,1)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)
(1,0)	(1,0)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)
(2,1)	(2,1)	(0,0)	(1,1)	(5,0)	(0,1)	(4,0)	(2,3)	(3,0)	(1,3)	(2,0)	(3,1)	(1,0)

5. (a) If (a_1, a_2) and (a_1', a_2') are two representatives of the same $(\mathcal{B})$-coset, they differ by $n(3,2)$. What, we ask, is the image of $(a_1 + 3n, a_2 + 2n)$? It is the coset $(2a_1, 2a_2) + (2n(3,2) + \mathcal{B})$. But, since $(3,2) \in \mathcal{B}$, $2n(3,2) \in \mathcal{B}$, so $2n(3,2) + \mathcal{B} = \mathcal{B}$. Thus the mapping is "well defined".

   (b) $f((a_1, a_2) + (a_1', a_2'))$

$$\begin{array}{lll} = & f(a_1 + a_1', a_2 + a_2') & \text{by def. of } + \text{ in } \mathbb{Z}_{12} \oplus \mathbb{Z}_4 \\ = & (2(a_1 + a_1'), 2(a_2 + a_2')) + \mathcal{B} & \text{by definition of } f \\ = & (2a_1, 2a_2) + (2a_1', 2a_2') + \mathcal{B} & \text{algebraic properties of } \mathbb{Z}_n \\ = & (2a_1, 2a_2) + \mathcal{B} + (2a_1', 2a_2') + \mathcal{B} & \end{array}$$

   showing that f is a homomorphism.

   (c) $f(a_1, a_2)$ is the zero element — i.e. the coset $\mathcal{B}$ iff $(2a_1, 2a_2) \in \mathcal{B}$ — i.e. iff $\exists n \in \mathbb{Z}$ such that

$$\begin{aligned} 2a_1 - 3n &\equiv 0 \pmod{12} \\ 2a_2 - 2n &\equiv 0 \pmod{4} \end{aligned}$$

   i.e. iff $\exists k, \ell, n \in \mathbb{N}$ such that

$$\begin{aligned} 2a_1 - 3n &= 12k \\ 2a_2 - 2n &= 4\ell. \end{aligned}$$

   The second equation reduces to $a_2 = n + 2\ell$, which we may substitute into the first to yield $2a_1 - 3a_2 = -6\ell + 12k$. Thus it is equivalent to look for

points (a_1, a_2) such that $2a_1 - 3a_2 \equiv 0 \pmod 6$. This implies that $3|a_2$ and that $2|a_3$. Conversely, when both of these conditions hold, (a_1, a_2) represents a solution. Thus the kernel consists of the cosets representable by points in $3\mathbb{Z}_{12} \oplus 2\mathbb{Z}_4$, i.e. by

$$\{(0,0), (0,2), (3,0), (3,2), (6,0), (6,2), (9,0), (9,2)\}.$$

But

$$(0,0) + \mathcal{B} = (3,2) + \mathcal{B} = (6,0) + \mathcal{B} = (9,2) + \mathcal{B}$$

and

$$(0,2) + \mathcal{B} = (3,0) + \mathcal{B} = (6,2) + \mathcal{B} = (9,0) + \mathcal{B},$$

so the kernel is the subgroup $\{(0,0) + \mathcal{B},\ (0,2) + \mathcal{B}\}$ of order 2.

The image consists of all cosets representable by an ordered pair whose both coordinates are even; but $(6,0) + \mathcal{B} = (0,0) + \mathcal{B}$, $(6,2) + \mathcal{B} = (0,2) + \mathcal{B} = (3,0) + \mathcal{B}$, $(8,0) + \mathcal{B} = (2,0) + \mathcal{B}$, $(8,2) + \mathcal{B} = (2,2) + \mathcal{B} = (5,0) + \mathcal{B}$, $(10,0) + \mathcal{B} = (4,0) + \mathcal{B}$, $(10,2) + \mathcal{B} = (4,2) + \mathcal{B} = (1,0) + \mathcal{B}$; these can be seen to form the cyclic subgroup of order 6 generated by $(1,0) + \mathcal{B}$.

(Note how the present situation compares with what would have happened if our homomorphism had been between vector spaces over some field. With vector spaces the kernel and image are completely determined by their dimensions; and the domain is the direct sum of the kernel and a subspace isomorphic to the image. But here the domain has the structure of $\mathbb{Z}_{12}$, and the kernel and image respectively have the structures of $\mathbb{Z}_2$ and $\mathbb{Z}_6$; but $\mathbb{Z}_{12}$ cannot be expressed as a direct sum of subgroups of these two structures, since — in such a direct sum — no element has order 12.)

A.6.5.3 Exercise. Let $f : \mathcal{A} \longrightarrow \mathcal{B}$, $g : \mathcal{B} \longrightarrow \mathcal{A}$ be homomorphisms of abelian groups, such that the composition $g \circ f$ maps every $a \in A$ on to a.

1. Show, by providing a single example, that it is possible for f *not* to be onto.
2. Show, by providing a single example, that it is possible for g *not* to be one-to-one.
3. Show that f is one-to-one. Show that g is onto.

Solution:

1. Let $\mathcal{A} = \mathbb{Z}_1$, $\mathcal{B} = \mathbb{Z}_2$, and let f map (0) on to (0) (there's no choice, anyhow). Define $g : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_1$ to be the constant mapping on to (0) (again there's no choice). Then $g \circ f$ is the zero homomorphism, which, in the present case, is also the identity homomorphism. But f maps no element on to (1).

2. The same example has g mapping both (0) and (1) both on to (0).
3. $f(a) = f(a') \Rightarrow g(f(a) = g(f(a')) \Leftrightarrow (g \circ f)(a) = (g \circ f)(a') \Leftrightarrow a = a'$.
4. Let $a \in \mathcal{A}$. Then $a = (g \circ f)(a) = g(f(a)) \in \text{ im}(g)$.

A.6.5.4 EXERCISE. Let $\mathcal{A}$ be the direct sum of seven copies of $\mathbb{Z}_2$ and define the function $f : \mathcal{A} \longrightarrow \mathbb{Z}_2$ to be the linear transformation whose matrix is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Determine a set of generators for each of $\ker f$ and $\text{im } f$.

Solution: This may be solved as a problem in linear algebra, over the *field* $\mathbb{Z}_2$. Reducing the matrix to row echelon form yields $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$ yielding a 4-dimensional solution space, one of whose bases is $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. (This kernel is what is called a "Hamming code".)

The image of f consists of all linear combinations of columns of the given matrix; evidently the rank of this column space is 3, so the image consists of all of ${\mathbb{Z}_2}^3$; one generating set is $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

A.7 Rings and Fields

A.7.1 Rings

A.7.1.1 DEFINITION. 1. A ring $\mathcal{R} = (\mathfrak{A}, +, 0, *)$ is an abelian group $(\mathfrak{A}, +, 0)$, endowed with a composition $*$ such that

(a) $(\mathfrak{A}, *)$ is a semigroup — i.e., $*$ is associative

(b) [Distributive Laws:]

$$\begin{aligned}(a_1 + a_2) * a_3 &= (a_1 * a_3) + (a_2 * a_3)\\ a_1 * (a_2 + a_3) &= (a_1 * a_2) + (a_1 * a_3)\end{aligned}$$

for all $a_1, a_2, a_3 \in \mathfrak{A}$.

2. Where $*$ is commutative, $\mathcal{R}$ is said to be *commutative*.

3. Some authors permit the composition $*$ to be non-associative, and call the structure we have defined above an *associative* ring.[377]

4. Where there exists an element $e \in \mathcal{R}$ such that $(\mathfrak{A}, *, e)$ is a monoid, e is called a *unit element* or *unity*;[378] the ring is then called a *ring with unity*, or *ring with unit element*. It may be denoted by $(\mathfrak{A}, +, 0, *, e)$. It is customary to require that e and 0 be distinct elements.

A.7.1.2 EXERCISE. Suppose that we were to relax the customary requirement that $e \neq 0$ in a ring with unity $(\mathfrak{A}, +, 0, *, e)$. Investigate the structure of such a ring.

A.7.1.3 EXAMPLE. Examples of rings:

1. Let $(\mathcal{G}, +, 0)$ be any abelian group. We may impose a "trivial" or "zero" multiplicative structure by defining $g_1 * g_2 = 0$.

2. $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{C}$, $\mathbb{Q}$, are all commutative rings.

3. for any ring $\mathcal{R}$, the ring $\mathcal{R}[x]$ of polynomials in an indeterminate x with coefficients in $\mathcal{R}$ (to be defined formally below in §A.7.3)

4. for any ring $\mathcal{R}$, the ring $\mathcal{R}\{x\}$ (also denoted by $\mathcal{R}[[x]]$) of formal power series in an indeterminate x with coefficients in $\mathcal{R}$ (to be defined formally below in §A.7.3)

[377] An example of a *non-associative ring* would be $(\mathbb{R}^3, +, \vec{0}, \times)$, where $\times$ is the cross product.
[378] but not a *unit* which has a more general meaning.

5. for any ring $\mathcal{R}$ and any natural number n, the ring of square $n \times n$ matrices with coefficients in $\mathcal{R}$

6. for any set $\mathfrak{A}$, the *Boolean ring of subsets* $(P(\mathfrak{A}), +, \emptyset, \cap)$, where

$$A + B = (A - B) \cup (B - A)$$

7. $(\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}, +, 0, \times)$

8.

A.7.1.4 EXERCISE. 1. In Example A.7.1.3.1 above, let g_0 be any fixed element of $\mathcal{G}$ distinct from 0. Show that we *cannot* define a "trivial" ring structure by defining $g_1 * g_2 = g_0$ for all $g_1, g_2 \in \mathcal{G}$.

2.

A.7.1.5 EXERCISE. Prove that the identity $(c + d)^2 = c^2 + 2cd + d^2$ holds for all c and d in a ring $\mathcal{R}$ iff $\mathcal{R}$ is commutative.

Solution: $(c + d)(c + d) = cc + cd + dc + dd$. This is equal to $c^2 + 2cd + d^2$ iff $cd = dc$. Thus, if $\mathcal{R}$ is commutative, the identity holds $\forall c, d$. And, if the identity holds $\forall c, d$, then $cd = dc$ always, i.e. $\mathcal{R}$ is commutative. □

A.7.1.6 EXERCISE. 1. Let $\mathcal{R} = (\mathfrak{A}, +, 0, *)$ be a ring. Then $\forall a, , b \in \mathcal{R}$

(a) $0 * a = 0 = a * 0 \ \forall a \in \mathcal{R}$

(b) $(-a) * b = -(a * b) = a * (-b)$

(c) $(-a) * (-b) = a * b$

2. Let $\mathcal{R} = (\mathfrak{A}, +, 0, *, e)$ be a ring with unity. Define elements $\overline{n} \in \mathcal{R}$ recursively by

$$\overline{1} = e$$

$$\overline{n + 1} = \overline{n} + e$$

Then[379]

(a) $\overline{n} * r = nr \ \forall r \in \mathcal{R}$

(b) $\overline{m + n} = \overline{m} + \overline{n}$

(c)

[379]The iterated sum ne in the Abelian group $(\mathfrak{A}, +, 0)$ is defined in Definition A.5.1.6.

A.7.1.7 DEFINITION. Let $\mathcal{R} = (\mathfrak{A}, +, 0, *)$ be a ring.

1. A *zero divisor* in $\mathcal{R}$ is a non-zero element $r \in \mathcal{R}$ such that there exists a non-zero element $s \in \mathcal{R}$ with the property that $r * s = 0$,

2. A *commutative* ring with unity, $(\mathfrak{A}, +, 0, *, e)$ having no zero divisors is called an *integral domain* or *domain of integrity*.

If $(\mathfrak{A}, +, 0, *, e)$ is a ring with unit element, it may happen that certain of its elements possess *multiplicative* inverses, i.e. inverses in the monoid $(\mathfrak{A}, *, e)$. Of course, 0 cannot possess an inverse, by virtue of Exercise A.7.1.6.1.1a.

In the course of the preceding theorem we have *defined* $\overline{n}$. Since, as we have shown, $\overline{n} * r = nr$, there is little danger of confusion if the bar is suppressed. However, the student is cautioned that there is no assurance that $\overline{n}$ has a multiplicative inverse. Thus it may well happen that $n * r = 0$ (or, equivalently, $nr = 0$) even though neither n nor r is zero: i.e. that n is a zero divisor. (For example, there are such zero divisors in all rings $(\mathbb{Z}_n, +, 0, *, 1)$ whenever n is composite.)

A.7.1.8 DEFINITION. 1. An element of a ring which possesses a multiplicative inverse is called a *unit*.

2. A ring $\mathcal{R} = (\mathfrak{A}, +, 0, *, e)$ in which every element except 0 is a unit, i.e. in which every element except 0 has a multiplicative inverse — i.e. in which $(\mathfrak{A} - \{0\}, *, e)$ is a group — is called a *division ring* or *skew field* or *sfield*[380]

3. A commutative division ring is called a *field*.

A.7.1.9 EXERCISE. 1. When is a unity is a unit?

2. Determine the smallest field.

3.

4.

5.

We state without proof the following theorem [46].

A.7.1.10 THEOREM (WEDDERBURN). *Every finite division ring is a field.*

[380]Some authors even call it a *field*; what we call a field they then call a *commutative* field.

A.7.1.11 Example. The *quaternions*, defined in §A.5.8, form a non-commutative division ring.

A.7.1.12 Definition. If $(\mathfrak{A}, +, 0, *)$ is a ring, the additive abelian group $(\mathfrak{A}, +, 0)$ may or may not have an *exponent* (cf. Definition A.5.6.5). Where the exponent exists, it is called the *characteristic* of the ring. Where no exponent exists — i.e. where the periods of the elements of the additive group are either infinite, or, as a set, unbounded, the ring is said to have *characteristic zero*. (For a justification of this terminology, cf. [20, p. 103].)

A.7.1.13 Exercise. If $(\mathfrak{A}, +, 0, *, e)$ is a ring with unity, having characteristic m, show that $ma = 0$ for all $a \in \mathfrak{A}$, and hence $m * a = 0$ for all $a \in \mathfrak{A}$. Conclude that if $(\mathfrak{A}, +, 0, *)$ has no zero divisors, then $m = 0$ — i.e. that the iterated sum of m copies of e is 0. Then examine the prime decomposition of m and show that, in such a case, m must be a prime. Finally, show that all non-zero elements of $(\mathfrak{A}, +, 0)$ have period *exactly* the prime m.

A.7.2 Ring Homomorphisms. Subrings. Ideals

A.7.2.1 Definition. Let $(\mathfrak{A}, +, 0, *)$ and $(\mathfrak{A}', +', 0', \star)$ be rings. A function $\phi : \mathfrak{A} \longrightarrow \mathfrak{A}'$ is said to be a *ring homomorphism* if

1. $\phi : (\mathfrak{A}, +, 0) \longrightarrow (\mathfrak{A}', +', 0')$ is a group homomorphism; and if
2. $\phi : (\mathfrak{A}, *) \longrightarrow (\mathfrak{A}', \star)$ is a semigroup homomorphism.

If, moreover, $(\mathfrak{A}, +, 0, *)$ and $(\mathfrak{A}', +', 0', \star)$ are rings having respective unities e and f, then we will say that $\phi : \mathfrak{A} \longrightarrow \mathfrak{A}'$ is a *homomorphism of rings with unity* if, in addition to the preceding conditions,

3. $\phi(e) = f$

That is, if, in place of condition 2, the following holds:

2′. $\phi : (\mathfrak{A}, *, e) \longrightarrow (\mathfrak{A}', \star, f)$ is a monoid homomorphism.

A.7.2.2 Definition. A ring $(\mathfrak{A}', +', 0', \star)$ is said to be a *subring* of the ring $(\mathfrak{A}, +, 0, *)$ if

1. $(\mathfrak{A}', +', 0')$ is a subgroup of the group $(\mathfrak{A}, +, 0)$, and
2. $(\mathfrak{A}', \star)$ is a subsemigroup of the semigroup $(\mathfrak{A}, *)$

When we apply this concept to rings with unity $(\mathfrak{A}', +', 0', \star, e)$, $(\mathfrak{A}, +, 0, *, e)$ we shall also postulate that

$3'.\ e = f$

The concept of *subring* is inadequate for the development of results involving quotients, analogous to those for the quotient of a normal subgroup in a group. Since a subring is, in particular, a subgroup of the additive *abelian* group of its "parent" — hence a *normal* subgroup, there will be a quotient structure insofar as addition is concerned. We wish to be able to define the product of cosets analogously to (352). For this purpose additional restrictions will be required.

Suppose that $(\mathfrak{B}, +, 0, *)$ is a subring of $(\mathfrak{A}, +, 0, *)$. We should like to define the *product* of cosets $a_1 + \mathfrak{B}$ and $a_2 + \mathfrak{B}$ to be the coset $a_1 * a_2 + \mathfrak{B}$, as we did in Corollary A.1.7.7 to Theorem A.1.4.5. For this composition to be well defined, it will be necessary and sufficient that, for all $b_1, b_2 \in \mathfrak{B}$,

$$(a_1 + b_1) * (a_2 + b_2) \in a_1 * a_2 + \mathfrak{B}$$

i.e. that

$$(a_1 * b_2) + (a_2 * b_1) \in \mathfrak{B}$$

By considering special cases where either of the elements b_1, b_2 is zero, this can be seen to be equivalent to requiring that, for all $b \in \mathfrak{B}$, *both* of the following conditions hold:

$$a_1 * b \in \mathfrak{B} \tag{359}$$

$$b * a_2 \in \mathfrak{B} \tag{360}$$

A subring which satisfies condition (359) is called a *left*[381] *ideal*; one which satisfies condition (360) is called a *right*[382] ideal. A *two-sided ideal* is both a left ideal and a right ideal, and is usually called simply an *ideal*. We have proved that a definition of coset multiplication through the use of arbitary coset representatives will be well defined iff $\mathfrak{B}$ is an ideal of $\mathfrak{A}$. Calling this multiplication $*$, we may now extend Theorem A.5.5.10:

A.7.2.3 THEOREM. *Let $(\mathfrak{B}, +, 0, *)$ be an ideal of a ring $(\mathfrak{A}, +, 0, *)$. Then the quotient group $\mathfrak{A}/\mathfrak{B}$ may be endowed with a ring structure by defining*

$$(a_1 + \mathfrak{B}) * (a_2 + \mathfrak{B}) = a_1 * a_2 + \mathfrak{B}$$

The ring is $(\mathfrak{A}/\mathfrak{B}, +, 0 + \mathfrak{B}, *)$. (Remember that the symbols $+$ and $*$ are used with several meanings here.)

A.7.2.4 EXERCISE. Prove Theorem A.7.2.3.

[381] with the usual caveat that some authors reverse our use of the words *left* and *right*.

[382] cf. footnote 381

A.7.2.5 DEFINITION. $(\mathfrak{A}/\mathfrak{B}, +, 0+\mathfrak{B}, *)$ is called a *factor ring*.

A.7.2.6 EXERCISE. 1.

2.

3.

A.7.2.7 EXERCISE. Let $(\mathfrak{A}, +, 0, *)$ be a *commutative* ring, and $s \in \mathfrak{A}$. Then the set of all multiples

$$(s) = \{as : a \in \mathfrak{A}\}$$

is an ideal of $(\mathfrak{A}, +, 0, *)$.

A.7.2.8 DEFINITION. 1. (s) is called a *principal* ideal.

2. A ring in which every ideal is principal is called a *principal ideal domain*.

A.7.2.9 EXERCISE. Let $(\mathfrak{A}, +, 0, *, e)$ be a commutative ring with unity. Then $(e) = (\mathfrak{A}, +, 0, *, e)$ and $(0) = (0, +, 0, *)$.

A.7.2.10 EXAMPLE. *$\mathbb{Z}$ is a principal ideal domain.* Let $(\mathfrak{B}, +, 0) \leq (\mathbb{Z}, +, 0)$. If $\mathfrak{B} = \{0\}$, then $\mathfrak{B}$ is the ideal (0). Otherwise, if $0 \neq x \in \mathfrak{B}$, then $|x| \in \mathfrak{B}$. Among all elements of $\mathfrak{B}$, let m be the smallest positive element. For any other element $n > 0$ we can find q and r such that $n = q \cdot m + r$, where $0 \leq r \leq m-1$, i.e. such that

$$0 \leq r = n - mq < n$$

From the minimality of m we may conclude that $r = 0$, i.e. that $m \mid n$. We have thus shown that all subgroups of $(\mathbb{Z}, +, 0)$ are cyclic, of the form (m). But any such additive subgroup is an ideal, generated by m.

A.7.2.11 EXERCISE. 1. Let $(\mathfrak{A}, +, 0, *, e)$ be a ring with unity. Show that, for fixed invertible $c \in \mathfrak{A}$, the mapping $a \mapsto c^{-1}ac$ is a homomorphism — indeed, an *automorphism*.

2. Show that the mapping $f : \mathbb{C} \longrightarrow M(2, \mathbb{R})$ defined by $a+ib \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ defines a one-to-one ring homomorphism. (This shows that the complex numbers may be *represented* as a subfield of the ring of 2×2 real matrices.)

3. Show that the following tables define a field with 4 elements. Explain why this field cannot be constructed from the ring $\mathbb{Z}_4$ of residues modulo 4:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

.

4. Consider the ring of quotients $\dfrac{a+b\sqrt{5}}{c+d\sqrt{5}}$, where $a, b, c, d \in \mathbb{Z}$, and c and d are *not both zero*. Show that this ring is a *field*. Then show that if we replace $\sqrt{5}$ by $\sqrt{2}$, we obtain a different field.

A.7.2.12 DEFINITION. The *kernel* and *image* of a ring homomorphism are defined to be the *kernel* and *image* of the corresponding homomorphism of abelian groups.

A.7.2.13 THEOREM. *Let* $\phi : (\mathfrak{A}, +, 0, *) \longrightarrow (\mathfrak{B}, +, 0, *)$ *be a ring homomorphism. Then* $\ker \phi$ *is a two-sided ideal of the domain, and* $\operatorname{im} \phi$ *is a subring of the codomain.*

A.7.2.14 EXERCISE. Prove Theorem A.7.2.13.

Note that the image need not be an ideal of the codomain.

A.7.3 Polynomials and Power Series

We propose to generalize well known algebraic properties of real polynomials and power series to environments where the coefficients are no longer real numbers. Certain of our generalizations can be extended to the very general rings; however, to simplify the treatment, and because the present generalization is sufficient for most practical applications, we confine ourselves to taking coefficients from rings $(\mathfrak{A}, +, 0, *, e)$ which are *commutative* and posssess a unity. For the remainder of this chapter all rings will have these properties. Wherever possible we shall abbreviate $(\mathfrak{A}, +, 0, *, e)$ to $\mathfrak{A}$. We may also use the symbol 1 for the unity.

We shall have several instances in this subsection where we reuse symbols that already have defined meanings. This reuse will be in the spirit of §A.1.7, where we defined operations $\boxplus$, etc., and later replaced $\boxplus$ by $+$.

A.7.3.1 DEFINITION. Let $\mathfrak{A}$ be a ring[383]. Let x be a symbol, called an *indeterminate*.

[383]Remember – we are assuming all rings are commutative and have a unity, denoted by e or 1.

1. A *polynomial* is a "formal sum" of the form

$$a_0x^0 + a_1x^1 + ... + a_nx^n \tag{361}$$

where a_0, a_1, ..., a_n are elements of $\mathfrak{A}$, and, for the present, both the exponentiation and the apparent addition should be treated as simply parts of the formal notation. That is, it is not intended yet that 361 should be interpreted as a sum; nor should x^r be interpreted as a product of x's. Notwithstanding the foregoing, we may abbreviate the "term" a_0x^0 to a_01, or simply to a_0, and the "term" a_1x^1 to a_1x; "terms" with zero coefficients may be suppressed entirely. (These conventions will be justified when we show that the + symbols which form part of the notation for a polynomial are consistent with the operation of addition which we shall define for polynomials; and that that operation is associative.)

2. If $a_0 = a_1 = ... = a_n$, the polynomial is said to be the *zero* polynomial. We will usually denote this polynomial by the same symbol 0 as the zero element of the ring of coefficients.

3. If the polynomial is not the zero polynomial, and if $m = \max\{0, 1, ..., n : a_i \neq 0\}$, then a_mx^m is called its *leading term*, and m is called its *degree*. We may also say that the zero polynomial has degree $-\infty$.

4. More generally than part 2 above, we may denote any polynomial $a_0x^0 + 0x^1 + 0x^2 + ...$ simply by a_0. In this way we interpret the set $\mathfrak{A}$ as a subset of the set of polynomials.

5. We have assigned no significance to the parameter n which appears in (361). More precisely, we intend by (361) a formal sum of the form

$$a_0x^0 + a_1x^1 + ... + a_nx^n + ... \tag{362}$$

where a_0, a_1, ..., a_n, ... are elements of $\mathfrak{A}$, *no more than a finite number of which are not zero*. Thus, we might have been advised to define formal power series first, and then define polynomials a power series with only finitely many non-zero coefficients.

6. Where the ring of coefficients has a unity, a polynomial of degree n having *leading term* ex^n is said to be *monic*.

7. It is convenient to denote polynomials in a ring $\mathfrak{A}[x]$ by symbols like $f(x)$, although we have not yet contemplated any substitution of ring elements for the indeterminate; a symbol $f(x)$ may be abbreviated to simply f, where there is no need to specify the indeterminate.

8. The *degree* of a polynomial $f(x)$ may be denoted by $\deg f(a)$, or simply by $\deg f$.

Initially the symbol x will only serve as a "marker" to keep the coefficients in their places. The following definitions could be stated exclusively in terms of those coefficients. It is, however, more convenient to phrase the definition in more suggestive terms.

A.7.3.2 DEFINITION. The set of all polynomials in x with coefficients from a ring $\mathfrak{A}$ is denoted by $\mathfrak{A}[x]$. We *define* an operation of addition on this set, by

$$\begin{aligned} & (a_0x^0 + a_1x^1 + ... + a_nx^n) + (a'_0x^0 + a'_1x^1 + ... + a'_nx^n) && (363) \\ = \; & (a_0 + a'_0)x^0 + (a_1 + a'_1)x^1 + ... + (a_n + a'_n)x^n && (364) \end{aligned}$$

Note that there are three uses of the + symbol in this equation. The central use in (363) is what we are defining here; there is also the use of the symbol in the formal notation for polynomials; and, finally, in (364) we are expressing our definition in terms of the sums of elements in the ring $(\mathfrak{A}, ..., +, ...)$. We also define an operation of multiplication on the set of polynomials:

$$\begin{aligned} & (a_0x^0 + a_1x^1 + ... + a_nx^n) * (a'_0x^0 + a'_1x^1 + ... + a'_nx^n) \\ & = (a_0 * a'_0)x^0 + (a_0 * a'_1 + a_1 * a'_0)x^1 + ... \\ & \quad + (a_0 * a'_r + a_1 * a'_{r-1} + ... + a_{r-1} * a'_1 + a_r * a'_0)x^r + ... \end{aligned} \tag{365}$$

A.7.3.3 THEOREM. *Under the operations + and ∗ defined above,* $(\mathfrak{A}[x], +, 0, *, 1)$ *is a commutative ring with unity.*

A.7.3.4 EXERCISE. Prove Theorem A.7.3.3

Analogous to the preceding definitions for polynomials, we may define *formal power series*. The reader is cautioned that no attempt is being made at the present time to define the *value* of a power series at a point. Thus there is no need to consider questions of *convergence*.

A.7.3.5 DEFINITION. Let $\mathfrak{A}$ be a ring, and x an *indeterminate*.

1. A *formal power series* is a "formal sum" of the form

$$a_0x^0 + a_1x^1 + ... + a_nx^n + ...$$

   where a_0, a_1, ..., a_n, ... are elements of $\mathfrak{A}$.

2. The set of formal power series in the indeterminate x *over* the ring $\mathfrak{A}$ will be denoted by[384] $\mathfrak{A}\{x\}$.

[384]Some authors denote it by $\mathfrak{A}[[x]]$.

3. Addition and multiplication of formal power series is defined "termwise", generalizing Definition A.7.3.2.

4. We shall interpret $\mathfrak{A}[x]$ as a subset of $\mathfrak{A}\{x\}$, in the obvious sense.

5. We shall interpret $\mathfrak{A}$ as the subset consisting of the polynomials of degree not exceeding zero.

A.7.3.6 Corollary (to Theorem A.7.3.3). *Under the operations $+$ and $*$ defined above, $(\mathfrak{A}\{x\}, +, 0, *, 1)$ is a commutative ring with unity.*

The reader has certainly observed that the definition we have chosen for multiplication is consistent with the familiar *Cauchy* or *convolution product* of power series or sequences.

A.7.3.7 Exercise. Suppose that we define on the set $\mathfrak{A}[x]$ a "termwise" product different from the convolution product:

$$\begin{aligned}&(a_0x^0 + a_1x^1 + ... + a_nx^n) \star (a'_0x^0 + a'_1x^1 + ... + a'_nx^n)\\ &= (a_0 * a'_0)x^0 + (a_1 * a'_1)x^1 + ... + (a_r * a'_r)x^r + ...\end{aligned}$$

Show that $(\mathfrak{A}\{x\}, +, 0, \star)$ is a commutative ring. But show that except for a "trivial" case, this ring has no unity.

A.7.3.8 Exercise. 1. Let $(\mathfrak{A}, +, 0, *, e)$ be a commutative ring with unity, and let x and y be distinct indeterminates. Show that the rings $(\mathfrak{A}[x])[y]$ and $(\mathfrak{A}[x])[y]$ are isomorphic. (This ring, in any of its isomorphic forms, is usually denoted by $\mathfrak{A}[x, y]$.)

2. Consider the subset of $(\mathfrak{A}[x])[y]$ consisting of all polynomials of the form

$$a_0(x)y^0 + a_1(x)y^1 + ... + a_n(x)y^n + ...$$

where $a_i(x) \in \mathfrak{A}[x]$ $(i = 0, 1, ..., n, ...)$ in which $a_0 = a_{00}x^0 + a_{01}x^1 + ... + a_{0m}x^m + ...$ and

$$a_{00} = 0$$

(i.e. the polynomials in x and y with zero "constant term") is <u>not</u> principal.

A.7.4 Factorization of Polynomials

We shall apply terms like *factor*, *multiple*, *divides*, etc. to rings in the obvious generalizations of the meanings defined in $\mathbb{Z}$, without formal definitions. It is natural to investigate the extent to which theorems proved for $\mathbb{Z}$ can be generalized to all rings. This we shall not do in generality, but shall confine our investigation here to rings of polynomials. We begin by proving an analogue of the Division Algorithm.

We shall require, in this subsection, that the ring of coefficients be a *field*, which we shall denote by $\mathbb{F}$.

A.7.4.1 THEOREM (DIVISION ALGORITHM). *Let $\mathbb{F}[x]$ be a ring of polynomials with coefficients in a* field *$(\mathbb{F}, +, 0, *, e)$. Let $a(x)$ and $b(x)$ be polynomials such that the degree of $b(x)$ is $n > 0$. Then there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that*

$$a(x) = (q(x) * b(x)) + r(x)$$

where

$$\deg(r) < \deg(b)$$

The polynomials q and r are respectively called the quotient *and* remainder.

A.7.4.2 EXERCISE. 1. Prove Theorem A.7.4.1 by formalizing the familiar mechanical procedure of division of real polynomials.

2.

A.7.4.3 EXERCISE. 1.

2.

We have been able to delay the concept of *substitution* for an indeterminate until this point. In order to characterize divisibility of a polynomial by a *linear* factor — i.e. by a factor of degree 1 — we shall require the concept of evaluating a polynomial at a point in the field of coefficients.

A.7.4.4 DEFINITION. Let $f(x) = a_0x^0 + a_1x^1 + ... + a_nx^n \in \mathbb{F}[x]$, and let $b \in \mathbb{F}$.

1. We define a function
$$f : \mathbb{F} \longrightarrow \mathbb{F}$$
by
$$b \longmapsto a_0b^0 + a_1b^1 + ... + a_nb^n\,.$$
The value to which b is mapped is denoted by $f(b)$.

2. If $f(b) = 0$, we may describe b as *zero* of the polynomial $f(x)$.

A.7.4.5 THEOREM (REMAINDER THEOREM). *Let $f(x) \in \mathbb{F}[x]$, and let $x - b$ be a polynomial of degree 1 in $\mathbb{F}[x]$. Then $x - b$ divides $f(x)$ iff $f(b) = 0$.*

A.7.4.6 DEFINITION. 1. Let α be a non-zero element of $\mathbb{F}$. Then any polynomial $a(x) \in \mathbb{F}[x]$ admits a *trivial* factorizations of the form $a = \alpha * \frac{a}{\alpha}$, where the first factor α is the polynomial of degree 0, and where $\frac{a}{\alpha}$ is the polynomial obtained from $a(x)$ by dividing each of its coefficients by α. Equivalently, a factorization $a(x) = b(x) * c(x)$ of a polynomial $a(x)$ is non-trivial only if the degrees of both b and c are strictly less than the degree of a.

2. A polynomial which admits no factorization except the trivial factorizations is said to be *irreducible*; a polynomial which is not irreducible is said to be *reducible*.

3. Since we may have occasion to consider the same polynomial over various fields, we may specify the field under consideration by saying that the polynomial is *irreducible over* $\mathbb{F}$, or *reducible over* $\mathbb{F}$.

A.7.4.7 EXERCISE.

Show that the polynomial $x^2 + 1$ is irreducible over the field $\mathbb{R}$, but that it is reducible over the field $\mathbb{C}$.

Show that the polynomial $x^2 - 3$ is irreducible over the field $\mathbb{Q}$.

A.7.5 Fields

In Definition A.7.1.8.3 we defined a *field* to be a *commutative division ring* $(\mathfrak{A}, +, 0, *, e)$, where $e \neq 0$. In this section we will investigate properties and construction of certain fields. We make no attempt at completeness.

Among infinite fields that the student has met thus far are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. However, we have seen others[385] In this section we will concentrate our attention on *finite* fields, because of their usefulness in constructions in computer science. The student has already encountered the fields $\mathbb{Z}_p$, where p is a prime. But there exist other finite fields, not isomorphic to any $\mathbb{Z}_p$. In fact, there will be, up to isomorphism, just one field of order n where n is any power of any prime, and no other fields of finite order. We will describe constructions for such fields, and some applications.

[385]For example, (cf. Exercise A.7.2.11.4) the field consisting of all quotients $\frac{a + b\sqrt{5}}{c + d\sqrt{5}}$ is a subfield of $\mathbb{R}$, but a *superfield* of $\mathbb{Q}$.

A.7.5.1 EXERCISE. We have claimed that there will be just one field of order 2^2. Since the rings $\mathbb{Z}_n$ are known to be fields when n is a prime, one might have been led to suspect that $\mathbb{Z}_4$ is a field. Show that the identity element under multiplication in $(\mathbb{Z}_4, *)$ is $[1]_4$, but that $(\mathbb{Z}_4, +, [0]_4, *, [1]_4)$ is *not* a field.

We have observed earlier (cf. Exercise A.7.1.13) that the characteristic of a finite field must be a prime p. Any finite field $\mathbb{F}$ of characteristic p will, therefore, contain a subfield — let's denote it by $\mathbb{F}_1$ — of structure $\mathbb{Z}_p$, generated by its unity. Suppose that $\alpha \in \mathbb{F}$ is not in this subfield. It cannot happen that all polynomials in α with coefficients taken from $\mathbb{F}_1$ are all different, since $\mathbb{F}$ is finite. Hence two such polynomials are equal; or, equivalently, there exists a non-zero polynomial $f(x) = a_0 + a_1 x + ... + a_k x^k \in \mathbb{F}_1[x]$ such that $f(\alpha) = 0$. Among all such polynomials *satisfied by* α we may select one of minimum degree; let us denote one such polynomial by $f(x) = a_0 + a_1 x + ... + a_k x^k$. Then it cannot happen that f is reducible. For, if $f(x) = f_1(x) * f_2(x)$ is a non-trivial factorization into polynomials of strictly lower degrees, the absence of zero-divisors in a field would imply from $f_1(\alpha) * f_2(\alpha) = 0$ that $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$, contradicting the minimality of the degree of f. It is this property which motivates the construction we shall describe below for fields of order p^k from the field $\mathbb{Z}_p$.

The construction uses irreducible polynomials. We shall show that any field of order p^k can be constructed from $\mathbb{Z}_p$ by using a polynomial of degree k which is irreducible over $\mathbb{Z}_p$.

We can then look for the "smallest" subfield of $\mathbb{F}$ which contains α:

B 1997 Problem Assignments, with Solutions

B.1 First 1997 Problem Assignment

1. [8, Problems 1.28, 1.29]

   (a) Prove that if $\alpha : S \to T$, and A and B are subsets of S, then

   $$\alpha(A \cap B) \subseteq \alpha(A) \cap \alpha(B)\,.$$

   (b) Give an example (specific S, T, A, B, and α) to show that equality need not hold in part 1a. (For the simplest examples S will have two elements.)

   (c) Prove that equality holds *for all A and B* iff α is injective.

   Solution: (A problem similar to this appeared on the 1996 examination in 189-240A.)

   (a) To prove that set $\alpha(A \cap B)$ is contained in set $\alpha(A) \cap \alpha(B)$ we must show that any point in the first set is a member of the second. This part of the proof depends on the definition of α(subset) [8, p. 14, l. 7]:

   $$\alpha(A) = \{\alpha(x) : x \in A\}\,;$$

   equivalently,

   $$x \in \alpha(A) \Leftrightarrow (\exists y \in A)(x = \alpha(y))\,;$$

   or, more precisely,

   $$(\forall x \in T)(x \in \alpha(A) \Leftrightarrow (\exists y \in A)(x = \alpha(y)))\,.$$

   Thus a point x is in $\alpha(C)$ iff there exists a point $y \in C$ such that $x = \alpha(y)$. We will give below a "pedantic" proof, some of whose steps we would normally suppress. We will indicate which lines of this proof could be suppressed.

   $$\begin{aligned}
   & x \in \alpha(A \cap B) && (1001)\\
   \Leftrightarrow\ & (\exists y \in A \cap B)(x = \alpha(y)) \quad \text{definition of } \alpha\text{(subset)} && (1002)\\
   \Rightarrow\ & (x = \alpha(y_0)) \wedge (y_0 \in A \cap B) && (1003)\\
   & \text{naming one point whose existence has been proved} \\
   \Leftrightarrow\ & (x = \alpha(y_0)) \wedge ((y_0 \in A) \wedge (y_0 \in B)) \quad \text{definition of } \cap && (1004)\\
   \Leftrightarrow\ & ((x = \alpha(y_0)) \wedge (x = \alpha(y_0))) \wedge ((y_0 \in A) \wedge (y_0 \in B)) && (1005)\\
   & \text{"idempotency" of } \wedge
   \end{aligned}$$

$$\Leftrightarrow \quad (x = \alpha(y_0)) \wedge ((x = \alpha(y_0) \wedge ((y_0 \in A) \wedge (y_0 \in B))) \qquad (1006)$$
"associativity" of $\wedge$

$$\Leftrightarrow \quad (x = \alpha(y_0)) \wedge (((x = \alpha(y_0)) \wedge (y_0 \in A)) \wedge (y_0 \in B)) \qquad (1007)$$
"associativity" of $\wedge$

$$\Leftrightarrow \quad (x = \alpha(y_0)) \wedge ((y_0 \in B) \wedge ((x = \alpha(y_0)) \wedge (y_0 \in A))) \qquad (1008)$$
"commutativity" of $\wedge$

$$\Leftrightarrow \quad ((x = \alpha(y_0)) \wedge (y_0 \in B)) \wedge ((x = \alpha(y_0)) \wedge (y_0 \in A)) \qquad (1009)$$
"associativity" of $\wedge$

$$\Rightarrow \quad (x \in \alpha(B)) \wedge (x \in \alpha(A)) \quad \text{definition of } \alpha\text{(subset)} \qquad (1010)$$

$$\Leftrightarrow \quad (x \in \alpha(A)) \wedge (x \in \alpha(B)) \quad \text{"commutativity" of } \wedge \qquad (1011)$$

$$\Leftrightarrow \quad x \in \alpha(A) \cap \alpha(B) \quad \text{definition of } \cap \qquad (1012)$$

In the preceding proof mathematicians would often suppress line (1003), and would often use the same symbol for the specific point as was quantified in the previous line; lines (1005), (1006), (1007), (1008), and possibly even (1009) could be omitted; line (1010) might also be omitted. Note that, with the exception of line (1003), which is a technical definition, all the implications are reversible, except line (1010). This line holds the key to the other parts of the problem.

(b) For the simplest possible counterexample take $S = \{a, b\}$ where $a \neq b$; $A = \{a\}$, $B = \{b\}$, $T = \{t\}$. The mapping $\alpha : S \to T$ is uniquely determined as the constant mapping $a \mapsto t$, $b \mapsto t$. But $A \cap B = \varnothing$, so $\alpha(A \cap B) = \varnothing \neq \{t\} = \alpha(a) \cap \alpha(b)$.

(c) We generalize the preceding counterexample to show that injectivity is *necessary*, that is, shows that equality holds *for all A and B* only if α is injective. If α is not injective, then there exist two points $a, b \in S$ mapped on to the same point $t \in T$. Define $A = \{a\}$, $B = \{b\}$ as in the preceding example. Then, as before, $\alpha(A \cap B) = \varnothing \neq \{t\} = \alpha(A) \cap \alpha(B)$.

Conversely, suppose that $\alpha : S \to T$ is injective. Then

$$\begin{aligned}
& x \in \alpha(A) \cap \alpha(B) \\
\Rightarrow \quad & ((\exists y_1 \in A)(x = \alpha(y_1)) \wedge ((\exists y_2 \in B)(x = \alpha(y_2)) \\
\Rightarrow \quad & (\exists y_1 \in A)(\exists y_2 \in B)(x = \alpha(y_1) = \alpha(y_2)) \\
\Rightarrow \quad & y_1 = y_2 \quad \text{since } \alpha \text{ is injective} \\
& \text{thus } (\exists y_1 \in A \cap B)(x = \alpha(y_1)) \\
\Leftrightarrow \quad & x \in \alpha(A \cap B)
\end{aligned}$$

□

2. Prove that a (binary) operation $\heartsuit : S \times S \to S$ cannot have more than one identity element.

   Solution: Suppose that u and v are both identity elements. Since u is an identity element, $u\heartsuit x = x$ for all x; in particular, taking $x = v$, we have $u\heartsuit v = v$. Since v is an identity element, $x\heartsuit v = x$ for all x, in particular, when $x = u$, $u\heartsuit v = v$; hence $u = u\heartsuit v = v$.

3. [8, Problem 3.24] Showing all your work — every step must be justified — complete the following table in such a way that $*$ is commutative and has an identity element, and that each element has an inverse. (There is only one correct solution. First explain why y must be the identity element.)

$*$	w	x	y	z
w	y			x
x	z	w		
y				
z				w

   Solution: We shall first prove that none of x, z, w can be the identity. Since $w*w = y$, w cannot be the identity, for that would entail that $w * u = u$ for all u, in particular when $u = w$. Similarly, we may infer from $x*x = w$, i.e. from $x*x \neq x$, that x is not the identity. Finally, from $w * z = x$ we may infer that z is not the identity, as that would entail that $w * z = w$. Thus, if there is an identity, that identity must be y. We may thus enter the appropriate elements into both the row and column labelled y; also, as $*$ is to be commutative, we may enter the values of $x * w$, $z * w$ by reflecting the table in the main diagonal. The result is

$*$	w	x	y	z
w	y	z	w	x
x	z	w	x	
y	w	x	y	z
z	x		z	w

   This leaves the products $z * x$ amd $x * z$ un determined, although we know they are equal, since $*$ is commutative.

   We haven't yet used the fact that every element must have an inverse. This says that every column and every row must contain the identity, y. That is the element presently missing from, for example, the second column. This permits us to

complete the table:

$*$	w	x	y	z
w	y	z	w	x
x	z	w	x	y
y	w	x	y	z
z	x	y	z	w

4. (a) [8, Problem 5.17] Verify that the set of all invertible (non-singular) 2×2 matrices with real numbers as entries forms a group with respect to matrix multiplication.

   (b) Explain why each of the following is not a group:

      i. (invertible [non-singular] 2×3 real matrices, matrix multiplication)

      ii. (invertible [non-singular] real square matrices, matrix multiplication)

Solution:

(a) Denote the set of invertible non-singular 2×2 real matrices by $M(2, \mathbb{R})$.

- Matrix multiplication is defined for all ordered pairs of 2×2 matrices, in particular, for all ordered pairs of *invertible* matrices. To show that this multiplication constitutes an *operation* on $M(2, \mathbb{R})$, we must prove that the image of the mapping is in the set $M(2, \mathbb{R})$, i.e. that the product is invertible. We know that a matrix is invertible iff its determinant is non-zero; also that the determinant of a product is the product of the determinants. Hence, for any two matrices $A, B \in M(2, \mathbb{R})$, $\det AB = \det A \cdot \det B$ which is the product of two non-zero determinants, hence also non-zero. Thus AB is also invertible.
- **Associativity.** The associativity of matrix multiplication is usually proved in linear algebra courses, either directly, or by passing to the linear transformations represented by the matrices. Following is a direct proof:

$$
\begin{aligned}
& \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \left[\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \right] \\
= & \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11}c_{11} + b_{12}c_{21} & b_{11}c_{12} + b_{12}c_{22} \\ b_{21}c_{11} + b_{22}c_{21} & b_{21}c_{12} + b_{22}c_{22} \end{pmatrix} \\
= & \begin{pmatrix} a_{11}(b_{11}c_{11} + b_{12}c_{21}) + a_{12}(b_{21}c_{11} + b_{22}c_{21}) & a_{11}(b_{11}c_{12} + b_{12}c_{22}) + a_{12}(b_{21}c_{12} + b_{22}c_{22}) \\ a_{21}(b_{11}c_{11} + b_{12}c_{21}) + a_{22}(b_{21}c_{11} + b_{22}c_{21}) & a_{21}(b_{11}c_{12} + b_{12}c_{22}) + a_{22}(b_{21}c_{12} + b_{22}c_{22}) \end{pmatrix} \\
= & \begin{pmatrix} (a_{11}b_{11} + a_{12}b_{21})c_{11} + (a_{11}b_{12} + a_{12}b_{22})c_{21} & (a_{11}b_{11} + a_{12}b_{21})c_{12} + (a_{11}b_{12} + a_{12}b_{22})c_{22} \\ (a_{21}b_{11} + a_{22}b_{21})c_{11} + (a_{21}b_{12} + a_{22}b_{22})c_{21} & (a_{21}b_{11} + a_{22}b_{21})c_{12} + (a_{21}b_{12} + a_{22}b_{22})c_{22} \end{pmatrix} \\
= & \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}
\end{aligned}
$$

$$= \left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right] \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

- **Existence of identity element.** The matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has the property that, $\forall A \in M(2,\mathbb{R})$, $AI = IA = A$. This matrix I is evidently in $M(2,\mathbb{R})$, since it is invertible — it is its own inverse.
- **Existence of inverse elements.** We are confining our attention to those 2×2 matrices that are invertible. What then is there to prove? Only that the inverses whose existence we assume are also in the set $M(2,\mathbb{R})$, i.e. that the inverse of an invertible matrix A is also invertible. But since $AA^{-1} = A^{-1}A = I$, it follows that $A^{-1}A = AA^{-1} = I$, which asserts that A acts as the inverse of A^{-1}, i.e. that $(A^{-1})^{-1} = A$.

(b) i. This set is empty! A non-square matrix is never invertible. But an empty set can never be endowed with a group structure: a group must always contain an identity element.

ii. This set is not empty. However, matrix multiplication is not defined between all ordered pairs of elements: for example, the product $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ is not defined.

5. [8, Problems 5.20, 5.21] Showing all your work, determine the Cayley tables for a group $(\{e,a\},*)$ and for a group $(\{e,a,b\},*)$, where, in each case, e is the identity element; $e \neq a$, $e \neq b$, $a \neq b$.

Solution:

Group $(\{e,a\},*)$. Since e is the identity element, the row and column headed by e are completely determined, as

$*$	e	a
e	e	a
a	a	

. It remains to determine $a * a$. Could it happen that $a * a = a$? If that were the case, then

$$a = e * a = (a^{-1} * a) * a = a^{-1} * (a * a) = a^{-1} * a = e$$

which contradicts the hypothesis that $a \neq e$; hence the only admissible table is

$*$	e	a
e	e	a
a	a	e

(Actually, this proof is still incomplete. We have proved that, if there exists a group with 2 elements, then this is its Cayley table. We really should prove explicitly that all the group axioms hold.)

Group $(\{e, a, b\}, *)$**.** As in the preceding, the designation of the identity element leads to a partial table

$*$	e	a	b
e	e	a	b
a	a		
b	b		

. The reasoning in the preceding part also shows that $a * a \neq a$; and, analogously, $b * b \neq b$.

There cannot be any repetitions in any row of the Cayley table. If, for example, $a * a = a * b$, then multiplication on the left by a^{-1} would yield that $a = b$; an analogous argument holds for columns. Let us consider two cases:

$\underline{a * a = e}$ The table becomes

$*$	e	a	b
e	e	a	b
a	a	e	
b	b		

. But then the last entry of the second row must be $a * b = b$, since only b has not yet appeared in that row: but this causes a repetition in the last column. This case is impossible.

$\underline{a * a = b}$

$*$	e	a	b
e	e	a	b
a	a	b	
b	b		

. The last entry in the second row is $a * b = e$, the only remaining element available for that row. Then the remaining elements in the second and third columns can be determined by elimination to be $b * a = e$, $b * b = a$, so the table is

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Again, these proofs show only that, if there is a group with 3 elements, this is the only possible Cayley table; we should now show that all axioms are satisfied. That is somewhat tedious. We will see in [8, Theorem 7.2] that there does indeed exist a group having 3 elements; what we have shown above is that there can exist *at most one* such type of group.

6. [8, Problem 3.23(c)] (This problem was inadvertently omitted from the assignment. Try to solve it from the hint before you look at the solution.) Prove that if u and v identity elements for a binary operation $\diamondsuit : S \times S \to S$, then $u = v$. (Hint: The fact that u is an identity element gives rise to $2|S| - 1$ equations; similarly the fact the v is an identity element. Select two appropriate equations to prove that $u = v$. You may also wish to attempt the other parts of the cited problem in preparation for the present problem.)

Solution: Since u is a *"left"* identity, $u \diamondsuit v = v$; since v is a *"right"* identity, $u \diamondsuit v = u$. From these two equations, having a common member, it follows that $u = v$.

B.2 Second 1997 Problem Assignment

1. [8, Problem 6.5]

   (a) Write all of the elements of S_4 both in two-row form and using (disjoint) cyclic notation.

   (b) Determine which elements of S_4 are their own inverse.

   Solution:

   (a) We will list the permutations in lexicographic order of the second row of the two-row notation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1342)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (23) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (234) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (134)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (243) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (142)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (143)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (14)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1243) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1423)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

(b) For an element to be its own inverse, the inverse of each of its cycles must be a cycle in the disjoint cycle decomposition. Cycles of length 1 are, of course, their own inverse; so are cycles of length 2. A cycle of length 3 or 4 is not its own inverse; as none of the permutations can have more than one cycle of length more than 2, no permutation in S_4 which is its own inverse will have such a cycle as a factor. The the permutations which are their own inverse are those with any of the following cycle types:

$$\begin{aligned} (\bullet)(\bullet)(\bullet)(\bullet) &: \{(1)(2)(3)(4)\} = \{(1)\} = \{e\} \\ (\bullet\bullet)(\bullet)(\bullet) = (\bullet\bullet) &: \{(12), (13), (14), (23), (24), (34)\} \\ (\bullet\bullet)(\bullet\bullet) &: \{(12)(34), (13)(24), (14)(23)\} \end{aligned}$$

2. [8, Problem 6.13] Let A denote the set of all mappings $\alpha_{a,b} : \mathbb{R} \to \mathbb{R}$ defined by $x \overset{\alpha_{a,b}}{\longmapsto} ax + b$, where $a, b \in \mathbb{R}$ and $a \neq 0$. With composition of mappings as the operation, this set of *affine mappings of the real line* is a group. Prove that this group is non-Abelian.

   Solution: It suffices to exhibit two elements $\alpha_{a,b}$ and $\alpha_{c,d}$ of A which do not commute, i.e. such that $\alpha_{a,b} \circ \alpha_{c,d} \neq \alpha_{c,d} \circ \alpha_{a,b}$. The two compositions are both bijections of $\mathbb{R}$ with itself, so they have the same domain and the same codomain. To show they are not the same mapping we have to produce one point $x_0 \in \mathbb{R}$ where they act differently, i.e. such that

   $$(\alpha_{a,b} \circ \alpha_{c,d})(x_0) \neq (\alpha_{c,d} \circ \alpha_{a,b})(x_0). \tag{1013}$$

   There is no need to work in this generality: all we need is *one* set of values for (a, b, c, d, x_0) where the inequality in (1013) holds. For example, taking $(a, b, c, d) = (2, 0, 1, 1)$, we have $\alpha_{2,0}(\alpha_{1,1}(x_0)) = 2(x_0 + 1)$, but $\alpha_{1,1}(\alpha_{2,0}(x_0)) = 2x_0 + 1$, and these values are different for *any* value of x_0; for example, for $x_0 = 0$.

   To summarize, a group is abelian if every pair of elements commute. It is non-abelian if that fails: if there is one pair of elements that do not commute. Here the elements are functions, and the commuting of two of them requires an equation between the actions of compositions at all points in $\mathbb{R}$. To show the failure of such an equation it suffices to find one point in $\mathbb{R}$ where the compositions differ in action.

3. [8, Problem 7.8] Determine all the elements of A_4, and list them in both the two-row form and disjoint cycle notation.

   Solution: As observed in [8, p. 45], a cycle of odd length is even, and a cycle of even length is odd; the product of even cycles is even, of even and odd cycles is

odd, and of two odd cycles is even. Thus, looking at the various possible cycle decompositions in S_4 we have the following:

$$\begin{aligned}(\bullet)(\bullet)(\bullet)(\bullet) &= \text{even}\\ (\bullet\bullet)(\bullet)(\bullet) &= \text{odd}\\ (\bullet\bullet)(\bullet\bullet) &= \text{even}\\ (\bullet\,\bullet\,\bullet)(\bullet) &= \text{even}\\ (\bullet\,\bullet\,\bullet\bullet) &= \text{odd}\end{aligned}$$

We extract from the list determined above in Problem 1 the even permutations in S_4:

$$\begin{array}{lll}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = e & & \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = (132)\\ \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix} = (234) & & \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix} = (134)\\ \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix} = (243) & & \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = (13)(24)\\ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = (12)(34) & & \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix} = (142)\\ \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = (123) & & \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} = (143)\\ \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix} = (124) & & \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = (14)(23)\end{array}$$

4. The hexagon graph is an undirected graph

$$G = (\{1,2,3,4,5,6\}, \{12, 23, 34, 45, 56, 61\});$$

it can also be represented as the regular hexagon whose vertices in the plane are at the points with coordinates $\left(\cos n\frac{\pi}{3}, \sin n\frac{\pi}{3}\right)$ $(n = 0, 1, 2, 3, 4, 5)$.

   (a) Show that if α and β are isomorphisms of the graph G with itself — i.e. bijections of $V(G)$ with itself which map adjacent vertices on to adjacent vertices, and non-adjacent vertices on to non-adjacent vertices — then α^{-1} and $\alpha \circ \beta$ are also isomorpmisms.

   (b) Show that, for every element $i \in V(G)$, there are exactly two isomorphisms which map 1 on to i: one mapping 2 on to $i + 1$, and the other mapping 2 on to $i - 1$ (labels taken modulo 6).

   (c) Show that the isomorphisms of G form a subgroup of $S_{\{1,2,3,4,5,6\}}$.

(d) Determine the subgroups $G_{\{1,4\}}$ and $G_{(\{1,4\})}$.

Solution:

(a) An isomorphism of G with itself is a bijection $\alpha : V(G) \to V(G)$ such that $\alpha(x)\,\alpha(y)$ is an edge of G iff xy is an edge of G.

i. If α is an isomorphism, then, it being a bijection, α^{-1} exists and is itself a bijection. Suppose that $xy \in E(G)$, i.e. $\alpha(\alpha^{-1}(x))\,\alpha(\alpha^{-1}(y)) \in E(G)$. Then, since α is an isomorphism, $\alpha^{-1}(x)\,\alpha^{-1}(y) \in E(G)$; an analogous argument holds if we replace both $\in$ by $\notin$. Thus α^{-1} is also an isomorphism.

ii. Suppose that α and β are both isomorphisms of G. The composition of two bijections is a bijection; indeed, we know that their composition $\alpha \circ \beta$ has inverse $\beta^{-1} \circ \alpha^{-1}$. It remains to show that the composition has the appropriate action on adjacent and non-adjacent vertices.
Suppose that $xy \in E(G)$. Then, since β is an isomorphism, $\beta(x)\,\beta(y) \in E(G)$. And, since α is an isomorphism, $\alpha(\beta(x))\,\alpha(\beta(y)) \in E(G)$, i.e. $(\alpha \circ \beta)(x)\,(\alpha \circ \beta)(y) \in E(G)$; an analogous result holds with $\in$ replaced by $\notin$. We have shown that $\alpha \circ \beta$ is an isomorphism.

(b) If 1 is mapped on to i, its neighbours must be mapped on to neighbours of i: i.e. on to either $i+1$ or on to $i-1$. Once the action of 2 is determined, *its* neighbours must map on to neighbours of the image of 2; but there is only one such point available, as the other is the image of 1. Thus we can prove — by induction — that the action on 2 determines the action of the mapping completely. In the case where 2 maps on to $i+1$ the mapping is a rotation: $j \mapsto j+i-1$. In the case where 2 maps on to $i-1$ there are two possible subcases. When $i = 1$, the mapping is a reflection which fixes 1 and 4: (26)(35); similarly, when $i = 3$, the mapping is (13)(46); and, when $i = 5$, (15)(24); when $i = 2, 4, 6$, the mapping is a reflection that has no fixed vertices: one of (12)(36)(45), (23)(14)(56), (16)(25)(34). Since we proved above that there are at most 2 mappings of each type, it suffices to verify that the mappings we have listed here have the properties claimed.

(c) By [8, Theorem 7.1] it suffices to prove that the set of isomorphisms is nonempty, closed under composition, and closed under the taking of inverses. The two closures were proved above. That the set is not empty is obvious: the identity mapping is an isomorphism.

(d) i. $G_{\{1,4\}}$ is the group of isomorphisms which map 1 on to 1 and 4 on to 4. We have seen above that there are just two isomorphisms that fix 1: the identity, and (26)(35). This group has just these two elements.

ii. $G_{(\{1,4\})}$ is the group of isomorphisms that fix the set $\{1,4\}$. It is made up of the 2 isomorphisms in $G_{\{1,4\}}$ and also the isomorphisms that map 1 on to 4; these must necessarily map 4 on to 1, since the image of 4 must be the element of the set $\{1,4\}$ which is not 1. As seen above, when 1 is mapped to 4 there are two possible completions: (14)(25)(36), and (14)(23)(56). The group consists of all four of these elements.

5. [8, Problem 9.6] For points (x_1, y_1) and (x_2, y_2) in the plane $\mathbb{R}^2$, let $(x_1, y_1) \sim (x_2, y_2)$ mean that either $x_1 = x_2$ or $y_1 = y_2$ or both. Explain why $\sim$ is *not* an equivalence relation.

   Solution: This relation is reflexive and symmetric, but it is not transitive. For example, $(1,2) \sim (1,3)$ and $(1,3) \sim (2,3)$. But $(1,2) \nsim (2,3)$.

6. (a) [8, Problem 11.13] Prove or disprove that $\mathbb{Z}_3^{\#}$ is a group with respect to $\odot$.

   (b) [8, Problem 11.14] Prove or disprove that $\mathbb{Z}_4^{\#}$ is a group with respect to $\odot$.

   Solution:

   (a) $\mathbb{Z}_3^{\#} = \{[1],[2]\}$. Since $[2] \odot [2] = [4] = [1]$, the action of composition $\odot$ is given by the table:

$\odot$	[1]	[2]
[1]	[1]	[2]
[2]	[2]	[1]

   .

   This is the Cayley table of the smallest non-trivial group; its structure is the same as that of $(\mathbb{Z}_2, +)$, or of S_2. More rigorously, we know from [8, Lemma 11.3] that $\odot$ is associative and commutative, and has [1] as an identity. The only group property remaining to be proved is that every element has an inverse. But we see from the table that an inverse of [1] is [1], and an inverse of [2] is [2], so this must be a group.

   (b) The set $\{[1],[2],[3]\}$ is not closed under the given operation, for $[2] \odot [2] = [4] = [0]$, which is not in the set.

7. [8, Problem 12.13] Prove carefully that, if c is a positive integer, $(ac, bc) = (a, b)c$.

   Solution: Since (a, b) is a common divisor of a and b, there exist integers u and v such that $a = u(a, b)$, $b = v(a, b)$. Hence, multiplying by c, $ac = u \cdot ((a, b)c)$, $bc = v \cdot ((a, b)c)$. Thus

   $$(a, b)c \quad \text{is a common divisor of } ac \text{ and } bc. \tag{1014}$$

   Now suppose that d is any common divisor of ac and bc, i.e. that there exist integers r and s such that $ac = rd$, $bc = sd$. By [8, Theorem 12.2] there exist integers m

and n such that $(a,b) = am + bn$, hence

$$\begin{aligned}(a,b)c &= m(ac) + n(bc)\\ &= (mr + ns)d\end{aligned}$$

so $d|(a,b)c$. This fact, combined with (1014), shows that $(a,b)c = (ac,bc)$ in the sense of the definition contained in [8, Theorem 12.1].

8. For each integer $n > 1$, let

$$\phi(n) = |\{m \in \mathbb{N} | (1 \leq m < n) \wedge ((m,n) = 1)\}| \ .$$

Define $\phi(1) = 1$.

(a) (cf. [8, Problem 12.10(a)]) Determine $\phi(k)$ for $1 \leq k \leq 12$.
(Note that it is often simpler to modify the definition to the following equivalent form:

$$\phi(n) = |\{m \in \mathbb{N} | (1 \leq m \leq n) \wedge ((m,n) = 1)\}| \ .)$$

The point n which is added to the interval is deleted, since $(n,n) = n \neq 1$ for $n > 1$. This modified definition has the added advantage that it agrees with the previously defined value of $\phi(1)$.

(b) [8, Problem 12.10(b)] Determine the value of $\phi(p)$ when p is a prime.

(c) [8, Problem 13.13] For any prime p and any non-negative integer k, determine the value of $\phi\left(p^k\right)$.

Show all your work.

Solution:

(a) **1:** By definition, $\phi(1) = 1$.
2,3,5,7,11: A prime p has no positive divisors except 1 and itself; hence $\phi(p) = p - 1$.
4,9: The square of a prime, p^2, has, as its only positive divisors, 1, p, p^2; any integer n in the interval $1 \leq n < p^2$ which is not prime to n must be divisible by p, i.e. one of p, $2p$, $3p$, ... $(p-1)p$; hence $\phi(p^2) = (p^2 - 1) - (p - 1) = p^2 - p$.
6: 2, 3, 4 are not prime to 6; hence $\phi(6) = (6 - 1) - 3 = 2$.
8: $\phi(2^3)$ will be the number of integers between 1 and 7 inclusive which do not share a factor with 2^3, i.e. which are not even; hence $\phi(8) = 4$.

10: From the integers in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ we must delete the even integers and the multiples of 5, since only these can share a factor greater than 1 with $2 \cdot 5$. The set of survivors is $\{1, 3, 7, 9\}$, so $\phi(10) = 4$.

(b) This was proved above, in the discussion for 2, 3, 5, 7, 11.

(c) Any integer not relatively prime to p^k will be divisible by a power of p, hence by p itself. Conversely, any integer n divisible by p is such that $\left(n, p^k\right) = \left(\frac{n}{p}, p^{k-1}\right) \cdot p$, so it is not relatively prime to p^k. The multiples of p in the set $\left\{1, 2, ..., p^k - 2, p^k - 1, p^k\right\}$ are precisely 1, p, $2p$, ..., p^2, $p^2 + p$, ..., $p^k - p$, p^k; they are equally spaced along the real line, p units apart, starting with p. Their number is, therefore, $\frac{p^k}{p}$. Of these, p^k itself is not less than p^k; but, instead of counting the positive integers less than and prime to p^k we can count the integers *no greater than* and prime to p^k. Their number will be $p^k - \frac{p^k}{p} = p^{k-1}(p-1)$.

B.3 Third 1997 Problem Assignment

1. (a) Prove that, for any element g of a group G with identity e, g^{-1} is the only element h with the property that $gh = e$; and, similarly, it is the only element k with the property that $kg = e$.

   (b) Conclude from the preceding that, for every $a \in G$, $(a^{-1})^{-1} = a$.

   (c) Use associativity and the uniqueness of inverses in a group G to show that $\forall a, b \in G[(ab)^{-1} = b^{-1}a^{-1}]$.

   (d) [8, Problem 14.25] Prove that a group G is Abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

   (e) [8, Problem 14.29] Prove that a group G is Abelian if each of its non-identity elements has order 2.

   (f) Prove that a group G can be Abelian even though some of its non-identity elements do not have order 2.

   Solution:

   (a)

$$\begin{aligned} gh = e &\Leftrightarrow g^{-1}(gh) = g^{-1}e \\ &\Leftrightarrow \left(g^{-1}g\right)h = g^{-1}e \quad \text{by associativity} \\ &\Leftrightarrow eh = g^{-1}e \quad \text{property of inverse} \\ &\Leftrightarrow h = g^{-1} \quad \text{properties of identity} \end{aligned}$$

$$\begin{aligned} kg = e &\Leftrightarrow (kg)g^{-1} = eg^{-1} \\ &\Leftrightarrow k\left(gg^{-1}\right) = eg^{-1} \quad \text{by associativity} \\ &\Leftrightarrow ke = eg^{-1} \quad \text{property of inverse} \\ &\Leftrightarrow k = g^{-1} \quad \text{properties of identity} \end{aligned}$$

(b) The inverse of a has, (together with the property that $a^{-1}a = e$), the property that $aa^{-1} = e$. It follows, taking in (1a) $a^{-1} = g$ and $k = a$, that $k = (a^{-1})^{-1}$.

(c)

$$\begin{aligned} ab\left(b^{-1}a^{-1}\right) &= a\left(bb^{-1}\right)a^{-1} \\ &= aea^{-1} \\ &= aa^{-1} \\ &= e \end{aligned}$$

Hence, by (1a) with $h := b^{-1}a^{-1}$ and $g := ab$, $(ab)^{-1} = b^{-1}a^{-1}$.

(d) i. Suppose that G is Abelian. Then

$$\begin{aligned} (ab)^{-1} &= b^{-1}a^{-1} \quad \text{by (1c)} \\ &= a^{-1}b^{-1} \quad \text{by hypothesized commutativity.} \end{aligned}$$

ii. Suppose that, for all a, b, $(ab)^{-1} = a^{-1}b^{-1}$. Then

$$\begin{aligned} ab &= \left((ab)^{-1}\right)^{-1} \\ &= \left(a^{-1}b^{-1}\right)^{-1} \quad \text{by hypothesis} \\ &= \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} \quad \text{by (1c)} \\ &= ba \quad \text{by (1b), twice.} \end{aligned}$$

(e) If an element a has order 2, then $aa = e$, from which it follows, by (1c), that $a^{-1} = a$; of course, e has the same properties: $ee = e$, $e^{-1} = e$. Let a and b be any elements of G. Then

$$\begin{aligned} ab &= (ab)^{-1} \quad \text{by hypothesis} \\ &= b^{-1}a^{-1} \quad \text{by (1c)} \\ &= ba \quad \text{just proved} \end{aligned}$$

so G is Abelian. Alternatively

$$\begin{aligned} ab &= b^2aba^2 \quad \text{since } b^2 = e = a^2 \\ &= b(ab)(ab)a \quad \text{by associativity} \\ &= bea \quad \text{since } (ab)^2 = e \\ &= ba \end{aligned}$$

(f) There exist Abelian groups with elements of orders distinct from 2. For example, the cyclic subgroup of S_3 generated by (123) is Abelian — as are all cyclic groups, but its elements have orders 3 (for (123) and (132)) and 1 (for the identity).

2. [8, Problem 14.38] Prove that if $(A, *, e)$ and $(B, *, e)$ are subgroups of a group[1001] $(G, *, e)$, and $(A \cup B, *, e)$ is also a subgroup, then $A \subseteq B$ or $A \supseteq B$. (Compare [8, Problem 7.13] and [8, Theorem 15.1].) [Hint: First show that

$$\neg((A \subseteq B) \vee (A \supseteq B)) \Rightarrow ((\exists a \in A \cap \overline{B}) \wedge (\exists b \in B \cap \overline{A}))$$

Then investigate whether $a * b \in A$ or $a * b \in B$.]

Solution:

$$\begin{array}{rl} & \neg((A \subseteq B) \vee (A \supseteq B)) \\ \Leftrightarrow & (\neg(A \subseteq B)) \wedge (\neg(A \supseteq B)) \quad \text{de Morgan laws} \\ \Leftrightarrow & (\exists a((a \in A) \wedge (a \notin B))) \wedge (\exists b((b \in B) \wedge (b \notin A))) \end{array}$$

Since $a \in A \subseteq A \cup B$ and $b \in B \subseteq A \cup B$, a and b are elements of the subgroup $A \cup B$; hence $a * b$ is also an element of $A \cup B$. That implies that either (a) $a * b \in A$ or (b) $a * b \in B$.

(a) $\underline{a * b \in A.}$ Since the subgroup A is closed under the taking of inverses, $a \in A \Rightarrow a^{-1} \in A$. Since A is closed under products,

$$\begin{array}{rcl} (a^{-1} \in A) \wedge (a * b \in A) & \Rightarrow & a^{-1} * (a * b) \in A \\ & \Rightarrow & (a^{-1} * a) * b \in A \\ & \Rightarrow & e * b \in A \\ & \Rightarrow & b \in A \end{array}$$

contrary to hypothesis.

(b) $\underline{a * b \in B.}$ This case may be eliminated analogously to the preceding case.

From this contradiction we may conclude that there cannot exist a and b with the desired properties. That is, the disjunction $(A \subseteq B) \vee (A \supseteq B)$ must hold.

[1001] Note that we are using a more detailed notation than usual for the group G; namely, we are specifying explicitly what is the group operation; and, what is the identity element. This additional information is useful in writing out the proof. However, it is of no use in the description of the 3 subgroups. By [8, Theorem 7.1] a subgroup must have the same identity element as the supergroup.

3. [8, Problem 15.12] Construct a Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_3$. Show that the group is cyclic *by exhibiting a generator*. For ease of writing, represent an element $([m]_2, [n]_3)$ simply by (m, n): we add the first coordinates modulo 2, and the second coordinates modulo 3.

   Solution:

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

   There are two elements which generate this group: $(1,1)$, and its (additive) inverse, $(1,2)$. For

$$\begin{aligned}
(1,1) &= (1,1) \\
(1,1)+(1,1) &= (0,2) \\
(1,1)+(1,1)+(1,1) &= (1,1)+(0,2) = (1,0) \\
(1,1)+(1,1)+(1,1)+(1,1) &= (1,1)+(1,0) = (0,1) \\
(1,1)+(1,1)+(1,1)+(1,1)+(1,1) &= (1,1)+(0,1) = (1,2) \\
(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1) &= (1,1)+(1,2) = (0,0)
\end{aligned}$$

   so we have succeeded in expressing each of the elements of the group as a "power"[1002] of the generator.

4. (cf. [8, Problem 16.14])

   (a) [8, Problem 16.6] Determine the right cosets of $\langle(13)\rangle$ in S_3.

   (b) Determine the left cosets of $\langle(13)\rangle$ in S_3.

   (c) Determine all sets which are both left cosets and right cosets of $\langle(13)\rangle$ in S_3, i.e. the intersection of the families of left and right cosets.

   Solution:

   (a)

$$\begin{aligned}
\langle(13)\rangle e &= \{e,(13)\}e = \{e,(13)\} \\
\langle(13)\rangle(13) &= \{e,(13)\}(13) = \{(13),e\}
\end{aligned}$$

[1002]Here the group is being written additively, so a power is an iterated sum

$$\begin{aligned}
\langle(13)\rangle(12) &= \{e,(13)\}(12) = \{(12),(123)\} \\
\langle(13)\rangle(23) &= \{e,(13)\}(23) = \{(23),(132)\} \\
\langle(13)\rangle(123) &= \{e,(13)\}(123) = \{(123),(12)\} \\
\langle(13)\rangle(132) &= \{e,(13)\}(132) = \{(132),(23)\}
\end{aligned}$$

We see that there are three distinct cosets:

$$\begin{aligned}
\langle(13)\rangle e &= \langle(13)\rangle(13) = \{e,(13)\} \\
\langle(13)\rangle(12) &= \langle(13)\rangle(123) = \{(12),(123)\} \\
\langle(13)\rangle(23) &= \langle(13)\rangle(132) = \{(23),(132)\}
\end{aligned}$$

(b) Proceeding analogously to the preceding part, we may show that there are three distinct cosets:

$$\begin{aligned}
e\langle(13)\rangle &= (13)\langle(13)\rangle = \{e,(13)\} \\
(12)\langle(13)\rangle &= (132)\langle(13)\rangle = \{(12),(132)\} \\
(23)\langle(13)\rangle &= (123)\langle(13)\rangle = \{(23),(123)\}
\end{aligned}$$

(c) The left and right cosets consist together of five distinct sets. Only one set appears as both a left and a right coset — the set $\langle(13)\rangle = \{e,(13)\}$.

5. (a) [8, Problem 17.25] Prove that, if H is a subgroup of index 2 in G, then

$$(a \notin H) \wedge (b \notin H) \Rightarrow ab \in H$$

Conclude, in particular, that if $a \in G$, $a^2 \in H$.

(b) (cf. [8, Problem 17.28]) The subgroup $G = \langle(123),(12)(34)\rangle$ of S_4 has order 12. Show that G is precisely A_4. Then show that no subgroup H of G has order 6. [Hint: Apply (5a) twice to elements like (123), considering $[(123)^2]^2$.]

Solution:

(a) We are assuming that $[G : H] = 2$; that is, that G may be expressed as the union of the subgroup H and of one coset of H that is disjoint from H. (There is no need to distinguish between left and right cosets here, since the only coset which is not H itself is the complement of the set H in G: it is both a left and a right coset.) If $a \notin H$, then $G = H \cup Ha$ is a right coset decomposition. All elements of G which are not in H must be in the coset Ha.

Suppose that $b^{-1} \in H$; then, by closure of H under inverses, $b \in H$, a contradiction; we conclude that $b^{-1} \in Ha$; hence $\exists h \in H[b^{-1} = ha]$, so $b = a^{-1}h^{-1}$. But then $ab = aa^{-1}h^{-1} = h^{-1} \in H$. $\square$

(b)

$$\begin{aligned}(123)\cdot(12)(34)\cdot(123)^2 &= (14)(23)\\ (123)^2\cdot(12)(34)\cdot(123) &= (13)(24)\end{aligned}$$

Thus all elements of S_4 of the form $(\bullet\bullet)(\bullet\bullet)$ are in G.

$$\begin{aligned}(12)(34)\cdot(123)\cdot(12)(34) &= (142)\\ (12)(34)\cdot(132)\cdot(12)(34) &= (124)\\ (13)(24)\cdot(123)\cdot(13)(24) &= (134)\\ (13)(24)\cdot(132)\cdot(13)(24) &= (143)\\ (14)(23)\cdot(123)\cdot(14)(23) &= (243)\\ (14)(23)\cdot(132)\cdot(14)(23) &= (234)\end{aligned}$$

and also (123) and $(123)^2 = (132)$ are in G. Thus G contains all 8 3-cycles.

The two generators given are both even permutations. All products of them will, therefore, also be even. We have shown that the above 11 permutations are in G. And, of course, e is also expressible in terms of these generators, so it also is in G. Thus G contains all $\frac{4!}{2}$ even permutations in S_4; it must, therefore, be A_4 [8, Theorem 7.2].

Suppose that there existed a subgroup H of G of order 6. Each of the $(3-1)!\times\binom{4}{3} = 8$ elements of the form $(\bullet\bullet\bullet)$ is equal to its 4th power, since its cube is the identity. By (5a) each of these 8 elements is in H; but H was to have exactly 6 elements. From this contradiction we conclude that H does not exist.

6. [8, Problem 18.12] Verify that the group[1003] $(\mathbb{Z}_4, \oplus, [0])$ is isomorphic to $(\mathbb{Z}_5^{\#}, \odot, [1]) = (\mathbb{Z}_5 - \{[0]\}, \odot, [1])$, whose structure is given by [8, Table 11.2, Example 11.4]:

$\odot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

[1003]Note the notation we are using: the first argument, here $\mathbb{Z}_4$, is the underlying set. The second argument is the binary group operation. The last argument is the identity element. Where it is clear from the context, the identity element is not specifically named. Where the group operation is clear from the context, the group may be represented by giving only the set.

Solution: We can rewrite the Cayley table given above with the common order of rows and columns changed, as follows:

$\odot$	$[1]$	$[2]$	$[4]$	$[3]$
$[1]$	$[1]$	$[2]$	$[4]$	$[3]$
$[2]$	$[2]$	$[4]$	$[3]$	$[1]$
$[4]$	$[4]$	$[3]$	$[1]$	$[2]$
$[3]$	$[3]$	$[1]$	$[2]$	$[4]$

Evidently this group is isomorphic to the additive group $\mathbb{Z}_4$. whose Cayley table is

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

under the bijection $[1]_5 \mapsto [0]_4$, $[2]_5 \mapsto [1]_4$, $[3]_5 \mapsto [3]_4$, $[4]_3 \mapsto [2]_4$. It is easy to see that $[2]_5$ *generates* the multiplicative group $(\mathbb{Z}_5^{\#}, \odot, [1]) = (\mathbb{Z}_5 - \{[0]\}, \odot, [1])$.

7. [8, Problem 19:15] If p is a prime, then there are five isomorphism classes of Abelian groups of order p^4. Describe one group from each class, and explain carefully why groups from the various isomorphism classes are not isomorphic. (Compare [8, Example 19.1].)

   Solution: By the Fundamental Theorem of Finite Abelian Groups, any Abelian group of order p^4 is the direct product of cyclic groups of prime power order. We list the various factorizations of p^4 into prime power factors, and an Abelian group for which that is the order:

$$\begin{aligned} p^4 &: \mathbb{Z}_{p^4} \\ p^3 \cdot p^1 &: \mathbb{Z}_{p^3} \times \mathbb{Z}_p \\ p^2 \cdot p^2 &: \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \\ p^2 \cdot p^1 \cdot p^1 &: \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \\ p^1 \cdot p^1 \cdot p^1 \cdot p^1 &: \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \end{aligned}$$

   The first group shown contains an element of order p^4; none of the others has elements of order exceeding p^3, so the first group is not isomorphic to any of the others. The second group has no element of order p^4, but does have elements of order p^3; none of the third, fourth, fifth groups have elements of order p^3, so the second group is not isomorphic to any of the others. The third and fourth groups

have elements of order p^2, but the fifth group dies not; thus the fifth group is not isomorphic to any of the other groups.

To distinguish between $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$ is more difficult. One way to do so is to count the elements of order p. In $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$ an element $([a]_p, [b]_p, [c]_p)$ has order p iff it is distinct from the identity, and if $p|a$: there are $p^3 - 1$ such non-identity elements. In $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ there are only $p^2 - 1$ elements of order p. $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$ thus has $p^4 - p^3$ elements of order p^2; $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ has $p^4 - p^2$ elements of order p^2.

8. (cf. [8, Problem 19.26]) For any group G, define a unary operation $\theta : G \to G$ by $\theta(a) = a^{-1}$. Prove that G is abelian iff θ is an isomorphism[1004].

   Solution: Since, for any $g \in G$, $g = (g^{-1})^{-1} = \theta(g^{-1})$, in the image of θ, θ is surjective. Since $\theta(a) = \theta(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow b = a$, θ is injective; hence θ is a bijection.

   (a) Suppose that θ is an isomorphism. Then, for all $a, b \in G$,

$$\begin{aligned} ab &= \theta\left(a^{-1}\right)\theta\left(b^{-1}\right) \\ &= \theta\left(a^{-1}b^{-1}\right) \quad \text{since } \theta \text{ is an isomorphism} \\ &= \left(a^{-1}b^{-1}\right)^{-1} \quad \text{by definition of } \theta \\ &= ba \quad \text{by (1a), (1c)} \end{aligned}$$

   (b) Suppose that G is abelian. Then, for all $a, b \in G$,

$$\begin{aligned} \theta(ab) &= \theta(ba) \quad \text{since } G \text{ is Abelian} \\ &= (ba)^{-1} \quad \text{by definition of } \theta \\ &= a^{-1}b^{-1} \quad \text{by (1c)} \\ &= \theta(a)\,\theta(b) \quad \text{by definition of } \theta \end{aligned}$$

   Hence θ is an isomorphism.

B.4 Fourth 1997 Problem Assignment

1. [8, Problem 21.16] Prove that

$$a^2 - b^2 = (a - b)(a + b) \tag{1015}$$

[1004] More precisely, an *automorphism*, i.e. an isomorphism with itself.

for all elements a, b in a ring R iff R is commutative.[1005] (You may assume, in your proof, that the "familiar" properties of $-$ have been proved; for example, that multiplication distributes over subtraction in the same way as it distributes over addition.)

Solution: This identity looks "obvious" because we are accustomed to working in the real field, which is a commutative ring. Starting from the right side, in a general ring, we have, for any $a, b \in R$,

$$\begin{aligned}(a-b)(a+b) &= (a-b)a + (a-b)b \quad \text{by left distributive law} \\ &= (aa - ba) + (ab - bb) \quad \text{by right distributive law, twice} \\ &= a^2 - ba + ab - b^2 \quad \text{by definition of 2nd power} \\ &= (a^2 - b^2) + (ab - ba) \quad \text{(by associativity, commutativity of +)}\end{aligned}$$

Thus equation (1015) holds iff $ab - ba = 0$, i.e. iff R is a commutative ring.

2. Let S denote the set of *sequences* of elements from a given commutative ring R with unity 1 distinct from 0, i.e. of objects of the form $(a_0, a_1, ..., a_r, ...)$ where $a_i \in R$ $(i = 0, 1, 2, ...)$; (recall that such a sequence may be thought of as a *function* a from the non-negative integers to R, given by $r \mapsto a_r$). Define operations of $+$ and $\circledcirc$ on S by

$$\begin{aligned}&(a_0, a_1, ..., a_r, ...) + (b_0, b_1, ..., b_r, ...) \\ = \ &(a_0 + b_0, a_1 + b_1, ..., a_r + b_r, ...); \qquad (1016)\end{aligned}$$

$$\begin{aligned}&(a_0, a_1, ..., a_r, ...) \circledcirc (b_0, b_1, ..., b_r, ...) \\ = \ &(a_0b_0, a_0b_1 + a_1b_0, ..., a_0b_r + a_1b_{r-1} + ... + a_{r-1}b_1 + a_rb_0, ...) \qquad (1017)\end{aligned}$$

The product is called the *Cauchy product* of sequences; such a product, where a sum of variables remains constant, is often called a *convolution product*. With this definitions of $+$, and with $\circledcirc$ serving as multiplication, S is a commutative ring. This ring is usually represented in terms of an "indeterminate", e.g. x, and denoted by $R[[x]]$ or $R\{x\}$; it is called the *ring of formal power series* in this indeterminate, with coefficients chosen from R. In the representation using the indeterminate x, the element $(a_0, a_1, ..., a_r, ...)$ is denoted by $\sum_{r=0}^{\infty} a_r x^r = a_0x^0 + a_1x^1 + a_2x^2 + ... + a_rx^r + ...$; we may, in practice, make obvious abbreviatons: x^0 may be replaced by 1, or omitted entirely; x^1 may be replaced by x; summands with 0 coefficients may

[1005] Remember that, in any ring — indeed, in any additive Abelian group, we define $x - y$ to mean $x + (-y)$, where $-y$ is the additive inverse of y. The symbol $-$, hitherto defined only as a unary operation, is now given a meaning as a binary operation.

be omitted entirely, etc. Then the usual operation of term-by-term addition gives the additive structure; and the usual operation induced by $(a_r x^r, b_s x^s) \mapsto a_r b_s x^{r+s}$ gives the multiplicative structure.

You are not asked to prove the foregoing. You *are* asked to prove the following properties. Where there is no danger of confusion, you may wish to represent the operation $\circledcirc$ by juxtaposition.

(a) $(1, 0, 0, ..., 0, ...) = 1x^0 = 1x^0 + 0x^1 + ... + 0x^r + ...$ is the unity of this ring.

(b) Multiplication is commutative in $R[[x]]$.

(c) $(1+(-1)x) \circledcirc (1x^0 + 1x^1 + 1x^2 + ... + 1x^r + ...) = 1x^0 + 0x^1 + 0x^2 + ... + 0x^r + ...$

(d) An element $(a_0, a_1, ..., a_r, ...)$ cannot have a multiplicative inverse unless $a_0 \neq 0$. (The converse is also true if a_0 is invertible, but you are not being asked to prove it.)[1006]

(e) $R[[x]]$ is not a field.

Solution:

(a) When we form the product

$$\left(1 + 0x + 0x^2 + ... + 0x^r + ...\right) \circledcirc \left(a_0 + a_1 x + a_2 x^2 + ... + a_r x^r + ...\right)$$

the coefficient of x^0 is $1a_0 = a_0$; the coefficient of x^r is $1a_r + 0a_{r-1} + 0a_{r-2} + ... + 0a_1 + 0a_0 = a_r$, so the product is $a_0 + a_1 x + a_2 x^2 + ... + a_r x^r + ...$; the same result holds when the order of multiplication is reversed. Thus $1 + 0x + 0x^2 + ... + 0x^r + ...$, which we normally denote simply by 1, is the multiplicative identity — i.e. the unity.

(b) It suffices to observe in definition (1017) that the sum $a_0 b_r + a_1 b_{r-1} + ... + a_{r-1} b_1 + a_r b_0$ is equal to $b_0 a_r + b_1 a_{r-1} + ... + b_{r-1} a_1 + b_r a_0$, by virtue of commutativity of addition and multiplication.

(c) The 0th term of the sequence $(1, -1, 0, 0, ..., 0, ...) \circledcirc (1, 1, 1, ..., 1, ...)$ is, by definition $1 \times 1 = 1$. By definition (1017), for $r > 0$, the rth term of the sequence is $a_0 b_r + a_1 b_{r-1} + ... + a_{r-1} b_1 + a_r b_0 = a_0 + a_1 + ... + a_r = 1 + (-1) + 0 + ... + 0 = 0$; thus the product sequence is $(1, 0, 0, ..., 0, ...)$, represented by the power series $1x^0 + 0x^1 + 0x^2 + ... + 0x^r + ...$, which we usually abbreviate to 1 — the unity of $R[[x]]$.

(d) Suppose that $(b_0, b_1, ..., b_r, ...)$ were the multiplicative inverse of $(0, a_1, ..., a_r, ...)$, i.e. that

$$(0, a_1, ..., a_r, ...) \circledcirc (b_0, b_1, ..., b_r, ...) = (1, 0, ..., 0, ...)\,.$$

[1006] Note that the invertibility condition was erroneously omitted on the question sheet.

then, computing the products on the left and equating them to the terms on the right,

$$\begin{aligned} 0a_0 &= 1 \\ 0b_1 + a_1b_0 &= 0 \\ 0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \cdots &= \cdots \end{aligned}$$

The first equation yields a contradiction, since any product in which one factor is 0, is equal to 0 [8, Theorem 21.2(a)]. It follows that there can exist no multiplicative inverse $(b_0, b_1, ..., b_r, ...)$ for an element whose 0th coefficient is 0.

(e) By the preceding part there exist more than one element having no multiplicative inverse; for example x and x^2. In a field there is a unique element — the additive identity — that has no multiplicative inverse.

3. (a) [8, Problem 22.12] A ring structure is defined on the set of real valued functions of a real variable by[1007] $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x) \cdot g(x)$ (cf. [8, Example 21.5]). Prove that this ring contains zero divisors.

(b) [8, Problem 21.10] We define addition of real-valued functions of a real variable by $(f + g)(x) = f(x) + g(x)$, and multiplication by the composition, $f \circ g$. Show that, under these definitions, the set of functions $f : \mathbb{R} \longrightarrow \mathbb{R}$ is *not* a ring.

Solution:

(a) Define $a : \mathbb{R} \to \mathbb{R}$, $b : \mathbb{R} \to \mathbb{R}$ by

$$a(x) = \begin{cases} 0 & x \neq 2 \\ 1 & x = 2 \end{cases} \qquad b(x) = \begin{cases} 0 & x \neq 1 \\ 1 & x = 1 \end{cases} .$$

Then neither a nor b is the zero function, since there exists, for each of them, a point where the function does not take the value 0. However, the product of the function values $a(x)$ and $b(x)$ is always zero, so ab is the zero function, i.e. $ab = 0$.[1008]

[1007] Do not confuse fg — the point-by-point product of functions f and g — with the composition, which we usually denote by $f \circ g$.

[1008] Note that we are using the symbol 0 here not for the zero real number, but for the zero *function*. There is no danger of confusion here, since we can tell from the context that 0 has to be a function.

(b) There is no problem with the addition operation; it is shown in [8, Example 21.5] that, endowed with this addition rule, the set of such functions becomes an Abelian group. The problem must be either in the associativity of multiplication, or in the distributivity of multiplication over addition. By [8, Theorem 4.1(a), p. 28], function composition is associative. Thus, if there is a counterexample, it will relate to distributivity. Define functions a and b as above. Then the function $b+b$ maps 1 on to $1+1=2$ and all other numbers on to 0; $a \circ (b+b)$ maps 1 on to 1 and all other numbers on to 0. but $a \circ b$ is the zero function, so $a \circ b + a \circ b$ is also the zero function; as the action of $(a \circ b) + (a \circ b)$ differs from $a \circ (b+b)$ at at least one point of their common domain, the functions cannot be equal (as functions); thus the distributive law fails.

4. (cf. [8, Problem 23.14]) Verify that $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a \in \mathbb{Q} \wedge b \in \mathbb{Q}\}$ is a subfield of the field of real numbers [8, Example 23.2]. In the course of your solution give explicit values for the additive and multiplicative identities, and for the additive and multiplicative inverses of a given non-zero element. (This construction depends on the well known fact proved in [8, Theorem 28.1], that $\sqrt{2} \notin \mathbb{Q}$. Suppose that

$$a + b\sqrt{2} = c + d\sqrt{2}\,, \tag{1018}$$

where a, b, c, d are rationals. Then, were $d \neq b$, it would follow that $\sqrt{2} = \frac{a-c}{d-b}$, a rational number; we conclude that $d = b$. But then (1018) would imply that $a = c$. It follows that all elements of $\mathbb{Q}[\sqrt{2}]$ are uniquely representable as a sum $a + b\sqrt{2}$. You are not required to prove the preceding facts in your solution.)

Solution: We can apply [8, Theorem 23.2, p. 120].

(a) The real number 0 is expressible in the form $0 + 0\sqrt{2}$, so $0 \in \mathbb{Q}[\sqrt{2}]$. (We are showing that 0 is expressible as the sum of a rational number and the product of a rational number and $\sqrt{2}$.) This is the additive identity of the subfield. Similarly, $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$; this is the multiplicative identity of the subfield.

(b) If a, b, c, d are rational numbers, then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + b) + (c+d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, so the set is closed under addition; $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, so the set is also closed under multiplication.

(c) If $a, b \in \mathbb{Q}$, then, by virtue of closure of the additive group structure of $\mathbb{Q}$ under the taking of inverses, $-a, -b \in \mathbb{Q}$. It follows that whenever $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $(-a) + (-b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, i.e. that the additive inverse, $-(a + b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$; so the set is closed under the taking of additive inverses.

(d) Let $a + b\sqrt{2}$ be a non-zero element of $\mathbb{Q}[\sqrt{2}]$. Since every element of this set is expressible in just one way in the form

$$\text{“ rational}_1 \quad + \quad \text{rational}_2\,\sqrt{2}\text{ ”}, \tag{1019}$$

the only way in which the real number 0 is expressible is as $0+0\sqrt{2}$. Thus the hypothesis that $a + b\sqrt{2}$ is non-zero is equivalent to requiring that not both a and b be zero. The multiplicative inverse is

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a-b\sqrt{2})(a+b\sqrt{2})} \\ &= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\,,\end{aligned}$$

which is of the desired form (1019). That is, the multipicative inverse of a non-zero element $a + b\sqrt{2}$ in $\mathbb{R}$ actually is a member of the set $\mathbb{Q}[\sqrt{2}]$.

Having proved the existence of 0 and 1, and the truth of the three closure properties, we may conclude that the set is, in fact, a subfield of the reals.

5. (a) [8, Problem 23.16] In [8, Example 23.1] the following tables are presented:

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\times$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

It is claimed that these tables define a field, but that fact is not required to be proved here. Show that the additive group is isomorphic, as a group, to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) [8, Problem 23.17] Show that the *ring* $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not a field.[1009]

Solution:

[1009]The problem in the text also asks why this is not in conflict with the preceding part. The answer to this is that the author is using the same notation for two different purposes. When he speaks of the *group* $\mathbb{Z}_2 \times \mathbb{Z}_2$, only the group structure is at issue. When, however, he uses the same notation, but speaks of the *ring* $\mathbb{Z}_2 \times \mathbb{Z}_2$, two operations have been defined. The ring fails to be a field because of a problem with the multiplication, defined in [8, Example 21.6, p. 112]. Use of the same notation for multiple purposes is common in mathematics, (cf., for example, the multiple uses given to the symbol $-$ in problem 1 above, footnote 1005); it usually leads to no problems. There are various routes out of the present dilemma. Some authors reserve the notation involving the letter $\mathbb{Z}$ for rings, and use some other letter for the corresponding groups; some authors denote groups and rings by a fuller notation: we could speak of the *ring* — actually, it is a field — $(\mathbb{Z}_2, +, [0], \times, [1])$, but of the *group* $(\mathbb{Z}_2, +, [0])$.

(a) Under the bijection $([0]_2,[0]_2) \mapsto 0$; $([0]_2,[1]_2) \mapsto e$; $([1]_2,[0]_2) \mapsto a$; $([1]_2,[1]_2) \mapsto b$, the addition table of the field transforms to the following, which is precisely the addition table of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$+$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$
$([0]_2,[0]_2)$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$
$([0]_2,[1]_2)$	$([0]_2,[1]_2)$	$([0]_2,[0]_2)$	$([1]_2,[1]_2)$	$([1]_2,[0]_2)$
$([1]_2,[0]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$
$([1]_2,[1]_2)$	$([1]_2,[1]_2)$	$([1]_2,[0]_2)$	$([0]_2,[1]_2)$	$([0]_2,[0]_2)$

.

Note that this group — the Klein 4-group — is characterized by the property that the product of any two of the non-identity elements — in either order — is equal to the third.

(b) By the definition given in [8, Example 21.6, p. 112], $(1,0)(0,1) = (1\cdot 0, 0\cdot 1) = (0,0)$, the zero element of the ring. Thus $(1,0)$ and $(0,1)$ are zero divisors. If it were true that $(1,0)$ had a multiplicative inverse r, then $r(1,0) = (1,1)$; hence $(0,0) = r(0,0) = r(1,0)(0,1) = (1,1)(0,1) = (0,1)$, implying that $0 = 1$, a contradiction. The existence of a non-zero element lacking a multiplicative inverse shows that the ring is not a field.

6. [8, Problem 24.19] Give an example of a ring of characteristic 3 that is not a field.

Solution: One example is the ring of power series $\mathbb{Z}_3[[x]]$. As seen above, the power series x (i.e. $0x^0 + 1x^1 + 0x^2 + 0x^3 + ...$) is not invertible. However, the sum of three copies of the same power series is always the zero power series.

A simpler example could be had by taking $\mathbb{Z}_3 \times \mathbb{Z}_3$. This ring has zero divisors, for example $([0]_3,[1]_3)([1]_3,[0]_3) = ([0]_3,[0]_3)$; a zero divisor cannot have a multiplicative inverse.

7. [8, Problems 22.22, 22.23] The *centre* of a ring R is defined to be $Z(R) = \{c \in R : \forall r \in R[cr = rc]\}$.

(a) Prove, using the characterization of subring in [8, Theorem 22.2], that $Z(R)$ is a subring of R.

(b) Determine $Z(R)$ when R is commutative.

(c) Determine $Z(M(2,\mathbb{R}))$.

Solution:

(a) i. $Z(R)$ is non-empty. By virtue of [8, Theorem 21.2(a)], $\forall r \in R[0r = 0 = r0]$. Hence $0 \in R$.

ii. $Z(R)$ is closed under the mapping $r \mapsto -r$. Suppose that $c \in Z(R)$. Then $\forall r \in R[cr = rc]$. In particular, taking r to be $-s$, where s is any element of R, $c(-s) = (-s)c$. But, by [8, Theorem 21.2(b)], $c(-s) = (-c)s$; $(-s)c = s(-c)$. It follows that $(-c)s = s(-c)$, implying that $-c \in Z(R)$.

iii. $Z(R)$ is closed under addition and multiplication. Suppose that $a, b \in Z(R)$. Then $\forall r \in R[ar = ra]$ and $\forall r \in R[br = rb]$. It follows that

$$\begin{aligned}
\forall r \in R, \quad (a+b)r &= ar + br \quad \text{distributivity} \\
&= ra + rb \quad a, b \in Z(R) \\
&= r(a+b) \quad \text{distributivity} \\
\Rightarrow \quad & a + b \in Z(R) \text{ ; and} \\
\forall r \in R, \quad (ab)r &= a(br) \quad \text{associativity of multiplication} \\
&= a(rb) \quad b \in Z(R) \\
&= (ar)b \quad \text{associativity of multiplication} \\
&= (ra)b \quad a \in Z(R) \\
&= r(ab) \quad \text{associativity of multiplication} \\
\Rightarrow \quad & ab \in Z(R)
\end{aligned}$$

(b) When R is commutative, every element of R commutes with all elements, so $Z(R) = R$.

(c) The problem is to determine the 2×2 matrices which commute with all 2×2 matrices. Evidently, among those matrices will be all scalar multiples of the identity matrix. Conversely, suppose that $E = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(2, \mathbb{R})$. This matrix must commute with, among other matrices, $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Hence

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = AE = EA = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}$$

$$\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = BE = EB = \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix}$$

from which it follows that $b = c = 0$, and that $a = d$. Thus the *only* matrices in the centre are scalar multiples of the identity matrix. That is,

$$Z(M(2, \mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R} \right\}$$

B.5 Fifth 1997 Problem Assignment

1. For any complex number $z = x + iy = x + y\sqrt{-1} = (x, y)$, we define the *(complex) conjugate* z^* or $\overline{z}$ to be $x - iy = x - y\sqrt{-1} = (x, -y)$, i.e. the image of z under reflection in the *real axis* (x-axis). Prove the following:

   (a) [8, Problem 29.16(a)] Conjugation is an *involutary* unary operation on $\mathbb{C}$; i.e. $\forall z \in \mathbb{C}[(z^*)^* = z]$.

   (b) [8, Problem 29.14] Conjugation is a ring isomorphism of $\mathbb{C}$ with itself.[1010]

   (c) [8, Problem 29.16(b)] For any $z \in \mathbb{C}$, $z + z^*$ lies on the real axis.

   (d) For any $z \in \mathbb{C}$ $z - z^*$ lies on the "imaginary" axis — i.e. on the line $x = 0$.

   (e) [8, Problem 29.16(d)] Conjugation commutes with the taking of inverses; i.e. $\forall z \in \mathbb{C}\left[(z^{-1})^* = (z^*)^{-1}\right]$.

   Solution:

   (a) $((x + iy)^*)^* = (x - iy)^* = x - i(-y) = x + iy$.

   (b) **Conjugation is injective.**

$$\begin{aligned} & (x + iy)^* = (u + iv)^* \\ \Leftrightarrow\ & x - iy = u - iv \\ \Leftrightarrow\ & x = u \quad \wedge \quad -y = -v \\ & \text{by definition of equality of points in } \mathbb{R}^2 \\ \Leftrightarrow\ & x = u \quad \wedge \quad y = v \\ \Leftrightarrow\ & x + iy = u + iv \end{aligned}$$

   The preceding proof is inelegant, as it fails to make use of the fact, already proved, that conjugation is involutary. That fact permits us to proceed as follows:

$$\begin{aligned} & z^* = w^* \quad \text{hypothesis} \\ \Leftrightarrow\ & (z^*)^* = (w^*)^* \quad \text{conjugating both sides} \\ \Leftrightarrow\ & z = w \quad \text{since conjugation is involutory} \end{aligned}$$

   Conjugation is surjective. Any point $x + iy \in \mathbb{C}$ is equal to $(x - iy)^*$.

[1010] An isomorphism of a structure with itself is often called an *automorphism*.

Conjugation commutes with addition.

$$\begin{aligned} & ((x+iy)+(u+iv))^* \\ = \; & ((x+u)+i(y+v))^* \quad \text{by definition of addition in } \mathbb{C} \\ = \; & (x+u)+i(-y-v) \quad \text{by definition of conjugation} \\ = \; & (x-iy)+(u-iv) \quad \text{by definition of addition in } \mathbb{C} \end{aligned}$$

Conjugation commutes with multiplication.

$$\begin{aligned} & ((x+iy)(u+iv))^* \\ = \; & ((xu-yv)+i(xv+yu))^* \quad \text{by definition of multiplication in } \mathbb{C} \\ = \; & (xu-yv)+i(-xv-yu) \quad \text{by definition of conjugation} \\ = \; & (xu-(-y)(-v)+i(x(-v)+(-y)u) \\ = \; & (x+i(-y))(u+i(-v)) \quad \text{by definition of multiplication in } \mathbb{C} \\ = \; & (x+iy)^*(u+iv)^* \quad \text{by definition of conjugation} \end{aligned}$$

(cf. [8, Definition, p. 121].

(c) For any $x+iy \in \mathbb{C}$,

$$\begin{aligned} & (x+iy)+(x+iy)^* \\ = \; & (x+iy)+(x-iy) \quad \text{by definition of conjugation} \\ = \; & (x+x)+i(y-y) \quad \text{by definition of } + \text{ in } \mathbb{C} \\ = \; & 2x+i0\,, \end{aligned}$$

a point on the "real" axis. We have identified points $(u,0) \in \mathbb{C}$ with the corresponding real numbers $u \in \mathbb{R}$; more precisely, we have *embedded* $\mathbb{R}$ in $\mathbb{C}$ by showing that the complet points on the real axis form a subfield of $\mathbb{C}$ which is isomorphic to $\mathbb{R}$.

(d) Analogously to the preceding, we can show that $(x+iy)-(x+iy)^* = 0+2iy$, a point on the y-axis (the *imaginary* axis.

(e)

$$\begin{aligned} (x+iy)(x+iy)^* &= (x+iy)(x-iy) \\ &= (x^2+y^2)+i0 \end{aligned}$$

Hence,

$$(x+iy)\left(\frac{x}{x^2+y^2}-i\frac{y}{x^2+y^2}\right) = 1+i0 \quad \text{the unity of } \mathbb{C}\,,$$

so

$$(x+iy)^{-1} = \frac{x}{x^2+y^2} + i\frac{y}{x^2+y^2}\,. \tag{1020}$$

Replacing y by $-y$ in (1020) yields

$$\begin{aligned}((x+iy)^*)^{-1} &= (x-iy)^{-1} \\ &= \left(\frac{x}{x^2+(-y)^2} + i\frac{-y}{x^2+(-y)^2}\right) \\ &= \left(\frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}\right) \\ &= \left(\frac{x}{x^2+y^2} + i\frac{y}{x^2+y^2}\right)^* \\ &= \left((x+iy)^{-1}\right)^*\,.\end{aligned}$$

(Alternatively,

$$\begin{aligned}z\cdot\left(z^{-1}\right)* &= \left(z\cdot z^{-1}\right)^* \quad * \text{ commutes with multiplication} \\ &= 1^* = 1,\end{aligned}$$

so $(z^{-1})* = (z^*)^{-1}$.)

2. Consider the set $\mathbb{Z}[i]$, called the *Gaussian integers*, defined to consist of all complex numbers of the form $m+in$, where m and n are integers.

   (a) Show that $\mathbb{Z}[i]$ is an integral domain.

   (b) Summarize the construction of [8, §27] of the field of quotients of this integral domain. In particular, show how every element of this field is expressible in the form $[a+ib, c]$, where $a, b, c \in \mathbb{Z}$, and $c > 0$.

   (c) Prove that $1+i$ is not the square of a ratio $\frac{a+bi}{c+di}$ of two Gaussian integers, where $c+di \neq 0$.

   Solution:

   (a) We must prove that $\mathbb{Z}[i]$ is a commutative ring with unity distinct from 0, and containing no zero divisors. As $\mathbb{Z}[i]$ consists of points in $\mathbb{C}$, we can apply [8, Theorem 22.2, p. 117] to prove that it is a subring of the field (hence, in particular, a commutative ring) $\mathbb{C}$.

   $\mathbb{Z}[i]$ **is not empty.** The zero element of $\mathbb{C}$, viz. $0+i0$ is of the form "integer + i(integer)". hence is contained in $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ **is closed under addition.** Let $m + in$ and $r + is$ be elements of $\mathbb{Z}[i]$. Their sum in $\mathbb{C}$ is $(m + r) + i(n + s)$, which is of the form "integer + i(integer)". hence is contained in $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ **is closed under the taking of the additive inverse.** For $m, n \in \mathbb{Z}$,

$$\begin{aligned} & -(m + in) \\ = \; & (-m) + i(-n) \quad \text{by definition of additive inverse in } \mathbb{C} \\ \in \; & \mathbb{Z}[i] \end{aligned}$$

$\mathbb{Z}[i]$ **is closed under multiplication.** Let $m + in$ and $r + is$ be elements of $\mathbb{Z}[i]$. Their product in $\mathbb{C}$ is $(mr - ns) + i(ms + nr)$, which is of the form "integer + i(integer)". hence is contained in $\mathbb{Z}[i]$.

The foregoing shows that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. This frees us from the chores of proving, for example, that multiplication is associative. It also implies that, since multiplication in the superring is commutative, multiplication in $\mathbb{Z}[i]$ must also be commutative. There can be no zero divisors in a subring of a ring without zero divisors. Finally, since the unity of the superring, viz. $1 + i0$, is in $\mathbb{Z}[i]$, $\mathbb{Z}[i]$ is an integral domain.

(b) As in [8, §27], we define an equivalence relation $\sim$ on the set of ordered pairs $(m + in, r + is)$ where m, n, r, s are integers, and not both of r and s are zero:

$$\begin{aligned} & (m_1 + in_1, r_1 + is_1) \sim (m_2 + in_2, r_2 + is_2) \\ \Leftrightarrow \; & (m_1 + in_1)(r_2 + is_2) = (r_1 + is_1)(m_2 + in_2) \end{aligned}$$

In particular, $(m + in, r + is) \sim ((m + in)(r - is), (r + is)(r - is)) \sim ((mr + ns) + i(-ms + nr), r^2 + s^2))$, which is of the desired form, $(a + ib, c)$, and c, being the sum of squares of two integers, not both zero, must surely be a positive integer.

(c)

$$\begin{aligned} 1 + i &= \left(\frac{a + bi}{c + di}\right)^2 \\ \Rightarrow (1 + i)^* &= \left(\left(\frac{a + bi}{c + di}\right)^2\right)^* = \left(\frac{(a + bi)^*}{(c + di)^*}\right)^2 \\ & \quad \text{by properties of conjugation} \\ \text{i.e. } 1 - i &= \left(\frac{a - bi}{c - di}\right)^2 \\ \Rightarrow (1 + i)(1 - i) &= \left(\frac{(a + bi)(a - bi)}{(c + di)(c - di)}\right)^2 \end{aligned}$$

$$\Leftrightarrow 2 = \left(\frac{a^2+b^2}{c^2+d^2}\right)^2$$

implying that 2 is the square of a rational number. From this contradiction we conclude that our original assumption $1+i = \left(\frac{a+bi}{c+di}\right)^2$ is false.

3. [8, Problem 41.8] Prove that, for any field F with unity 1, and any indeterminate x, the polynomial ring $F[x]$ is not a field.

   Solution: A multiplicative identity, if it exists, is unique.[1011] The polynomial $1x^0$ evidently acts as identity.

   We can show that $F[x]$ is not a field by proving the existence of non-zero elements that do not have a multiplicative inverse. For example, consider the polynomial x^1. If $a_0 + a_1x + ... + a_nx^n$ were its inverse, then we would have

   $$1x^0 = x^1(a_0x^0 + a_1x^1 + ... + a_nx^n) = 0x^0 + a_0x^1 + a_1x^2 + ... + a_nx^{n+1}$$

   which would entail (comparing coefficients of x^0) $1 = 0$, contradicting the requirement that the $0 \neq 1$ in an integral domain [8, p. 116]. From this contradiction we conclude that $F[x]$ is not a field.

4. [8, Problem 42.12] Showing all your work, use the Factor Theorem to answer the following questions:

   (a) Is $x - 3 \in \mathbb{Q}[x]$ a factor of $3x^3 - 9x^2 - 7x + 21 \in \mathbb{Q}[x]$?

   (b) Is $x + 2 \in \mathbb{R}[x]$ a factor of $x^3 + 8x^2 + 6x - 8 \in \mathbb{R}[x]$?

   (c) For which $k \in \mathbb{Q}$ is $x - 1$ a factor of $x^3 + 2x^2 + x + k \in \mathbb{Q}[x]$?

   (d) Is $x - 2 \in \mathbb{Z}_5[x]$ a factor of $2x^5 - 3x^4 - 4x^3 + 3x \in \mathbb{Z}_5[x]$?

   (e) For which $k \in \mathbb{C}$ is $x + i$ a factor of $ix^9 + 3x^7 + x^6 - 2ix + k \in \mathbb{C}[x]$?

   Solution:

   (a) Let $f(x) = 3x^3 - 9x^2 - 7x + 21$. Then $f(3) = 3 \cdot 3^3 - 9 \cdot 3^2 - 7 \cdot 3 + 21 = 0$. By the Factor Theorem, this implies that $(x - 3)|f(x)$.

   (b) Let $g(x) = x^3+8x^2+6x-8$. Then $g(-2) = (-2)^3+8(-2)^2+6(-2)-8 = 4 \neq 0$ over the field $\mathbb{R}$. It follows by the Factor Theorem that $(x - (-2)) \nmid g(x)$.

   (c) Let $h(x) = x^3 + 2x^2 + x + k$. Then $h(1) = 1 + 2 + 1 + k = 4 + k$. $h(1) = 0 \Leftrightarrow k = -4$. Thus $x - 1$ divides $h(x)$ iff $k = -4$.

[1011] The proof of [8, Theorem 5.1(a)], althgouh written for groups, is also valid for the multiplicative structure of rings.

(d) Let $m(x) = 2x^5 - 3x^4 - 4x^3 + 3x$. Then $m(2) = 2 \cdot 2^5 - 3 \cdot 2^4 - 4 \cdot 2^3 + 3 \cdot 2 = -10$ over any field. For the field $\mathbb{Z}_5$, $5 = 0$, so then $m(2) = 0$, and, by the Factor Theorem, $(x-2)|m(x)$.

(e) Define $a(x) = ix^9 + 3x^7 + x^6 - 2ix + k$. Then $a(-i) = i \cdot (-i)^9 + 3 \cdot (-i)^7 + (-i)^6 - 2i \cdot (-i) + k = 3i - 2 + k$. By the Factor Theorem, $(x+i)|a(x) \Leftrightarrow 3i - 2 + k = 0 \Leftrightarrow k = 2 - 3i$.

5. (cf. [8, Problem 43.10]) Consider the polynomial $f(x) = x^4 + x^2 + 1$. Show that the textbook is in error when it claims that $f(x)$ is irreducible over the field $\mathbb{Z}_5$. Find all factorizations into monic polynomials.

Solution: We may begin by looking for first degree factors. We compute $f(4) = f(1) = 3 \neq 0$, $f(0) = f(2) = f(3) = 1 \neq 0$. Thus $f(x)$ has no first degree factors; if it factorizes over $\mathbb{Z}_5$, it can only be into factors of degrees at least 2 — hence into exactly 2 factors of degree 2; since $f(x)$ is *monic* (it has leading coefficient equal to 1), these factors, if they exist, may be assumed to be both monic. Assume

$$x^4 + x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

Comparing coefficients of degrees 3, 2, 1, 0, yields, respectively,

$$0 = a + c \tag{1021}$$
$$1 = b + d + ac \tag{1022}$$
$$0 = bc + ad \tag{1023}$$
$$1 = bd \tag{1024}$$

From (1021) it follows that $c = -a$, so (1023) reduces to $a(d-b) = 0$. We can consider two cases.

Case 1. $a = c = 0$**.** Equations (1022) and (1024) reduce to $b + d = 1$, $bd = 1$. From the latter we infer that b and d are mutual inverses, so (b, d) is one of $(1,1)$, $(2,3)$, $(3,2)$, $(4,4)$; however, none of these ordered pairs satisfies the condition $b + d = 1$. There are thus no factorizations of this type.

Case 2. $d = b$**,** $c = -a$**.** Here the equations reduce to $2b - a^2 = 1$, $b^2 = 1$. The only solutions of these equations are $(a, b) \in \{(1,1), (4,1)\}$; these both lead to the same factorization:

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + 4x + 1) \tag{1025}$$

If, however, we look at this factorization in the equivalent form

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1) \tag{1026}$$

we have a factorization that holds *over all fields!* This polynomial is *never* irreducible!

6. (a) Show that $g(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$, but is reducible over $\mathbb{Z}_3$.
   (b) Repeat the preceding for $h(x) = x^4 + x + 1$.

   Solution:

   (a) Over $\mathbb{Z}_3$, $g(1) = 1+1+1 = 0$, so $(x-1)|g(x)$; indeed, $g(x) = (x-1)(x^2+x+2)$, where the latter quadratic factor is irreducible, since $a^2 + a + 2 \neq 0$ for all $a \in \mathbb{Z}_3$.

   For the remainder of this solution we are working in $\mathbb{Z}_2$. $g(0) = 1 = g(1)$, so g has no *linear* factors. But, if $g(x)$ admitted a factorization in which one factor had degree 2, then the other factor would be of degree $3 - 2 = 1$, i.e. would be linear. It follows that $g(x)$ has no polynomial factors of degree less than 3, i.e. that it is irreducible.

   (b) The same approach as above shows that $x - 1$ divides $h(x)$ over $\mathbb{Z}_3$; the factorization is $h(x) = (x - 1)(x^3 + x^2 + x - 1)$. As in the last part of the preceding proof, the polynomial $x^3 + x^2 + x - 1$ has no linear factors, and it must therefore be irreducible.

   For the remainder of this solution we are working in $\mathbb{Z}_2$. $h(0) = 1 = h(1)$, so h has no *linear* factors. If it factorizes at all, it will be into factors of degree at least 2. As there would have to be at least 2 such factors, the factorization would have to be into exactly 2 factors of degree 2. We assume a factorization of the form

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) \tag{1027}$$

   and derive a contradiction. Comparing coefficients of degrees 3, 2, 1, 0, yields, respectively,

$$\begin{aligned} 0 &= a + c && (1028)\\ 0 &= b + d + ac && (1029)\\ 1 &= bc + ad && (1030)\\ 1 &= bd && (1031) \end{aligned}$$

   From (1031) b and d must be non-zero, hence $b = d = 1$, the only non-zero element of the field $\mathbb{Z}_2$. But then (1030) becomes $a + c = 1$, which contradicts (1028). We conclude that no factorization of the form (1027) can exist, and hence that $h(x)$ is irreducible over the field $\mathbb{Z}$.

   Another approach to this problem would be to catalogue the irreducible polynomials of degrees 1, 2, and 3, and then show that no products of these could yield the present polynomial. The irreducible polynomials of degrees 1 and 2 can be shown to be x, $1 + x$ and $1 + x + x^2$; there are two irreducible polynomials of degree 3: $1 + x + x^3$ and $1 + x^2 + x^3$.

There are two other irreducible binary polynomials of degree 4: the first is obvious, $1 + x^3 + x^4$; the other is $1 + x + x^2 + x^3 + x^4$.

B.6 Sixth 1997 Problem Assignment

1. (a) Show that the set $\{a^2 | a \in \mathbb{Z}_3\}$ does not contain 2 (i.e. $[2]_3$).[1012]

   (b) Explain why this proves that the polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$.

   (c) Showing all your work, determine the multiplication table of the field $\mathbb{F} = \mathbb{Z}_3[x]/(x^2 + 1)$. (It will not be sufficient to simply write down the table, without showing how you were able to compute the various entries.)

   (d) In any finite field it is possible to find elements, each of which generates the multiplicative group of non-zero elements. Show that, for the field you have constructed, x is not a generator of this type; show also that $1 + x$ *is* such a generator. Express each of the elements shown in your table as powers of $y = 1 + x$.

   (e) Determine whether the polynomial $1 + X^2 \in \mathbb{F}[X] = \mathbb{Z}_3[x]/(x^2 + 1)[X]$ is reducible. (The indeterminate here is X; x has been used in the naming of the elements of $\mathbb{F}$.)

   Solution:

   (a) $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1$ modulo 3.

   (b) We have shown that there is no root for $1+x^2$. Hence, by the Factor Theorem, there exists no $c \in \mathbb{Z}_3$ such that $(x - c) \mid (1 + x^2)$. Thus $1 + x^2$ has no 1st degree factors. The only monic factors of degree less than 2 will then have to have degree 0, i.e. can only be the unique monic polynomial 1. Thus $1 + x^2$ admits only the trivial factorization, $1 + x^2 = 1(1 + x^2)$.

   (c) The table is shown below, but we have not shown all the computations needed to determine this table. Those computations could be different for each student, since they can refer back to earlier computations in building the same table. For example, a typical computation is

$$\begin{aligned}(1 + 2x)(2x) &= 2x + 4x^2 \\ &= 2x + x^2 \quad \text{reducing coefficient of } x^2 \text{ mod } 3 \\ &= 1(1 + x^2) + (2 + 2x) \quad \text{by Division Algorithm} \\ &= 2 + 2x \quad \text{reducing modulo } 1 + x^2\end{aligned}$$

[1012] We say that 2 *is not a quadratic residue modulo 3.*

The last line of the table refers to part 1d of this problem.

$\cdot$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
2	0	2	1	$2x$	$2+2x$	$1+2x$	x	$2+x$	$1+x$
x	0	x	$2x$	2	$2+x$	$2+2x$	1	$1+x$	$1+2x$
$1+x$	0	$1+x$	$2+2x$	$2+x$	$2x$	1	$1+2x$	2	x
$2+x$	0	$2+x$	$1+2x$	$2+2x$	1	x	$1+x$	$2x$	2
$2x$	0	$2x$	x	1	$1+2x$	$1+x$	$2x$	$2+2x$	$2+x$
$1+2x$	0	$1+2x$	$2+x$	$1+x$	2	$2x$	$2+2x$	x	1
$2+2x$	0	$2+2x$	$1+x$	$1+2x$	x	2	$2+x$	1	$2x$
		y^8	y^4	y^6	y	y^7	y^2	y^3	y^5

(d) Since

$$\begin{aligned} x^4 &= \left(x^2\right)^2 \\ &= 2^2 \quad \text{from the table} \\ &= 1 \quad \text{modulo 3} \end{aligned}$$

the order of x in the multiplicative group $\mathbb{F}^{\#}$ is not more than 4. Thus there cannot be $3^2 - 1 = 8$ distinct values representable by powers of x.

However, computing powers of $1 + x$ by repeated reference to the table or otherwise, we can show that the 8 powers are as shown on the bottom line of the table.

In such a situation, where x does not generate the field, we say that the polynomial $1 + x^2$ used to construct the field is *not primitive*; we say that $1 + x$ is a *primitive root* of the field.

(e) The polynomial $1+X^2$ has 2 roots in $\mathbb{F}$: x and $2x$. Indeed, $(X-x)(X-2x) = X^2 - 3xX + 2x^2 = X^2 - x^2 = X^2 - 2 = X^2 + 1$; the construction we used to create $\mathbb{F}$ could be thought of as *adjoining* to $\mathbb{Z}_3$ a root of the polynomial $X^2 + 1$.

2. In an important research paper [18][1013] the authors prove the non-existence of graphs having d^2+1 vertices, each of degree d, in which there is no cycle of length less than 5, except for $d = 2$, 3, 7, and, possibly, 57. Their proof is based on determining the values of s for which the polynomial $f(s) = s^5 + s^4 + 6s^3 - 2s^2 + (9-32m)s-15$ has rational roots over $\mathbb{R}$; here m is some integer whose value is not known, and d and s are related by the equation $d = \frac{s^2+3}{4}$. Determine all possible

[1013]The precise reference will be circulated with the solutions.

rational roots of $f(s)$, showing what integer values m must have. Show that $f(s)$ cannot have more than 1 rational root.

Solution: Since $f(s)$ is monic, any rational roots will be integer roots [8, Corollary to Theorem 52.1]. Those integer roots can only be divisors of the constant term, -15; i.e. in the set $\{\pm 1, \pm 3, \pm 5, \pm 15\}$. We tabulate the results of substituting each of these values into $f(s)$, showing also the value of m needed to make $f(s)$ equal to 0.

s	$f(s)$	$f(s) = 0$ when $m =$
1	$-32m$	0
-1	$-32 + 32m$	1
3	$480 - 96m$	5
-3	$-384 + 96m$	4
5	$4480 - 160m$	28
-5	$-3360 + 160m$	21
15	$829920 - 480m$	1729
-15	$-729600 + 480m$	1520

Thus there is, for each of the possible roots, an integer value of m that makes this indeed a root. However, as the values of m corresponding to the various possible roots are all distinct, there cannot be more than one rational root. That is, in each of the 8 cases the quintic polynomial may be factorized into a linear and a fourth degree monic factor; in no case will that 4th degree factor have a rational root.

The authors of the cited paper then show that graphs of the type described do indeed exist for $d = 2, 3, 7$. No one has yet succeeded in proving the existence of such a graph for $d = 57$; neither has it been possible to prove non-existence.

3. [The following theory is completely general; we discuss it only for the case of polynomials of degree 3; there are some sign changes between the case of even degree and odd degree. Also, to simplify the discussion, we confine ourselves to *monic* polynomials.]

Suppose that a polynomial $f(x) = a_0 + a_1x + a_2x^2 + x^3$ is given, having roots r_1, r_2, r_3, where a root of multiplicity m is listed m times. Then

$$(x - r_1)(x - r_2)(x - r_3) = f(x) = a_0 + a_1x + a_2x^2 + x^3$$

so, comparing coefficients of corresponding powers of x, we have the identities:

$$\begin{array}{rrcl} x^0: & -r_1r_2r_3 & = & a_0 \\ x^1: & r_2r_3 + r_3r_1 + r_1r_2 & = & a_1 \\ x^2: & -r_1 - r_2 - r_3 & = & a_2 \\ x^3: & 1 & = & 1 \end{array}$$

With the signs adjusted, the sums on the left are called the *elementary symmetric functions* of the roots, viz:

$$\begin{aligned}\sigma_1 &= r_1 + r_2 + r_3\\ \sigma_2 &= r_2r_3 + r_1r_3 + r_1r_2\\ \sigma_3 &= r_1r_2r_3\end{aligned}$$

In general, the elementary symmetric function σ_k of n variables r_1, r_2, ..., r_n is defined to be the sum of all $\binom{n}{r}$ products of variables with distinct subscripts, taken k at a time.

You are given the polynomial $f(x) = x^3 - 2x - 5$. *Without determining the roots of* f, determine the monic polynomials whose roots are

(a) the reciprocals of the roots of f; (for this part only you must assume that $5 \neq 0$ in the field of coefficients);

(b) the "negatives" of the roots of f (meaning, multiply each root by -1);

(c) the squares of the roots of f;

(d) the roots of f, each with twice the multiplicity it has in f;

(e) the excesses of each of the roots of f over 1 (i.e. $1 - r$ for each of the roots r).

Solution: These problems were to be solved without determining the roots of f. If f is interpreted as a polynomial with complex coefficients, those roots are approximately

$$2.094551482, \quad -1.04727541 \pm 1.135939890\sqrt{-1}\,.$$

However, the following discussion is completely general, and does not require specification of the field. If we denote the symmetric functions *of the roots of* f by σ_i $(i = 1, 2, 3)$, we have, from the coefficients in f, that $\sigma_1 = 0$, $\sigma_2 = -2$, $\sigma_3 = 5$.

(a) This problem can be solved naïvely as follows: The sum of roots is $\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3} = \frac{\sigma_2}{\sigma_3} = -\frac{2}{5}$. The sum of products of pairs of roots is $\frac{1}{r_1r_2} + \frac{1}{r_2r_3} + \frac{1}{r_3r_1} = \frac{\sigma_1}{\sigma_3} = 0$. The product of roots is $\frac{1}{\sigma_3} = \frac{1}{5}$. Hence the polynomial is $x^3 - \left(-\frac{2}{5}\right)x^2 + 0x - \frac{1}{5}$. But there is an easier method. We seek a polynomial g such that $g(x) = 0 \Leftrightarrow f\left(\frac{1}{x}\right) = 0$. Since roots are distinct from zero, the condition $g(x) = 0$ is thus equivalent to the condition $x^3 f\left(\frac{1}{x}\right) = 0$, i.e. to $-5x^3 - 2x^2 + 1 = 0$. Since we require that the polynomial be monic, we scale the coefficients: $x^3 + 2 \cdot 5^{-1}x^2 - 5^{-1}$.

(b) The sum of the roots of the polynomial sought is $-\sigma_1 = -0 = 0$; the sum of the products of pairs is $(-1)^2\sigma_2 = -2$; and the product of the three roots is $-\sigma_3 =$

-5. We can now reconstruct the polynomial to be $x^3 - 0x^2 + (-2)x^1 - (-5)$, i.e. $x^3 - 2x + 5$.

Alternatively, we could observe that, if $h(x)$ is the polynomial we seek, then $h(x) = 0$ iff $f(-x) = 0$. The polynomial $f(-x)$ is $-x^3 + 2x - 5$; rendered monic, this becomes $x^3 - 2x + 5$, as before.

(c) The sum of the roots will be $r_1^2 + r_2^2 + r_3^2 = (r_1 + r_2 + r_3)^2 - 2(r_1r_2 + r_2r_3 + r_3r_1) = \sigma_1^2 - 2\sigma_2 = 0^2 - 2(-2) = 4$. The sum of products of pairs will be $(r_1r_2)^2 + (r_2r_3)^2 + (r_3r_1)^2 = \sigma_2^2 - 2\sigma_3\sigma_1 = (-2)^2 - 2 \cdot 5 \cdot 0 = 4$. The product of the roots will be $\sigma_3^2 = 25$. Hence the polynomial is $x^3 - 4x^2 + 4x - 25$.

This operation of replacing a polynomial by one whose roots are the squares of its roots is at the heart of an algorithm for finding roots of polynomials called the *Graefe* method, which is particularly effective where there is one root whose modulus is larger than that of the others. After k repetitions of the procedure, the negative of the coefficient of x^2 approaches the 2^kth power of this root. (Why?)

(d) Since f is the product of first degree factors, one for each of the roots, f^2 will be the desired polynomial: $x^6 - 4x^4 - 10x^3 + 4x^2 + 20x + 25$.

(e) The sum of the roots will be $3 - \sigma_1 = 3$. The sum of products of pairs will be

$$(1 - r_1)(1 - r_2) + (1 - r_2)(1 - r_3) + (1 - r_3)(1 - r_1)$$

$$= 3 - 2\sigma_1 + \sigma_2 = 3 + 0 + (-2) = 1\,.$$

The product of roots is $(1 - r_1)(1 - r_2)(1 - r_3) = f(1) = 1 - 2 - 5 = -6$. Hence the polynomial is $x^3 - 3x^2 + 1x - (-6)$, i.e. $x^3 - 3x^2 + x + 6$.

4. (a) Determine all positive integers a such that $\varphi(a) = 1$.

(b) Prove that the function φ is multiplicative.

(c) Determine all positive integer pairs (a, b) such that $\varphi(ab) = \varphi(a)$.

Solution:

(a) $\varphi(n)$ is the number of generators of the additive group $\mathbb{Z}_n$, equal to the number of integers between 1 and n which are relatively prime to n. One of these is 1; another will be -1, which will be distinct from 1 iff $n \geq 3$, so $n \geq 3 \Rightarrow \varphi(n) \geq 2$. When $n = 2$ there is just the one generator; evidently the group of one element has only one generator also. Thus $n \geq 3 \Leftrightarrow \varphi(n) \geq 2$.

(b) We give two proofs. Let m and n be relatively prime positive integers.

i. *Using the explicit formula for φ.* By the Fundamental Theorem of Arithmetic, m and n admit factorizations of the form

$$\begin{aligned} m &= p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \\ n &= q_1^{s_1} q_2^{s_2} ... q_\ell^{s_\ell} \end{aligned}$$

where $p_1, ..., p_k, q_1, ..., q_\ell$ are distinct (positive) primes, and all exponents shown are *positive* integers. Then, by Theorem A.6.2.5,

$$\begin{aligned} \varphi(m) &= m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right) \\ \varphi(n) &= n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)...\left(1-\frac{1}{q_\ell}\right) \end{aligned}$$

As the lists of prime divisors of m and n are disjoint, the prime decomposition of mn is precisely

$$mn = p_1^{r_1} p_2^{r_2} ... p_k^{r_k} q_1^{s_1} q_2^{s_2} ... q_\ell^{s_\ell}$$

so $\varphi(mn)$

$$\begin{aligned} &= mn\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)...\left(1-\frac{1}{q_\ell}\right) \\ &= \varphi(m)\cdot\varphi(n) \end{aligned}$$

ii. Recall that we defined $\varphi(m)$ to be the number of elements of $\mathbb{Z}_{(m)}$, i.e., the number of residue classes $[a]_m$ such that $(a, m) = 1$. Let $[x_1]_m$, $[x_2]_m$ be such that $(x_1, m) = 1 = (x_2, m)$, and let $[y_1]_n$, $[y_2]_n$ be such that $(y_1, n) = 1 = (y_2, n)$. Then, if $[x_1 n + y_1 m]_{mn} = [x_2 n + y_2 m]_{mn}]$, $mn \mid ((x_1 - x_2)m + (y_1 - y_2)n)$. Hence m divides $(y_1 - y_2)n$, and, as $(m, n) = 1$, $m \mid (y_1 - y_2)$ (cf. [8, Problem 12.17]), i.e., $[y_1]_m = [y_2]_m$; in the same way we can argue that $[x_1]_n = [x_2]_n$. It follows that the classes $[xm + yn]_{mn}$ are unique, as x and y respectively range over the residue classes which consistute the groups $\mathbb{Z}_{(m)}$ and $\mathbb{Z}_{(n)}$. We have shown that there are at least $\varphi(m) \cdot \varphi(n)$ elements in $\mathbb{Z}_{(mn)}$.
But, by hypothesis, $(m, n) = 1$. Hence there exist integers a and b such that $am + bn = 1$. Thus, for any class $[u]_{(mn)}$, $u = u \cdot 1 = u(am + bn) = (ua)m + (ub)n$, so u is of the type discussed above. Hence there are at most $\varphi(m) \cdot \varphi(n)$ elements in $\mathbb{Z}_{(mn)}$.

(c) [28, Problem 2.4.9] One solution is $b = 1$, and any a. Suppose now that $b > 1$, and that the prime decompositions of a and b are

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} ... p_k^{r_k} q_1^{s_1} q_2^{s_2} ... q_\ell^{s_\ell} \\ b &= p_1^{t_1} p_2^{t_2} ... p_k^{t_k} n_1^{u_1} n_2^{u_2} ... n_m^{u_m} \end{aligned}$$

where $p_1, ..., p_k, q_1, ..., q_\ell, n_1, ..., n_m$ are distinct (positive) primes, and all exponents shown are *positive* integers; $k \geq 0$, $\ell \geq 0$, $m \geq 0$. Then, by Theorem A.6.2.5,

$$\begin{aligned}
\varphi(a) &= a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)...\left(1-\frac{1}{q_\ell}\right) \\
\varphi(ab) &= ab\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)...\left(1-\frac{1}{q_\ell}\right) \\
&\quad \times\left(1-\frac{1}{n_1}\right)\left(1-\frac{1}{n_2}\right)...\left(1-\frac{1}{n_m}\right)
\end{aligned}$$

hence

$$\begin{aligned}
1 &= p_1^{t_1}p_2^{t_2}...p_k^{t_k}n_1^{u_1}n_2^{u_2}...n_m^{u_m}\left(1-\frac{1}{n_1}\right)\left(1-\frac{1}{n_2}\right)...\left(1-\frac{1}{n_m}\right) \\
&= p_1^{t_1}p_2^{t_2}...p_k^{t_k}\cdot\varphi(n_1^{u_1}n_2^{u_2}...n_m^{u_m})
\end{aligned}$$

But the two factors separated by $\cdot$ in the preceding equation are both positive integers, hence both are equal to 1. From the equation $p_1^{t_1}p_2^{t_2}...p_k^{t_k} = 1$ it follows that $k = 0$: a and b must be relatively prime. From the equation $\varphi(n_1^{u_1}n_2^{u_2}...n_m^{u_m}) = 1$ if follows that $n_1^{u_1}n_2^{u_2}...n_m^{u_m} = 1$ or $= 2$; thus $b = 1$ or $b = 2$.

C 1998 Problem Assignments, with Solutions

C.1 First 1998 Problem Assignment

1. Prove or disprove[1014]: for sets A, B, C, and mappings $\phi : A \to B$ and $\psi : B \to C$, if $\psi \circ \phi$ is surjective, then ϕ must be surjective.

   Solution: As stated in [8, Problem 2.21, p. 21], this statement is false. Let $A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$. Any mapping $\psi : B \to C$ will be surjective; indeed, the *constant* mapping $b_i \mapsto c$ $(i = 1, 2)$ is the only possible mapping from B to C; and, no matter what mapping $\phi : A \to B$ we select, $\psi \circ \phi$ will have to be the constant mapping, and will be surjective. It suffices to exhibit a mapping $\phi : A \to B$ which is not surjective. One of the two mappings with that property is given by $a \mapsto b_1$, and can serve as a counterexample.

   This is the "smallest" counterexample. Had we taken B to have fewer than 2 elements — i.e. only 1 element — then, as already observed, ϕ would be surjective.

2. (a) [8, Problem 3.30] Assume that $*$ is a binary operation having identity e on a set S, and that
   $$\forall x \forall y \forall z [(x * y) * z = x * (z * y)] . \tag{1032}$$
   Prove that $*$ is associative and commutative. [Hint: You have been given a triply quantified true statement. Make suitable specializations, beginning with a specializiation of x.]

   (b) On a set S define a binary operation $*$ by $\forall a \forall b [a * b = a]$. Show that, if $|S| > 1$,

   i. $*$ is not commutative;

   ii. $*$ is associative;

   iii. $*$ has no identity element;

   iv. $*$ satisfies (1032).

   Conclude that, if $|S| > 1$, (1032) implies both associativity and commutativity only if $*$ is known to possess an identity element.

   Solution:

   (a) Specializing $x := e$ in (1032) yields
   $$\forall y \forall z [(e * y) * z = e * (z * y)] ,$$

[1014] *Prove or disprove* will always mean, unless otherwise stated, *Prove, showing all your work, or disprove with an explicit counterexample.*

from which follows, by virtue of the fact that e is an identity, so $\forall u[e * u = u]$,

$$\forall y \forall z[y * z = (e * y) * z = e * (z * y) = z * y]$$

proving that $*$ is commutative.
But this implies that, for all a, b, c,

$$\begin{aligned} a * (b * c) &= a * (c * b) \quad \text{by comutativity} \\ &= (a * b) * c \quad \text{by (1032).} \end{aligned}$$

and so $*$ is also associative.

(b) i. Suppose that a and b are distinct elements of S. Then

$$a * b = a \neq b = b * a$$

so $*$ is not commutative.

ii. The multiplication we have defined could be called *absorption to the left*. No matter what we choose for b, and c, $a * (b * c) = a$; and, as $a * b = a$, $(a * b) * c = a * c = a$. Thus $*$ is associative.

iii. Suppose that there is an identity element e. Then, for every element x, $e * x = x$. However, we have defined $*$ so that $e * x = e$. So we need only choose some element x different from e to have a contradiction; as $|S| > 1$, there exists such an element different from e. From this contradiction we conclude that there exists no identity element for $*$.

iv. $\forall x \forall y \forall z[(x * y) * z = x * z = x * (z * y)]$.

Of course, when $|S| \leq 1$, $*$ is evidently both associative and commutative. And, when $|S| = 1$, it has an identity element.

3. [8, Problem 4.11] Let S denote the set $\mathbb{R} - \{0, 1\}$. In addition to the identity function $\iota_S : S \to S$, we define 5 other functions α_i $(i = 2, 3, 4, 5, 6)$ from S to S as follows:

$$\begin{aligned} \forall x \quad \alpha_2(x) &= \frac{1}{x} \\ \alpha_3(x) &= 1 - x \\ \alpha_4(x) &= 1 - \frac{1}{x} \\ \alpha_5(x) &= \frac{1}{1 - x} \\ \alpha_6(x) &= 1 - \frac{1}{1 - x} \end{aligned}$$

(a) Defining $\alpha_1 = \iota_S$, compute all 6^2 of the compositions $\alpha_i \circ \alpha_j$ $(i, j = 1, 2, 3, 4, 5, 6)$ and show that composition is an operation on the set $A = \{\alpha_i : i = 1, ..., 6\}$.

(b) Show that the elements of A are all different.

(c) Represent the composition information in a Cayley table.

(d) Show that one of the elements of A serves as an identity element for function composition.

(e) From your table show that each of the 6 elements of A has an inverse under the operation of function composition.

(f) Show that the operation is not commutative.

(g) Explain how we know that each of the elements of A is a bijection.

(h) Explain why there is no function in the set A which has the property that compositions of it with itself yield all elements of A.

(i) There are several subsets B of A with the property that products of elements of B yield all elements of A. Show that $\{\alpha_2, \alpha_3\}$ is one such subset.

(That the operation is associative follows from [8, Theorem 4.1(a)].)

Solution:

(a) By [8, Theorem 4.1(a)], $\alpha_1 \circ \alpha_i = \alpha_i \circ \alpha_1 = \alpha_i$ for all i.

$$\begin{aligned}
&\forall x \quad \left[\alpha_2 \circ \alpha_2(x) = \frac{1}{\frac{1}{x}} = x = \alpha_1(x)\right] \\
&\Rightarrow \quad \alpha_2 \circ \alpha_2 = \alpha_1 \\
&\forall x \quad \left[\alpha_2 \circ \alpha_3(x) = \frac{1}{1-x} = \alpha_5(x)\right] \\
&\Rightarrow \quad \alpha_2 \circ \alpha_3 = \alpha_5 \\
&\forall x \quad \left[\alpha_2 \circ \alpha_4(x) = \frac{1}{1-\frac{1}{x}} = 1 - \frac{1}{1-x} = \alpha_6(x)\right] \\
&\Rightarrow \quad \alpha_2 \circ \alpha_4 = \alpha_6 \\
&\forall x \quad \left[\alpha_2 \circ \alpha_5(x) = \frac{1}{\frac{1}{1-x}} = 1 - x = \alpha_3(x)\right] \\
&\Rightarrow \quad \alpha_2 \circ \alpha_5 = \alpha_3 \\
&\forall x \quad \left[\alpha_2 \circ \alpha_6(x) = \frac{1}{1-\frac{1}{1-x}} = 1 - \frac{1}{x} = \alpha_4(x)\right] \\
&\Rightarrow \quad \alpha_2 \circ \alpha_2 = \alpha_4 \\
&\forall x \quad \left[\alpha_3 \circ \alpha_2(x) = 1 - \frac{1}{x} = \alpha_4(x)\right]
\end{aligned}$$

$$
\begin{aligned}
&\Rightarrow \quad \alpha_3 \circ \alpha_2 = \alpha_4 \\
&\forall x \quad [\alpha_3 \circ \alpha_3(x) = 1 - (1 - x) = x = \alpha_1(x)] \\
&\Rightarrow \quad \alpha_3 \circ \alpha_3 = \alpha_1 \\
&\forall x \quad \left[\alpha_3 \circ \alpha_4(x) = 1 - \left(1 - \frac{1}{x}\right) = \frac{1}{x} = \alpha_2(x)\right] \\
&\Rightarrow \quad \alpha_3 \circ \alpha_4 = \alpha_2 \\
&\forall x \quad \left[\alpha_3 \circ \alpha_5(x) = 1 - \frac{1}{1-x} = \alpha_6(x)\right] \\
&\Rightarrow \quad \alpha_3 \circ \alpha_5 = \alpha_6 \\
&\forall x \quad \left[\alpha_3 \circ \alpha_6(x) = 1 - \left(1 - \frac{1}{1-x}\right) = \frac{1}{1-x} = \alpha_5(x)\right] \\
&\Rightarrow \quad \alpha_3 \circ \alpha_6 = \alpha_5 \qquad \text{etc.}
\end{aligned}
$$

Since the composition of two of the functions is, in every case, another element of the set of functions, composition is an *operation* on the set; alternatively, we say that the set of functions is *closed* under composition.

(b) To show that two functions are different we must show either that their domains are different, or their codomains are different, or they differ in their action on at least one point in the domain. As the domains and codomains are here all the same set S, we shall have to show the functions different by examination their actions at points in the domain. If we want the same point in the domain to serve for all pairs of functions we shall have to be judicious in choosing it; for example, the point $\frac{1}{2}$ will not do, since $\alpha_1(\frac{1}{2}) = \alpha_3(\frac{1}{2})$. However, the point $\frac{1}{3}$ can be used: $\alpha_1\left(\frac{1}{3}\right) = \frac{1}{3}$, $\alpha_2\left(\frac{1}{3}\right) = 3$, $\alpha_3\left(\frac{1}{3}\right) = \frac{2}{3}$, $\alpha_4\left(\frac{1}{3}\right) = -2$, $\alpha_5\left(\frac{1}{3}\right) = \frac{3}{2}$, $\alpha_6\left(\frac{1}{3}\right) = -\frac{1}{2}$. Thus the six functions are all distinct.

(c) There are 6! orders in which the rows/columns of the Cayley table may be labelled. We present the table first in "lexicographic" order; then in an order that better reveals the structure of the group; (we shall return to this topic later in the course.)

$\circ$	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_1	α_2	α_3	α_4	α_5	α_6
α_2	α_2	α_1	α_5	α_6	α_3	α_4
α_3	α_3	α_4	α_1	α_2	α_6	α_5
α_4	α_4	α_3	α_6	α_5	α_1	α_2
α_5	α_5	α_6	α_2	α_1	α_4	α_3
α_6	α_6	α_5	α_4	α_3	α_2	α_1

or

$\circ$	α_1	α_4	α_5	α_2	α_3	α_6
α_1	α_1	α_4	α_5	α_2	α_3	α_6
α_4	α_4	α_5	α_1	α_3	α_6	α_2
α_5	α_5	α_1	α_4	α_6	α_2	α_3
α_2	α_2	α_6	α_3	α_1	α_5	α_4
α_3	α_3	α_2	α_6	α_4	α_1	α_5
α_6	α_6	α_3	α_2	α_5	α_4	α_1

The internal subdivisions in the second table are to illustrate the salient features of this particular presentation of the information.

(d) α_1 is seen from the table to be the (unique) identity element.

(e) Pairs of mutual inverses are identified by the elements α_1 in the table. Thus α_4 and α_5 are each other's inverse; and each of the other 4 elements is its own inverse.

(f) To show that composition is not commutative it suffices to find one pair of functions whose compositions are different in the two orders. Here any two functions, both distinct from α_1, have that property: for example,

$$\alpha_2 \circ \alpha_3 = \alpha_5 \neq \alpha_4 = \alpha_3 \circ \alpha_2 \,.$$

(We shall see later in the course that, under function composition, these six functions constitute a *dihedral group of order 6*. Students familiar with complex numbers should observe that everything we have done makes sense if we interpret the functions as acting on the complex plane with the points 0 and 1 excluded.)

(g) We could, of course, prove laboriously that each of the elements of A is injective and surjective. We can also derive this information using the fact that each function has an inverse, by virtue of [8, Theorem 2.1(b)(d)]. Since the composition of α with its inverse — call it β — is α_1, which we know to be both injective and surjective, α has those properties also.

(h) Since $\alpha_4 \circ \alpha_4 = \alpha_5$, and $\alpha_4 \circ \alpha_5 = \alpha_1$, powers of α_4 can only take three different values: α_4, α_5, α_1; the same is true for α_5. Of the other elements, α_1 yields only itself under composition; the other 3 elements each yield either themselves or the identity, since each is its own inverse, so its square is the identity element. In no case do we obtain all 6 elements of A by repeated compositions. We say that the *group* $(A, \circ)$ is *not cyclic*.

(i) We will exhibit each of the elements of A as an iterated composition of α_2 and/or α_3: $\alpha_1 = \alpha_2 \circ \alpha_2$; $\alpha_2 = \alpha_2$; $\alpha_3 = \alpha_3$; $\alpha_4 = \alpha_3 \circ \alpha_2$; $\alpha_5 = \alpha_2 \circ \alpha_3$; $\alpha_6 = \alpha_2 \circ \alpha_3 \circ \alpha_2$. These factorizations are not unique; for example, α_6 can also be expressed as $\alpha_3 \circ \alpha_2 \circ \alpha_3$.

4. For each of the following sets and alleged operations,

- determine whether the alleged operation is, indeed, an operation;
- if it is an operation, determine whether the structure is a group;
- if the structure is a group, determine the identity element and the inverse of each element;

- if the structure is not a group, prove this fact convincingly.

(a) (all 2×2 matrices, matrix addition)

(b) (all 2×2 invertible[1015] matrix, matrix addition)

(c) $(\mathbb{R}, a * b = \max(a, b))$

(d) (non-negative integers, $m * n = \max(m, n)$)

(e) $(\mathbb{R}, a * b = 6(a + b))$

(f) $(\mathbb{Z}, a * b = a - b)$

Solution: In order to show that a group is defined, we have to prove

- that the set is closed under the given function
- that the function — now known to be an *operation* — is associative
- that this associative operation has an identity element
- that each element has an inverse

(a) **Closure:** The set of matrices is closed under matrix addition (cf. [8, Problem 5.16]); that is, the sum of two such matrices is another such 2×2 matrix.

Associativity:

$$\begin{aligned}
& \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right) \\
= & \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{bmatrix} \\
= & \begin{bmatrix} a_{11} + (b_{11} + c_{11}) & a_{12} + (b_{12} + c_{12}) \\ a_{21} + (b_{21} + c_{21}) & a_{22} + (b_{22} + c_{22}) \end{bmatrix} \\
& \text{by definition of matrix addition} \\
= & \begin{bmatrix} (a_{11} + b_{11}) + c_{11} & (a_{12} + b_{12}) + c_{12} \\ (a_{21} + b_{21}) + c_{21} & (a_{22} + b_{22}) + c_{22} \end{bmatrix} \\
& \text{by associativity of } + \text{ in } \mathbb{R} \\
= & \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \\
= & \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \right) + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}
\end{aligned}$$

[1015] *invertible* = *non-singular* = possessing an inverse

Identity element: As

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

the zero matrix serves as the identity element.

Inverses: As

$$\begin{aligned} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \end{aligned}$$

the inverse of $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is $\begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix}$; this latter is the matrix usually denoted by $-\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$.

(b) The sum of two invertible matrices need not be invertible. For example, the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ are both invertible — each is its own inverse. But their sum is the zero matrix, which does not have an inverse. Thus the set is not closed under the given function.

(c) The maximum function does indeed map pairs of real numbers on to a real number, so it is an *operation* on $\mathbb{R}$. However, this operation does not have an identity element, since such an element would have to be less than or equal to all real numbers.

(d) This example is similar to the preceding, but here there is an identity element: 0. Nevertheless, this is still not a group. In fact, the operation is associative. But there does not exist an inverse for every element. For example, there exists no element b such that $0 = \max(b, 1)$, so 1 does not have an inverse.

(e) This structure is not a group, since the operation is not associative. For certain values of a, b, c,

$$\begin{aligned} a * (b * c) &= 6(a + 6(b + c)) = 6a + 36b + 36c \\ \neq \quad 36a + 36b + 6c &= 6(6(a + b) + c) = (a * b) + c \end{aligned}$$

The inequality does not hold for all a, b, c; for example, it does not hold when $a = c$. However, there exist some sets of values for which the inequality

holds, and that is sufficient to support our claim that the operation is not associative. One such set of values is $a = b = 0$, $c = 1$.

(f) This operation is not associative.
For example $(1 - 1) - 1 = -1$, but $1 - (1 - 1) = 1$.

5. [8, Problem 5.22] Prove that if $(G, *)$ is a group, and elements a and b in G have the property that $a * b = b$, then a must be the identity element of the group.

Solution: Denote the identity element of the group by e. Then

$$\begin{aligned} a &= a * e \quad \text{since } e \text{ is the identity} \\ &= a * (b * b^{-1}) \quad \text{by definition of } b^{-1} \\ &= (a * b) * b^{-1} \quad \text{by associativity of } * \\ &= b * b^{-1} \quad \text{by hypothesis } a * b = b \\ &= e \quad \text{by definition of } b^{-1} \end{aligned}$$

C.2 Second 1998 Problem Assignment

1. (a) [8, Problem 7.14] Let $H = \{(1), (12)\}$, $K = \{(1), (123), (132)\}$. Both H and K are subgroups of S_3. Show that $H \cup K$ is not a subgroup of S_3. (cf. [8, Problems 7.13, 14.38]).

(b) [8, Problem 7.13] Prove that if H and K are subgroups of a group $(G, *)$, then $H \cap K$ is a subgroup of $(G, *)$.

Solution:

(a) The set $H \cup K$ is not closed under the operation of the group. (It is, however, closed under the taking of inverses.) For example, $(12)(123)$, the composition of two elements of the union, is (23), which is not an element of the union.

(b) To apply [8, Theorem 7.1] we prove that

i. $H \cap K$ **is not empty.** H and K, being subgroups, both contain the identity element, e. Consequently $e \in H \cap K$.

ii. $H \cap K$ **is closed under** $*$**.** This proof is given in greater detail than was expected of students.

$a \in H \cap K$	Premiss	(1033)
$b \in H \cap K$	Premiss	(1034)
$(a \in H) \wedge (a \in K)$	(1033), Definition of $\cap$	(1035)
$(b \in H) \wedge (b \in K)$	(1034), Definition of $\cap$	(1036)

$((a \in H) \wedge (a \in K)) \wedge ((b \in H) \wedge (b \in K))$	(1035), (1036) (by Rule of Conjunction)	(1037)
$((a \in H) \wedge (b \in H)) \wedge ((a \in K) \wedge (b \in K))$	(1037), properties of $\wedge$	(1038)
$(a * b \in H) \wedge (a * b \in K)$	(1038), closure of H, K under $*$	(1039)
$\therefore a * b \in H \cap K$	Definition of $\cap$	(1040)

As the foregoing argument is valid $\forall a \in H$ and $\forall b \in K$, the intersection is closed under $*$.

iii. $H \cap K$ **is closed under the taking of inverses (under $*$).** We present this proof in a slightly different format from the preceding.

$$\begin{array}{rll} & a \in H \cap K & \\ \Leftrightarrow & (a \in H) \wedge (a \in K) & \\ \Rightarrow & (a^{-1} \in H) \wedge (a^{-1} \in K) & \text{by closure of } H, K \text{ under inverses} \\ \Leftrightarrow & a^{-1} \in H \cap K & \text{by definition of } \cap \end{array}$$

2. Consider the graph $G = (\{1,2,3,4,5,6\}, \{12, 23, 34, 45, 56, 61\})$. (By 12 we mean the edge $\{1,2\}$; thus 12 and 21 denote the same edge.) Among the automorphisms of this graph (isomorphisms of the graph with itself) are the following: $\alpha = (12)(36)(45)$, $\beta = (14)(23)(56)$.

   (a) Determine the smallest group $\mathfrak{G}$ which contains these permutations of the vertices.

   (b) Express all elements of $\mathfrak{G}$ in both the "two-line" notation, and as products of disjoint cycles.

   (c) Give the Cayley table of $\mathfrak{G}$.

   (d) Determine a complete set of representatives for the equivalence classes of $\{1,2,3,4,5,6\}$ under the operation of $\mathfrak{G}$ (in the sense of [8, Theorem 9.2]).

   Solution:

   (a) A group containing α and β must contain their respective inverses; however, each of these permutations is its own inverse! The group must be closed under multiplication:

$$\begin{aligned} \alpha\beta &= (12)(36)(45)(14)(23)(56) = (153)(264) \\ \beta\alpha &= (14)(23)(56)(12)(36)(45) = (135)(246) \\ \alpha\beta\alpha &= (153)(264)(12)(36)(45) = (16)(25)(34) \end{aligned}$$

And, it must contain the identity. We shall see from the Cayley table below that these 6 elements do, indeed, form a subset that is closed under multiplication and the taking of inverses, and so must constitute a subgroup. Since the presence of these elements was a consequence of closure, this must be the smallest group. We call it the subgroup *generated by α and β*.

(b) The elements we have found are

$$\begin{aligned}
e &= (1)(2)(3)(4)(5)(6) = \begin{pmatrix} 1&2&3&4&5&6 \\ 1&2&3&4&5&6 \end{pmatrix} \\
\alpha &= (12)(36)(45) = \begin{pmatrix} 1&2&3&4&5&6 \\ 2&1&6&5&4&3 \end{pmatrix} \\
\beta &= (14)(23)(56) = \begin{pmatrix} 1&2&3&4&5&6 \\ 4&3&2&1&6&5 \end{pmatrix} \\
\alpha\beta\alpha &= (16)(25)(34) = \begin{pmatrix} 1&2&3&4&5&6 \\ 6&5&4&3&2&1 \end{pmatrix} \\
\alpha\beta &= (153)(264) = \begin{pmatrix} 1&2&3&4&5&6 \\ 5&6&1&2&3&4 \end{pmatrix} \\
\beta\alpha &= (135)(246) = \begin{pmatrix} 1&2&3&4&5&6 \\ 3&4&5&6&1&2 \end{pmatrix}
\end{aligned}$$

(c) This Cayley table has been encountered before, in §C.1.

$\circ$	e	$\alpha\beta$	$\beta\alpha$	β	α	$\alpha\beta\alpha$
e	e	$\alpha\beta$	$\beta\alpha$	β	α	$\alpha\beta\alpha$
$\alpha\beta$	$\alpha\beta$	$\beta\alpha$	e	α	$\alpha\beta\alpha$	β
$\beta\alpha$	$\beta\alpha$	e	$\alpha\beta$	$\alpha\beta\alpha$	β	α
β	β	$\alpha\beta\alpha$	α	e	$\beta\alpha$	$\alpha\beta$
α	α	β	$\alpha\beta\alpha$	$\alpha\beta$	e	$\beta\alpha$
$\alpha\beta\alpha$	$\alpha\beta\alpha$	α	β	$\beta\alpha$	$\alpha\beta$	e

(d) The group element (135)(246) and its powers map every vertex on to every other vertex whose label has the same parity; that is — 1 on to 1 or 3 or 5, and 2 on to 2 or 4 or 6. Thus $\{1, 3, 5\}$ and $\{2, 4, 6\}$ are subsets of equivalence classes. But, as 1 and 2 are equivalent by virtue of the automorphism (12)(36)(45), the equivalence classes containing 1 and 2 overlap; hence there is just one equivalence class, or *orbit*: V itself. We call a permutation group with a unique equivalence class *transitive*.

3. (a) [8, Problem 9.20] For polynomials $f(x)$ and $g(x)$ with real coefficients, let $f(x) \sim g(x)$ mean that $f'(x) = g'(x)$ (where the primes denote derivatives). Prove that $\sim$ is an equivalence relation on the set of all real polynomials, and give a complete set of equivalence class representatives.[1016]

   (b) [8, Problem 9.22] Find a flaw in the following "proof" that a relation $\sim$ on a set S is reflexive if it is both symmetric and transitive: Let $x \in S$. From $x \sim y$, by symmetry, we have $y \sim x$. By transitivity, $x \sim y$ and $y \sim x$ imply $x \sim x$. Therefore, $\sim$ is reflexive.

   Solution:

   (a) **Reflexivity** Since, for any polynomial, $f'(x) = f'(x)$, $f \sim f$.
   Symmetry

$$\begin{aligned} f \equiv g &\Leftrightarrow f' = g' \quad \text{Definition of } \equiv \\ &\Leftrightarrow g' = f' \\ &\Leftrightarrow g \equiv f \quad \text{Definition of } \equiv \end{aligned}$$

   Transitivity Suppose that $f \sim g$ and $g \sim h$. Then $f'(x) = g'(x)$ and $g'(x) = h'(x)$; accordingly $f'(x) = h'(x)$, i.e. $f \sim h$.

   There are infinitely many sets of equivalence class representatives. One such set consists of the set of polynomials with zero constant term. (By the Mean Value Theorem, $f' = g' \rightarrow f(x) = g(x) + \text{constant}$, i.e. f and g are identical, except possibly for their constant terms. This could be proved without use of the calculus, using (1041) as the definition of differentiation.)

   (b) The argument given is indeed valid, provided $\exists y \in S[x \sim y]$. If, however, x is not related to any other point in S, this reasoning is not sufficient to ensure that $x \sim x$. To demonstrate this, consider $S = \{x\}$, and define $\sim = \varnothing$. Then $\sim$ is symmetric and transitive, but not reflexive.

4. (a) [8, Problem 10.16] Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

   (b) [8, Problem 10.24] Prove that if a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

[1016] A polynomial with real coefficients is an expression of the form $a_0x^0 + a_1x^1 + a_2x^2 + ... + a_nx^n$, where a_0, a_1, ..., a_n are real numbers; its derivative, of course, is the polynomial

$$f'(x) = a_1x_0 + 2a_2x^1 + 3a_3x^2 + ... + na_nx^{n-1}\,. \tag{1041}$$

(c) [8, Problem 10.18] Prove or disprove: For all integers a, b, $n \neq 0$,

$$a \equiv b \pmod{n} \quad \Rightarrow \quad a^2 \equiv b^2 \pmod{n^2}\,.$$

(d) i. Prove by induction on non-negative integers m that $10^m \equiv 1 \pmod{3}$ and that $10^m \equiv 1 \pmod{9}$.

ii. Then use these facts to argue that

$$\sum_{m=0}^{n} a_m 10^m \equiv \sum_{m=0}^{n} a_m \pmod{q} \tag{1042}$$

where $q = 3$ or $q = 9$.

iii. Explain how this justifies the divisibility tests

$$q| \sum_{m=0}^{n} a_m 10^m \Leftrightarrow q| \sum_{m=0}^{n} a_m$$

for $q = 3$ and $q = 9$.

iv. Generalize these ideas to develop a test for divisibility of a decimal integer $\sum_{m=0}^{n} a_m 10^m$ by 11.

Solution:

(a)

$$\begin{aligned}
a \equiv b \pmod{n} &\quad \text{Premiss} &(1043)\\
c \equiv d \pmod{n} &\quad \text{Premiss} &(1044)\\
\exists q[a - b = qn] &\quad (1043), \text{ definition of } \equiv &(1045)\\
\exists s[c - d = sn] &\quad (1044), \text{ definition of } \equiv &(1046)\\
ac - bd &= (qn + b)(sn + d) - bd &\\
&= n(qsn + bs + qd) \quad \text{by (1045), (1046)} &(1047)\\
\therefore ac \equiv bd \pmod{n} &\quad (1047), \text{ definition of } \equiv &(1048)
\end{aligned}$$

(b) By [8, Theorem 10.2], a is congruent to precisely one of the integers 0, 1, 2, ..., 7 modulo 8; i.e. there exists an integer $r \in \{0, 1, ..., 7\}$ such that $a = 8q + r$, where $q \in \mathbb{Z}$. When $r \in \{0, 2, 4, 8\}$, $2|a$; hence $r \in \{1, 3, 5, 7\}$. Then

$$\begin{aligned}
(8q + 1)^2 &= 64q^2 + 16q + 1 = 8(8q^2 + 2q) + 1 \equiv 1 \pmod{8}\\
(8q + 3)^2 &= 64q^2 + 48q + 1 = 8(8q^2 + 6q) + 1 \equiv 1 \pmod{8}\\
(8q + 5)^2 &= 64q^2 + 80q + 1 = 8(8q^2 + 10q) + 1 \equiv 1 \pmod{8}\\
(8q + 7)^2 &= 64q^2 + 112q + 1 = 8(8q^2 + 14q) + 1 \equiv 1 \pmod{8}
\end{aligned}$$

A more elegant approach might have been to square $a = 2k + 1$, obtaining $a^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$, and to observe that at least[1017] one of k, $k + 1$ is even, so $8|4k(k + 1)$, and $a^2 \equiv 1 \pmod 8$.

(c) Squaring of both sides of a congruence is justified by part (a), taking $c = a$, $d = b$; thus

$$a \equiv b \pmod n \quad \Rightarrow a^2 \equiv b^2 \pmod n$$

Note that the modulus is n, not n^2. A counterexample to the square modulus is $4 \equiv 1 \pmod 3$, but $4^2 \not\equiv 1^2 \pmod{3^2}$.[1018]

(d) i. Let $P(m)$ denote the statement $10^m \equiv 1 \pmod 9$. $P(0)$ is true, since $10^0 - 1 = 0 = 0 \cdot 9$. Now suppose that $P(m)$ is true. Then we *would like* to apply part (a) to the congruences $P(m)$ and $P(1)$, obtaining $10^{m+1} \equiv 1 \cdot 1 \pmod 9$, which is $P(m+1)$. However, we do not yet have the right to use $P(1)$; its truth cannot be established from $P(0)$ alone. So we prove $P(1)$, by observing that $10 - 1 = 9$, evidently a multiple of 9. Now that $P(1)$ has been established, we may derive $P(m + 1)$ from $P(m)$ for all $m \geq 1$, so we have completed the induction step. By transitivity of divisibility [8, Problem 10.13] since $3|9$ and $9|(10^m - 1)$, $3|10^m - 1$.

ii. We have proved above and in part (a) that congruences to the same modulus can be added and multiplied. We may multiply a congruence $10^m \equiv 1$ by $a_m \equiv a_m$, to obtain $a_m 10^m \equiv a_m$, and then sum over m, to obtain (1042).

iii. An integer N is divisible by q iff $N \equiv 0 \pmod q$. Hence, when $q = 3, 9$, divisibility of a decimal integer is equivalent to divisibility of the sum of its decimal digits. This summing of the decimal digits may be iterated. Thus, for example, we know that $9|182798847$ since $1+8+2+7+9+8+8+4+7 = 54$, and $5 + 4 = 9 \equiv 0 \pmod 9$.

iv. Modulo 11, $10 \equiv -1$, so $\sum_{m=0}^{n} a_m 10^m \equiv \sum_{m=0}^{n} a_m (-1)^m \equiv a_0 - a_1 + a_2 - a_3 + ...$ An integer is divisible by 11 iff the alternating sum of its digits in decimal representation is also a multiple of 11.

5. Let n be a positive integer. Show that $\mathbb{Z}_n^\#$ [8, Page 68] is not closed under the operation $\odot$ if n is a positive integer which is not prime.

Solution: If $n = ab$, where $a > 1$ and $b > 1$, then $[a]$ and $[b]$ are elements of $\mathbb{Z}_n^\#$ whose product is $[a] \odot [b] = [ab] = [n] = [0] \notin \mathbb{Z}_n^\#$.

[1017] in fact, exactly one

[1018] Note that 3 is the "best possible" modulus for a counterexample, since we cannot find a counterexample with modulus 2. This is because $b \equiv -b \pmod 2$, since $2b \equiv 0 \pmod 2$. Hence, if $a \equiv b \pmod 2$, $a \equiv -b \pmod 2$, by transitivity of $\equiv$. Hence the product $a^2 - b^2 = (a + b)(a - b)$ is divisible by 2^2. Indeed, we have proved in part (b) that, when $a \equiv 1 \pmod 2$, $a^2 \equiv 1^2 \pmod{2^3}$.

6. [8, Corollary to Theorem 12.2] states that

   > *If a and b are integers, then $(a, b) = 1$ iff there are integers m and n such that $am + bn = 1$.*

   Apply this result to prove [8, Problem 12.20] that, if $(a, m) = 1$, there is a solution x to the congruence $ax \equiv b \pmod{m}$. In particular, show that, for any fixed positive prime p, every element of $\mathbb{Z}_p^{\#}$ possesses an inverse relative to the operation $\odot$.

   Solution: We apply [8, Corollary to Theorem 12.2], taking $b := m$, and using the symbol ℓ for the symbol m of the Theorem. There thus exist integers ℓ and n such that $a\ell + mn = 1$; hence, multiplying by b, $a(\ell b) + m(bn) = b$. If we define $x = \ell b$, we have

   $$ax = b + (-bn)m \equiv b \pmod{m}\,.$$

   Any element of $\mathbb{Z}_p^{\#}$ is of the form $[a]$, where $1 \leq a \leq p-1$. As $(a, p) = 1$, there will exist an element x such that $ax \equiv 1 \pmod{p}$, hence $[a] \odot [x] = [1]$, by definition of $\odot$. As $\odot$ is commutative, $[x]$ is thus an inverse of $[a]$ relative to the operation $\odot$.

7. (cf. [8, Problem 11.11]) Let n be an integer greater than 1.

   (a) Show that $[1]$ is the identity element for $(\mathbb{Z}_n, \odot)$.

   (b) Show that there is no inverse for $[0]$ in $(\mathbb{Z}_n, \odot)$.

   Solution:

   (a) For any $[a] \in \mathbb{Z}_n$, $[a] \odot [1] = [a1] = [a] = [1a] = [1] \odot [a]$.

   (b) Suppose that $[a]$ were an inverse of $[0]$. Then we would have $[a] \odot [0] = [1]$, which implies $[a0] = [1] \Rightarrow [0] = [1] \Rightarrow n|(1 - 0)$, which is a contradiction. (Why did we have to require $n > 1$?)

C.3 Third 1998 Problem Assignment

Distribution Date: *Caveat lector!* Some solutions may contain misprints.

1. [8, Problem 13.12] For a positive integer n with standard decomposition $n = \prod_{i=1}^{k} p_i^{e_i}$, where $\{p_1, p_2, ..., p_k\}$ is a set of k (distinct) positive primes, define

   $$\mathfrak{D}(n) = \{d | (d \in \mathbb{N}) \wedge (d|n)\}\,.$$

Determine $|\mathfrak{D}(n)|$, the number of positive integral divisiors of n (cf. [8, Problem 13.11]).

Solution: By [8, Problems 13.5, 13.6], the positive integral divisors d of n have the form $d = \prod_{i=1}^{k} p_i^{f_1}$, where $0 \leq f_i \leq e_i$ $(i = 1, 2, ..., k)$; and, conversely, any product of this type is evidently a positive integer divisor of n. The set of positive divisors may thus be put into one-to-one correspondence with the Cartesian product

$$\{0, 1, ..., f_1 - 1, f_1\} \times \{0, 1, ..., f_2 - 1, f_2\} \times \cdots \times \{0, 1, ..., f_k - 1, f_k\}$$

whose cardinality is evidently $(e_1 + 1) \times (e_2 + 1) \times ... \times (e_k + 1)$.

2. (a) Prove that $\sqrt{7}$ is not rational. [Hint: Assume that

$$\sqrt{7} = \frac{n}{m}\,, \tag{1049}$$

where n and m are integers and $(n, m) = 1$, and show that this leads to a contradiction.]

(b) Show, in your solution to the previous part, why your argument would not hold for $\sqrt{9}$.

Solution:

(a) If $\sqrt{7}$ were rational, then there would exist integers n and m such that $\sqrt{7} = \frac{n}{m}$, so $n^2 = 7m^2$. Then $7\,|n^2$. Let $|n| = \prod_{i=1}^{k} p_i^{e_1}$ be the standard decomposition of $|n|$, so

$$n^2 = \prod_{i=1}^{k} p_i^{2e_1} = 7m^2 \tag{1050}$$

is the standard decomposition of n^2. As $7|n^2$, 7 must be one of the primes in the set $\{p_1, p_2, ..., p_k\}$ — without limiting generality, call it p_1 — and the corresponding exponent — e_1 — must be positive. It follows from (1050) that

$$7^{2e_1 - 1} \times \prod_{i=2}^{k} p_i^{2e_1} = m^2 \tag{1051}$$

so $7|m^2$. The same reasoning applied to m shows that $7|m$ also. But now 7 is a common divisor of both n and m, contradicting the hypothesis that $(n, m) = 1$. We conclude that (1049) was impossible, i.e. that 7 is not rational.

(b) Where, above, we asserted that $7|n^2 \Rightarrow 7 \in \{p_1, p_2, ..., p_k\}$, we can here assert only that $3^2|n^2 \Rightarrow 3 \in \{p_1, p_2, ..., p_k\}$, and could, without limiting generality, take $p_1 = 3$, and $e_1 \geq 1$. If, however, $e_1 = 1$ exactly, we cannot continue to prove that $3|m$.

3. (a) [8, Problem 14.26] There is only one way to complete the following Cayley table so as to get a group. Find it. Why is it unique? ([8, Problem 5.22] may help.)

$*$	a	b	c
a		b	
b			
c			

[In solving this problem at this time it is intended that you not use any material from beyond §14 of the textbook. However, when you reread this problem before the examination, you might wish to ask whether you can now solve the problem in a simpler way.]

(b) There is only one way to complete the following Cayley table so as to get a group. Find it, explaining every step of your work.

$*$	a	b	c	d
a				
b		a		
c		b		
d				

[Here again, when you reread this problem before the examination, you should try to find a quick solution that uses material beyond [8, §14]; in this case [8, §17] will suffice.]

Solution:

(a) Since $a*b = b$, $a = a*e = a*(b*b^{-1}) = (a*b)*b^{-1} = b*b^{-1} = e$. The table is now

$*$	a	b	c
a	a	b	c
b	b		
c	c		

. What can be the value of $b*b$? By [8, Theorem 14.1], every element of the group appears in the second row of the table exactly once. As b has already appeared, $b*b$ is either a or c; but, if it were a, then the only value remaining for $b*c$ would be c, which would imply, by a similar computation to that given above, that $b = e$; this contradicts the proven fact that $a = e$. We

conclude that the table may be completed as far as

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c		

. Now we can complete the third row by chosing, in the two vacancies, the only available element for the respective columns:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

.

[If we had available [8, Corollary to Lagrange's Theorem, §17], we could immediately assert that the group is isomorphic to $\mathbb{Z}_3$. Once we had determined that $a = e$ we could then assert that the table is as determined above, since, in $\mathbb{Z}_3$, each non-identity element is the square of the other, etc.]

(b) As a first step we can argue, as above, that $c = e$; this gives the third row and third column of the table:

$*$	a	b	c	d
a			a	
b		a	b	
c	a	b	c	d
d			d	

. In the second row of the table elements c and d are missing; we cannot place d in the fourth column, for it would follow from $b * d = d$ that $b = e$, and we know that $c = e$. Hence d appears in the first column, and so c appears in the fourth column:

$*$	a	b	c	d
a			a	
b	d	a	b	c
c	a	b	c	d
d			d	

. The fourth column is now lacking a and b; but a cannot be placed in the first row, since there is already an a there; the table has now developed to

$*$	a	b	c	d
a			a	b
b	d	a	b	c
c	a	b	c	d
d			d	a

. We may continue in various ways. For example, the first row requires a d, which cannot be placed in the first column, as it already contains a d. Hence the first row may be completed to

$*$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d			d	a

. All that remain to be supplied are the entries in the fourth row, and there is no

choice, since there is one missing column entry in each case. The completed Cayley table is

$*$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

.

[Had we more machinery available at this stage, the problem would have been easier to solve. For, after proving that c is the identity, we then observe that $b*b = a \neq e$, i.e. that b is an element distinct from the identity, whose order is not 2. In a group of order 4 the only available orders for elements are divisors of 4, viz. 1, 2, 4 [8, Corollary to Lagrange's Theorem, §17]. Hence b has order 4, which is the order of the group. Thus the group must be cyclic, generated by b. We know that $b^4 = e = c$, so the only possible exponent which will yield d is $b^3 = d$, and we have enough information to complete the table.]

4. [8, Problems 14.30, 14.31, 14.32]

   (a) Define what is meant by the *order* of an element of a group.

   (b) Prove that, for any element a of any group G, a and a^{-1} have the same orders.

   (c) Prove that, for any elements a and b of any group G, a and $b^{-1}ab$ have the same orders.

   (d) Prove that, for any elements a and b of any group G, ab and ba have the same orders. [Hint: Remember, G need not be Abelian!]

   Solution:

   (a) [8, p. 81] If the set $S = \{n | (n \in \mathbb{Z}) \wedge (n > 0) \wedge (a^n = e)\}$ is non-empty, then the order of a is its least element (whose existence is asserted in the Least Integer Principle). If $S = \varnothing$, then a is said to be *of infinite order*.

   (b) Suppose that a has finite order n. Then, by the usual exponent rules, $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. Hence there exist positive powers of a^{-1} which are equal to e, so a^{-1} has finite order also; define order$(a^{-1}) = m$. By [8, Theorem 14.3(b)] $m|n$. But, as $a^m = \left((a^{-1})^m\right)^{-1} = e^{-1} = e$, $n|m$, again by [8, Theorem 14.3(b)]. We conclude that $m = n$.

   The preceding argument shows that if either a or its inverse has finite order, then the other has the same finite order. There remains the possibility that neither has finite order; this is the case that is called *infinite order*, so here again both will have the same order. $\square$.

(c) For any positive integer n, $(b^{-1}ab)^n = b^{-1}a^nb$; (this can be proved by induction). Hence, if a has finite order n, then $(b^{-1}ab)^n = b^{-1}eb = e$, so $b^{-1}ab$ has finite order, which divides n; call its order m. Then, if $(b^{-1}ab)^m = e$, $b^{-1}a^mb = e$, so, multiplying both sides of the equation on the left by b, and on the right by b^{-1}, we obtain that $a^m = beb^{-1} = e$, so $n|m$. It follows again that $m = n$. This also shows that, if $b^{-1}ab$ has finite order m, then a has finite order, which must be equal to m.

In the remaining case both a and $b^{-1}ab$ have infinite order. □

(d) Since $a^{-1}(ab)a = ba$, the preceding problem, with $b := a$, $a := ab$, ensures that ab and ba have the same orders.

5. (a) [8, Problem 15.13] The subgroup $G = \langle(1234), (24)\rangle$ of S_4 has order 8. Showing all your work, determine the elements of the subgroup, expressing each of them as a product of disjoint cycles.

(b) Determine the left and right cosets of G in S_4.

Solution:

(a) Forming the powers of (1234) we have,

$$\langle(1234)\rangle = \{(1234), (13)(24), (1432), e\},$$

all 4 of which must be elements of G. Multiplying each of these elements on the left by (24) yields

$$\begin{aligned}(24)\langle(1234)\rangle &= \{(24)(1234), (24)(13)(24), (24)(1432), (24)e\}\\ &= \{(14)(23), (13), (12)(34), (24)\}\end{aligned}$$

As we are told that the group has order 8, we have all its elements. (Without this information, we could have laboriously determined the Cayley table to show that the set is closed under composition and the taking of inverses.)

(b)

$$\begin{aligned}G &= \{(1234), (13)(24), (1432), e, (14)(23), (13), (12)(34), (24)\}\\ (12)G &= \{(12)(1234), (12)(13)(24), (12)(1432), (12)e,\\ &\qquad (12)(14)(23), (12)(13), (12)(12)(34), (12)(24)\}\\ &= \{(234), (1324), (143), (12), (1423), (132), (34), (124)\}\\ (14)G &= \{(14)(1234), (14)(13)(24), (14)(1432), (14)e,\\ &\qquad (14)(14)(23), (14)(13), (14)(12)(34), (14)(24)\}\\ &= \{(123), (1342), (243), (14), (23), (134), (1243), (142)\}\end{aligned}$$

As we have listed 3 disjoint left cosets, each containing 8 elements, the 24 elements we have in all constitute the entire group S_4 of order 4!. We repeat the computations for right cosets:

$$\begin{aligned} G &= \{(1234), (13)(24), (1432), e, (14)(23), (13), (12)(34), (24)\} \\ G(12) &= \{(1234)(12), (13)(24)(12), (1432)(12), e(12), \\ &\qquad (14)(23)(12), (13)(12), (12)(34)(12), (24)(12)\} \\ &= \{(134), (1423), (243), (12), (1324), (123), (34), (142)\} \\ G(14) &= \{(1234)(14), (13)(24)(14), (1432)(14), e(14), \\ &\qquad (14)(23)(14), (13)(14), (12)(34)(14), (24)(14)\} \\ &= \{(234), (1243), (132), (14), (23), (143), (1342), (124)\} \end{aligned}$$

While G is both a left and a right coset, no other left (respectively, right) coset is also a right (respectively, left) coset.

6. It is known [8, Problem 17.25] that, if H is a subgroup of index 2 in a group G, then the product of two elements of G not in H must be in H. Use that fact to complete the following solution to [8, Problem 17.28], that A_4 contains no subgroup of order 6.

   > Suppose that some element of $a \in A_4$ of the form $(\bullet\ \bullet\ \bullet)(\bullet)$ is not in a subgroup H of index 2. Then $a^2 \in A_4$. But $a = a^4 = (a^2)^2$ is then the product of two elements of H, so it also is in H, a contradiction. We conclude that H, if it existed, would contain *all* elements of the given form. However, there are precisely $\binom{4}{3}(3-1)! = 8$ such elements; and $|H| = 6 < 8$.

   The preceding proof is only a sketch. Write it out carefully, explaining each of the steps; you may appeal to [8, Problem 17.25] without proof.

   This serves as a counterexample to the converse of [8, First Corollary to Lagrange's Theorem, p. 92]: while the order of a subgroup must divide the order of the parent group, there may exist divisors of the order of the parent group which are not the order of any subgroup.

   Solution: Suppose that H is a subgroup of A_4 of order 6, and that some element of $a \in A_4$ of the form $(\bullet\ \bullet\ \bullet)(\bullet)$ is not in H. By [8, Problem 17.25], $aa \in H$; since H is closed under composition, $(aa)(aa) \in H$. But, as a is a 3-cycle, its cube is e; so its 4th power, shown to be in H, is equal to a. This contradicts the hypothesis that $a \notin H$. From this contradiction we conclude that H, if it existed, could not contain any element of the given form. However, there are precisely $\binom{4}{3}(3-1)! = 8$

such elements; it none is in H, then there remain only 4 candidates of A_4 for membership in H, which is fewer than 6.

7. [8, cf. Problem 17.26] Give examples to show that there is a subgroup of S_4 of order d for each of the positive divisors of $|S_4|$.

   Solution: The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24. Students were asked only for one example of each type, but we give an exhaustive list below. Students were not expected to provide such an exhaustive list, just one example of each order.

   Subgroups of order 1. There is only one subgroup of order 1 in any group — the subgroup $\{e\}$.

   Subgroups of order 2. As 2 is prime, any subgroup of order 2 is cyclic, generated by an element of order 2. The disjoint cycle decomposition of an element of order 2 must consist only of cycles of lengths 1 (i.e. fixed points) and 2; thus, in S_4, these are precisely the elements of types $(\bullet\bullet)(\bullet\bullet)$ and $(\bullet\bullet)(\bullet)(\bullet)$. There are $\frac{\binom{4}{2}}{2} = 3$ elements of the first type, and $\binom{4}{2} = 6$ of the second type. Thus there are 9 subgroups of order 2; for example, $\langle(12)(3)(4)\rangle$.

   Subgroups of order 3. As 3 is prime, subgroups of this order are also cyclic, each being generated by an element of order 3. All elements of order 3 have disjoint cycle decomposition of the form $(\bullet\ \bullet\ \bullet)(\bullet)$. There are $\binom{4}{3}(3-1)! = 8$ such elements, and each subgroup of order 3 contains exactly 2 of them. Thus there are 4 subgroups of this order; for example, $\langle(123)\rangle$.

   Subgroups of order 4. There are two different types of groups of order 4, and both can occur as subgroups of S_4.

      Cyclic subgroups of order 4. These are generated by an element of order 4, which must be a 4-cycle. Each such subgroup contains 2 such 4-cycles. The number of such subgroups is $\frac{1}{2}3! = 3$; one is $\langle(1234)\rangle = \{(1234), (13)(24), (1432), e\}$.

      Non-cyclic subgroups of order 4. These subgroups consist of 3 elements of order 2 and the identity. There are 2 different types; there are 3 like (we give one example) $\{(12), (34), (12)(34), e\}$; and one of a different type, $\{(12)(34), (13)(24), (14)(23), e\}$

   Subgroups of order 6. There are only two isomorphism types of groups of order 6 — $\mathbb{Z}_6$, and the group S_3 or, equivalently (i.e. isomorphic to it) D_3.

      Cyclic subsgroups of order 6. These groups have to be generated by an element of order 6. But none of the elements of S_4 has order 6. Thus there are no cyclic subgroups of S_4 of order 6.

Non-cyclic subgroups of order 6. It can be shown that the only subgroups of this type are the symmetric subgroups on subsets of 3 elements of $\{1,2,3,4\}$. Thus there are $\binom{4}{3} = 4$ of these; for example

$$\{(123),(132),(12),(23),(13),e\}$$

Subgroups of order 8. There are, in fact 5 different isomorphism types of groups of order 8; but not all of these can occur as the isomorphism type of a subgroup of S_4.

Cyclic subgroups of order 8. No element of S_4 has order 8; there are no subgroups of this type.

Subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. There are no subgroups of this type.

Subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. There are no subgroups of S_4 of this type.

Subgroups isomorphic to D_4. There are 3 of these

$$\{(1234),(13)(24),(1432),e,(12)(34),(13),(23)(14),(24)\}$$

$$\{(1243),(14)(23),(1342),e,(12)(34),(14),(24)(13),(23)\}$$

$$\{(1423),(12)(34),(1324),e,(14)(23),(12),(12)(34),(34)\}$$

Subgroups isomorphic to the "Quaternion" Group. This group contains 6 elements of order 4, 1 of order 2, and e. There are precisely $(4-1)! = 6$ elements of order 4 in S_4, but any set containing them all contains, for example, $(1234)(1243) = (132)$, of order 3; no such element can be present in a group of order 8. Hence there are no quaternion subgroups of S_4.

Subgroups of order 12. The only subgroup of S_4 of order 12 is the alternating group, A_4.

Subgroups of order 24. The only subgroup of order 24 is S_4 itself.

C.4 Fourth 1998 Problem Assignment

1. (cf. [8, Problem 18.13]) It is claimed that, for any positive integers m and n, functions

$$\theta : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \tag{1052}$$

$$\psi : \mathbb{Z}_m \to \mathbb{Z}_n \tag{1053}$$

can be defined by $\theta([a]_{mn}) = ([a]_m, [a]_n)$ and $\psi([a]_m) = [a]_n$.

(a) Show that θ is well defined; that is, that the information given above is sufficient to always determine the image on to which an element of the domain is to be mapped.

(b) Show that θ will not be onto when $(m,n) = d > 1$. (Hint: Show that $([1]_m, [0]_n)$ will never be the image of a point of $\mathbb{Z}_{mn}$. You may wish to use [8, Corollary to Theorem 12.2] the fact that $(m,n) = 1 \Leftrightarrow \exists (r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ such that $rm + sn = 1$.)

(c) Show that, when $m = 2$ and $n = 3$, θ is an isomorphism. (You may wish to denote the operation of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$ by $\#$.)

(d) Show that the "definition" of ψ is ambiguous[1019] unless $n|m$. (Hint: Consider the action that ψ is supposed to have on $[a + km]_n$.)

(e) Show that, when $n|m$, ψ is indeed well defined, and is a surjective function.

Solution:

(a) For the "function" to be well defined we must know, without ambiguity, what is the image of any element of $\mathbb{Z}_{mn}$. These elements are all *residue classes modulo* m; i.e. they are subsets of $\mathbb{Z}$ of the form $\{a+km : k \in \mathbb{Z}\}$; equivalently, they are cosets of the subgroup $m\mathbb{Z}$ (also denoted by (m)) in the group $\mathbb{Z}$. The "definition" above has been given in terms of the representative a chosen for the element $[a]_{mn}$. There is no ambiguity in the meaning of $[a]_m$ or $[a]_n$. The difficulty is in the fact that, had we selected a different representative — call it a' — for the class $[a]_{mn}$ — we might have obtained a different image point. We show that is not the case.

$$\begin{aligned}
& [a']_{mn} = [a]_{mn} \\
\Rightarrow\ & a' = a + kmn \quad \text{for some } k \in \mathbb{Z} \\
\Rightarrow\ & [a']_m = [a + kmn]_m = [a]_m \oplus [(kn)m]_m \quad \text{by definition of } \oplus \\
\Rightarrow\ & [a']_m = [a]_m \oplus [0]_m \quad \text{by definition of } [0]_m \\
\Rightarrow\ & [a']_m = [a + 0]_m = [a]_m \quad \text{by definition of } \oplus
\end{aligned}$$

and, similarly, it may be shown that, if $[a']_{mn} = [a]_{mn}$, then $[a']_n = [a]_n$ $\square$.

(b) Suppose that $(m,n) = d > 1$. Then the hint suggests we prove that there is no $a \in \mathbb{Z}$ such that

$$[a]_m = [1]_m \tag{1054}$$
$$[a]_n = [0]_n\,. \tag{1055}$$

[1019] We say that the function is then *ill defined* or is *not well defined*.

It would follow from (1055) that $n|a$, i.e. that there exists an integer s such that $a = sn$. But then (1054) would imply that $m|(1 - sn)$, i.e. that there exists an integer r such that $rm = 1 - sn$, i.e. that $rm + sn = 1$, which is equivalent to $(m, n) = 1$, contradicting the hypothesis.

(c) To show that θ is one-to-one and onto it is easiest, in this "small" case, to simply tabulate the values of $\theta([a]_6)$ as $[a]_6$ ranges over the 6 elements of $\mathbb{Z}_6$.

$[a]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$\theta([a]_6)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([2]_2, [2]_3)$ $= ([0]_2, [2]_3)$	$([3]_2, [3]_3)$ $= ([1]_2, [0]_3)$	$([4]_2, [4]_3)$ $= ([0]_2, [1]_3)$	$([5]_2, [5]_3)$ $= ([1]_2, [2]_3)$

We observe that the 6 image points are all different, and (equivalently) are the 6 elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$; θ is both injective and surjective, i.e. is a bijection. To complete the proof we observe that

$$\begin{aligned} & \theta([a]_6 \oplus [b]_6) \\ = \ & \theta([a+b]_6) \quad \text{by definition of } \oplus \text{ in } \mathbb{Z}_6 \\ = \ & ([a+b]_2, [a+b]_3) \quad \text{by definition of } \theta \\ = \ & ([a]_2 \oplus [b]_2, [a]_3 \oplus [b]_3) \quad \text{by definitions of } \oplus \text{ in } \mathbb{Z}_2, \mathbb{Z}_3 \\ = \ & ([a]_2, [a]_3) \# ([b]_2, [b]_3) \quad \text{by definition of } \# \\ = \ & \theta([a]_2) \# \theta([b]_3) \end{aligned}$$

(d) For ψ to be well defined by (1053) we require that, whenever $[a']_m = [a]_m$, $[a']_n = [a]_n$. For a given residue class $[a]_m$, such an a' must be of the form $a' = a + km$. Then $[a']_n = [a + km]_n = [a]_n \oplus [km]_n$, by definition of $\oplus$; so, for this to equal $[a]_n$, it will be necessary that $[km]_n = [0]_n$, i.e. that

$$n|km \tag{1056}$$

where (1056) must hold for all $k \in \mathbb{Z}$. In particular, taking $k = 1$, we have that $n|m$.

(e) Now suppose that $n|m$. If $[a']_m = [a]_m$, $m|(a' - a)$. But then, from $n|m$ and the transitivity of the relation $|$, $n|(a' - a)$, so $[a']_n = [a]_n$. Thus ψ is well defined.

Any element of $\mathbb{Z}_n$ is a congruence class of the form $[a]_n$, which, by definition of ψ, is equal to $\psi([a]_m)$. Thus ψ is surjective.

2. [8, Problem 19.8] Prove that the following groups are not isomorphic:

$$\mathbb{Z}_8 \times \mathbb{Z}_4 \qquad \text{and} \qquad \mathbb{Z}_{16} \times \mathbb{Z}_2 \, .$$

Solution: As the two underlying sets both have 32 elements, there certainly can exist bijections between them. Both of the groups are Abelian, and neither is cyclic.

Thus we cannot appeal to [8, Theorem 19.1(a)(b)(c)]. The element $([1]_{16}, [0]_2)$ of $\mathbb{Z}_{16} \times \mathbb{Z}_2$ has order 16; convince yourself of this by listing the iterated sums of this element with itself. But, in $\mathbb{Z}_8 \times \mathbb{Z}_4$, the sum of 8 copies of any element is the identity, so, by [8, Theorem 14.3(b)], all elements have orders that divide 8, so none has order 16.

3. Showing all your work, determine which of the following are rings.

   (a) The set of 2×2 matrices with integer entries[1020], of the form $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$, where $a, b, c \in \mathbb{Z}$. The operations of the ring are to be the familiar operations of matrix addition and matrix multiplication.

   (b) [8, Problem 22.8] The set of *non-singular* 2×2 matrices with real entries[1021], of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, where $a, b, c \in \mathbb{R}$. As in the preceding problem, the operations of the ring are to be the familiar operations of matrix addition and matrix multiplication.

   Solution:

   (a) This set is not closed under matrix multiplication. for example,

   $$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

   which is not in the set.

   (b)

   $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} = \begin{bmatrix} a+d & b+e \\ 0 & c+f \end{bmatrix}$$

   so the sum of two "upper triangular" matrices is again upper triangular, and

   $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} = \begin{bmatrix} ad & ae+bf \\ 0 & cf \end{bmatrix}$$

   so the product of upper triangular matrices is again upper triangular; also, that the negative of an upper triangular matrix is again upper triangular. If the set under consideration consisted simply of upper triangular matrices — which was the version of the problem in the textbook — they would constitute

[1020] i.e. the subset of the ring denoted by $M(2, \mathbb{Z})$

[1021] i.e. the subset of the ring denoted by $M(2, \mathbb{R})$

a subring, of $M(2,\mathbb{R})$, by [8, Theorem 22.2], However, the set under consideration here is restricted to *non-singular*, real, upper triangular matrices. This set is *not* closed under addition; for example, the zero matrix, which is the sum of the identity matrix and its (additive) inverse, is singular! Thus this set is *not* a subring of the ring $M(2,\mathbb{R})$.

4. [8, Problem 22.11] The ring $\mathbb{Z}[\sqrt{7}]$ is defined to be the subring of $\mathbb{R}$ consisting of numbers of the form $a + b\sqrt{7}$, where $a, b \in \mathbb{Z}$. Assuming that this is indeed a subring[1022], prove that $\mathbb{Z}[\sqrt{7}]$ is an integral domain.

   Solution: Suppose that $a, b, c, d \in \mathbb{Z}$, and that

   $$(a + b\sqrt{7})(c + d\sqrt{7}) = 0\,. \tag{1057}$$

   We must show that either $a = b = 0$, or else $c = d = 0$. If $ad + bc \neq 0$, then $\frac{ac+7bd}{-ad-bc} = \sqrt{7}$. This contradicts the fact that $\sqrt{7}$ is irrational, proved in the preceding assignment. We conclude that

   $$ad + bc = 0\,. \tag{1058}$$

   Then it follows from (1057) that

   $$ac + 7bd = 0\,. \tag{1059}$$

   If a and b are not both zero, then we have a non-zero vector solution $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$ to the equation

   $$\begin{bmatrix} d & c \\ c & 7d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

   implying that the matrix of coefficients is singular, i.e. that

   $$7d^2 - c^2 = \det \begin{bmatrix} d & c \\ c & 7d \end{bmatrix} = 0$$

   But, if $d \neq 0$, this equation would again imply that $\sqrt{7} = \pm\frac{c}{d}$, again a contradiction. We conclude that $d = 0$, hence also $c = 0$. We have thus proved that the ring $\mathbb{Z}[\sqrt{7}]$ is an integral domain.

5. [8, Problem 23.17]

   (a) Show that the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not a field.

[1022] You should be able to establish this fact, but are not being asked here to do that.

(b) Explain why this is not in conflict with the claim (cf. [8, Example 23.1]) that the following tables define a field:

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

·	00	01	10	11
00	00	00	00	00
01	00	11	01	10
10	00	01	10	11
11	00	10	11	01

(We have abbreviated the element $([a]_2, [b]_2)$ to ab. You are not required to verify that the tables do, indeed, define a field.)

(c) [8, Problem 23.18] Generalize from the foregoing to prove that the direct sum[1023] of two fields is never a field. (You may assume that the zero element in the direct sum is $(0, 0)$, and that the unity element is $(1, 1)$ — remembering, of course, that the 0 and 1 which appear in the first coordinate refer to the first summand, and those in the second coordinate refer to the second summand — yet another example where we use the same symbol to denote different objects.)

Solution:

(a) We exhibit a pair of zero divisors:

$$([1]_2, [0]_2)([0]_2, [1]_2) = ([1 \cdot 0]_2, [0 \cdot 1]_2) = ([0]_2, [0]_2)\,, \tag{1060}$$

the zero element (additive identity) of the ring.

(b) The additive structures of the ring and of the field defined by the tables are the same: they are both the Abelian group known as the *Klein 4-group*. The multiplicative structure — i.e. the operation of multiplication — is defined differently in the two cases. While it is associative and commutative in both cases, the operation given by the tables has the property that there are no zero divisors.

(c) As in equation (1060), the product of ordered pairs $(1, 0)$ and $(0, 1)$ will always be $(0, 0)$, which is the zero element of the direct sum.

This example shows that, while we will be able to construct fields whose orders are every power of every prime, these cannot be formed by direct sums of copies of the "prime" fields $\mathbb{Z}_p$.

[1023] cf. Definition [8, Example 21.6, p. 112]

6. (cf. [8, Problem 27.3]) In [8, §24, p. 121] the notion of *isomorphism* of rings is introduced. Two rings are isomorphic if there exists a bijection between their sets of elements which commutes with addition and with multiplication; that is, two elements can be added before or after being mapped, and the result will be the same, and similarly for multiplication. It is claimed that the field of quotients of the integral domain $\mathbb{Z}[\sqrt{7}]$ (cf. [8, Example 21.4], Problem 4 above) is isomorphic to the field $\mathbb{Q}[\sqrt{7}]$, consisting of all real numbers of the form $r+s\sqrt{7}$, where r and s are rationals. You are to describe a function θ which can realize this isomorphism. Remember that the set on which θ is to act consists of equivalence classes of ordered pairs $(a+b\sqrt{7}, c+d\sqrt{7})$, where c and d are integers, not both 0. Describe precisely what you would have to prove about θ in order to establish that it is an isomorphism; you are not expected to actually complete the proof.

   Solution: We verify that the fields are isomorph*ic* by exhibiting an isomorph*ism*. The ordered pairs on which we establish the equivalence relation denoted by $\sim$ in [8, §27] are of the form $(a+b\sqrt{7}, c+d\sqrt{7})$, where c and d are not both 0 (since the element $c+d\sqrt{7}$ is to be a non-zero element of the integral domain). Referring to the equations

$$\begin{aligned} \frac{a+b\sqrt{7}}{c+d\sqrt{7}} &= \frac{(a+b\sqrt{7})(c-d\sqrt{7})}{c^2-7d^2} \\ &= \frac{(ac-7bd)+(-ad+bc)\sqrt{7}}{c^2-7d^2} \end{aligned}$$

   we see that one representative for the equivalence class containing the given element is $((ac-7bd)+(-ad+bc)\sqrt{7}, c^2-7d^2)$; note that the second member of the ordered pair is, as required, non-zero, since $\sqrt{7}$ is not rational. This suggests that the following defines an isomorphism:

$$\theta([a+b\sqrt{7}, c+d\sqrt{7}]) = \frac{ac-7bd}{c^2-7d^2} + \frac{-ad+bd}{c^2-7d^2}\sqrt{7}\,. \tag{1061}$$

   To complete this proof, we would have to prove that

   - θ is well defined.
   - θ commutes with addition.
   - θ commutes with multiplication.

   While students were not asked to actually carry out this proof, we sketch what remains to be proved.

θ **is well defined.** Suppose that $(a+b\sqrt{7}, c+d\sqrt{7}) \sim (a'+b'\sqrt{7}, c'+d'\sqrt{7})$. Then, after reduction, we obtain that

$$(ac' - a'c + 7bd' - 7b'd) + (ad' + bc' - a'd - b'c)\sqrt{7} = 0\,.$$

As $\sqrt{7}$ is not rational, we cannot solve this equation for $\sqrt{7}$, so both $ac' - a'c + 7bd' - 7b'd$ and $ad' + bc' - a'd - b'c$ must be 0. This can be shown to be sufficient to ensure that (1061) defines a function without ambiguity, i.e. that

$$\frac{ac - 7bd}{c^2 - 7d^2} + \frac{-ad + bd}{c^2 - 7d^2}\sqrt{7} = \frac{a'c' - 7b'd'}{(c')^2 - 7(d')^2} + \frac{-a'd + b'd\prime}{(c')^2 - 7(d')^2}\sqrt{7}\,.$$

θ **commutes with addition.** Here we must show that

$$\theta([a + b\sqrt{7}, c + d\sqrt{7}]) + \theta([a' + b'\sqrt{7}, c' + d'\sqrt{7}])$$

is equal to

$$\theta\left([(a + b\sqrt{7})(c' + d'\sqrt{7}) + (a' + b'\sqrt{7})(c + d\sqrt{7}), (c + d\sqrt{7})(c' + d'\sqrt{7})]\right)$$

θ **commutes with multiplication.** Here we must prove that

$$\theta([a + b\sqrt{7}, c + d\sqrt{7}])\theta([a' + b'\sqrt{7}, c' + d'\sqrt{7}])$$

is equal to

$$\theta([(a + b\sqrt{7})(a' + b'\sqrt{7}), (c + d\sqrt{7})(c' + d'\sqrt{7})])\,.$$

7. (a) [8, Problem 21.18] Show that it is possible to make any abelian group $(G, +, 0)$ into a ring by defining the product of any two elements to be 0.

   (b) Show that there are, up to isomorphism, precisely two types of rings with 2 elements. You may do this by investigating what possible multiplicative structures may be imposed on the group $\mathbb{Z}_2$.

   (c) Analogously to the preceding, determine, up to isomorphism, the possible rings of order 3.

   (d) Explain why there are at least 5 non-isomorphic rings of order 4.

Solution:

(a) The multiplication rule is well defined: all ordered pairs of elements that are to be multiplied are mapped on to 0. Since the distributive and associative rules both involve equations whose members are products or sums of products, these equations all reduce to tautologies of the form $0 = 0$. So this is, indeed, a ring; we may call this ring *trivial*.

(b) We know from [8, Theorem 21.2] that any product involving 0 must be equal to 0. Thus only the product of $[1]_2$ with itself remains to be determined. When we define this to be $[1]_2$, we obtain the *field* $\mathbb{Z}_2$; when we take it to be $[0]_2$ we obtain the trivial ring.

(c) Since the underlying group has order 3, it is cyclic, and there is not restriction on generality in taking it to be $\mathbb{Z}_3$. All products are determined by the product $[1]_3[1]_3$, since every element of $\mathbb{Z}_3$ is a sum of copies of $[1]_3$. Thus — we suppress the brackets and subscripts — $1 \cdot 2 = 1 \cdot (1 + 1) = 1 \cdot 1 + 1 \cdot 1$; $2 \cdot 2 = (1 + 1) \cdot (1 + 1) = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 = 1 \cdot 1$, since addition is modulo 3 in this additive group. Thus there appear to be at most three possible rings that we can construct with underlying group $\mathbb{Z}_3$: the field $\mathbb{Z}_3$, in which $1 \cdot 1 = 1$ — in fact 1 is the unity element; the trivial ring; and, finally, a ring with multiplication table

	0	1	2
0	0	0	0
1	0	2	1
2	0	1	2

Is this a different ring from the others? Scrutiny of the multiplication table shows that 2 is the unity element. In fact, this ring is isomorphic to the field $\mathbb{Z}_3$, under the correspondence induced by $[2]_3 \mapsto [1]$. So here again there are only two isomorphism types of rings.

(d) For order 4 there will be more than 2 types, however. There are 2 different types of underlying group: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. In the cyclic case there are at least two possible ring structures: the trivial ring, and the usual structure denoted by $\mathbb{Z}_4$, in which multiplication is modulo 4. In the case where the underlying group is the Klein 4-group, we have, in addition to the trivial ring, the sum of the field $\mathbb{Z}_2$ and a trivial ring, and the sum of two copies of the field.

And, in addition to the 5 rings mentioned, there is at least one more: the finite field of order 4, denoted by $\mathbb{F}_4$ or by $GF(4)$. (All of the 5 rings listed above contain zero divisors, so none of them is isomorphic to the field.)

C.5 Fifth 1998 Problem Assignment

Caveat lector! These solutions are being posted before being thoroughly checked. They may contain misprints and/or errors.

1. (cf. [8, Problem 41.9])

(a) Prove or disprove: The degree[1024] of the sum of two non-zero polynomials $f(x)$, $g(x)$ over any field $\mathbb{F}$ is at least as large as the maximum of the degrees of $f(x)$ and $g(x)$.

(b) Prove or disprove: The degree of the product of two non-zero polynomials $f(x)$, $g(x)$ over any field $\mathbb{F}$ is at least as large as the sum of the degrees of $f(x)$ and $g(x)$.

Solution:

(a) This statement is not true for any field. For example, consider the polynomials $f(x) = 1 + x$ and $g(x) = -x$, both of degree 1. The sum $f(x) + g(x) = 1$, whose degree is 0, which is less than $1 = \max(\deg f, \deg g)$.

(b) (Note that this statement would be false if just one of $f(x)$ or $g(x)$ were the zero polynomial; in that case the degree of the product would be $-\infty$, but the maximum of the degrees would be at least 0.)

Let $f(x) = a_0 + a_1x^1 + ... + a_ix^i + ... + a_nx^n$, and $g(x) = b_0 + b_1x^1 + ... + b_jx^j + ... + b^mx^m$, where $a_n \neq 0$ and $b_m \neq 0$. Then the product may be computed by term-by-term multiplication; it consists of all terms of the form $a_ib_jx^{i+j}$, summed as $0 \leq i \leq n$ and $0 \leq j \leq m$. The value $i + j = n + m$ is the maximum, and is realized in only one way — when $i = m$ and $j = n$. Thus the coefficient of x^{N+M} is precisely a_nb_m. As we assumed each of the factors is non-zero, and we are working in a field — which is, in particular, an integral domain — their product is also non-zero. Thus the product $f(x)g(x)$ contains a term in x^{n+m}, and no terms in higher powers; so its degree is precisely $n+m$, the sum of the degrees of the factors.

(If we were to permit the coefficients to come from a ring containing zero divisors, then the statement would not always be true. For example, the polynomial $2x$ has degree 2 over $\mathbb{Z}_4$, but its square is 0, with degree $-\infty$.)

2. [8, Problem 42.13] Find all odd primes for which $x-2$ is a factor of $x^4+x^3+x^2+x$ in $\mathbb{Z}_p$.

Solution: By the Factor Theorem the problem is equivalent to finding all odd primes p such that $2^4 + 2^3 + 2^2 + 2 \equiv 0 \pmod{p}$, i.e. such that $30 \equiv 0 \pmod{p}$, i.e. such that $p|2^13^15^1$. Thus the odd prime p can only be 3 or 5.

3. Let p be a prime.

[1024] We define the *degree* of the zero polynomial to be $-\infty$; the sums and products involving $-\infty$ are defined in the obvious ways.

(a) Explain why every non-zero element $a \in \mathbb{Z}_p$ has the property that $a^{p-1} = 1$. [Hint: Use the first corollary to [8, Lagrange's Theorem, pp. 91-92] and [8, Corollary to Theorem 23.1].]

(b) [8, Problem 42.18] Prove that each element of $\mathbb{Z}_p$ is a root of $x^p - x$.

(c) Prove that the product $x(x-1)(x-2)\cdots(x-(p-1))|x^p - x$.

(d) Prove that $x(x-1)(x-2)\cdots(x-(p-1)) = x^p - x$.

Solution:

(a) By [8, Corollary to Theorem 23.1] $\mathbb{Z}_p$ is a field, so $\mathbb{Z}_p - \{0\}$ is a group under multiplication; the order of this group is $p-1$, so, by [8, First Corollary to Lagrange's Theorem], the order of each element $a \neq 0$ is a divisor $d|p-1$. Hence $a^{p-1} = \left(a^d\right)^{\frac{p-1}{d}} = 1^{\frac{p-1}{d}} = 1$.

(b) Since every non-zero element of $\mathbb{Z}_p$ satisfies $x^{p-1} - 1$, it surely satisfies

$$x\left(x^{p-1} - 1\right) = x^p - x\,.$$

But 0 satisfies the polynomial x, so it also is a root of $x^p - x$. Thus all elements of the field have been accounted for.

(c) By the Factor Theorem, $(x-a)|(x^p - x)$ for all $a \in \mathbb{Z}_p$. Each of these factors $x - a$ being an irreducible factor of $x^p - x$, and any two of them being relatively prime, their product must divide $x^p - x$.

(d) As the product has the same degree as $x^p - x$, i.e. p, the quotient of this product in $x^p - x$ must have degree 0, i.e. must be a non-zero constant — call it C. We can show that $C = 1$ by comparing coefficients of x^p on the two sides of the equation

$$x^p - x = Cx(x-1)(x-2)\cdots(x-p+1)\,.$$

4. [8, Problem 43.12] Express $x^5 + x^4 + x^2 + 2x \in \mathbb{Z}_3[x]$ as a product of irreducible polynomials. You are expected to show how you discover the various factors, and how you know your factors are irreducible.

Solution: If we define $f(x) = x^5 + x^4 + x^2 + 2x$, then evaluation of the polynomial at all field elements yields

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 2 \neq 0 \\ f(2) &= 2 \neq 0 \end{aligned} \tag{1062}$$

so $x-0$ is the only 1st degree factor. That leaves the possibility that x^4+x^3+x+2 admits a factorization into 2nd degree factors, of the form

$$x^4 + x^3 + x + 2 = (x^2 + ax + b)(x^2 + cx + d) \tag{1063}$$

where a, b, c, d are constants to be determined. Comparing coefficients of corresponding powers of x yields

$$\begin{aligned} 1 &= a + c && \text{coefficient of } x^3 && (1064)\\ 0 &= b + d + ac = 0 && \text{coefficient of } x^2 && (1065)\\ 1 &= ad + bc && \text{coefficient of } x^1 && (1066)\\ 2 &= bd && \text{coefficient of } x^0 && (1067) \end{aligned}$$

Of the 3^2 possible values for the ordered pair (b, d), only $b = 1$, $d = 2$ or $b = 2$, $d = 1$ satisfy (1067). Without limiting the generality of (1063), we may take $b = 1$, $d = 2$. The system then reduces to

$$\begin{aligned} a + c &= 0 && (1068)\\ ac &= 0 && (1069)\\ 2a + c &= 1 && (1070) \end{aligned}$$

from which we may conclude that $a = 0$, $c = 1$, giving the factorization $x^5 + x^4 + x^2 + 2x = x(x^2 + 1)(x^2 + x + 2)$ in which all factors shown are irreducible: the two quadratic factors could not be reducible, since that would entail having 1st degree factors, and we know that $x^4 + x^3 + x + 2$ has none.

5. (cf. [8, Problem 43.20]) Let p be a prime.

   (a) By counting the number of distinct possibilities for $(x - a)(x - b)$, verify that there are precisely $\binom{p+1}{2}$ monic reducible polynomials of degree 2 over $\mathbb{Z}_p$. [Hint: You may assume that a *reducible* 2nd-degree monic polynomial must be the product of two monic first-degree polynomials.]

   (b) Determine the numbers of monic irreducible polynomials of degrees 0, 1, and 2 over $\mathbb{Z}_p$.

   (c) Determine the numbers of irreducible polynomials of degrees 0, 1, and 2 over $\mathbb{Z}_p$.

   (d) Determine the number of monic irreducible polynomials of degree 3 over $\mathbb{Z}_p$.

   Solution:

(a) There are p perfect squares of : $(x-0)^2$, $(x-1)^2$, ..., $(x-p+1)^2$, and $\binom{p}{2}$ ways of multiplying two distinct monic 1st-degree factors. This yields $p + \binom{p}{2} = \binom{p+1}{2}$ reducible monic polynomials.

(b) The only monic 0th-degree polynomial is the only monic constant, i.e. 1. Every 1st-degree polynomial is irreducible; so the monic irreducible 1st degree polynomials are $x - a$ $(a = 0, 1, ..., p-1)$ — p in number.

As there are precisely p^2 ways of constructing a monic 2nd-degree polynomial, the number which are *irreducible* must be $p^2 - \binom{p+1}{2} = \binom{p}{2}$.

(c) Any *monic* irreducible polynomial yields $p-1$ irreducible polynomials through multiplication by a non-zero field element. Thus, the numbers of such polynomials of degrees 0, 1, 2 are respectively $p-1$, $(p-1)p$, $(p-1)\binom{p}{2}$.

(d) A 3rd-degree polynomial which is reducible is either the product of 3 1st-degree polynomials, or the product of one 1st-degree and one 2nd-degree polynomial.

i. **3 distinct 1st degree factors:** $\binom{p}{3}$ polynomials

ii. **1 squared 1st degree factor times another 1st degree factor:** choose the squared factor in $\binom{p}{1}$ ways, and the other factor in $\binom{p-1}{1}$ ways; for a total of $p(p-1)$ reducible polynomials.

iii. **1 cubed 1st degree factor:** Choose the factor in $\binom{p}{1}$ ways.

iv. **1 1st degree factor and 1 irreducible 2nd degree factor:** Choose the 1st-degree factor in $\binom{p}{1}$ ways, and the 2nd-degree factor in $\binom{p}{2}$ ways (as determined above).

Summing, we find the number of *reducible* cubic polynomials to be

$$\binom{p}{3} + p(p-1) + p + p\binom{p}{2} = \frac{p(2p^2+1)}{3}$$

Hence the number of *irreducible* polynomials is

$$p^3 - \frac{p(2p^2+1)}{3} = \frac{p(p-1)(p+1)}{3}$$

6. (cf. [8, Problem 50.6])

(a) Verify that $1 + x^2 + x^3 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$.

(b) Construct addition and multiplication tables for the field $\mathbb{Z}_2[x]/(1 + x^2 + x^3)$.

(c) Give an example of a finite field where $1 + x^2 + x^3$ is reducible. Explain.

Solution:

(a) For a cubic polynomial to be reducible it must has at least one factor of degree 1. (Why?) Hence we may appeal to the Factor Theorem, and simply evaluate $1 + x^2 + x^3$ at 0 and 1 — in both cases obtaining the value 1 (not zero), so there are no 1st degree factors, and the polynomial is irreducible.

(b) The 8 elements of the field may be represented by 0, 1, α, $1 + \alpha$, α^2, $1 + \alpha^2$, $\alpha+\alpha^2$, $1+\alpha+\alpha^2$. All computations must be done *modulis*[1025] 2 and $1+\alpha^2+\alpha^3$. In order to simplify the table, we observe that

$$\begin{aligned}
\alpha^3 &= 1 + \alpha^2 \\
\alpha^4 &= \alpha \cdot \alpha^3 = \alpha + \alpha^3 = \alpha + 1 + \alpha^2 \\
\alpha^5 &= \alpha \cdot \alpha^4 = \alpha^2 + \alpha + \alpha^3 = \alpha^2 + \alpha + 1 + \alpha^2 = 1 + \alpha \\
\alpha^6 &= \alpha + \alpha^2 \\
\alpha^7 &= \alpha^2 + \alpha^3 = \alpha^2 + 1 + \alpha^2 = 1
\end{aligned}$$

Thus we may represent the multiplication table as follows, (remembering to reduce the exponents upon multiplication by 7 since $\alpha^7 = 1$).

$\times$	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
$1 = \alpha^0$	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
$\alpha = \alpha^1$	0	α^1	α^2	α^3	α^4	α^5	α^6	α^0
$\alpha^2 = \alpha^2$	0	α^2	α^3	α^4	α^5	α^6	α^0	α^1
$1 + \alpha^2 = \alpha^3$	0	α^3	α^4	α^5	α^6	α^0	α^1	α^2
$1 + \alpha + \alpha^2 = \alpha^4$	0	α^4	α^5	α^6	α^0	α^1	α^2	α^3
$1 + \alpha = \alpha^5$	0	α^5	α^6	α^0	α^1	α^2	α^3	α^4
$\alpha + \alpha^2 = \alpha^6$	0	α^6	α^0	α^1	α^2	α^3	α^4	α^5

Note that the multiplicative group of the field is cyclic.

The addition table is, (again remembering to reduce the exponents upon multiplication by 7 since $\alpha^7 = 1$).

$+$	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
0	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
$1 = \alpha^0$	α^0	0	α^5	α^3	α^2	α^6	α^1	α^4
$\alpha = \alpha^1$	α^1	α^5	0	α^6	α^4	α^3	α^0	α^2
$\alpha^2 = \alpha^2$	α^2	α^3	α^6	0	α^0	α^5	α^4	α^1
$1 + \alpha^2 = \alpha^3$	α^3	α^2	α^4	α^0	0	α^1	α^6	α^5
$1 + \alpha + \alpha^2 = \alpha^4$	α^4	α^6	α^3	α^5	α^1	0	α^2	α^0
$1 + \alpha = \alpha^5$	α^5	α^1	α^0	α^4	α^6	α^2	0	α^3
$\alpha + \alpha^2 = \alpha^6$	α^6	α^4	α^2	α^1	α^5	α^0	α^3	0

[1025]plural of *modulo*

This additive group is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(c) Since $1 + 1^2 + 1^3 = 3 \equiv 0 \pmod 3$, $1 + x^2 + x^3$ has factor $x - 1$ over $\mathbb{Z}_3$. The irreducible factorization is then

$$1 + x^2 + x^3 = (x - 1)(x^2 - x - 1)$$

as $x^2 - x - 1$ has no roots in $\mathbb{Z}_3$.

7. [8, Problem 51.4] Determine, for each of the monic polynomials of degree 2 over $\mathbb{Z}_3$, the multiplicities of all roots over $\mathbb{Z}_3$.

Solution: We will approach this problem from the factorizations. Roots of 0, 1, 2 (i.e. $[0]_3$, $[1]_3$, $[2]_3$) correspond to factors of x, $x - 1$, $x + 1$ of the polynomial. We list the various possibilities:

(a) x^2 has two roots of 0.

(b) $(x - 1)^2 = x^2 + x + 1$ has two roots of 1.

(c) $(x - 2)^2 = x^2 - x + 1$ has two roots of 2 (or -1).

(d) $x(x - 1) = x^2 - x$ has one root of 0 and one root of 1.

(e) $x(x - 2) = x^2 + x$ has one root of 0 and one root of 2.

(f) $(x - 1)(x - 2) = x^2 - 1$ has one root of 1 and one root of 2.

(g) **Irreducible polynomials.** These will be those $3^2 - 6 = 3$ polynomials not listed above, namely $x^2 - x - 1$, $x^2 + x - 1$, and $x^2 + 1$; of course, each of these has 0 roots over $\mathbb{Z}_3$.

8. (cf. [8, Problem 52.6]) Explaining your work, factorize each of the following polynomials over $\mathbb{Q}$ as a product of irreducible factors.

(a) $x^3 - x^2 - 5x + 5$

(b) $3x^3 - 2x^2 + 3x - 2$

(c) $x^3 - 2x + 2$

Solution:

(a) By [8, Theorem 52.1] r/s is a rational root, where $(r, s) = 1$ only if $r|5$ and $s|1$. As 5 is prime, this implies that r is either ± 1 or ± 5; and that s is 1 or -1. Since we are concerned only with the ratio r/s, we may require, without limiting generality, that $s > 0$. This leads to only four possible roots: ± 1 and ± 5. Testing the values of $f(x) = x^3 - x^2 - 5x + 5$, we find only one case which vanishes: $f(1) = 0$. By the Factor Theorem, $x - 1$ is a divisor of $f(x)$; we

find, upon division, that $f(x) = (x-1)(x^2-5)$.[1026] We know that $\sqrt{5}$ is not rational (similar proof to the irrationality of 2); hence x^2-5 is irreducible.

(b) Assume that r/s is a root of $g(x) = 3x^3 - 2x^2 + 3x - 2$, and that $(r,s) = 1$, where r and s are integers, and $s > 0$. Then, by [8, Theorem 52.1], $r|(-2)$ and $s|3$; thus $r = \pm 1$ or $r = \pm 2$ and $s = 1$ or $s = 3$. The candidates for roots are then ± 1, $\pm\frac{1}{3}$, ± 2, $\pm\frac{2}{3}$. Testing the value of $g(x)$ at these eight points, we find that g vanishes at each of $\frac{2}{3}$, ± 1, so that $g(x)$ is divisible by the product $(x-\frac{2}{3})(x-1)(x+1)$; upon division, we find the quotient to be 3, so the factorization is

$$g(x) = 3x^3 - 2x^2 + 3x - 2 = (3x-2)(x-1)(x+1)$$

This factorization could also have been discovered by grouping; for $3x^3-2x^2+3x-2 = 3(x^3-x)-2(x^2-1) = 3x(x^2-1)-2(x^2-1) = (3x-2)(x^2-1) = (3x-2)(x-1)(x+1)$.

(c) The version of this problem shown on the question sheet differs from the problem in the textbook. The problem we printed involves the polynomial $x^3 - 2x + 2$. If $\frac{r}{s}$ is a root, where r and s are integers, $s \neq 0$, $(r,s) = 1$, then by [8, Theorem 52.1], $r|2$ and $s|1$; this means that the only possible rational roots are 2 and -2. Applying the Factor Theorem, we see that neither of these is a root. Thus this cubic polynomial has no first degree factors; but a reducible cubic polynomial cannot have only factors of degree ≥ 2. It follows that the polynomial is irreducible.

Now let us discuss the polynomial shown in the textbook, $x^3 - 2x^2 + 2x$. As the constant term of the given polynomial is 0, 0 is a root, so the polynomial is divisible by x, yielding $x^3 - 2x^2 + 2x = x(x^2 - 2x + 2)$. The quadratic factor $x^2 - 2x + 2 = (x-1)^2 + 1$ is a sum of squares. For any real number a, hence *a fortiori* for any rational number a, $a^2 - 2a + 2$ cannot be less than 0+1, so it cannot vanish. Thus the quadratic factor $x^2 - 2x + 2$ can have no roots, and admits no further factorization, i.e. it is irreducible, and the desired factorization is $x(x^2 - 2x + 2)$.

[1026] Of course, many students could have observed this factorization as a result of grouping the summands of the polynomial.

D 1999 Problem Assignments, with Solutions

D.1 First 1999 Problem Assignment

1. Prove that a non-negative integer $a = (a_k a_{k-1} \dots a_1 a_0)_{16}$ is divisible by 15 iff the sum of its hexadecimal digits, $\sum_{i=0}^{k} a_i$, is divisible by both 3 and 5.

   Solution: $16 = 15 + 1 \equiv 1 \pmod{15} \Rightarrow 16^i \equiv 1 \pmod{15}$ by Theorem A.1.4.5.4 for $(i = 0, 1, ..., k)$. Hence

   $$\begin{aligned} \sum_{i=0}^{k} a_i &\equiv \sum_{i=0}^{k} a_i 16^i \pmod{15}. \\ &= a \end{aligned}$$

   Thus

   $$a \equiv 0 \pmod{15} \Leftrightarrow \sum_{i=0}^{k} a_i \equiv 0 \pmod{15}. \tag{1071}$$

   Since $3|15$ and $5|15$, the *necessity (only if)* part of the theorem follows from the transitivity of $|$.

   Suppose now that the sum $\sum_{i=0}^{k} a_i$ of the hexadecimal digits is divisible by both 3 and 5. Then, by Lemma A.1.6.12, it is also divisible by $[3, 5]$, i.e. by 15. (Alternatively, if $3u = \sum_{i=0}^{k} a_i = 5v$, then $\sum_{i=0}^{k} a_i = 15(2u - 3v)$, so it is a multiple of 15; by (1071) a must then also be a multiple of 15.) This proves the *sufficiency (if)* part of the theorem.

2. Prove that, for any integers a and b both greater than 1, the integer $a^{4b} + a^{2b} + 1$ is composite.

   Solution: The polynomial $x^4 + x^2 + 1$ admits the factorization

   $$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1).$$

   With $x = a^b$, this yields the decomposition

   $$a^{4b} + a^{2b} + 1 = (a^{2b} + a^b + 1)(a^{2b} - a^b + 1). \tag{1072}$$

   To show this is a (non-trivial)[1027] factorization, we must demonstrate that both of the factors shown, i.e. $a^{2b} + a^b + 1$ and $a^{2b} - a^b + 1$, exceed 1 in absolute value. Were

[1027] i.e. a factorization wherein none of the factors is ± 1.

either of them equal to 1, that would imply that either $a^b = 1$ or $a^b = 0$, neither of which is possible because of the hypothesis that $a > 1$ and $b > 1$. Were either of the factors equal to -1, one of the equations $a^{2b} \pm a^b + 2 = 0$ would hold; but the polynomial $x^2 + x + 2$ has no real roots. From these contradictions we conclude that (1072) is a (non-trivial) factorization of the given integer, which, therefore, is composite.

3. For every positive integer k, find all positive integers n such that $n + 1$ divides $n^k + 1$.

   Solution: When k is odd, the familiar formula for the sum of a geometric progression

   $$1 + (-n) + (-n)^2 + \ldots + (-n)^{k-1} = \frac{1 - (-n)^k}{1 - (-n)}$$

   demonstrates the factorization

   $$n^k + 1 = (1 + (-n) + (-n)^2 + \ldots + (-n)^{k-1})(1 + n)\,;$$

   so $n + 1$ divides $n^k + 1$ for all odd positive integers k.

   When k is even,

   $$n^k + 1 = -(1 + (-n) + (-n)^2 + \ldots + (-n)^{k-1})(1 + n) + 2$$

   so divisibility would hold only if $(n + 1)|2$, i.e. only when $n = 1$. (The fact that the remainder of $n^k + 1$ is then 2 can also be shown using the *Remainder Theorem*, which we will meet in Theorem A.7.4.5.)

4. Let $a = 43732$, $b = 15863$.

   (a) Apply the Euclidean Algorithm to determine (a, b), and also to determine integers k and ℓ such that
   $$(a, b) = ka + \ell b$$

   (b) Find another set of integers, k', ℓ' such that $(a, b) = ka + \ell b$. Explain how you found these integers.

   (c) Apply the Stein Algorithm (cf. Exercise A.1.6.8.2) to determine (a, b).

   (d) Using your calculator, apply the information accumulated above to determine the prime factorizations of a and b.

   You may use a calculator, but should show every step of your computations, in a systematic fashion.

   Solution:

(a)

$$\begin{aligned} 43732 &= 2 \cdot 15863 + 12006 \\ 15863 &= 1 \cdot 12006 + 3857 \\ 12006 &= 3 \cdot 3857 + 435 \\ 3857 &= 8 \cdot 435 + 377 \\ 435 &= 1 \cdot 377 + 58 \\ 377 &= 6 \cdot 58 + 29 \\ 58 &= 2 \cdot 29 + 0 \end{aligned}$$

Thus, working upwards from the second last line of the preceding calculations, we obtain

$$\begin{aligned} 29 &= 1 \cdot 377 + (-6) \cdot 58 = 1 \cdot 377 + (-6) \cdot (435 - 1 \cdot 377) \\ &= (-6) \cdot 435 + 7 \cdot 377 = (-6) \cdot 435 + 7 \cdot (3857 - 8 \cdot 435) \\ &= 7 \cdot 3857 + (-62) \cdot 435 = 7 \cdot 3857 + (-62) \cdot (12006 - 3 \cdot 3857) \\ &= (-62) \cdot 12006 + 193 \cdot 3857 = (-62) \cdot 12006 + 193 \cdot (15863 - 1 \cdot 12006) \\ &= 193 \cdot 15863 - 255 \cdot 12006 = 193 \cdot 15863 + (-255) \cdot (43732 - 2 \cdot 15863) \\ &= (-255) \cdot 43732 + 703 \cdot 15863 \end{aligned}$$

Thus we have found $k = -255$, $\ell = 703$.

(b) By Lemma A.1.6.9.4, we obtain all other solutions by adding to k, $t\frac{b}{(a,b)} = t\frac{15863}{29} = 547t$, and subtracting from ℓ, $t\frac{a}{(a,b)} = t\frac{43732}{29} = 1508t$. For example, taking $t = 1$ yields the solution $k' = 292$, $\ell' = -805$.

(c)

$$\begin{aligned} (43732, 15863) &= (10933, 15863) \\ &= (10933, 4930) = (10933, 2465) \\ &= (8468, 2465) = (2117, 2465) \\ &= (348, 2117) = (87, 2117) \\ &= (87, 2030) = (87, 1015) \\ &= (87, 928) = (87, 29) \\ &= (58, 29) = (29, 29) = 29 \end{aligned}$$

(d) We have determined a common divisor 29 to the two given integers. Thus we know that $43732 = 29 \cdot 1508$. But 1508 is evidently even, and we can repeatedly factor out powers of 2, ultimately obtaining $1508 = 2^2 \cdot 377$, so

$43732 = 2^2 \cdot 29 \cdot 377$. To further factorize 377 we could test for divisibility by odd primes not exceeding $\sqrt{377}$ =19.42.... (cf. Lemma A.1.8.3). By familiar tests, it is not divisible by 3, 5, 11; so we attempt to divide by 7 (failure), 13 (success). At the worst we would have had to test 17 and 19 also. We thus obtain $43732 = 2^2 \cdot 13^1 \cdot 29^2$.

As $15863 = 29 \cdot 547$ we need, at worst, to test 547 for divisibility by odd primes not exceeding 23.3... $= \sqrt{547}$. After applying the familiar tests for divisibility by 3, 5, 11, we attempt to divide by 7, 13, 17, 19, 23, all of which fail. We conclude that 547 is prime, and that $15863 = 29^1 \cdot 547^1$ is the prime decomposition.

5. Let $a = 43732$, $b = 15863$, $u_1 = 10$, $u_2 = 11$, $u_3 = 19$, $u_4 = 29$.

   (a) Determine, for each of a and b, the minimum non-negative remainders $r(t, 1)$, $r(t, 2)$, $r(t, 3)$, $r(t, 4)$ modulo u_i $(i = 1, 2, 3, 4)$ respectively, $(t = a, b)$. Then solve the simultaneous set of congruences

   $$x \equiv r(a, i) + r(b, i) \pmod{u_i} \tag{1073}$$

   by determining inverses and applying the formula of Theorem A.1.9.9, after explaining why the theorem is applicable; show all your work. Verify that the smallest non-negative solution is equal to $a + b$.

   (b) Solve (1073) again, this time recursively, finding the form of integers satisfying the first congruence, and subjecting this to the constraint of the second congruence, etc.

   You may use a calculator for the arithmetic in this problem, but should report fully on your calculations.

   Solution:

   (a) The four moduli given are relatively prime, so the Chinese Remainder Theorem is applicable.

   By division we determine the following minimum non-negative remainders to the given four moduli:

t	$r(t,1)$	$r(t,2)$	$r(t,3)$	$r(t,4)$
43732	2	7	13	0
15864	3	1	17	0
59595	5	8	11	0

To solve the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{10} && (1074)\\ x &\equiv 8 \pmod{11} && (1075)\\ x &\equiv 11 \pmod{19} && (1076)\\ x &\equiv 0 \pmod{29} && (1077)\\ & && (1078) \end{aligned}$$

we compute, for $M = 10 \times 11 \times 19 \times 29 = 60610$, inverses of M/u_i modulo u_i to be 1, 10, 9, and 15 respectively ($i = 1, 2, 3, 4$). Of these the first is obvious, since the inverse of 1 is 1; the second is also obvious, since $10 \equiv -1$, which is its own inverse; the fourth is also easily obtained, since $2 \times 15 = 30 \equiv 1$ — and, in any case — this particular inverse will not be needed in the actual calculations. As for the inverse of 17 modulo 19, this can be determined by the Euclidean algorithm:

$$\begin{aligned} 19 &= 1 \cdot 17 + 2\\ 17 &= 8 \cdot 2 + 1\\ 2 &= 2 \cdot 1 + 0\\ \Rightarrow 1 &= 17 - 8 \cdot 2\\ &= 17 - 8 \cdot (19 - 1 \cdot 17)\\ &= (-8) \cdot 19 + 9 \cdot 17 \equiv 9 \cdot 17 \pmod{19} \end{aligned}$$

All solutions to the system of congruences will then be congruent modulo 60,610 to

$$(6061 \times 1 \times 5) + (5510 \times 10 \times 8) + (3190 \times 9 \times 11) + (2090 \times 15 \times 0)$$

i.e. 786,915. Reducing modulo 60,610, we find the smallest non-negative remainder to be 55,595 as expected.

(b)

$$\begin{aligned} (1074) &\Rightarrow (\exists u \in \mathbb{Z})[x = 10u + 5]\\ (1075) &\Rightarrow u \equiv 8 \pmod{11}\\ &\Rightarrow (\exists v \in \mathbb{Z})[u = 11v + 8]_{13}\\ &\Rightarrow x = 110v + 85\\ (1076) &\Rightarrow 110v \equiv -74 \pmod{19}\\ &\Rightarrow 15v \equiv 2 \pmod{19} \end{aligned}$$

$$\begin{aligned}
&\Rightarrow\quad 14\cdot 15v \equiv 14\cdot 2 \pmod{19}\\
&\Rightarrow\quad v \equiv 9 \pmod{19}\\
&\Rightarrow\quad v = 19c + 9\\
&\Rightarrow\quad x = 2090c + 1075\\
(1077)\quad &\Rightarrow\quad 2090c \equiv -1398 \pmod{29}\\
&\Rightarrow\quad 2c \equiv 27 \pmod{29}\\
&\Rightarrow\quad 15\cdot 2c \equiv 15\cdot 27 \pmod{29}\\
&\Rightarrow\quad c \equiv 28 \pmod{29}\\
&\Rightarrow\quad (\exists d\in\mathbb{Z})[c = 29d + 28]\\
&\Rightarrow\quad x = 60610d + 59595\,,
\end{aligned}$$

so the smallest non-negative solution is $x = 59595$, as before. In the preceding calculations most of the inverses were easily determined by observation. An exception was $(15)^{-1}$ modulo 19, which we determined using the Euclidean algorithm.

6. (a) For a fixed positive prime p, the set of *cubic residues modulo* p consists of the cosets of $p\mathbb{Z}$ in $\mathbb{Z}$ of the form $[a^3]_p$, where a may be any element of $\mathbb{Z}$ not divisible by p. Show that $[b]_p$ is a cubic residue iff $[-b]_p$ is a cubic residue.

   (b) (cf. Exercise A.1.8.12) Prove that the cubic residues modulo 13 are $[1]_{13}$, $[5]_{13}$, $[8]_{13}$, or $[12]_{13}$.

   (c) Defining a relation R on the set $V = \{[0]_{13}, [1]_{13}, [2]_{13}, ..., [12]_{13}\}$ by

$$(m,n)\in R \Leftrightarrow m-n \in \{[1]_{13}, [5]_{13}, [8]_{13}, [12]_{13}\}\,,$$

   show that R is symmetric and irreflexive.

   (d) Show that R is not transitive.

   (e) Show that if $(x,y)\in R$ and $(y,z)\in R$, it *never* happens that $(x,z)\in R$.

Solution:

(a) For any $a\in\mathbb{Z}$,

$$[-a^3]_p = [-a^3 + 3a^2p - 3ap^2 + p^3]_p = [(p-a)^3]_p\,.$$

If $p\nmid a$, then $[-a^3]_p$ is thus a cubic residue.

(b)

$$1^3 \;=\; 1$$

$$\begin{aligned} 2^3 &= 8 \\ 3^3 &= 27 \equiv 1 \pmod{13} \\ 4^3 &= 64 \equiv 12 \pmod{13} \\ 5^3 &= 125 \equiv 8 \pmod{13} \\ 6^3 &= 216 \equiv 8 \pmod{13} \end{aligned}$$

By virtue of the preceding part, we need not examine 7 through 12, provided we adjoin to the list of cubes found so far, their negatives. The negative of 8 is $-8 \equiv 5$; of 1 is 12, already in the list.

(c) For two points to be related they must be distinct, as $[0]_{13}$ is not a cubic residue. Thus the relation is irreflexive.

Let us denote the set of cubic residues modulo 13 by W. Then

$$\begin{aligned} ([x]_{13}, [y]_{13}) \in R &\Leftrightarrow [x]_{13} - [y]_{13} \in W \\ &\Leftrightarrow [x - y]_{13} \in W \\ &\Leftrightarrow [y - x]_{13} \in W \\ &\Leftrightarrow [y]_{13} - [x]_{13} \in W \\ &\Leftrightarrow ([y]_{13}, [x]_{13}) \in R \end{aligned}$$

(d) The failure of transitivity will follow from the next part of the problem.

(e) Suppose that

$$\begin{aligned} x - y &\equiv a^3 \pmod{13} \\ y - z &\equiv b^3 \pmod{13} \\ z - x &\equiv c^3 \pmod{13} \end{aligned}$$

Then, summing the congruences, we find that

$$0 \equiv a^3 + b^3 + c^3 \pmod{13}$$

Thus the sum of three members of W would be $[0]$. We can test all such sums and demonstrate that these are never zero.

3 distinct cubic residues: Since the sum of all the cubic residues is congruent to zero, the sum of any three of them will surely not be congruent to zero.

3 like cubic residues: To add three copies of the same residue is equivalent to multiplying it by 3 modulo 13; this cannot yield 0, since that would entail that $3 \equiv 0 \pmod{13}$, which is false.

2 like residues added to one other: Consider two cases: If one is the negative of the other; and, if that is not the case.

The relation described in this problem was used by R. E. Greenwood and A. M. Gleason in a construction to establish the value of several *Ramsey numbers* [12]. They also proved that among any 5 points in V at least one pair are related in R.

D.2 Second 1999 Problem Assignment

1. (a) Determine the Cayley table for the permutation group whose elements are $e = (1)(2)(3)(4)(5)(6)$, $(26)(35)$, $(15)(24)$, $(13)(46)$, $(135)(246)$, $(153)(264)$.

   (b) If the permutation group is assumed to operate on the set $\{1, 2, 3, 4, 5, 6\}$, give each of its elements in the 2-line notation; as, for example, $(26)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}$.

   (c) With the exception of the identity, each of the elements of this permutation group is representable in more than one way in the *reduced disjoint cycle notation*. Determine, for each of the elements, the number of such representations.

   (d) Determine the orbits of the permutation group.

   Solution:

   (a)

	e	$(26)(35)$	$(15)(24)$	$(13)(46)$	$(135)(246)$	$(153)(264)$
e	e	$(26)(35)$	$(15)(24)$	$(13)(46)$	$(135)(246)$	$(153)(264)$
$(26)(35)$	$(26)(35)$	e	$(135)(246)$	$(153)(264)$	$(15)(24)$	$(13)(46)$
$(15)(24)$	$(15)(24)$	$(153)(264)$	e	$(135)(246)$	$(13)(46)$	$(26)(35)$
$(13)(46)$	$(13)(46)$	$(135)(246)$	$(153)(264)$	e	$(26)(35)$	$(15)(24)$
$(135)(246)$	$(135)(246)$	$(13)(46)$	$(26)(35)$	$(15)(24)$	$(153)(264)$	e
$(153)(264)$	$(153)(264)$	$(15)(24)$	$(13)(46)$	$(26)(35)$	e	$(135)(246)$

   (b)

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \qquad (26)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}$$

$$(15)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} \qquad (13)(46) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$$

$$(135)(246) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \qquad (153)(264) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$$

   (c) In the *reduced* disjoint cycle notation, the identity has only one representation — as an empty product of cycles, which we usually denote by a symbol like e.

   The permutations having reduced disjoint cycle form $(\bullet\bullet)(\bullet\bullet)$ each have $2 \times 2 \times 2 = 8$ representations: the first factor 2 is from the possible arrangements

of the first cycle, the second 2 is from the second cycle in the product, and the third is from the possibility of writing the cycles in the reverse order. Thus, for example, (26)(35) = (62)(35) (cyclically permuting the symbols in the first cycle); (26)(35) = (26)(53) (cyclically permuting the symbols in the second cycle); and (26)(35) = (35)(26), permuting the cycles. We have not listed the representations that derive from combinations of these changes: (62)(53), (35)(62), (53)(26), (53)(62).

The permutations of the form (•••)(•••) each have $3 \times 3 \times 2! = 18$ representations in disjoint cycle notation: there are three choices of the first element shown in each of the two factors, and $2! = 2$ orders in which the factors may be listed.

(d) If we examine the cycles which affect 1 in the six group elements, we find them to be (1), (13), (15). Thus the cycle containing 1 must be precisely $\{1, 3, 5\}$. The other elements must therefore form an invariant set $\{2, 4, 6\}$. That this set is, in fact, an orbit, can be seen from the fact that 2 can be mapped into each of 4 and 6 by some element of the permutation group.

2. (a) Consider the undirected simple graph $G_1 = (V_1, E_1)$ where $V_1 = \{1, 2, 3, 4, 5, 6, 7\}$ and $E_1 = \{12, 13, 15, 35, 34, 56, 64, 47, 67, 27\}$. The *automorphisms* of this graph are its isomorphisms with itself, i.e. the functions $f : V_1 \to V_1$ such that $f(v_1)$ is adjacent to[1028] $f(v_2)$ iff v_1 is adjacent to v_2. Carefully determine all the automorphisms of this graph, and, using a Cayley table, show that they form a permutation group.

(b) Determine the group of automorphisms of the undirected simple graph

$$G_2 = (\{1, 2, 3, 4\}, \{13, 14, 23, 24, 34\}) .$$

Show that this permutation group is isomorphic[1029] to the group of automorphisms of G_1.

(c) Determine the orbits of the two permututation groups.

Solution:

(a) From an examination of the adjacencies in G_1, we see that there is just one vertex whose degree is different from the others: namely, vertex 2, whose neighbours are 1 and 7. Vertex 2 must be mapped by any automorphism on to a vertex of the same degree, hence on to itself. Then its neighbours —

[1028] joined by an edge to

[1029] An isomorphism from a permutation group $\mathcal{G}_1$ to a permutation group $\mathcal{G}_2$ is a bijection λ such that if $u_1 \mapsto \lambda(u_1)$ $u_2 \mapsto \lambda(u_2)$, then $u_1 u_2 \mapsto \lambda(u_1)\lambda(u_2)$.

vertices 1 and 7 — must be mapped on to neighbours of 2; thus either $1 \mapsto 7$ and $7 \mapsto 1$; or 1 and 7 are both fixed. We consider these two cases below:

i. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & & & & & 1 \end{pmatrix}$: The neighbours of 1 other than 2 — i.e. vertices 3 and 5 — must be mapped onto neighbours of 7 other than 2. Thus we have either $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 6 & & 4 & & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & & 6 & & 1 \end{pmatrix}$. Then the third neighbour of 3, namely 4, must be mapped on to the third neighbour of the image of 3, i.e. respectively on to 4 or 6; thus we have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 6 & 5 & 4 & & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 3 & 6 & & 1 \end{pmatrix}$, which can each be completed in only one way, to $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 6 & 5 & 4 & 3 & 1 \end{pmatrix} = (17)(36)(45)$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix} = (17)(34)(56)$, respectively.

ii. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & & & & & 7 \end{pmatrix}$: The neighbours of 1 other than 2 — i.e. vertices 3 and 5 — must be mapped onto neighbours of 7 other than 2. Thus we have either $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & & 5 & & 7 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & & 3 & & 7 \end{pmatrix}$. Then the third neighbour of 3, namely 4, must be mapped on to the third neighbour of the image of 3, i.e. respectively on to 4 or 6; thus we have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & & 7 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 6 & 3 & & 7 \end{pmatrix}$, which can be completed in only one way, to $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \iota_{V_1}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 6 & 3 & 4 & 7 \end{pmatrix} = (35)(46)$.

Each of the four permutations is its own inverse, since it is a product of disjoint transpositions. Since composition of permutations is associative, the fact that they constitute a permutation group acting on V_1 will follow from the fact that the set is closed under composition, which can be seen from the Cayley table:

	ι	$(17)(34)(56)$	$(35)(46)$	$(17)(36)(45)$
ι	ι	$(17)(34)(56)$	$(35)(46)$	$(17)(36)(45)$
$(17)(34)(56)$	$(17)(34)(56)$	ι	$(17)(36)(45)$	$(35)(46)$
$(35)(46)$	$(35)(46)$	$(17)(36)(45)$	ι	$(17)(34)(56)$
$(17)(36)(45)$	$(17)(36)(45)$	$(35)(46)$	$(17)(34)(56)$	ι

(b) Proceeding as in the preceding problem, we observe that there are two vertices of the graph having degree 2, and two having degree 3; any automorphism must permute the vertices of each degree. So either both vertices 1 and 2 are fixed, or they are interchanged. Then either permutation of the other two vertices is feasible, and we obtain the permutation group with Cayley table

	ι	(12)	(34)	(12)(34)
ι	ι	(12)	(34)	(12)(34)
(12)	(12)	ι	(12)(34)	(34)
(34)	(34)	(12)(34)	ι	(12)
(12)(34)	(12)(34)	(34)	(12)	ι

In general it is not a simple problem to show that two groups are isomorphic, given only their Cayley tables. In the present cases, however, the problem is indeed trivial, provided the first column of each table is the identity element. It is evident from the two Cayley tables that, under the correspondence of permutations given by the row of labels at the top of each table, one table can be transformed into the other; i.e. the groups are distinct only to the extent that their elements are labelled differently. (Indeed, the group in question here — called the *Klein 4-group* has the property that, were we to rearrange the last three columns (and correspondingly, the last three rows) of the table, the new arrangement would again exhibit the isomorphism of the two permutation groups.)

(c) G_1:We have already observed that, because of valency considerations alone, one orbit is $\{2\}$; and that, by virtue of adjacency to vertex 2, $\{3,5\}$ is also an orbit — or, more precisely — that the set $\{3,5\}$ is *invariant* (mapped into itself) under any permutation; a similar analysis shows that $\{4,6\}$ is also invariant. We need only observe that there is a permutation that maps 3 to 5 — for example (35)(46) — to conclude that $\{3,5\}$ is an orbit; by the same reasoning, $\{4,6\}$ is also an orbit. These orbits together partition V_1.

G_2: By valency considerations, the set $\{1,2\}$ of vertices is mapped into itself (invariant). Since one permutation is (12), this set is indeed an orbit. Then $\{3,4\}$, being the complement of an orbit, must be invariant; and, as (34) is a permutation, this set is also an orbit. These two orbits partition V_2.

3. (a) In the group $GL(3,\mathbb{R})$, interpreted as a permutation group acting on $\mathbb{R}^3$ (written as column 3-vectors), determine the stabilizer of the element $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.

(b) In the dihedral group $\mathcal{D}_5$, interpreted as the symmetry group of a pentagon with vertices, in cyclic order, 1, 2, 3, 4, 5, determine the stabilizer of vertex 2.

Solution:

(a) The equation $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ is satisfied by *all* matrices in the group. Hence the stabilizer is the entire group $GL(3, \mathbb{R})$.

(b) There are only two symmetries that fix 2: the identity, and the reflection (13)(45). Thus the stabilizer of 2 is a group of order 2.

4. Let $\mathfrak{A} = \{1, 2, ..., n\}$.

(a) Show that, if $a_1, a_2, ..., a_k$ are any distinct elements of $\mathfrak{A}$, the cycle $(a_1 a_2 ... a_k)$ is expressible as a product $(2i_1)(2i_2)\cdots(2i_\ell)$, whether or not 2 is one of the elements $a_1, a_2, \ldots a_k$. Illustrate your proof by applying to the cycles (41236) and (41736) in S_7.

(b) Show that, if $2 \neq a$ and $2 \neq b$, where $a, b \in \mathfrak{A}$, any product $(2a)(2b)$ is expressible as a product of 3-cycles[1030]. Explain how this implies that any element of $\mathcal{A}_n$ is expressible as a product of 3-cycles. Illustrate your proof by applying the procedure to the permutations (41236) and (4156)(37) in $\mathcal{A}_7$.

(c) Show that, if $i \neq j$,

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} (ij) \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1} = (a_i a_j)\,.$$

Explain how this implies that, for any permutation $f \in S_n$, the permutation $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} f \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1}$ can be determined by replacing, in the disjoint cycle representation for f, each symbol i by a_i $(i = 1, 2, ..., n)$. Illustrate your discussion by determining the value of

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix} (4156)(37) \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}^{-1}.$$

Solution:

[1030] i.e. cycles of length 3

(a) If 2 is distinct from all of $a_1, a_2, ..., a_k$, then

$$(a_1 a_2 ... a_k) = (2a_k)(2a_{k-1}) \dots (2a_2)(2a_1)(2a_k)\,.$$

Suppose that 2 is one of the elements $a_1, a_2, ..., a_k$. Since

$$(a_1 a_2 ... a_k) = (a_2 a_3 ... a_k a_1) = \dots = (a_k a_1 ... a_{k-2} a_{k-1})\,,$$

we may, without limiting generality, assume that 2 is the first symbol in the cycle: i.e. that $2 = a_1$. Then $(2a_2 ... a_k) = (2a_k)(2a_{k-1}) \dots (2a_3)(2a_2)$.
In particular,

$$\begin{aligned} (41236) &= (21)(24)(26)(23) \quad \text{and} \\ (41736) &= (26)(23)(27)(21)(24)(26)\,. \end{aligned}$$

(b) If $a = b$, then $(2a)(2b) = e$, which is a product of 0 3-cycles.[1031]
We have seen above that every cycle is expressible as a product of transpositions of the form $(2\bullet)$. Any element of $\mathcal{S}_n$ is expressible as a product of cycles, and each of these cycles can, in turn, be expressed as a product of transpositions of the form $(2\bullet)$. The total number of such transpositions in an element of $\mathcal{A}_n$ will be *even*; hence we may group these into successive pairs, and multiply each pair to obtain a 3-cycle of the form $(2 \bullet \bullet)$. In particular, $(41236) = (21)(24)\cdot(26)(23) = (241)(236)$; $(4156)(37) = (26)(25)(21)(24)(26)\cdot (27)(23)(27) = (26)(25)\cdot(21)(24)\cdot(26)(27)\cdot(23)(27) = (256)(241)(276)(273)$.

(c) Suppose that a permutation f is expressible as a product of disjoint cycles, $f = f_1 f_2 ... f_r$. Then, if we denote $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ by g,

$$gfg^{-1} = gf_1g^{-1}g2g^{-1}\cdots grg^{-1}\,.$$

Thus it suffices to prove the claim for any one of the cycles; equivalently, it suffices to assume that f is a cycle. By a further extension of the same reasoning, it suffices to consider the effect of this transformation (premultiplication by g and postmultiplication by g^{-1}) on a single transposition $(2\bullet)$. In the product $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & n \end{pmatrix} (ij) \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & n \end{pmatrix}^{-1}$ any symbol a_k, distinct from i and j, is moved first to k, then not moved by the transposition (ij), then moved back to a_k, so it is fixed. But $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & n \end{pmatrix}^{-1} (a_i) = i$,

[1031] If the reader finds the empty product troublesome she could take this to be equal to (123)(123).

which is then moved by (ij) to j, and then by $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & n \end{pmatrix}$ to a_j; and, similarly, a_j is moved to a_i; to the product is equal to the transposition $(a_i a_j)$, as claimed.

D.3 Third 1999 Problem Assignment

1. For each of the following sets, determine whether the information given defines an associative binary operation $*$. If that is the case, prove it; if not, provide a counterexample.

   (a) On $\mathbb{Z}$, $(a, b) \mapsto a - 2b$.

   (b) On $\mathbb{R} - \{0\}$, $(a, b) \mapsto (a^{-1} + b^{-1})^{-1}$

   (c) On $\mathbb{N}$, $(a, b) \mapsto \max\{a, b\}$.

   Solution:

   (a) This operation is not associative. For associativity is defined to mean the truth, for all $a, b, c \in \mathbb{Z}$, of the equation

   $$\begin{aligned} (a * b) * c &= a * (b * c) \\ \text{i.e. of} \quad a - 2b - 2c &= a - 2b + 4c \\ \text{equivalently, of} \quad c &= 0 \end{aligned}$$

   So we can find a counterexample by taking any value $c \neq 0$, and any a and any b. For example, with $a = 0 = b$, $c = 1$, we have the counterexample

   $$(0 * 0) * 1 = 0 * 1 = -2 \neq 4 = 0(-2) = 0 * (0 * 1)\,.$$

   (b) Where the operation is defined, its behavior is indeed associative, since

   $$(a * b) * c = \left(\left(\left(a^{-1} + b^{-1}\right)^{-1} \right)^{-1} + c^{-1} \right)^{-1} = \left(a^{-1} + b^{-1} + c^{-1}\right)^{-1} = \ldots$$

   The problem is that the definition does not always give an image in $\mathbb{R}$ for a pair of points in $\mathbb{R}^2$. For example, when $0 \neq a = -b$, the sum $(a^{-1} + b^{-1}) = 0$, which is not invertible. Thus $*$ is not an operation on $\mathbb{R}$.

   (c) This operation is indeed associative. While we could perhaps reason it out verbally, we will provide a formal proof based on the 3! possible orders of the

three points in $\mathbb{N}$:

Case	$a * b$	$(a * b) * c$	$b * c$	$a * (b * c)$
$a \leq b \leq c$	b	c	c	c
$a \leq c \leq b$	b	b	b	b
$b \leq a \leq c$	a	c	c	c
$b \leq c \leq a$	a	a	c	a
$c \leq a \leq b$	b	b	b	b
$c \leq b \leq a$	a	a	b	a

Associativity follows from the identity of columns ##3,5.

2. Suppose that a set $\mathfrak{A}$ consists of three distinct members, a, b, c. Showing all your work, determine all semigroups — if there are any — $(\mathfrak{A}, *)$ whose Cayley table contains the following three entries:

$*$	a	b	c
a		b	
b		c	
c		a	

Solution: The entire solution will be based on the consequences of associativity. From the table $(a * a) * b = a * (a * b) = a * b$, and this, again from the table, $= b$. Thus $a * a$ must be one of the elements of $x \in \mathfrak{A}$ such that $x * b = b$. Looking down the column for b we see that there is precisely one element x with this property — $x = a$, so $a * a = a$. The same type of argument, when applied to $(b * a) * b$ and $(c * a) * b$, yields $b * a = b$, $c * a = c$. The table is now

$*$	a	b	c
a	a	b	
b	b	c	
c	c	a	

Moving on to the last column of the table, $(a * c) * b = a * (c * b) = a * a = a$, so $a * c$ is the unique element y such that $y * b = a$, i.e. c. Proceeding in this way we can complete the table:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Thus there is at most one semigroup consistent with the given information. Does this prove that the table we have found actually defines a semigroup? No. It

could be possible that associativity might fail for some ordered triple other than the six that we checked.[1032] However, we recognize this table as corresponding to a familiar semigroup — indeed, it is a monoid, since a is evidently an identity. In fact, the monoid is a group. This group could be presented in various ways; for example, as $\mathcal{A}_3$ (taking, for example, $a = e$, $b = (123)$, $c = (132)$).

3. In Theorem A.4.3.5 it is shown that, if $(\mathfrak{A}, *)$ is a semigroup, there exists a superset $\mathfrak{B}$ of $\mathfrak{A}$ such that $\mathfrak{B} = \mathfrak{A} \cup \{u\}$ $(u \notin \mathfrak{A})$ to which we can extend the composition of the given semigroup so that u is an identity of the composition of $(\mathfrak{B}, *)$. But suppose that $(\mathfrak{A}, *)$ has an identity e. Does this mean that $(\mathfrak{B}, *)$ has two identities, contradicting Theorem A.4.3.3? Explain by considering the semigroup $(\mathfrak{A}, *) = (\mathcal{D}_4, \circ)$ (the symmetry group of the square).

   Solution: When this construction is applied, the element which was an identity — the unique identity, by virtue of Theorem A.4.3.3 — of $(\mathfrak{A}, *)$ does not become an identity of the larger semigroup. For example, in the group $(\mathcal{D}_4, \circ)$, the identity element e is the identity function $\iota_{\{1,2,3,4\}} = (1)(2)(3)(4)$. When we adjoin a new identity u, we obtain a monoid with the Cayley table

	u	e	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(23)	(24)
u	u	e	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(23)	(24)
e	e	e	(1234)	(13)(24)	(1432)	(12)(34)	(13)	(14)(23)	(24)
(1234)	(1234)	(1234)	(13)(24)	(1432)	e	(13)	(14)(23)	(24)	(12)(34)
(13)(24)	(13)(24)	(13)(24)	(1432)	e	(1234)	(14)(23)	(24)	(12)(34)	(13)
(1432)	(1432)	(1432)	e	(1234)	(13)(24)	(24)	(12)(34)	(13)	(14)(23)
(12)(34)	(13)(34)	(12)(34)	(24)	(14)(23)	(13)	e	(1432)	(13)(24)	(1234)
(13)	(13)	(13)	(12)(34)	(24)	(14)(23)	(1234)	e	(1432)	(13)(24)
(14)(23)	(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(13)(24)	(1234)	e	(1432)
(24)	(24)	(24)	(14)(23)	(13)	(12)(34)	(1432)	(13)(24)	(1234)	e

   In this table only u is an identity. The element e is not an identity, since $u * e = e$; were it an identity, we would have to have $u * e = u$. (Of course, the 9-element monoid we have constructed is not a group: for example, there are repetitions in rows and columns of the table; alternatively, as there are no u's in most of the rows or columns of the table, most of the elements do not have inverses.)

4. Consider the set of all permutations of the natural numbers $\mathbb{N}$, i.e. the set of bijections $f : \mathbb{N} \to \mathbb{N}$. We cannot express all of these bijections using disjoint cycle notation, but they still form a permutation group. Give an example of a submonoid of this group which is not a subgroup.

   Solution: It was announced in the tutorial and the lectures that, if they wished, students could replace $\mathbb{N}$ by $\mathbb{Z}$.

   Referring to the same composition rule, when we speak of a submonoid, we require the presence of the identity and closure under composition; when we speak of a

[1032] For this operation associativity consists of 27 equations.

subgroup we require the presence of the identity and closure under both composition and the taking of inverses. One example of a submonoid is the that generated by non-negative powers of the function given by

(...864213579...)

That is, any even integer $2n > 2$ is mapped on to $2(n-1)$; 2 is mapped on to 1; and every odd integer $2m-1$ is mapped on to the next larger odd integer. If the set is changed to $\mathbb{Z}$, then a simple example is the set of translations to the right: $\phi_a : \mathbb{N} \to \mathbb{N}$ defined by $\phi_a = n + a$, where $a \geq 0$. Here $\phi_0 = \iota$. This set is not closed under the taking of inverses, and is therefore not a subgroup.

(In constructing these examples we were forced to consider permutations of an *infinite* set, since the set of permutations of a finite set forms a finite group; and, in a finite group, a subset is a subgroup iff it contains the identity and is closed under composition — it is not necessary to check for closure under the taking of inverses, as this is a consequence of the other conditions, *for a finite subset of a group*.)

5. Let V be a real vector space of dimension 3.

   (a) Show that the set of linear transformations from V to V form a semigroup under composition. Explain with an example why this semigroup is not a permutation group. Determine whether or not it is a monoid.

   (b) Prove or disprove: Aside from the subgroup consisting of the identity function alone, every subsemigroup of the semigroup studied in the preceding part of this problem is not a permutation group on V.

   Solution:

   (a) Some of the elements of this semigroup are not permutations. Indeed, any linear transformation having a non-trivial kernel[1033] is such that two distinct vectors — here 0 and at least one other vector — are mapped to the same vector, so such a linear transformation is not injective.

   (b) There are subsemigroups that are permutation groups of V. One example is the set consisting of the identity transformation I and of $-I$. A larger example is the subset of *invertible* linear transformations $GL(3, \mathbb{R})$, of which $\{I, -I\}$ is a subgroup; there are other subgroups of $GL(3, \mathbb{R})$, for example $\{rI | r \in \mathbb{R} - \{0\}\}$.

[1033]= null space = the set of vectors mapped on to $\vec{0}$

6. Let $\mathfrak{A}$ be a given set containing an element a, and $f : \mathfrak{A} \times \mathfrak{A} \to \mathfrak{A}$ a binary operation such that

$$(\forall b \in \mathfrak{A})[f(a,b) = b = f(b,a)] \tag{1079}$$

$$(\forall b \in \mathfrak{A})(\forall c \in \mathfrak{A})(\forall d \in \mathfrak{A})[f(f(d,c),b) = f(d,f(b,c))] \tag{1080}$$

Prove that $(\mathfrak{A}, f)$ is a commutative monoid.

Solution: (cf. [8, Problem 3.30]) Setting $d := a$ in (1080), and applying (1079) twice, we obtain

$$(\forall b \in \mathfrak{A})(\forall c \in \mathfrak{A})[f(c,b) = f(b,c)]\,, \tag{1081}$$

which proves commutativity of f.[1034] Knowing this, we may return to (1080) to conclude that

$$(\forall b \in \mathfrak{A})(\forall c \in \mathfrak{A})(\forall d \in \mathfrak{A})[f(f(d,c),b) = f(d,f(b,c)) = f(d,f(c,b))] \tag{1082}$$

thereby proving associativity. Thus $(\mathfrak{A}, f)$ is a commutative semigroup.

By (1079), the element $a \in \mathfrak{A}$ is an identity element for f. Thus $(\mathfrak{A}, f, a)$ is a commutative monoid. □

D.4 Fourth 1999 Problem Assignment

1. (Exercise A.5.2.10) Certain pairs of the following groups are isomorphic. Where that is so, give an isomorphism. Where that is false, prove it.

   (a) $(\mathbb{Z}_6, +, (6))$ and $(\mathbb{Z}_7^\times, \times, 1 + (7))$.

   (b) $(\mathbb{Z}_6, +, (6))$ and $\mathcal{S}_3$.

   Solution:

   (a) The group $(\mathbb{Z}_7^\times, \times, 1 + (7))$ contains all the invertible elements of $\mathbb{Z}_7$, i.e. all but $[0]_7$. Thus it is an abelian group of order 6. As we shall see later that there is only one such group, we know that an isomorphism must exist with the cyclic group $(\mathbb{Z}_6, +, (6))$. This "existence" result is insufficient here, as we have to produce an isomorphism. We know that the identity elements must correspond. As for the others, an element of order k must correspond to one of order k for all k. So a first step will be to determine the orders of elements of $(\mathbb{Z}_7^\times, \times, 1 + (7))$. By repeated multiplication we determine that $[2]^2 = [4]$, $[2]^3 = [8] = [1]$, so the order of $[2]$ is 3; $[3]^2 = [9] = [2]$, $[3]^3 = [27] = [6]$, $[3]^4 = [81] = [4]$, $[3]^5 = [3 \cdot 4] = [12] = [5]$, $[3]^6 = [729] = [1]$. Thus $[3]$ is

[1034] Note that (1079) is not the full commutativity property: it asserts only that one element a commutes with any element of the set, not that *any* element commutes with any element!

a generator of this group. An isomorphism will then be given by $[k] \mapsto [3]^k$. (Another generator is [5], so another isomorphism is given by $[k] \mapsto [5]^k$.)

(b) The group $(\mathbb{Z}_6, +, (6))$ is abelian, while $\mathcal{S}_3$ is not. Thus these groups cannot be isomorphic.

2. (a) (Exercise A.5.2.11) When $(\mathfrak{B}, *, e)$ is a *non*-abelian group, the function $a \longmapsto a^n$ is still well defined for every integer n; thus $\mathbb{Z}$ still *operates* on $(\mathfrak{B}, *, e)$. But there the function need not be a homomorphism. Prove that the mapping $a \longmapsto a^2$ is a homomorphism iff the group is abelian!

(b) Show that an abelian group cannot be isomorphic to a non-abelian group.

(c) Determine for which groups $(\mathfrak{B}, *, e)$ the function $x \mapsto x^{-1}$ is an isomorphism.

Solution:

(a) i. Suppose that the function $a \mapsto a^2$ is a homomorphism. Then for all $a_1, a_2 \in \mathfrak{B}$ $(a_1a_2)^2 = a_1^2a_2^2$, i.e. $a_1a_2a_1a_2 = a_1a_1a_2a_2$. Premultiplication by a_1^{-1} and postmultiplication by a_2^{-1} yield $a_2a_1 = a_1a_2$. But this (quantified $\forall a_1 \forall a_2$) is precisely the definition of commutativity.

ii. If $\mathfrak{B}$ is commutative, then, for all a_1, a_2,

$$\begin{aligned} (a_1a_2)^2 &= a_1a_2a_1a_2 && \text{by definition of 2nd power} \\ &= a_1a_1a_2a_2 && \text{by commutativity} \\ &= a_1^2a_2^2 \end{aligned}$$

proving that squaring is a homomorphism.

(b) Suppose that $\mathfrak{A}$ is an abelian group and $\mathfrak{B}$ is non-abelian; for convenience we will write both groups multiplicatively, by juxtaposition, and represent the identity by e in both cases, if needed. Suppose that $\phi : \mathfrak{B} \to \mathfrak{A}$ is an isomorphism.

Since $\mathfrak{B}$ is not abelian, it contains two elements b_1 and b_2 such that $b_1b_2 \neq b_2b_1$. Under the isomorphism ϕ these would be mapped on to distinct elements, so we have

$$\phi(b_1)\phi(b_2) = \phi(b_1b_2) \neq \phi(b_2b_1) = \phi(b_2)\phi(b_1)$$

but this is a contradiction to the commutativity of the group operation in $\mathfrak{A}$: we should have $\phi(b_1)\phi(b_2) = \phi(b_2)\phi(b_1)$. From this contradiction we conclude that no isomorphism ϕ can exist between a non-abelian and an abelian group.

(c) What, we ask, characterizes a group $\mathfrak{A}$ in which the following equation is true for all a: $(ab)^{-1} = a^{-1}b^{-1}$? Since the left side is equal to $b^{-1}a^{-1}$, the condition

we wish to characterize is $\forall a \forall b \left[b^{-1}a^{-1} = a^{-1}b^{-1}\right]$. Let a_1, a_2 be any two elements of the group. Then $a_2 a_1 = \left(a_2^{-1}\right)^{-1}\left(a_1^{-1}\right)^{-1} = \left(a_1^{-1}\right)^{-1}\left(a_2^{-1}\right)^{-1} = a_1 a_2$. (Note that we had to first show that every element could be expressed as the inverse of some element, in order to use the hypothesis.)

3. (a) (cf. Theorem A.5.4.6.2) Show that, for any group $\mathfrak{A}$, the mapping $R : \mathfrak{A} \to S_{\mathfrak{A}}$ given by $a \mapsto R_a$, where $R_a(x) = xa^{-1}$ is a one-to-one homomorphism.

   (b) When $\mathfrak{A}$ is the subgroup of A_4 (the alternating group) with elements e, (12)(34), (13)(24), (14)(23), determine the image of the homomorphism R, expressing each of its elements in disjoint cycle notation.

   (c) Determine the left cosets of the image of R in $S_{\mathfrak{A}}$.

   Solution: We will have to describe, in disjoint cycle notation, permutations of the elements of $S_{\mathfrak{A}}$, *which are themselves permutations, written in disjoint cycle notation.* In order to minimize confusion, we will write commas between the elements of the cycles of elements of $S_{\mathfrak{A}}$. Thus, for example, $(e, (12)(34))$ represents the 2-cycle

$$\begin{pmatrix} e & (12)(34) & (13)(24) & (14)(23) \\ (12)(34) & e & (13)(24) & (14)(23) \end{pmatrix}$$

   (a) i. To prove that R is a homomorphism, we have to prove that $R_a \circ R_b = R_{ab}$ for all $a, b, \in \mathfrak{A}$. This is an equation between functions, in particular, bijections — permutations of the *set* $\mathfrak{A}$. These functions all have domain and codomain equal to $\mathfrak{A}$, so that we need to prove they have the same *action* on all elements of their common domain, $\mathfrak{A}$. Let g be any element of $\mathfrak{A}$. Then

$$\begin{aligned} \left(R_a \circ R_b\right)(g) &= R_a\left(R_b(x)\right) && \text{by definition of } \circ \\ &= R_a\left(gb^{-1}\right) && \text{by definition of } R_b \\ &= \left(gb^{-1}\right)a^{-1} && \text{by definition of } R_a \\ &= g\left(b^{-1}a^{-1}\right) \\ &= g * (ab)^{-1} \\ &= R_{ab}(g) \end{aligned}$$

   so $R_a \circ R_b = R_{ab}$.

   ii. We need to show that if $R_a = R_b$, then $a = b$. We can actually prove a much stronger fact: even if $R_a(g) = R_b(g)$ for just one element g, from this alone it follows that $a = b$. For

$$R_a(g) = R_b(g) \quad \Rightarrow \quad ga^{-1} = gb^{-1}$$

$$\begin{aligned} &\Rightarrow\ g^{-1}ga^{-1} = g^{-1}gb^{-1} \\ &\Rightarrow\ a^{-1} = b^{-1} \\ &\Rightarrow\ a = b \end{aligned}$$

(b) $R_e = I$, since any homomorphism maps the identity on to the identity.
$R_{(12)(34)} = (e,(12)(34))((13)(24),(14)(23))$
$R_{(13)(24)} = (e,(13)(24))((14)(23),(12)(34))$
$R_{(14)(23)} = (e,(14)(23))((12)(34),(13)(24))$

(c) $S_{\mathfrak{A}}$ has $4! = 24$ elements, so there will be $24/4 = 6$ left cosets. Denote the image of R, studied in the previous part, by H. Then

IH is the subgroup H.
$(e,(12)(34))H$ contains

$$\begin{aligned} (e,(12)(34))I &= (e,(12)(34)) \\ (e,(12)(34))(e,(12)(34))((13)(24),(14)(23)) &= ((13)(24),(14)(23)) \\ (e,(12)(34))(e,(13)(24))((14)(23),(12)(34)) &= (e,(13)(24),(12)(34),(14)(23)) \\ (e,(12)(34))(e,(14)(23))((12)(34),(13)(24)) &= (e,(14)(23),(12)(34),(13)(24)) \end{aligned}$$

$(e,(13)(24))H$ contains

$$\begin{aligned} (e,(13)(24))I &= (e,(13)(24)) \\ (e,(13)(24))(e,(12)(34))((13)(24),(14)(23)) &= (e,(12)(34),(13)(24),(14)(23)) \\ (e,(13)(24))(e,(13)(24))((14)(23),(12)(34)) &= ((14)(23),(12)(34)) \\ (e,(13)(24))(e,(14)(23))((12)(34),(13)(24)) &= (e,(14)(23),(13)(24),(12)(34)) \end{aligned}$$

$(e,(14)(23))H$ contains

$$\begin{aligned} (e,(14)(23))I &= (e,(14)(23)) \\ (e,(14)(23))(e,(12)(34))((13)(24),(14)(23)) &= (e,(12)(34),(14)(23),(13)(24)) \\ (e,(14)(23))(e,(13)(24))((14)(23),(12)(34)) &= (e,(13)(24),(14)(23),(12)(34)) \\ (e,(14)(23))(e,(14)(23))((12)(34),(13)(24)) &= ((12)(34),(13)(24)) \end{aligned}$$

so we have now accounted for all $(4-1)! = 6$ of the 4-cycles, for all $\binom{4}{2} = 6$ of the 2-cycles — i.e. the permutations of form $(\bullet\bullet)(\bullet)(\bullet)$, for all $\frac{4!}{2!2!2!} = 3$ of the permutations of the form $(\bullet\bullet)(\bullet\bullet)$, and for the identity.

$(e,(12)(34),(13)(24))H$ contains

$$(e,(12)(34),(13)(24))I = (e,(12)(34),(13)(24))$$

$$\begin{aligned}
(e,(12)(34),(13)(24))(e,(12)(34))((13)(24),(14)(23)) &= (e,(13)(24),(14)(23))\\
(e,(12)(34),(13)(24))(e,(13)(24))((14)(23),(12)(34)) &= ((13)(24),\\
&\qquad (12)(34),(14)(23))\\
(e,(12)(34),(13)(24))(e,(14)(23))((12)(34),(13)(24)) &= (e,(14)(23),(12)(34))
\end{aligned}$$

$(e,(13)(24),(12)(34))H$ contains

$$\begin{aligned}
(e,(13)(24),(12)(34))I &= (e,(12)(34),(13)(24))\\
(e,(13)(24),(12)(34))(e,(12)(34))((13)(24),(14)(23)) &= ((12)(34),\\
&\qquad (13)(24),(14)(23))\\
(e,(13)(24),(12)(34))(e,(13)(24))((14)(23),(12)(34)) &= (e,(12)(34),(14)(23))\\
(e,(13)(24),(12)(34))(e,(14)(23))((12)(34),(13)(24)) &= (e,(14)(23),(13)(24))
\end{aligned}$$

D.5 Fifth 1999 Problem Assignment

1. Determine all positive integers m such that $\phi(m) = 10$.

   Solution: Let $m = p_1^{r_1}p_2^{r_2}\ldots p_n^{r_n}$ be the decomposition of m into distinct primes $p_1 < p_2 < \ldots < p_n$. As none of the factors of 10 exceeds 10, none of $p_1,\ldots,p_n$ can exceed 11 (since $\phi(m) = m\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)$). Since $(7-1)\nmid 10$ and $(5-1)\nmid 10$, the only possible prime decompositions of m are of the form $m = 2^{r_1}3^{r_2}11^{r_3}$. As $11\nmid\phi(m)$ and $3\nmid\phi(m)$, $r_3 \le 1$ and $r_2 \le 1$; as $4\nmid\phi(m)$, $r_1 \le 2$. The problem is thus reduced to $3\times 2\times 2 = 12$ cases. While it is possible to further refine the solution, we will content ourselves with tabulating these 12 values for m and the corresponding values for $\phi(m)$:

r_1	r_2	r_3	m	$\phi(m)$
0	0	0	1	1
0	0	1	11	10
0	1	0	3	2
0	1	1	33	20
1	0	0	2	1
1	0	1	22	10
1	1	0	6	2
1	1	1	66	20
2	0	0	4	2
2	0	1	44	20
2	1	0	12	4
2	1	1	132	40

   from which we see that $m = 11$ or $m = 22$.

2. Determine the structure of groups $\mathbb{Z}_n^\times$ until the first n where the group is not cyclic. Where the group is cyclic, determine all elements which can serve as generator.

   Solution: (A characterization of those groups which are cyclic is discussed in Theorem A.6.4.2 — which will not be discussed in this course.) We will examine the structure of these groups until we find the first n for which the group is not cyclic.

   $\mathbb{Z}_1^\times$**:** This group contains only the class $[1]_1$, so it is cyclic, generated by its identity element.

   $\mathbb{Z}_2^\times$**:** This group contains only the element $[1]_2$, — i.e. the identity element (under multiplication), so it is cyclic, again generated by its identity element.

   $\mathbb{Z}_3^\times$**:** This group contains only a prime number of elements, $[1]_3$ and $[2]_3$, so it is cyclic, generated by the only element which is not the identity — $[2]_3$.

   $\mathbb{Z}_4^\times$**:** The elements of this group are $[1]_4$ and $[3]_4$; being of prime order, this group is also cyclic, generated by $[3]_4$.

   $\mathbb{Z}_5^\times$**:** This group contains elements $[1]_5$, $[2]_5$, $[3]_5$, and $[4]_5$. While the order of the group is not prime, the group is still cyclic; it is generated by either of $[2]_5$ or $[3]_5$.

   $\mathbb{Z}_6^\times$**:** This group contains elements $[1]_6$ and $[5]_6$. As the order is prime, this group is cyclic — generated by $[5]_6$.

   $\mathbb{Z}_7^\times$**:** This group contains 6 elements. It is cyclic, generated by either of $[3]_7$ or $[5]_7$.

   $\mathbb{Z}_8^\times$**:** This group is not cyclic; it consists of $[1]_8$, $[3]_8$, $[5]_8$, and $[7]_8$ — all of which satisfy the equation $x^2 = e$ — i.e. all of which have order dividing 2, i.e. equal to 1 or 2. For a group of order m to be cyclic it must contain at least one element of order m.

   (In the theorem cited earlier it is shown that $\mathbb{Z}_n^\times$ is cyclic iff n is either 1, 2, or 4, or is a positive power of an odd prime, or twice a positive power of an odd prime.)

3. Determine the smallest non-negative member of the residue class $[a]_{72}$, where $a = 5^{1,111,111}$, by calculations similar to those in Exercise A.6.2.10. With the exception of the exponent 1,111,111, you should not have to work with decimal integers greater than 1000. No calculators should be used.

   Solution: $72 = 2^3 \times 3^2$, so $\phi(72) = 2^2 \cdot (2-1) \cdot 3^1 \cdot (3-1) = 24$. Since $(5, 2^3) = 1 = (5, 3^2)$, we may apply Euler's generalization of Fermat's Little Theorem, to obtain

$$5^{24} \equiv 1 \pmod{72}$$

or, better still,

$$\begin{aligned} 5^6 &\equiv 1 \pmod 9 \\ 5^4 &\equiv 1 \pmod 8 \end{aligned}$$

from which it follows that $5^{12} \equiv 1$ to both relatively prime moduli 8 and 9, so $5^{12} \equiv 1 \pmod{72}$. Since

$$1\,111\,111 = 92\,592 \cdot 12 + 7\,,$$

$[5^{1111111}]_{72} = ([5^{12}]_{72})^{92592}\,[5^7]_{72} = [1]_{72}\,[5^7]_{72} = [5^7]_{72}$.
Since $7 = (111)_2$, and $5^4 \equiv 25^2 \equiv 625 \equiv 49 \pmod{72}$, $5^7 \equiv 5^4 \cdot 5^2 \cdot 5^1 \equiv 49 \cdot 25 \cdot 5 \equiv 49 \cdot 53 \equiv 245 \cdot 25 \equiv 29 \cdot 25 \equiv 725 \equiv 5 \pmod{72}$.

4. (a) Supply explanations to the steps of the following proof that there do not exist integers a and b such that

$$a^2 = 2b^2 \ : \tag{1083}$$

   i. Without limiting generality, we may assume that $(a, b) = 1$.
   ii. a admits a factorization of the form $a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ where $p_1, p_2, \ldots, p_n$ are distinct primes, and $r_1, r_2, \ldots, r_n$ are positive integers.
   iii. One of $p_1, p_2, \ldots, p_n$ is 2; without limiting generality, take $p_1 = 2$.
   iv. $2|b^2$.
   v. $2^2|b^2$, so $2|b$.
   vi. $2|(a, b)$, a contradiction.

   (b) (cf. Exercise A.7.2.11.4) Consider the ring of quotients $\dfrac{a + b\sqrt{5}}{c + d\sqrt{5}}$, where $a, b, c, d \in \mathbb{Z}$, and c and d are *not both zero*. Show that this ring is a *field*. Then show that if we replace $\sqrt{5}$ by $\sqrt{2}$, we obtain a different field. Explain also what happens if we replace 5 by 4.

Solution:

(a) i. *Without limiting generality, we may assume that* $(a, b) = 1$. For equation (1083) may be rewritten as

$$(a, b)^2 \left(\frac{a}{(a, b)}\right)^2 = 2(a, b)^2 \left(\frac{b}{(a, b)}\right)^2$$

which implies that

$$\left(\frac{a}{(a, b)}\right)^2 = 2\left(\frac{b}{(a, b)}\right)^2 ;$$

in this version of (1083) the variables are relatively prime.

ii. *a admits a factorization of the form $a = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ where $p_1, p_2, \dots, p_n$ are distinct primes, and $r_1, r_2, \dots, r_n$ are positive integers.* This follows from the fundamental theorem of number theory.

iii. *One of $p_1, p_2, \dots, p_n$ is 2; without limiting generality, take $p_1 = 2$.* Since the 2 divides the right side of the equation, it must divide the left side, which has been factorized into a product of powers of primes. It must be one of those primes; we choose the labelling of those primes so that 2 is p_1.

iv. $2|b^2$. Since $a = 2^{r_1} p_2^{r_2} \dots p_n^{r_n}$, $a^2 = 2^{2r_1} p_2^{2r_2} \dots p_n^{2r_n}$, which is divisible by 2^2 since $r_1 \geq 1$.

v. *$2^2|b^2$, so $2|b$.* As $4|a^2$, $4|2b^2$, so $2|b^2$. By the same reasoning as above, we conclude that $2|b$.

vi. *$2|(a, b)$, a contradiction.* We have proved that $2|a$ and $2|b$, so 2 is a common factor of a, and b, and must therefore divide (a, b), by definition of the greatest common factor (defined to be a common factor which is divisible by all common factors).

The result we have just proved could be paraphrased as saying: $\sqrt{2}$ is irrational.

(b) First observe that, by the irrationality of $\sqrt{5}$ (which can be proved in the same way as the irrationality of $\sqrt{2}$ proved above), $c + d\sqrt{5}$ cannot be zero, so the quotients are well defined. Thus we are working with a subset of the real numbers, and can prove it is a ring simply by proving closure under addition and multiplication. To prove it is a sub*field* we will also have to prove closure under the taking of the multiplicative inverse (for any non-zero quotient). To prove that this field is "different" from the field obtained using quotients with $\sqrt{2}$, we can show that in this field there exists an element u such that $u^2 = 5$, whereas no such element exists in the field constructed with $\sqrt{2}$.

i. Since

$$\begin{aligned} & \frac{a + b\sqrt{5}}{c + d\sqrt{5}} + \frac{a' + b'\sqrt{5}}{c' + d'\sqrt{5}} \\ = \; & \frac{((ac' + a'c) + 5(bd' + b'd)) + (ad' + bc' + a'd + b'c)\sqrt{5}}{(cc' + 5dd') + (cd' + c'd)\sqrt{5}} \end{aligned}$$

which is a quotient of the same type, the set of these quotients is closed under addition.

ii. Since

$$\frac{a + b\sqrt{5}}{c + d\sqrt{5}} \cdot \frac{a' + b'\sqrt{5}}{c' + d'\sqrt{5}}$$

$$= \frac{(aa' + 5bb') + (ab' + a'b)\sqrt{5}}{(cc' + 5dd') + (cd' + c'd)\sqrt{5}}$$

which is a quotient of the same type, the set of these quotients is closed under multiplication.

iii. For a and b not both zero, $\left(\frac{a+b\sqrt{5}}{c+d\sqrt{5}}\right)\left(\frac{c+d\sqrt{5}}{a+b\sqrt{5}}\right) = 1$, so the inverse of $\left(\frac{a+b\sqrt{5}}{c+d\sqrt{5}}\right)$ is $\left(\frac{c+d\sqrt{5}}{a+b\sqrt{5}}\right)$, a quotient of the same type. Thus the set of non-zero quotients is closed under the taking of inverses.

We have thus proved that these quotients form a subfield of the field $\mathbb{R}$ of real numbers. This construction could have been carried out with any prime p replacing 5. Were we to replace 5 by 4, the resulting construction would still yield a field, provided we required, in place of requiring that not both c and d be zero, that $c + d\sqrt{4} \neq 0$; in this case the field obtained is $\mathbb{Q}$.

To show that the fields obtained when primes 2 and 5 are used are different, it suffices to observe that, when 5 is used, the resulting field contains an element whose square is 5: take $a = 0 = d$, $b = 1 = c$. But there exist no 4 integers a, b, c, d such that $\left(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}\right)^2 = 5$. For this would entail that

$$(a^2 + 2b^2) - 5(c^2 + 2d^2) = (10cd - 2ab) \cdot \sqrt{2}$$

This would imply the contradiction that $\sqrt{2}$ is rational, unless both of the following equations hold:

$$(a^2 + 2b^2) - 5(c^2 + 2d^2) = 0 \quad (1084)$$

$$10cd - 2ab = 0 \quad (1085)$$

Without limiting generality, let us assume that the greatest (positive) common divisor of a, b, c, d is 1. From (1085) it follows that $5|a$ or $5|b$. Applying this information to (1084) implies that $5|2b^2$ or $5|a^2$, which, in turn, implies that $5|b$ or $5|a$. (Why?). These results imply, when applied to (1084), that $5|a$ and $5|b$ respectively; thus $5|(a, b)$. Further analysis of the equations then implies that $5|(c, d)$, so 5 divides all 4 of a, b, c, d, contradicting our hypothesis.

5. In the 189-240A course we used ordinary generating functions to solve counting problems. In some instances we used methods from the calculus to obtain power series expansions — methods that, when developed within the calculus, required

that a variable lie within an interval of convergence. Thus, for example, we treated the power series $\sum_{n=0}^{\infty} x^n$ as being equivalent to $(1-x)^{-1}$, even though that equivalence, in the context of the calculus, requires that $|x| < 1$. Your problem here is to justify the statement

$$(1-x)^{-1} = \sum_{n=0}^{\infty} x^n$$

by proving that the product of the two power series $1-x$ and $\sum_{n=0}^{\infty} x^n$ is the power series 1 (i.e. $1x^0 + 0x^1 + 0x^2 + ...$). You are to do this formally by induction; that is, to prove by induction on n that the coefficient of x^n is 0 when $n > 0$.

Solution: The Cauchy product of the two power series

$$\sum_{i=0}^{\infty} a_i x^i = 1x^0 - 1x^1 + 0x^2 + 0x^3 + \ldots + 0x^i + \ldots$$

and

$$\sum_{j=0}^{\infty} b_j x^j = 1x^0 + 1x^1 + 1x^2 + 1x^3 + \ldots + 1x^j + \ldots$$

has, as the coefficient of x^k, the sum of all products $a_i b_j$ where $i+j = k$; i.e. the sum of all products $a_i b_{k-i}$ where $0 \leq i \leq k$. We have defined $a_0 = 1$, $a_1 = -1$, $a_i = 0$ $(i \geq 2)$, and $b_j = 1$ $(j \geq 0)$. Thus $\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_i$; denote this sum by c_k. Then $c_0 = a_0 = 1$, $c_1 = c_0 + a_1 = 1 + (-1) = 0$; this is the base case. Suppose that it has been proved that $c_n = 0$, $(n \geq 1)$. Then $c_{n+1} = \sum_{i=0}^{n+1} a_i = a_{n+1} + \sum_{i=0}^{n} a_i = a_{n+1} + c_n = 0 + 0 = 0$. Thus it follows by the Principle of Induction that $c_n = 0$ for all $n \geq 1$. We have proved that the product of the two series is the series

$$1x^0 + 0x^1 + 0x^2 + 0x^3 + \ldots + 0x^i + \ldots$$

which is the identity of the ring $\mathbb{R}\{x\}$; i.e. we have proved that that two series are each the inverse of the other, $\square$.

6. (a) Determine a relationship between the constants a and b so that the polynomial $2x^4 - 7x^3 + ax + b$ be divisible by $x - 3$ over the field $\mathbb{R}$.

   (b) Determine what constraint on a and b will ensure that the polynomial is divisible by $(x-3)^2$.

   Solution:

   (a) ([14, Example XXXIV.a.2]) The polynomial will be divisible by $x - 3$ iff its value at $x = 3$ is 0, i.e. iff $2 \cdot 3^4 - 7 \cdot 3^3 + a \cdot 3 + b = 0$, i.e. iff $3a + b = 27$.

(b) Evidently divisibility by the square of $x-3$ entails divisibility by $x-3$. Thus a necessary condition is that $3a+b=27$. The quotient upon dividing the polynomial by $x-3$ can be computed, by long division, to be $2x^3-x^2-3x+(a-9)$. This polynomial will be divisible by $x-3$ iff *its* value at $x=3$ is 0, i.e. iff $2\cdot 3^3-3^2-3\cdot 3+(a-9)=0$, i.e. iff $a=-27$, which, because of the condition proved earlier, implies that $b=108$. (Another way to prove this would be to consider the *derivative* of the polynomial, and to impose on it the condition that it be divisible by $x-3$, since it can be shown that a polynomial is divisible by $(x-a)^2$ iff its derivative is divisible by $x-a$. Here the second condition would become $8\cdot 3^3-21\cdot 3^2+a=0$.)

7. (a) Prove that the polynomial $1+x+x^2+x^3+x^4$ is irreducible over the field $\mathbb{Z}_2$. [Hint: First apply the Remainder Theorem to show that there are no 1st degree factors. Then investigate the possibility of factoring this 4th degree polynomial into two 2nd degree polynomials.]

(b) Factorize $1+x+x^2+x^3+x^4$ into irreducible factors over the field $\mathbb{Z}_5$.

Solution:

(a) We first test for divisibility by a 1st degree factor, $x-a$, where a is any element of the field $\mathbb{Z}_2$. There are only two elements to test: 0 and 1 (more precisely, $[0]_2$ and $[1]_2$). Evaluating the polynomial at either of these points yields the value 1 (more precisely, $[1]_2$). By the Remainder Theorem, neither $x-0$ nor $x-1$ can be a factor of the polynomial — i.e. it admits no factorization in which there are 1st degree factors. The only other nontrivial type of factorization would be where the polynomial is a product of two 2nd degree factors. Suppose that

$$1+x+x^2+x^3+x^4=(ax^2+bx+c)(dx^2+ex+f)\,. \tag{1086}$$

Comparing coefficients of powers of x yields

$$\begin{aligned} 1 &= cf && (1087)\\ 1 &= bf+ce && (1088)\\ 1 &= af+be+cd && (1089)\\ 1 &= ae+bd && (1090)\\ 1 &= ad && (1091) \end{aligned}$$

From equation (1087) we conclude that c and f are both 1, since if either of them were 0, their product would also be 0; similarly, from (1091) we conclude that a and d are both 1. Now both equations (1088) and (1090) yield

$$1=b+e \tag{1092}$$

while equation (1089) yields, since $1 + 1 = 0$, the equation

$$1 = be\,. \tag{1093}$$

But this last equation implies that $b = e = 1$, which contradicts equation (1092). From this contradiction we conclude that a factorization of type (1086) is impossible: since the given polynomial also has no degree one factors, the polynomial does not admit a non-trivial[1035] factorization.

(b) By the Factor Theorem we see that $x - 1$ is a factor. Further applications show that, in fact, $1 + x + x^2 + x^3 + x^4 = (x - 1)^4$ over this field.

[1035] We say *non-trivial* since it does admit the *trivial* factorization,

$$1 + x + x^2 + x^3 + x^4 = 1 \cdot (1 + x + x^2 + x^3 + x^4)\,.$$

E 2000 Problem Assignments, with Solutions

E.1 First 2000 Problem Assignment

Notes:

- Some of the following exercises are related to exercises in [4]. It had been planned that that book would serve as textbook for this course, but the McGill Bookstore was unable to ensure that sufficient supplies would be available at the beginning of the term, and so the plan was abandoned. Students do not need to consult [4] to attempt these exercises. You might keep in mind, however, that that book is an interesting source, both for additional information and problems, and for applications of this part of the theory in the course.
- The emphasis in grading this assignment has been on identifying and indicating errors on your solutions, rather than on assigning realistic grades. Thus it may occur that the grade for some questions is higher than the solution would have received in a test or examination. Assignments should be viewed as learning experiences, rather than as tests.

1. (cf. [4, Exercise 1.E2]) Verify that the relation,

   > an ordered pair (a, b) is *equivalent* to an ordered pair (c, d) (written $(a, b) \sim (c, d)$) iff $ad = bc$

   is an equivalence relation on the set $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$.

   Solution:

   (a) **Reflexivity.** Let a and b be integers, $b \neq 0$. Then $ab = ba$; (this is the property of *commutativity* of multiplication of integers). If we treat the 1st b as the denominator and the second a as the numerator of the second ordered pair, $ab = ba$ implies that $(a, b) \sim (a, b)$.

   (b) **Symmetry.** Suppose that $(a, b) \sim (c, d)$, where a, b, c, d are integers, and neither b nor d is zero. By definition of $\sim$, this means that $ad = bc$. Let us write the equation in the reverse order, as $bc = ad$, and then reverse the orders of multiplication (again by virtue of *commutativity* of multiplication): $cb = da$. But this last equation corresponds to the truth of the statement $(c, d) \sim (a, b)$.

   (c) **Transitivity.** Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, where a, b, c, d, e, $f \in \mathbb{Z}$, and b, d, f are all non-zero. Then

   $$ad = bc \tag{1094}$$

   $$cf = de\,. \tag{1095}$$

Multiplying (1094) by f, and (1095) by b yields

$$adf = bcf \tag{1096}$$
$$bcf = bde\,. \tag{1097}$$

It follows that $adf = bde$; as $d \neq 0$, this implies that $af = be$, which is represented by $(a, b) \sim (e, f)$.

We usually denote the equivalence class containing (a, b) by $[a, b]$, rather than by $[(a, b)]$. We could also denote the class $[a, b]$ by the symbol $\frac{a}{b}$, and proceed to define arithmetic operations on these classes, thereby constructing the *field* $\mathbb{Q}$ of *rational* numbers.

2. Using mathematical induction, prove that, for any integers x, y, and for all integers $n \geq 1$, $x - y$ divides $x^n - y^n$. [Hint [4, p. 483]: Try using $x^{n+1} - y^{n+1} = x^{n+1} - xy^n + xy^n - y^{n+1}$.] Then prove that $x + y$ divides $x^\ell + y^\ell$ for any *odd* integer ℓ; but show that the requirement that ℓ be odd may not be relaxed.

Solution:

(a) Let $P(n)$ denote the statement "$x - y$ divides $x^n - y^n$".

Basis Step. Since $x^1 - y^1 = x - y = 1 \cdot (x - y)$, $(x - y)|(x^1 - y^1)$, and $P(1)$ is true.

Induction Step. Suppose that n is any positive integer. As our *induction hypothesis*, let us assume that $P(n)$ is true; that is, there exists an integer m such that $x^n - y^n = m \cdot (x - y)$. Then $x^{n+1} - y^{n+1} = x^{n+1} - xy^n + xy^n - y^{n+1} = x \cdot (x^n - y^n) + (x - y) \cdot y^n = x \cdot m \cdot (x - y) + (x - y) \cdot y^n = (xm + y^n) \cdot (x - y)$, so $(x - y)|\,(x^{n+1} - y^{n+1})$, and $P(n + 1)$ is true.

Hence $P(n)$ is true for all $n \geq 1$.

(b) Let $Q(n)$ denote the statement "$x + y$ divides $x^{2n-1} + y^{2n-1}$".

Basis Step. Since $x^1 + y^1 = x + y = 1 \cdot (x + y)$, $(x + y)|(x^{2\cdot 1-1} + y^{2\cdot 1-1})$, and $Q(1)$ is true.

Induction Step. Suppose that n is any positive integer. As our *induction hypothesis*, let us assume that $Q(n)$ is true; that is, there exists an integer m such that $x^{2n-1} + y^{2n-1} = m \cdot (x + y)$. Then $x^{2(n+1)-1} + y^{2(n+1)-1} = x^{2n+1} + y^{2n+1} = x^{2n+1} + x^2y^{2n-1} - x^2y^{2n-1} + y^{2n+1} = x^2 \cdot (x^{2n-1} + y^{2n-1}) - (x^2 - y^2) \cdot y^{2n-1} = x^2 \cdot m \cdot (x + y) - (x + y) \cdot (x - y) \cdot y^{2n-1} = (x^2m - y^{2n-1}(x - y)) \cdot (x + y)$, so $(x + y)|\,(x^{2n+1} + y^{2n+1})$, and $Q(n + 1)$ is true.

Hence $P(n)$ is true for all $n \geq 1$.

(c) A specific counterexample would suffice; we give a family of counterexamples. Take $\ell = 2$. Then $1^2 + y^2 = (y-1)(y+1) - 2$, so $1 + y$ could divide $1 + y^2$ only if $1 + y$ divides 2. But this is false when y is any integer except -3, -2, 1, or 0.

3. (a) Prove that, for any natural number $n > 10$, $3^n - 1$ and $3^n + 1$ are both composite.

(b) Prove that, for a natural number n, $3^n - 2^n$ can be prime only if n is prime. Determine the smallest n for which $3^n - 2^n$ is composite. You may need to use a calculator to determine this smallest n, and to test certain integers by trial division and/or tests for divisibility. [Hint: cf. solution to Exercise A.1.8.8.2.]

(c) Prove that, for any natural number n, $3^n + 2^n$ can be prime only if n is a power of 2. Determine the smallest non-negative integer n for which $3^n + 2^n$ is composite. You may need to use a calculator to determine this smallest n, and to test certain integers by trial division and/or tests for divisibility. [Hint: cf. solution to Exercise A.1.8.8.1.]

Solution:

(a) For any positive integer n, $3^n \pm 1 \equiv 1 \pm 1 \equiv 0 \pmod 2$, so both $3^n \pm 1$ are always even. Except for the case $3^1 - 1 = 2$, this even sum or difference is always greater than 2, so it is always an even composite integer.

(b) If n admits a factorization $n = ab$, where a and b *are both integers greater than 1 and less than* n, then

$$3^{ab} - 2^{ab} = (3^a - 2^a)\left(3^{(b-1)a} + 3^{(b-2)a}2^a + ... + 3^a 2^{(b-2)a} + 2^{(b-1)a}\right) .$$

We must show that neither of these factors is 1. This can be done in various ways, but students were expected to observe that this step is required, and to carry it out in some way. For example,

$$\begin{aligned} 3^a - 2^a &= (2+1)^a - 2^a \\ &= \left(2^a + \binom{a}{1}2^{a-1} + ...\right) - 2^a \geq \binom{a}{1}2^{a-1} \\ &\geq 2; \end{aligned}$$

and $3^{(b-1)a} + 3^{(b-2)a}2^a + ... + 3^a 2^{(b-2)a} + 2^{(b-1)a}$ is a sum of more than one positive term. Thus $3^n - 2^n$ is composite.

Now suppose that n is prime. We have proved above only that $3^n - 2^n$ *may* be prime. Testing its value for n =prime, we have

$$3^2 - 2^2 = 9 - 4 = 5 \quad \text{which is prime;}$$

$$\begin{aligned} 3^3 - 2^3 &= 27 - 8 = 19 \quad \text{which is prime;} \\ 3^5 - 2^5 &= 243 - 32 = 211 \quad \text{which is prime;} \\ 3^7 - 2^7 &= 2187 - 128 = 2059 = 29 \cdot 71 \end{aligned}$$

Thus 7 is the smallest *prime* exponent where $3^7 - 2^7$ is composite.[1036] However, the question asked only for the *smallest* (integer) n. With this reading, the correct answer is $n = 4$, since $3^4 - 2^4 = 65 = 5 \cdot 13$, which is composite.

(c) As in the solution to Exercise A.1.8.8.1, we observe that, if $n = pm$ is a factorization where p is an odd prime, and $m > 1$, then

$$3^n + 2^n = (3^m + 2^m)\left(3^{(p-1)m} - 3^{(p-2)m}2^m + ... - 3^m 2^{(p-2)m} + 2^{(p-1)m}\right) .$$

Here $3^n + 2^n > 3^m + 2^m > 3 + 2 = 5 > 1$, so the factorization is not trivial (i.e., neither factor is 1). Thus the only way in which $3^n + 2^n$ can fail to be composite is for n to have no odd prime factors, i.e. to be a product of 2's.

However, the question asked for "the smallest non-negative integer n for which $3^n + 2^n$ is composite", and did not insist that n be a power of 2. With this simplistic reading, the smallest n is $n = 3$, since $3^3 + 2^3 = 35$, which is composite.

$$\begin{aligned} 3^{2^0} + 2^{2^0} &= 3^1 + 2^1 = 5 \quad \text{which is prime;} \\ 3^{2^1} + 2^{2^1} &= 3^2 + 2^2 = 13 \quad \text{which is prime;} \\ 3^{2^2} + 2^{2^2} &= 3^4 + 2^4 = 97 \quad \text{which is prime;} \\ 3^{2^3} + 2^{2^3} &= 3^8 + 2^8 = 6561 + 256 = 6817 = 17 \cdot 41. \end{aligned}$$

Here the arithmetic is easier than in the preceding case: the primeness of 97 is easily seen by testing for divisibility by all primes $< \sqrt{97}$, i.e. by 3, 5, 7; for 6817 the computations could have proved more difficult, as we might have had to test all primes less than $\sqrt{6817}$; fortunately a "small" prime proved to be a divisor.

4. (a) [4, Exercise 2F.E1] Showing all your work, write $(176)_{10}$ and $(398)_{10}$ in base 2 and multiply them. Check your multiplication by multiplying them in base 10 and converting the answer to base 2.

(b) Showing all your work, write the (fractional) decimal number $(176.3)_{10}$ in base 2.

Solution:

[1036] To observe this on has to examine each of 5, 19, 211, 2059 and to determine whether it was prime by carrying out trial divisions and/or using tests for divisibility.

(a)

$$\begin{aligned} 176 &= 2 \cdot 88 + 0 \\ 88 &= 2 \cdot 44 + 0 \\ 44 &= 2 \cdot 22 + 0 \\ 22 &= 2 \cdot 11 + 0 \\ 11 &= 2 \cdot 5 + 1 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \\ &\Rightarrow 176 = (10110000)_2 \end{aligned}$$

$$\begin{aligned} 398 &= 2 \cdot 199 + 0 \\ 199 &= 2 \cdot 99 + 1 \\ 99 &= 2 \cdot 49 + 1 \\ 49 &= 2 \cdot 24 + 1 \\ 24 &= 2 \cdot 12 + 0 \\ 12 &= 2 \cdot 6 + 0 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \\ &\Rightarrow 398 = (110001110)_2 \end{aligned}$$

								1	1	0	0	0	1	1	1	0
								×	1	0	1	1	0	0	0	0
				1	1	0	0	0	1	1	1	0				
			1	1	0	0	0	1	1	1	0					
	1	1	0	0	0	1	1	1	0							
1	0	0	0	1	0	0	0	1	1	0	1	0	0	0	0	0

Verification: Working in the decimal scale we see that

		3	9	8
	×	1	7	6
	2	3	8	8
2	7	8	6	
3	9	8		
7	0	0	4	8

$$\begin{aligned}
\text{and} \quad 70048 &= 2 \cdot 35024 + 0 \\
35024 &= 2 \cdot 17512 + 0 \\
17512 &= 2 \cdot 8756 + 0 \\
8756 &= 2 \cdot 4378 + 0 \\
4378 &= 2 \cdot 2189 + 0 \\
2189 &= 2 \cdot 1094 + 1 \\
1094 &= 2 \cdot 547 + 0 \\
547 &= 2 \cdot 273 + 1 \\
273 &= 2 \cdot 136 + 1 \\
136 &= 2 \cdot 68 + 0 \\
68 &= 2 \cdot 34 + 0 \\
34 &= 2 \cdot 17 + 0 \\
17 &= 2 \cdot 8 + 1 \\
8 &= 2 \cdot 4 + 0 \\
4 &= 2 \cdot 2 + 0 \\
2 &= 2 \cdot 1 + 0 \\
1 &= 2 \cdot 0 + 1 \\
&\Rightarrow 70048 = (10001000110100000)_2
\end{aligned}$$

(b) Suppose that

$$0.3 = \frac{a_1}{2^1} + \frac{a_2}{2^2} + \frac{a_3}{2^3} + \frac{a_4}{2^4} + \ldots + \frac{a_i}{2^i} + \ldots \tag{1098}$$

Then

$$\begin{aligned}
0.6 &= a_1 + \frac{a_2}{2^1} + \frac{a_3}{2^2} + \frac{a_4}{2^3} + \ldots + \frac{a_i}{2^{i-1}} + \ldots \\
&\Rightarrow a_1 = \lfloor 0.6 \rfloor = 0 \\
1.2 &= a_2 + \frac{a_3}{2^1} + \frac{a_4}{2^2} + \frac{a_5}{2^3} + \ldots + \frac{a_i}{2^{i-2}} + \ldots \\
&\Rightarrow a_2 = \lfloor 1.2 \rfloor = 1 \\
0.4 &= a_3 + \frac{a_4}{2^1} + \frac{a_5}{2^2} + \frac{a_6}{2^3} + \ldots + \frac{a_i}{2^{i-3}} + \ldots \\
&\Rightarrow a_3 = \lfloor 0.4 \rfloor = 0 \\
0.8 &= a_4 + \frac{a_5}{2^1} + \frac{a_6}{2^2} + \frac{a_7}{2^3} + \ldots + \frac{a_i}{2^{i-4}} + \ldots \\
&\Rightarrow a_4 = \lfloor 0.8 \rfloor = 0 \\
1.6 &= a_5 + \frac{a_6}{2^1} + \frac{a_7}{2^2} + \frac{a_8}{2^3} + \ldots + \frac{a_i}{2^{i-5}} + \ldots
\end{aligned}$$

$$\begin{aligned} & \Rightarrow a_5 = \lfloor 1.6 \rfloor = 1 \\ 1.2 \;=\; & a_6 + \frac{a_7}{2^1} + \frac{a_8}{2^2} + \frac{a_9}{2^3} + \ldots + \frac{a_i}{2^{i-6}} + \ldots \\ & \Rightarrow a_6 = \lfloor 1.2 \rfloor = 1 \end{aligned}$$

We can now see that $a_7 = a_3$, $a_8 = a_4$, $a_9 = a_5$, $a_{10} = a_6 = a_2$, etc.; $(0.3)_{10} = \left(\frac{1}{2^2} + \frac{1}{2^6} + \frac{1}{2^{10}} + ... + \frac{1}{2^{2+4k}} + ...\right) \cdot \left(1 + \frac{1}{2^3}\right) = (0.010011001100110011001...)_2$. Since $(176)_{10} = (10110000)_2$, it follows that

$$(176.3)_{10} = (10110000.010011001100110011001...)_2 .$$

5. (cf. [4, Exercise 2F.E5]) Showing all your work, divide $(110110011)_2$ into $(1100000100101)_2$ using long division in base 2. (The division is not exact — there will be a remainder.)

   Solution:

$$\begin{array}{rcccccccccccc} & & & & & & & & & 1 & 1 & 1 & 0 \\ \cline{2-13} 110110011) & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ & & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & & & \\ \cline{3-11} & & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & & \\ & & & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & & \\ \cline{4-12} & & & & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \\ & & & & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \\ \cline{5-13} & & & & & & & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}$$

6. (cf. [4, Exercise 3C.E4(iii)]) Determine integers r and s such that $600r + 11312s = (600, 11312)$. Then find a second solution to the same equation.

   Solution:

$$\begin{aligned} 11312 &= 18 \cdot 600 + 512 \\ 600 &= 1 \cdot 512 + 88 \\ 512 &= 5 \cdot 88 + 72 \\ 88 &= 1 \cdot 72 + 16 \\ 72 &= 4 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0 \\ 8 &= 72 - 4 \cdot 16 = 72 - 4(88 - 1 \cdot 72) \\ &= -4 \cdot 88 + 5 \cdot 72 = -4 \cdot 88 + 5(512 - 5 \cdot 88) \\ &= 5 \cdot 512 - 29 \cdot 88 = 5 \cdot 512 - 29(600 - 1 \cdot 512) \\ &= -29 \cdot 600 + 34 \cdot 512 = -29 \cdot 600 + 34(11312 - 18 \cdot 600) \\ &= 34 \cdot 11312 - 641 \cdot 600 \end{aligned}$$

So one solution is $(r, s) = (-641, 34)$. To find a second solution we may subtract $\frac{600}{8}$ from s, and add $\frac{11312}{8}$ to r, to obtain

$$8 = -41 \cdot 11312 + 773 \cdot 600\,.$$

7. (cf. [4, Exercise 4B.E7]) Explain how a student who was not paying attention might have thought that

$$\left(2^7 3^2 4^5 5^6 6^5, 2^4 3^5 4^3 5^3 6^7\right) = 2^4 3^2 4^3 5^3 6^5\,.$$

Find the correct value of $(2^7 3^2 4^5 5^6 6^5, 2^4 3^5 4^3 5^3 6^7)$.

Solution: By (317) in Exercise A.1.8.10, we can obtain the prime factorization of the greatest common divisor by first factorizing each of the two given integers, then taking, for each prime, the lower of the two exponents. But the two integers have been given in a factorized form which is not the unique factorization into *primes*; indeed,

$$2^7 3^2 4^5 5^6 6^5 = 2^7 3^2 2^{2\times 5} 5^6 2^5 3^5 = 2^{7+10+5} 3^{2+5} 5^6 = 2^{22} 3^7 5^6\,,$$

$$2^4 3^5 4^3 5^3 6^7 = 2^4 3^5 2^{2\times 3} 5^3 2^7 3^7 = 2^{4+6+7} 3^{5+7} 5^3 = 2^{17} 3^{12} 5^3\,,$$

It follows that $(2^7 3^2 4^5 5^6 6^5, 2^4 3^5 4^3 5^3 6^7) = 2^{\min\{22,17\}} 3^{\min\{7,12\}} 5^{\min\{6,3\}} = 2^{17} 3^7 5^3$, which is not equal to $2^4 3^2 4^3 5^3 6^5 = 2^{15} 3^7 5^3$.

8. (a) Prove that the product of any two consecutive integers is always even.
   (b) Prove that the product of any three consecutive integers is always divisible by both 2 and 3.
   (c) Prove that the product of any four consecutive integers is always divisible by 4!.

Solution: There are several ways to solve these problems.

Combinatorial proof. For any positive integers k, n, we know that $\binom{n}{k}$ is an integer, since it is the number of subsets of cardinality k of the set $\{1, 2, ..., n\}$. But

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)...(n-k+1)}{k!}$$

so any product $n(n-1)(n-2)...(n-k+1)$ is divisible by $k!$; $n(n-1)(n-2)...(n-k+1)$ is the product of the k consecutive integers of which the largest is n.

Proof by cases. (a) **Smaller number is even.** Given two numbers $2n$, $2n+1$, the product is $(2n)(2n+1) = 2[n(2n+1)]$.

Smaller number is odd. Given two numbers $2n+1$, $2n+2$, the product is $(2n+1)(2n+2) = 2[(2n+1)(n+1)]$.

(b) According as the smallest integer has residue 0, 1, or 2 modulo 3, the integers will be $3n, 3n+1, 3n+2$ or $3n+1, 3n+2, 3n+3$ or $3n+2, 3n+3, 3n+4$. Evidently the product in each case is divisible by 3. Moreover, the product of any *two* consecutive integers of the three will be divisible by 2. Thus the products are divisible by both 2 and 3. By Lemma A.1.6.12, $[3,2]$ divides the product; but $[3,2] = 6$.
This could also be argued without reference to the lemma, by considering *residues modulo 6*. The 6 cases would be

$$\begin{aligned}
6n(6n+1)(6n+2) &= 6[n(6n+1)(6n+2)] \\
(6n+1)(6n+2)(6n+3) &= 6[(6n+1)(3n+1)(2n+1)] \\
(6n+2)(6n+3)(6n+4) &= 6[(3n+1)(2n+1)(6n+4)] \\
(6n+3)(6n+4)(6n+5) &= 6[(2n+1)(3n+2)(6n+5)] \\
(6n+4)(6n+5)(6n+6) &= 6[(6n+4)(6n+5)(n+1)] \\
(6n+5)(6n+6)(6n+7) &= 6[(6n+5)(n+1)(6n+7)]
\end{aligned}$$

(c) But this case of 4 consecutive integers is more complicated. Since $4! = 3{\cdot}8$, and $[3,8] = 24$, we could try to prove that the product is divisible by both 3 and 8; we know from the result for 3 consecutive integers that their product is divisible by 6, hence, in particular, by 3. If we consider residues modulo 2, we have

$$\begin{aligned}
(2n+1)(2n+2)(2n+3)(2n+4) &= 4[(2n+1)(n+1)(2n+3)(n+2)] \\
&= ? \\
2n(2n+1)(2n+2)(2n+3) &= 4[n(2n+1)(n+1)(2n+3)] \\
&= ?;
\end{aligned}$$

divisibility by 4 is obvious; but, in order to prove that the product is divisible by 8, we have to argue that both $n(n+1)$ and $(n+1)(n+2)$ are even, by virtue of our first result.
Or, we could consider residues modulo 4:

$$\begin{aligned}
4n(4n+1)(4n+2)(4n+3) &= 8[n(4n+1)(2n+1)(4n+3)] \\
(4n+1)(4n+2)(4n+3)(4n+4) &= 8[(4n+1)(2n+1)(4n+3)(n+1)] \\
(4n+2)(4n+3)(4n+4)(4n+5) &= 8[(2n+1)(4n+3)(n+1)(4n+5)] \\
(4n+3)(4n+4)(4n+5)(4n+6) &= 8[(4n+3)(n+1)(4n+5)(2n+3)]
\end{aligned}$$

(An even longer solution, which avoids appealing to Lemma A.1.6.12, could be found by considering residues modulo 24.)

E.2 Second 2000 Problem Assignment

Note: The emphasis in grading this assignment has been on identifying and indicating errors on your solutions, rather than on assigning realistic grades. Thus it may occur that the grade for some questions is higher than the solution would have received for in a test or examination. Assignments should be viewed as learning experiences, rather than as tests.

1. Use the Euclidean algorithm to determine an inverse of 7 modulo 40.

   Solution:

$$\begin{aligned} 40 &= 5 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow 1 &= 5 - 2 \cdot 2 = 5 - 2(7 - 1 \cdot 5) \\ &= -2 \cdot 7 + 3 \cdot 5 = -2 \cdot 7 + 3(40 - 5 \cdot 7) \\ &= 3 \cdot 40 - 17 \cdot 7 \equiv -17 \cdot 7 \pmod{40} \end{aligned}$$

   It follows that one inverse of 7 modulo 40 is -17. The smallest positive member of $[7]_{40}^{-1}$ is 23.

2. Solve the following simultaneous systems of linear congruences:

   (a)

$$x \equiv 2 \pmod{7} \quad (1099)$$
$$x \equiv 4 \pmod{40} \quad (1100)$$

   (b)

$$x \equiv 4 \pmod{8} \quad (1101)$$
$$x \equiv 2 \pmod{7} \quad (1102)$$
$$x \equiv 4 \pmod{5} \quad (1103)$$

   (c) [37, p. 143, Exercise 3.3.20d]

$$x \equiv 2 \pmod{6} \quad (1104)$$
$$x \equiv 4 \pmod{8} \quad (1105)$$
$$x \equiv 2 \pmod{14} \quad (1106)$$
$$x \equiv 14 \pmod{15} \quad (1107)$$

[Hint: Begin by factorizing each modulus into a product of powers of primes, then replace the congruence by a set of congruences to each of the prime power moduli; use Lemma A.1.9.2.]

(d)

$$\begin{aligned} x &\equiv 4 \pmod 6 && (1108)\\ x &\equiv 4 \pmod 8 && (1109)\\ x &\equiv 2 \pmod{14} && (1110)\\ x &\equiv 14 \pmod{15} && (1111) \end{aligned}$$

(e)

$$\begin{aligned} 3x &\equiv 0 \pmod 6 && (1112)\\ 5x &\equiv 4 \pmod 8 && (1113)\\ -x &\equiv 12 \pmod{14} && (1114)\\ x^2 &\equiv 1 \pmod{15} && (1115) \end{aligned}$$

Solution:

(a) We use the notation of Theorem A.1.9.9.

$M_1 = 40 \equiv 5 \pmod 7$. With so small a modulus, an inverse could be determined by trying 1, 2, ..., to be $d_1 = 3$. Or, using the Euclidean algorithm, we have

$$\begin{aligned} 7 &= 1 \cdot 5 + 2\\ 5 &= 2 \cdot 2 + 1\\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow 1 &= 5 - 2 \cdot 2 = 5 - (7 - 1 \cdot 5) \cdot 2\\ &= -7 \cdot 2 + 3 \cdot 5 \end{aligned}$$

Taking residues modulo 7 in the equation $-7 \cdot 2 + 3 \cdot 5 = 1$, we find that $3 \cdot 5 \equiv 1 \pmod 7$, so one inverse of 5 modulo 7 is $d_1 = 3$.

$M_2 = 7 \pmod{40}$. An inverse is computed in Problem 1 above to be[1037] $d_2 = 23$.

One solution of the given system of congruences is, therefore, $M_1 d_1 2 + M_2 d_2 4 = 40 \cdot 3 \cdot 2 + 7 \cdot 23 \cdot 4 = 240 + 644 = 884$. The set of all solutions is therefore $884 + (280) = [44]_{280}$.

[1037] There was no reason to take the smallest positive inverse here; had we taken $d_2 = -17$, the representative of the solutions modulo 280 would have been $240 - 476 \equiv -236 \equiv 44 \pmod{280}$.

(b) Again using the notation of Theorem A.1.9.9, we have $M = 8 \cdot 7 \cdot 5 = 280$,

$$\begin{aligned} M_1 &= 35 \equiv 3 \pmod 8 \\ M_2 &= 40 \equiv 5 \pmod 7 \\ M_3 &= 56 \equiv 1 \pmod 5 \end{aligned}$$

The inverses could be determined using the Euclidean algorithm or by trial or observation to be $[35]_8^{-1} = [3]_8^{-1} = [3]_8$, $[40]_7^{-1} = [5]_7^{-1} = [3]_7$, $[56]_5^{-1} = [1]_5^{-1} = [1]_5$. Hence the set of solutions to the given system of congruences is represented modulo 280 by $35 \cdot 3 \cdot 4 + 40 \cdot 3 \cdot 2 + 56 \cdot 1 \cdot 4 = 420 + 240 + 224 = 884$, and the solution set is $[884]_{280} = [44]_{280}$. This is the same set as found in part 2a above; this is not surprising, since congruences (1101) and (1103) together are equivalent to congruence (1100), by virtue of Lemma A.1.9.2.

(c) Applying the hint, we find, by Lemma A.1.9.2, that the given system of congruences is equivalent to the system

$$\begin{aligned} x &\equiv 2 \equiv 0 \pmod 2 && (1116) \\ x &\equiv 2 \pmod 3 && (1117) \\ x &\equiv 4 \pmod 8 && (1118) \\ x &\equiv 2 \equiv 0 \pmod 2 && (1119) \\ x &\equiv 2 \pmod 7 && (1120) \\ x &\equiv 14 \equiv 2 \pmod 3 && (1121) \\ x &\equiv 14 \equiv 4 \pmod 5 && (1122) \end{aligned}$$

Here congruences (1116) and (1119) are identical, and are both implied by (1118), so it suffices to satisfy only the last of these three; similarly, (1117) is identical to (1121). Thus it is equivalent to solve the system

$$\begin{aligned} x &\equiv 4 \pmod 8 && (1123) \\ x &\equiv 2 \pmod 7 && (1124) \\ x &\equiv 2 \pmod 3 && (1125) \\ x &\equiv 4 \pmod 5 && (1126) \end{aligned}$$

Then an inverse modulo 8 of $M_1 = 105 \equiv 1$ is evidently $d_1 = 1$; an inverse modulo 3 of $M_2 = 280 \equiv 1 = 1$ is $d_2 = 1$; an inverse modulo 7 of $M_3 = 120 \equiv 1$ is 1; and an inverse modulo 5 of $M_4 = 168 \equiv 3$ is 2. Thus a representative modulo $M = 8 \cdot 3 \cdot 7 \cdot 5 = 840$ of the solution set is $105 \cdot 1 \cdot 4 + 280 \cdot 1 \cdot 2 + 120 \cdot 1 \cdot 2 + 168 \cdot 2 \cdot 4 = 2564 \equiv 44$, and the full solution set is $[44]_{840}$.

(d) If we proceed as with the preceding problem, we obtain, as a consequence of the first congruence, that $x \equiv 1 \pmod 3$; and, as a consequence of the last congruence, that $x \equiv 2 \pmod 3$. It is impossible to satisfy these congruences simultaneously; hence the solution set to the given system is empty.

(e) If we could transform this system into one in which the congruences are all *linear*, of the form $x \equiv b \pmod m$, we could proceed as in the previous parts of this problem.

We can apply Lemma A.1.9.1 to congruence (1112); from $x \cdot 3 \equiv 0 \cdot 3 \pmod 6$ we can conclude that $x \equiv 0 \pmod{\frac{6}{3}}$, i.e.

$$x \equiv 0 \pmod 2 . \tag{1127}$$

In the case of congruence (1113), we can effectively "divide" both sides by 5 by multiplying both sides by 5^{-1} modulo 8; one such inverse is 5, giving

$$5 \cdot 5x \equiv 5 \cdot 4 \Rightarrow x \equiv 4 \pmod 8 . \tag{1128}$$

Similarly, (1114) may be transformed by multiplying by $(-1)^{-1}$, i.e. by -1, giving

$$x \equiv -12 \equiv 2 \pmod{14} . \tag{1129}$$

Finally, (1115) may be rewritten as $x^2 - 1 \equiv 0 \pmod{15}$, equivalently as the pair of congruences

$$(x-1)(x+1) \equiv 0 \pmod 3 \tag{1130}$$
$$(x-1)(x+1) \equiv 0 \pmod 5 \tag{1131}$$

The product $(x-1)(x+1)$ will be divisible by a prime p iff one of the two factors is divisible by p. We thus see that the set of solutions to (1115) is the *union* of the solution sets of the following 4 sets of congruences:

$$x \equiv 1 \text{ or } -1 \pmod 3 \tag{1132}$$
$$x \equiv 1 \text{ or } -1 \pmod 5 \tag{1133}$$

where the signs in the two congruences may be chosen in any of the 2×2 combinations. Congruence (1129) is equivalent to the pair of congruences

$$x \equiv 0 \pmod 2 \tag{1134}$$
$$x \equiv 2 \pmod 7 , \tag{1135}$$

so congruence (1127) is identical with (1134). As in an earlier problem, (1128) implies (1134). We proceed to apply the Chinese Remainder Theorem with

$M = 840$, $M_1 = 105$, $M_2 = 120$, $M_3 = 280$, $M_4 = 168$; $b_1 = 4$, $b_2 = 2$, $b_3 = \pm 1$, $b_4 = 1$ or -1; $d_1 = 1$, $d_2 = 1$, $d_3 = 1$, $d_4 = 3$ as earlier. Representatives of the solutions modulo 840 are then

$$105 \cdot 1 \cdot 4 + 120 \cdot 1 \cdot 2 + 280 \cdot 1 \cdot \epsilon_1 \cdot 2 + 168 \cdot 1 \cdot \epsilon_2 \cdot 4$$

where ϵ_1 and ϵ_2 are each either 1 or -1; i.e., 3236 (equivalently, 716) or -796 (equivalently 44) or 2116 (equivalently 436) or -1916 (equivalently 604). The solution set is thus

$$[716]_{840} \cup [44]_{840} \cup [436]_{840} \cup [604]_{840} .$$

3. (a) Give an example of a function $f : \mathbb{Z} \to \mathbb{Z}$ which is surjective but not injective.
   (b) Give an example of a function $g : \mathbb{R} \to \mathbb{R}$ which is injective but not surjective.
   (c) Let $f : \mathfrak{A} \to \mathfrak{B}$ and $g : \mathfrak{B} \to \mathfrak{C}$ be bijections. Prove that

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} . \tag{1136}$$

Solution:

(a) There are infinitely many examples. One is the function $x \mapsto \left\lfloor \frac{x}{2} \right\rfloor$. This function is surjective, since any integer n is the image of $2n$. The function is not injective since n is also the image of $2n + 1$.

(b) There are infinitely many examples. One is the function $x \mapsto e^x$. This function is injective since $e^x = e^y \Rightarrow x = y$. The function is not surjective, since 0 is not in its image.

(c) Since f and g are bijections, and since the codomain of f is the domain of g, we know from Exercise A.2.3.2.3,4 that $g \circ f$ is a bijection.

$$\begin{aligned}
(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\
&= g \circ \iota_{\mathfrak{B}} \circ g^{-1} \\
&= g \circ g^{-1} = \iota_{\mathfrak{C}} \\
&\quad \text{by Exercise A.2.3.2.1,2; also} \\
(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\
&= f^{-1} \circ \iota_{\mathfrak{C}} \circ f \\
&= f^{-1} \circ f = \iota_{\mathfrak{A}}
\end{aligned}$$

We have thus proved that $f^{-1} \circ g^{-1}$ is an inverse of $g \circ f$. As the inverse is unique, we have proved that it is *the* inverse of $g \circ f$.

4. (a) Consider a graph with vertex-set $\mathfrak{V} = \{1, 2, 3, 4, 5, 6\}$, and edge-set $\mathfrak{E} = \{12, 13, 14, 25, 26\}$, where we are denoting an edge $\{x, y\}$ by the string xy. This graph has the "shape" of the letter H. There are exactly $2 \times 2 \times 2 = 8$ permutations f of $\mathfrak{V}$ which are *automorphisms* of the graph, i.e. which have the property that vertices x and y are adjacent iff $f(x)$ and $f(y)$ are adjacent. Express each of these automorphisms in two ways: in the 2-line matrix notation, and in the disjoint cycle notation.

   (b) Repeat the preceding instructions, this time for the graph whose vertices are 1, 2, 3, 4, 5, 6, and whose edges are 12, 23, 31, 14, 25, 36.

Solution:

(a) Under an automorphism f a vertex of degree 3 must be mapped onto a vertex of degree 3: this means that either $f(1) = 1$ (and hence $f(2) = 2$), or $f(1) = 2$ and $f(2) = 1$. Once we know the image of vertex 1, we know that its neighbours, 3 and 4, must be mapped on to neighbours of $f(1)$, etc. The 8 permutations are

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix} = (1)(2)(34)(5)(6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix} = (1)(2)(3)(4)(56)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = (1)(2)(34)(56)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix} = (12)(35)(46)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix} = (12)(3645)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix} = (12)(3546)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = (12)(36)(45)$$

(b) In this case the three vertices of degree 3, i.e. 1, 2, 3, must be permuted among themselves; and the other vertices — which have degree 1 — are also permuted among themselves. Each of the 3! permutations of 1, 2, 3 "induces"

a permutation of the six vertices in an obvious way. The 3! permutations are

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix} = (12)(3)(45)(6)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix} = (13)(2)(46)(5)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix} = (1)(23)(4)(56)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = (123)(456)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} = (132)(465)$$

5. (a) Determine the powers of the permutation $f = (123)(456789)$, expressing each in disjoint cycle notation.
   (b) Determine the powers of the permutation $g = (12)(3456)(78)(9)$, expressing each in disjoint cycle notation.
   (c) Construct a Cayley table for all powers of f and another for all powers of g.

   Solution:

   (a)

$$\begin{aligned} f^0 &= \iota_{\{1,2,3,4,5,6,7,8,9\}} = I \\ f^1 &= (123)(456789) \\ f^2 &= (132)(468)(579) \\ f^3 &= (1)(2)(3)(47)(58)(69) = (47)(58)(69) \\ f^4 &= (123)(486)(597) \\ f^5 &= (132)(498765) \\ f^6 &= f^0 \quad \text{etc.} \end{aligned}$$

   (b)

$$\begin{aligned} g^0 &= \iota_{\{1,2,3,4,5,6,7,8,9\}} = I \\ g^1 &= (12)(3456)(78)(9) = (12)(3456)(78) \\ g^2 &= (1)(2)(35)(46)(7)(8)(9) = (35)(46) \\ g^3 &= (12)(3654)(78)(9) = (12)(3654)(78) \\ g^4 &= g^0 \quad \text{etc.} \end{aligned}$$

(c) The two tables follow:

f \ g	I	(123)(456789)	(132)(468)(579)	(47)(58)(69)	(123)(486)(597)	(132)(498765)
I	I	(123)(456789)	(132)(468)(579)	(47)(58)(69)	(123)(486)(597)	(132)(498765)
(123)(456789)	(123)(456789)	(132)(468)(579)	(47)(58)(69)	(123)(486)(597)	(132)(498765)	I
(132)(468)(579)	(132)(468)(579)	(47)(58)(69)	(123)(486)(597)	(132)(498765)	I	(123)(456789)
(14)(25)(35)	(47)(58)(69)	(123)(486)(597)	(132)(498765)	I	(123)(456789)	(132)(468)(579)
(123)(486)(597)	(123)(486)(597)	(132)(498765)	I	(123)(456789)	(132)(468)(579)	(14)(25)(35)
(132)(498765)	(132)(498765)	I	(123)(456789)	(132)(468)(579)	(14)(25)(35)	(123)(486)(597)

f \ g	I	(12)(3456)(78)	(35)(46)	(12)(3654)(78)
I	I	(12)(3456)(78)	(35)(46)	(12)(3654)(78)
(12)(3456)(78)	(12)(3456)(78)	(35)(46)	(12)(3654)(78)	I
(35)(46)	(35)(46)	(12)(3654)(78)	I	(12)(3456)(78)
(12)(3654)(78)	(12)(3654)(78)	I	(12)(3456)(78)	(35)(46)

6. Suppose that $\mathfrak{A} = \{a_1, a_2, ..., a_{10}\}$, that f is the permutation $(a_1a_2a_3...a_9a_{10})$, and that g is some permutation of $\mathfrak{A}$ that "commutes with f", i.e. such that $fg = gf$. Prove that g is a power of f. [Hint: Suppose that $g(a_1) = a_i$, for some i. Show that $g(a_2) = a_{i+1}$, $g(a_3) = a_{i+2}$, etc., where subscripts are taken modulo n. Then show that g is the $(i-1)$th power of f.]

   Solution: If $g(a_1) = a_i$, then $(f \circ g)(a_1) = f(a_i) = a_{i+1}$. Imposing the condition of commutativity, we have that $(g \circ f)(a_1)$ is also equal to a_{i+1}. That is $a_{i+1} = (g \circ f)(a_1) = g(f(a_1)) = g(a_2)$. Repeating this step, we can prove by induction that $g(a_j) = a_{j+i-1}$ for all j (with indices taken modulo 10). But $a_{j+i-1} = f^{i-1}(a_j)$ for all j, so we have that $g = f^{i-1}$. (Remember that two functions are equal if they have the same domain, the same codomain, and the same action on every point of the domain.)

E.3 Third 2000 Problem Assignment

Note: The emphasis in grading this assignment has been on identifying and indicating errors in your solutions, rather than on assigning realistic grades. Thus it may occur that the grade for some questions is higher than the solution would have received in a test or examination. Assignments should be viewed as learning experiences, rather than as tests.

1. (a) If a_1, a_2, ..., a_n are distinct symbols ($n > 1$), determine the product

$$(a_1 a_2 ... a_i)(a_i a_{i+1} ... a_n) \quad (1 \leq i \leq n) .$$

   (b) Show that every permutation of $\{1, 2, ..., n\}$, where $n > 1$, is expressible as a product of the two permutations (12) and (23...n) (unlimited repetitions permitted). [Note that this problem resembles, but is different from Exercise A.3.2.6.5.]

   Solution:

   (a) The product is $(a_1 a_2 ... a_i a_{i+1} ... a_n)$.

   (b) By the preceding part, (12...n) is expressible as a product (12)(23...n). Hence the generators in Exercise A.3.2.6.5 are expressible in terms of the generators given here. Since every element of the symmetric group is expressible in terms of (12) and (123...n), and since (12) and (123...n) are together expressible in terms of (12) and (23...n), it follows that (12) and (23...n) is another set of generators of the symmetric group.

2. [47, Exercise 11, p. 24] Consider the 42 transformations of the set of residue classes modulo 7 defined by:

$$f_{i,j}(x) = ix + j \tag{1137}$$

   where $i = 1, 2, ..., 6$; $j = 0, 1, 2, ..., 6$; and all computations are taken modulo 7; that is, equation (1137) should be read as an abbreviation for

$$f_{i,j}\left([x]_7\right) = [ix + j]_7 .$$

   (a) Show that each of these transformations is a permutation of the residue classes modulo 7.

   (b) Show that the inverse of each of these transformations is also in the set.

   (c) Show that the composition of any two of these transformations is also in the set.

   (d) Show that the transformations form a permutation group acting on the set of residue classes modulo 7.

(e) Show that, for each of the 6×7 pairs of values (i, j), the 42 functions $f_{i,j}$ obtained are all different. [Hint: Since these functions all act on the set of equivalence classes $\{[0]_7, [1]_7, ..., [6]_7\}$, and take their values in the same set, we have to show that no two functions act the same way on all x (i.e. on all $[x]_7$). However, it is possible that two of the functions may act the same way on *some* elements of the domain. For example, $f_{1,1}([1]_7) = [2]_7 = f_{4,5}([1]_7)$ — but there are certain points in the domain where $f_{1,1}$ and $f_{4,5}$ act differently.]

(f) Show that the group of these transformations is generated by $f_{1,1}$ and $f_{3,0}$.

(g) Prove that there must exist permutations of the set of residue classes modulo 7 which are not among the 42 functions being considered here.

(h) List the orbits under this permutation group.

It is suggested that you suppress the notation of square brackets, and denote $[x]_7$ simply by x. Implicit in this is the understanding that $[x + y]_7 = [x]_7 + [y]_7$ and that $[x]_7 \odot [y]_7 = [xy]_7$.[1038]

Solution:

(a) For any values of i and j the mapping $f_{i,j}$ has the same domain and codomain. To prove it is a permutation we have to prove it is both injective and surjective.

Injective: Suppose that $f_{i,j}(x) = f_{i,j}(y)$, i.e. that $ix + j = iy + j$, which is an abbreviation for $[ix + j]_7 = [iy + j]_7$; which, in turn, means that $ix + j \equiv iy + j \pmod 7$. This last congruence implies that $ix \equiv iy \pmod 7$. Since 7 is prime, and $1 \leq i < 7$, $(i, 7) = 1$; hence, by Lemma A.1.9.1, $x \equiv y \pmod 7$, equivalently that $[x]_7 = [y]_7$. We have shown that $f_{i,j}$ is one-to-one for any choice of i and j.

Surjective: Let $[x]_7$ be any equivalence class modulo 7. We have to show that there exists an equivalence class $[y]_7$ such that $f_{i,j}([y]_7) = [x]_7$; that is, we have to show that the congruence $iy + j \equiv x \pmod 7$ admits a solution y. But this is equivalent to solving the congruence $iy \equiv x - j \pmod 7$. By Theorem A.1.9.7 the congruence has a solution since $(i, 7) = 1$.

By definition, a mapping which is a bijection, and such that its domain and codomain coincide, is a permutation.

(b) We may solve equation 1137 to obtain $ix = f_{i,j}(x) - j$; hence, if i^{-1} denotes an inverse of i modulo 7, i.e. an integer k such that $ik \equiv 1 \pmod 7$, we have

$$x \equiv i^{-1} f_{i,j}(x) - i^{-1} j \tag{1138}$$

[1038]These are properties that will be proved when we come to study *rings*. What we are assuming is that the mapping $x \mapsto [x]_7$ is a *ring homomorphism*.

But, for every x, the right side of this equation is the value of $f_{i^{-1},-i^{-1}j}(f_{i,j}(x))$. It follows that the inverse function to $f_{i,j}$ is the function $f_{i^{-1},-i^{-1}j}$.

(c) For any $i, j, k, \ell \in \{0, 1, 2, 3, 4, 5, 6\}$ where $i \neq 0$, $k \neq 0$, and any x,

$$\begin{aligned} (f_{i,j} \circ f_{k\ell})(x) &= f_{i,j}(kx + \ell) \\ &= i(kx + \ell) + j = (ik)x + (i\ell + j) \end{aligned}$$

so

$$f_{i,j} \circ f_{k,\ell} = f_{ik,i\ell+j}\,. \tag{1139}$$

We have shown that the composition of two of the 42 functions is again one of those functions — i.e. that the set of such functions is *closed under composition*.

(d) By Definition A.3.3.1 it remains only to prove that the identity function is among the elements of this set of permutations. But the identity function is $f_{1,0}$. Hence these 42 permutations constitute a permutation group.

(e) We will "test" the functions by their action on 0 (i.e. $[0]_7$). Since $f_{i,j}(0) = j$, we see that $f_{i,j}$ and $f_{k,\ell}$ cannot be the same function *unless* $j = \ell$. So let us now consider two functions $f_{i,j}$ and $f_{k,j}$. Now "test" their action on 1 (i.e. on $[1]_7$). We have $f_{i,j}(1) = i$, while $f_{k,j}(1) = k$. Thus the two functions will act differently on 1 *unless* $i = j$. We have shown that any set of subscripts yields a unique function; i.e. that the 42 functions are distinct (even though any two of them may act the in the same way on certain points of the domain, but not on all point of the domain).

(f) First observe that the powers (i.e. compositions) of $f_{3,0}$ give all permutations $f_{i,0}$. This is because, modulo 7, 3 is a *primitive element*: every residue class except $[0]_7$ may be expressed as a power of $[3]_7$. Since $[3]^2 = [9] = [2]$, $[3]^3 = [3 \times 2] = [6]$, $[3]^4 = [2^2] = [4]$, $[3]^5 = [3 \times 4] = [12] = [5]$, $[3]^6 = [6^2] = [1]$. Thus $f_{2,0} = f_{3,0}^2$; $f_{6,0} = f_{3,0}^3$; $f_{4,0} = f_{3,0}^4$; $f_{5,0} = f_{3,0}^5$; and $f_{1,0} = f_{3,0}^6$.

Now observe that $f_{i,j} = f_{1,j} \circ f_{i,0} = f_{1,1}^j \circ f_{i,0}$. The first factor is a power of the generator $f_{1,1}$, while the second factor has just been shown to be a power of the second generator, $f_{3,0}$.

(g) The total number of permutations of the set of 7 residue classes is 7!. As this is greater than 7×6, most of these permutations are not in the set of 42 permutations under consideration here. For example, the permutation (12) is not one of these 42 functions. (The functions under consideration could be called the *affine* transformations.)

(h) The permutation group is acting on the set of residue classes modulo 7. The permutation $f_{1,1}$ maps x on to $x + 1$. Thus repeated applications of $f_{1,1}$ will

map each residue class into every other residue class. The residue classes thus are all in the same orbit. (A permutation group with only one orbit is said to *act transitively* on the set.)

3. Suppose that in the immediately preceding problem we replace modulus 7 by 4, and permit $j = 0, 1, 2, 3$, and i to take values 1, 2, 3 for which the resulting function is a permutation. Consider the various parts of the problem and either answer them or show what limitations are imposed by the new modulus. (Since 4 is not prime, there will definitely be some restrictions. For example, $f_{2,2}$ is not a permutation, since its image does not include 1 (i.e. $[1]_4$).)

   Solution:

   (a) In general, if $f_{i,j}$ is to be an injection, then we need to be able to conclude from
   $$ix + j \equiv iy + j \pmod 4 \tag{1140}$$
   that $x \equiv y \pmod 4$; (see the solution given for the preceding problem). When $i = 1$ and $i = 3$ this is true; but, when $i = 2$, consider the case $x = 2$, $y = 0$. Here (1140) holds, yet $x \not\equiv y$. Thus we must exclude the value $i = 2$.

   When $i = 1$ or 3, or, equivalently (since we are working modulo 4) $i = \pm 1$, $f_{i,j}$ is indeed a surjection. For, given any y, we can solve the equation $f_{i,j}(x) = y$, i.e. $ix + j = y$; the solution is, in fact, $x = i(y - j)$. So any such function is onto.

   For the rest of the problem we will assume that $i = \pm 1$.

   (b) The inverse of $f_{1,j}$ is $f_{1,-j}$. The inverse of $f_{-1,j}$ is the same function, $f_{-1,j}$. In either case the function is in the set under consideration.

   (c) The discussion of the preceding problem is valid in this case. In (1139) we showed that the set was closed under composition. The essential step there is that $ik \neq 0$, i.e. that $ij \not\equiv 0 \pmod 4$; this follows since i and j are each ± 1.

   (d) As in the preceding problem, we need only show that the identity is in the set. But the identity is $f_{1,0}$.

   (e) If we consider the action of the 8 functions on 0 (i.e. on $[0]_4$), we see that for fixed i (equal to either $+1$ or -1), the images of 0 are different for the different values of j. It remains only to show that $f_{1,j}$ and $f_{-1,j}$ are distinct. But, these two functions always take 1 on to different values, since $(1 + j) - (-1 + j)$ is not a multiple of 4.

   (f) All the functions $f_{1,j}$ are powers of $f_{1,1}$. It can be shown by simple computations that $f_{3,2} = f_{3,3} \circ f_{1,1}$; $f_{3,1} = f_{3,2} \circ f_{1,1}$; and $f_{3,0} = f_{3,1} \circ f_{1,1}$. Thus our present group is generated by $f_{3,3}$ and $f_{1,1}$.

(g) Our group has 8 members. But there are $4! = 24$ permutations of the 4 residue classes modulo 4.

(h) Repeated action of $f_{0,1}$ maps each residue class on to every other residue class. Hence there is again only one orbit, and the group is transitive on the set of residue classes.

4. (a) The *alternating group* $\mathcal{A}_n$ is the group of permutations of the set $\{1, 2, ..., n\}$ each of whose members is expressible as a product of an even number of transpositions. Give the Cayley table of $\mathcal{A}_4$.

(b) For the element (123) of $\mathcal{A}_4$, determine the number of different products of transpositions equal to (123).

(c) Let $\mathfrak{B}$ be the set of elements of the symmetric group $\mathcal{S}_n$ which are expressible as the product of a number of transpositions which is a multiple of 3. Determine whether or not $\mathfrak{B}$ is a permutation group.

(d) Let $\mathfrak{C}$ be the set of elements of the symmetric group $\mathcal{S}_n$ which are expressible as the product of a number of transpositions which is $\equiv 1 \pmod 2$. Determine whether or not $\mathfrak{C}$ is a permutation group.

Solution:

(a) The upper left-hand corner of the table represents the subgroup whose structure is called a "four-group".

	e	(12)(34)	(13)(24)	(14)(23)	(234)	(243)	(134)	(143)	(124)	(142)	(123)	(132)
e	e	(12)(34)	(13)(24)	(14)(23)	(234)	(243)	(134)	(143)	(124)	(142)	(123)	(132)
(12)(34)	(12)(34)	e	(14)(23)	(13)(24)	(124)	(123)	(142)	(132)	(234)	(134)	(243)	(143)
(13)(24)	(13)(24)	(14)(23)	e	(12)(34)	(132)	(134)	(243)	(124)	(143)	(123)	(142)	(234)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	e	(143)	(142)	(123)	(234)	(132)	(243)	(134)	(124)
(234)	(234)	(124)	(132)	(143)	(243)	e	(14)(23)	(123)	(134)	(12)(34)	(13)(24)	(142)
(243)	(243)	(123)	(134)	(142)	e	(234)	(124)	(13)(24)	(14)(23)	(132)	(143)	(12)(34)
(134)	(134)	(142)	(243)	(123)	(14)(23)	(124)	(143)	e	(12)(34)	(234)	(124)	(14)(23)
(143)	(143)	(132)	(124)	(234)	(123)	(13)(24)	e	(134)	(123)	(13)(24)	(12)(34)	(243)
(124)	(124)	(234)	(143)	(132)	(134)	(14)(23)	(12)(34)	(123)	(142)	e	(14)(23)	(134)
(142)	(142)	(134)	(123)	(243)	(12)(34)	(132)	(234)	(13)(24)	e	(124)	(234)	(13)(24)
(123)	(123)	(243)	(143)	(134)	(13)(24)	(143)	(124)	(12)(34)	(14)(23)	(234)	(132)	e
(132)	(132)	(143)	(234)	(124)	(142)	(12)(34)	(14)(23)	(243)	(134)	(13)(24)	e	(123)

(b) (123) can be expressed as a product of transpositions in infinitely many ways. For example, $(123) = (13)(12) = (13)(12)(13)(12)(13)(12)(13)(12) = (13)(12)(13)(12)(13)(12)(13)(12)(13)(12)(13)(12)(13)(12) = ((13)(12))^n$, where n is any integer of the form $1 + 3k$.

(c) Suppose some element x of $\mathcal{A}_n$ is expressible as a product of $2k$ transpositions. Then x is also expressible as a product of $2k + 2$ transpositions — just multiply on the right by (12)(12); and as a product of $2k+4$ transpositions — just multiply by (12)(12)(12)(12). In this way we can express any even permutation as a product of any *sufficiently large* even number of permutations. One of $2k$, $2k + 2$, $2k + 4$ is congruent to 0 modulo 3 — just consider the

three cases, $k \equiv i \pmod 3$, where $i = 0, 1, 2$. Hence the subset in question includes all even permutations.

But it also includes all odd permutations. For, if a permutation is expressible as a product of $2k+1$ transpositions, we can again adjoin at the end a product $(12)(12)$, or $(12)(12)(12)(12)$ without changing the value. Here again, one of $2k+1$, $2k+3$, $2k+5$ must be a multiple of 3. Thus the set under consideration includes all members of the symmetric group: it certainly is a permutation group!

(d) This is not a subgroup. The problem here is that the set is not closed under composition — the product of two odd permutations is not odd.

5. (Exercise A.4.2.4) Show that the following operations are *not* associative:

   (a) $(a, b) \longmapsto a - b$, defined on $\mathbb{Z}$;

   (b) $(x, y) \longmapsto a/b$, defined on $\mathbb{R} - \{0\}$;

   (c) $(\vec{v}, \vec{w}) \longmapsto \vec{v} \times \vec{w}$, defined on $\mathbb{R}^3$.

   Solution: The definition of associativity requires the truth of a triply quatified predicate. Only one specific example is needed to show the falsity of such a proposition.

   (a) One counterexample is $0 - (0 - 1) = 1 \neq -1 = (0 - 0) - 1$

   (b) One counterexample is
   $$\frac{1}{\frac{1}{2}} = 2 \neq \frac{1}{2} = \frac{\frac{1}{1}}{2}$$

   (c) Suppose that the unit vectors $\vec{e}_1$, $\vec{e}_2$, $\vec{e}_3$ along the $x-$, $y-$, and z-axes form, in that order, a right-handed system (which is the usual convention). Then $(\vec{e}_1 \times \vec{e}_1) \times \vec{e}_2 = \vec{0} \times \vec{e}_2 = \vec{0}$; but $\vec{e}_1 \times (\vec{e}_1 \times \vec{e}_2) = \vec{e}_1 \times \vec{e}_3 = -\vec{e}_2$. This is a specific counterexample.

E.4 Fourth 2000 Problem Assignment

Distribution Date: (This is a preliminary version of the solutions, and could require corrections. Corrections introduced after the solutions have been printed will be available only over the Web.)

1. Let $\mathfrak{A}$ be a 3-element set whose elements are labelled e, a, b. Suppose that $*$ is a binary composition on $\mathfrak{A}$ in which e is an identity (i.e., $\forall x \in \mathfrak{A}[e * x = x = x * e]$), and in which $x * x = e \ \forall x \in \mathfrak{A}$.

(a) Prove carefully that $*$ is not associative.

(b) The information given above prescribes 7 of the 9 products in the Cayley table. Show that if $a*a$ is permitted to be changed into something other than e, then $*$ can, indeed, be associative.

Solution:

(a) The Cayley table for $*$ contains the following entries:

$*$	e	a	b
e	e	a	b
a	a	e	
b	b		e

. We shall suppose that $*$ is associative, and prove that this leads to a contradiction.

$$\begin{aligned} a &= a*e \quad \text{since } e \text{ is an identity} \\ &= a*(b*b) \quad \text{since } \forall x \in \mathfrak{A}[x*x=e] \\ &= (a*b)*b \quad \text{by associativity of } * \end{aligned}$$

As we know that $b = e*b$, and that $e = b*b$, $a*b$ cannot be equal to either e or b; it follows that $a*b = a$, the only remaining element of $\mathfrak{A}$. Similarly, as

$$\begin{aligned} b &= e*b \\ &= (a*a)*b \\ &= a*(a*b) \quad \text{by associativity} \end{aligned}$$

we can argue that $a*b$ cannot be either of e or a, so it must be b. But a and b are distinct, so $a*b$ cannot be equal to both of them. We conclude that the hypothesis that $*$ is associative is false.

(b) Suppose that the Cayley table contains the following entries:

$*$	e	a	b
e	e	a	b
a	a	b	
b	b		e

,

with $a*a = b$. Then, by the first line of reasoning above, we may again conclude that $a*b = a$. But then $b = a*a = a*(a*b) = (a*a)*b = b*b = e$, which is a contradiction. Hence the only possible definition of $a*a$ is $a*a = a$. We can then argue analogously to the earlier step that $b*a = a$. The table can only be completed as

$*$	e	a	b
e	e	a	b
a	a	a	a
b	b	a	e

. But does this table represent an associative binary operation? We could prove this by checking all $3^3 = 27$

possible ordered triples of products. Another way is to observe that this is the multiplication table of integers modulo 3, i.e. of the monoid we call $(\mathbb{Z}_3, \times, [1]_3)$, which we "know" to be associative. (The isomorphism is given by $\phi(e) = [1]_3$, $\phi(a) = [0]_3$, $\phi(b) = [2]_3$.)

2. In Definition A.4.3.6 three conditions are given for a function $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ to be an isomorphism from monoid $(\mathfrak{A}, *, e)$ to monoid $(\mathfrak{B}, \star, f)$:

   (a) ϕ is a bijection

   (b) $\phi(a_1 * a_2) = \phi(a_1) \star \phi(a_2)$ $\forall a_1 \in \mathfrak{A}$, $\forall a_2 \in \mathfrak{A}$.

   (c) $\phi(e) = f$.

   Show that condition 2c is not required, in the sense that it is a consequence of the preceding two conditions on ϕ.

   Solution: Let $b \in \mathfrak{B}$. Since ϕ is a bijection, there exists an element $a \in \mathfrak{A}$ such that $b = \phi(a)$. Then

$$\begin{aligned} b &= \phi(a) \\ &= \phi(e * a) \quad \text{since } e \text{ is the identity of } (\mathfrak{A}, *, e) \\ &= \phi(e) \star \phi(a) \quad \text{by condition 2b} \\ &= \phi(e) \star b \end{aligned}$$

   In the same way we can prove that $\forall b \in \mathfrak{B}$, $b = b \star \phi(e)$. Thus we have shown that $\phi(e)$ is an identity of the monoid $(\mathfrak{B}, \star, f)$. But, by Theorem A.4.3.3, the identity of a monoid is unique: hence $\phi(e) = f$.

   Why, then, was the condition listed in the definition? One reason is that, were we to generalize the concept to a *homo*morphism between monoids, then the condition would, indeed, be needed. This differs from the analogous situation for groups, where a condition on the identity is not required even for *homo*morphisms. In the case of groups the presence of inverses for elements renders this condition superfluous.

3. Let $f = (1234)(5678)$, $g = (1638)(5274)$

   (a) Show that f and g commute (i.e., that $fg = gf$).

   (b) Show carefully that the subgroup of $\mathcal{S}_8$ generated by f and g contains exactly 8 permutations.

   (c) Show that the subgroup generated is *not* isomorphic to $\mathcal{D}_4$.

   (d) Show that the subgroup generated is *not* cyclic.

Solution: (Parts of this problem appear — without solution — in [47, p. 36, #4].)

(a) $fg = (1234)(5678)(1638)(5274) = (17)(28)(35)(46)$;
$gf = (1638)(5274)(1234)(5678) = (17)(28)(35)(46)$.

(b) This subgroup contains all products of powers of f and g. Since f and g commute, we can replace any word in f's and g's by a product $f^i g^j$, where i and j are integers. Since $f^4 = g^4 = e$, $f^{-1} = f^3$, and $g^{-1} = g^3$, it suffices to assume that i and j take on values from $\{0, 1, 2, 3\}$. This could permit as many as 4×4 distinct elements in the subgroup. However, $f^2 = (13)(24)(57)(68) = g^2$. Thus, in considering the members of the subgroup, we need only consider products of the form $f^i g^j$ where $i = 0, 1; j = 0, 1, 2, 3$: this shows that the subgroup has *at most* $2 \times 4 = 8$ elements. Computing these products, we find them all different:

i	j	$f^i g^j$
0	0	e
0	1	(1638)(5274)
0	2	(13)(68)(57)(24)
0	3	(1836)(5472)
1	0	(1234)(5678)
1	1	(17)(28)(35)(46)
1	2	(1432)(5876)
1	3	(15)(26)(37)(48)

(c) The dihedral group $\mathcal{D}_4$ is not abelian. For example, if we label the vertices of the square 1,2,3,4, then the reflection $u = (12)(34)$ and the rotation $v = (1234)$ have the property that $uv = (24) \neq (13) = vu$. But the group generated by f and g is abelian, since its generators commute. The property of being abelian is preserved under isomorphism.

(d) A cyclic group of order 8 contains elements of order 8 — in fact, there will be 4 such elements. But the present group contains only elements of orders 1 (the identity), 2 (the elements whose disjoint cycle decompositions are products of disjoint transpositions), and 4 (the 4 elements that are expressible as a product of two 4-cycles).

4. Let a mapping $\phi : \mathcal{S}_n \longrightarrow \mathcal{S}_n$ be defined as follows: If

$$f = (a_{11}a_{12}...a_{1r_1})(a_{21}a_{22}...a_{2r_2})...(a_{k1}a_{k2}...a_{kr_k})$$

is in disjoint cycle notation, then

$$\phi(f) = (a_{11}a_{12}...a_{1r_1})^{-1}(a_{21}a_{22}...a_{2r_2})^{-1}...(a_{k1}a_{k2}...a_{kr_k})^{-1}$$

Determine which values of $n \geq 0$ are such that ϕ is a homomorphism.

Solution:

$n = 0$**:** $\mathcal{S}_\prime$ is the group of all permutations of the empty set. There is exactly one element in this group — the function $\iota_\varnothing$, and ϕ maps this element onto itself. This mapping is a homomorphism — indeed, it is an *iso*morphism.

$n = 1$**:** Here again there is only one permutation, and ϕ is an isomorphism.

$n = 2$**:** $\mathcal{S}_2 = \{e, (12)\}$. It can again be verified that ϕ is the identity mapping. It is a simple matter to verify that $\phi(f_1 f_2) = \phi(f_1)\phi(f_2)$ where each of f_1 and f_2 is either e or (12) — there are 4 cases to check, unless one appeals to a theorem.

$n = 3$**:** But here we can produce a counterexample. For $\phi(12) = (21) = (12)$, and $\phi(13) = (31) = (13)$. But $\phi((12)(13)) = \phi((132)) = (132)^{-1} = (123) \neq \phi(12)\phi(13)$.

$n > 3$**:** The counterexample given for $n = 3$ holds for all larger n also, without change.

5. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be given finite groups (where we write the group operation by juxtaposition, and where we denote the identity in both cases by e). Let

$$\phi : \mathcal{G}_1 \longrightarrow \mathcal{G}_2$$

be a homomorphism. Let $x \in \mathcal{G}_1$ be an element of period (order) k.

(a) Show that the period of $\phi(x)$ divides k.

(b) Explain why the period of $\phi(x)$ divides the greatest common divisor $(k, |\mathcal{G}_2|)$.

(c) Show that, if $\mathcal{G}_1$ is cyclic, with generator x, then the action of ϕ is determined for all $g \in \mathcal{G}_1$ by its action on x. That is, you are to show that you can determine all $\phi(g)$ from what you know about $\phi(x)$.

(d) Give an example with two finite cyclic groups, $\mathcal{G}_1$ and $\mathcal{G}_2$, where $\mathcal{G}_1 =< x >$, to show that not every point of $\mathcal{G}_2$ can be realized as the image of x. (This shows that the converse of the preceding result is not true: not every mapping $x \mapsto g_2 \in \mathcal{G}_2$ can be extended to a homomorphism $\phi : \mathcal{G}_1 \to \mathcal{G}_2$.)

(e) Determine all homomorphisms from $(\mathbb{Z}_6, +, [0]_6)$ to $(\mathbb{Z}_4, +, [0]_4)$. For each of them, give the kernel and the image.

Solution:

(a) Since $x^k = e$, $\phi(x)^k = \phi(e) = e$. Hence, by Theorem A.5.6.7, period$(\phi(x))|k$.

(b) Again by Theorem A.5.6.7, the period of $\phi(x)$ must also divide the order of the codomain. Since it is a common divisor of both this order and the period of x, it must divide the greatest common divisor.

(c) Since x is a generator, every element g of the domain of ϕ is expressible as a power — say the ℓth — of x. Then, since ϕ is a homomorphism, which "preserves products", $\phi(x^\ell) = (\phi(x))^\ell$. So, once we know $\phi(x)$, we know $\phi(g)$ for all $g \in \mathcal{G}_1$.

(d) The example which follows will do. Take $x = [1]_6$. As we show below, no homomorphism can map $[1]_6$ on to $[1]_4$. This would entail that $[6]_6$ would be mapped on to $[6]_4$, i.e. that $[0]_6$ would be mapped on to $[2]_4$. But this contradicts the fact that the identity element must be mapped on to the identity element, (cf. Theorem A.5.2.5).

(e) The action of a homorphism $\phi : (\mathbb{Z}_6, +, [0]_6) \to (\mathbb{Z}_4, +, [0]_4)$ is determined by the image of the generator $[1]_6$ (or, equivalently, the generator $[5]_6$ — there are only two generators for this group). The period of the image must divide the greatest common divisor $(4, 6) = 2$. As the periods of $[1]_4$ and $[3]_4$ are both 4 — they are generators for the cyclic group — neither of these can serve as the image of $[1]_6$. The mappings of $[1]_6$ on to either of $[0]_4$ or $[2]_4$ do extend to a homorphism:

$[1]_6 \mapsto [0]_4$**:** In this case the sum of n copies of $[1]_6$ must map to the sum of n copies of $[0]_6$, i.e., to $[0]_4$. This mapping carries the entire domain on to the identity. The kernel is $\mathbb{Z}_6$ (more precisely, $(\mathbb{Z}_6, +, [0]_6)$; the image is $\{[0]_4\}$.

$[1]_6 \mapsto [2]_4$**:** In this case $[1]_6 + [1]_6 \mapsto [2]_4 + [2]_4 = [0]_4$, $[1]_6 + [1]_6 + [1]_6 \mapsto [2]_4 + [2]_4 + [2]_4 = [6]_4 = [2]_4$, etc. The kernel is $\{[0]_6, [2]_6, [4]_6\}$, a subgroup of order 3; and the image is $\{[0]_4, [2]_4\}$, a subgroup of order 2.

6. (a) The left regular representation of $\mathcal{A}_4$ maps $\mathcal{A}_4$ into the group $\mathcal{S}_{\mathcal{A}_4}$ of permutations of the set $\mathcal{A}_4$. Showing all your work, determine the disjoint cycle representation of $L_{(234)}$.

(b) The right regular representation of $\mathcal{A}_4$ maps $\mathcal{A}_4$ into the group $\mathcal{S}_{\mathcal{A}_4}$ of permutations of the set $\mathcal{A}_4$. Showing all your work, determine the disjoint cycle representation of $R_{(12)(34)}$.

(c) Use the information you have accumulated to give the decomposition of $\mathcal{A}_4$ into right cosets of $\langle(234)\rangle$, and into left cosets of $\langle(12)(34)\rangle$.

Solution:

(a) Since $L^3_{(234)}$ is effected by premultiplying (on the left) by $(234)^3$, it is simply the identity. Thus each orbit contains 3 elements. More precisely, each of the

cycles in the disjoint cycle representation of $L_{(234)}$ will be a 3-cycle.

$$\begin{aligned}
L_{(234)}e &= (234)\\
L_{(234)}(234) &= (234)^2 = (243)\\
L_{(234)}(243) &= e\\
L_{(234)}(123) &= (234)(123) = (13)(24)\\
L_{(234)}(13)(24) &= (234)(13)(24) = (143)\\
L_{(234)}(143) &= (234)^3(123) = (123)\\
L_{(234)}(132) &= (234)(132) = (142)\\
L_{(234)}(142) &= (234)(142) = (12)(34)\\
L_{(234)}(12)(34) &= (234)(12)(34) = (132)\\
L_{(234)}(14)(23) &= (234)(14)(23) = (124)\\
L_{(234)}(124) &= (234)(124) = (134)\\
L_{(234)}(134) &= (234)(134) = (14)(23)
\end{aligned}$$

It follows that the disjoint cycle representation of $L_{(234)}$ is the product of the 4 3-cycles $(e, (234), (243))$, $((123), (13)(24), (143))$, $((142), (12)(34), (132))$, $((124), (134), (14)(23))$.

(b) Since $R^2_{(12)(34)}$ is effected by postmultiplying (on the right) by $(((12)(34))^{-1})^2$, it is simply the identity. Thus each of the cycles in the disjoint cycle representation of $R_{(12)(34)}$ will be a 2-cycle. Since the cyclic ordering of two elements is unique, we need only determine the pairs of elements of $\mathcal{A}_4$ that are interchanged by postmultiplication by $((12)(34))^{-1}$; note that $((12)(34))^{-1} = (12)(34)$. We observe that

$$\begin{aligned}
(12)(34)(12)(34) &= e\,,\\
(123)(12)(34) &= (134)\,,\\
(132)(12)(34) &= (234)\,,\\
(143)(12)(34) &= (124)\,,\\
(234)(12)(34) &= (132)\,,\\
(13)(24)(12)(34) &= (14)(23)\,.
\end{aligned}$$

The disjoint cycle representation of $R_{(12)(34)}$ is the product of the 2-cycles $(e, (12)(34))$, $((123), (134))$, $((132), (234))$, $((143), (124))$, $((234), (132))$, $((13)(24), (14)(23))$.

(c) The right cosets of $\langle(234)\rangle$ in $\mathcal{A}_4$ consist of sets of even permutations that are equivalent under pre-multiplication by powers of (234); these will be the sets

of elements which are ordered into 3-cycles in the disjoint cycle representation of $L_{(234)}$ determined above, i.e., $\{e, (234), (243)\}$, $\{(123), (13)(24), (143)\}$, $\{(142), (12)(34), (132)\}$, $\{(124), (134), (14)(23)\}$.

Similarly, the left cosets of $\langle(12)(34)\rangle$ in $\mathcal{A}_4$ will be $\{e, (12)(34)\}$, $\{(123), (134)\}$, $\{(132), (234)\}$, $\{(143), (124)\}$, $\{(234), (132)\}$, $\{(13)(24), (14)(23)\}$.

7. (cf. Exercise A.5.7.1.3) Explain the difference between the abstractly presented groups $\{a, b : a^2, b^2\}$ and $\{a, b : a^2, b^2, abab\}$

   Solution: Both of the groups are "freely" generated by two generators that each have period (order) 2. However, in the second case the generators commute, while in first case there is no such assumption. The second group is finite — it has the structure of the Klein 4-group. The first group is infinite. For example, the elements in the following sequence are all different: a, ab, aba, $abab$, $ababa$, $ababab$, ...

E.5 Fifth 2000 Problem Assignment

Distribution Date: *Caveat lector!* These solutions are in *preliminary* form, and may not have been fully checked. If errors are found, an undated version may be posted on the Web.

1. Where the direct product of *Abelian* groups is under consideration, and the groups are written *additively*, we may use the term *direct sum* in place of *direct product*, and replace the symbol $\times$ by $\oplus$.

   Suppose that we form the direct sum of 7 copies of $(\mathbb{Z}_2, +, 0)$; denote this group simply by $\mathbb{Z}_2^7$. We will denote its elements by strings of length 7 in the alphabet $\{0, 1\}$, suppressing parentheses and commas: strings are added "coordinate-wise" modulo 2. Let H denote the subgroup generated by the 4 strings 1011000, 0101100, 0010110, and 0001011.

   (a) List all elements of H.

   (b) Show that the difference of any two distinct members of H always has at least 3 1's.

   (c) Explain why every left coset of H in $\mathbb{Z}_2^7$ is a right coset, and every right coset is a left coset.

   (d) Determine the coset decomposition of $\mathbb{Z}_2^7$ into cosets of H. In each coset find the element(s) having the smallest number of 1's.

(e) Now consider a subgroup K of $\mathbb{Z}_2^8$ obtained by taking the elements of H and adding an 8th binary digit at the end in such a way that the sum of the 8 digits in each of the 16 words is always 0. Show that, except for the word 00000000, all words have at least 4 1's. Use this fact to show that the difference of two distinct words in K always has at least 4 1's.

You may wish to use methods of linear algebra to solve this problem. Just consider the "field" of coefficients to be the elements of $\mathbb{Z}_2$, where addition and multiplication are both modulo 2.

Solution:

(a) The four given vectors are *linearly independent*. We form linear combinations of them in all possible ways. Since there are only two available scalars — 0 and 1 — we are, in effect, taking all possible subsets of this set of 4 basis vectors. There are $2^4 = 16$ such subsets, and each of them yields a different sum. Defining $\vec{e}_1 = 1011000$, $\vec{e}_2 = 0101100$, $\vec{e}_3 = 0010110$, and $\vec{e}_4 = 0001011$, we have the following 16 vectors:

$$\begin{aligned}
0\vec{e}_1 + 0\vec{e}_2 + 0\vec{e}_3 + 0\vec{e}_4 &= 0000000 \\
1\vec{e}_1 + 0\vec{e}_2 + 0\vec{e}_3 + 0\vec{e}_4 &= 1011000 \\
0\vec{e}_1 + 1\vec{e}_2 + 0\vec{e}_3 + 0\vec{e}_4 &= 0101100 \\
0\vec{e}_1 + 0\vec{e}_2 + 1\vec{e}_3 + 0\vec{e}_4 &= 0010110 \\
0\vec{e}_1 + 0\vec{e}_2 + 0\vec{e}_3 + 1\vec{e}_4 &= 0001011 \\
1\vec{e}_1 + 1\vec{e}_2 + 0\vec{e}_3 + 0\vec{e}_4 &= 1110100 \\
1\vec{e}_1 + 0\vec{e}_2 + 1\vec{e}_3 + 0\vec{e}_4 &= 1001110 \\
1\vec{e}_1 + 0\vec{e}_2 + 0\vec{e}_3 + 1\vec{e}_4 &= 1010011 \\
0\vec{e}_1 + 1\vec{e}_2 + 1\vec{e}_3 + 0\vec{e}_4 &= 0111010 \\
0\vec{e}_1 + 1\vec{e}_2 + 0\vec{e}_3 + 1\vec{e}_4 &= 0100111 \\
0\vec{e}_1 + 0\vec{e}_2 + 1\vec{e}_3 + 1\vec{e}_4 &= 0011101 \\
1\vec{e}_1 + 1\vec{e}_2 + 1\vec{e}_3 + 0\vec{e}_4 &= 1100010 \\
1\vec{e}_1 + 1\vec{e}_2 + 0\vec{e}_3 + 1\vec{e}_4 &= 1111111 \\
1\vec{e}_1 + 0\vec{e}_2 + 1\vec{e}_3 + 1\vec{e}_4 &= 1000101 \\
0\vec{e}_1 + 1\vec{e}_2 + 1\vec{e}_3 + 1\vec{e}_4 &= 0110001 \\
1\vec{e}_1 + 1\vec{e}_2 + 1\vec{e}_3 + 1\vec{e}_4 &= 1101001
\end{aligned}$$

It can be seen that we have, in addition to 0000000 and 1111111, all *cyclic* permutations of 1011000 and of its complement in 1111111 — 0100111.

(b) It can be observed that the only vector having fewer than 3 1's is 0000000. Since H is a group, the sum of any two of its elements is also an element of the group. If $x + y = 0$, then $y = -x$. As this group has the property that $x = -x$ for all x, we can never have two *distinct* vectors summing to 0. Thus all sums of two distinct vectors must have *weight* at least 3 (i.e. must have at least 3 ones). But, in this group, *sum* and *difference* mean the same thing. So we have shown that all differences of distinct elements have *weight* at least 3.

(c) Let x be any element of $\mathbb{Z}_2^7$. Since $\mathbb{Z}_2^7$ is commutative, $\forall h \in H[x + h = h + x]$ is true; hence, $\{x + h | h \in H\} = \{h + x | h \in H\}$, i.e. $x + H = H + x$. In other terms, any subgroup of an abelian group is *invariant* or *normal*.

(d) There are 8 cosets. One of these is the subgroup H itself. The other 7 are

$$\begin{aligned}
1000000 + H &= \{1000000, ...\} \\
0100000 + H &= \{0100000, ...\} \\
0010000 + H &= \{0010000, ...\} \\
0001000 + H &= \{0001000, ...\} \\
0000100 + H &= \{0000100, ...\} \\
0000010 + H &= \{0000010, ...\} \\
0000001 + H &= \{0000001, ...\}
\end{aligned}$$

We know that two vectors of "weight" 1 cannot be in the same coset, since their difference is a vector of weight 2, and no such vector is present in the subgroup. Once we have 8 cosets, each containing 16 elements, we have accounted for all the points in $\mathbb{Z}_2^7$, so there cannot be any other cosets.

(e)

10110000	+	0000001	=	10110001
01011000	+	0000001	=	01011001
00101100	+	0000001	=	00101101
00010110	+	0000001	=	00010111
10001010	+	0000001	=	10001011
11000100	+	0000001	=	11000101
01100010	+	0000001	=	01100011
11111110	+	0000001	=	11111111
01001110	+	0000000	=	01001110
10100110	+	0000000	=	10100110
11010010	+	0000000	=	11010010
11101000	+	0000000	=	11101000
01110100	+	0000000	=	01110100
00111010	+	0000000	=	00111010
10011100	+	0000000	=	10011100
00000000	+	0000000	=	00000000

The vectors in H all had weight 0, 3, 4, 7; the vectors of weight 3 are converted into vectors of weight 4, while those of weight 4 in H are also converted into vectors of weight 4 in K. The only vector that had weight 0 was the zero element, and it becomes the zero element of K; the only vector that had weight 7 is transformed — because it has an odd number of 0's — into the vector 11111111. Thus the weights in non-zero vectors in K are all 4 or 8. As seen earlier in our solution to part 1b, this implies that all differences of elements of K have weight at least 4.

What we have created here is a *double-error-detecting, single-error-correcting linear code* (or a *double-error-detecting, single-error-correcting group code.*) If a vector is transmitted and as many as two of its bits are changed, we can detect that situation; if only one bit is changed, we can actually determine which bit that was, and correct the error!

2. Showing all of your work, determine the periods of all elements of each of the following groups:

   (a) The alternating group $\mathcal{A}_5$.

   (b) The dihedral group $\mathcal{D}_6$.

   (c) The direct product $\mathcal{A}_5 \times \mathcal{D}_6$.

   (Hint: All elements having the same "cycle type" in any permutation group will have the same period; thus it suffices to consider one element of each of these

types.)

Solution:

(a) We shall list the cycle types by the associated additive partitions of 5, which we will list in order of the largest part.

$5 = 1 + 1 + 1 + 1 + 1$. The identity is the only element of cycle type $(\bullet)(\bullet)(\bullet)(\bullet)(\bullet)$; its period is 1.

$5 = 2 + 2 + 1$. The period of any element of type $(\bullet\bullet)(\bullet\bullet)(\bullet)$ is 2, since the second power annihilates both of the 2-cycles.

$5 = 3 + 1 + 1$. The period of any element of type $(\bullet\,\bullet\,\bullet)(\bullet)(\bullet)$ is 3, since no smaller power of such an element is the identity, and all cycle lengths are divisors of 3.

$5 = 5$. Any 5-cycle has the property that the 5th power is the smallest to equal the identity.

(b) The elements of $\mathcal{D}_6$ are either powers of (123456) or reflections either in an axis through two vertices — like (26)(35) — or in an axis bisecting two opposite sides — like (16)(25)(34). The powers of (123456) are (123456), (135)(246), (14)(25)(36), (153)(264), (165432), and the identity. Thus we have the following partitions/cycle types:

$6 = 1 + 1 + 1 + 1 + 1 + 1$. Only the identity has this cycle type, and its period is 1.

$6 = 2 + 2 + 1 + 1$. As all cycles have lengths 1 or 2, the period is 2.

$6 = 2 + 2 + 2$. Again, the period is 2.

$6 = 3 + 3$. Both cycles have length 3, so the period of the product is the greatest common divisor $(3, 3) = 3$.

$6 = 6$. The period is 6.

(c) We tabulate the cycle types of the first and second arguments, and the period of the resulting element, which will always be the least common multiple of the periods of the two arguments.

$\mathcal{A}_5$ \ $\mathcal{D}_6$	6	$1+1+1+1+1+1$	$3+3$	$2+2+2$	$2+2+1+1$
$1+1+1+1+1$	6	1	3	2	2
$2+2+1$	6	2	6	2	2
$3+1+1$	6	3	3	6	6
5	30	5	15	10	10

3. Determine the left and right coset decompositions of $\mathcal{D}_8$ in cosets of each of the subgroups

(a) $\mathcal{L}_1 = \langle (1357)(2468) \rangle$;

(b) $\mathcal{L}_2 = \langle (28)(37)(46), (12)(38)(47)(56) \rangle$;

(c) $\mathcal{L}_3 = \langle (28)(37)(46) \rangle$.

In each case determine whether the sets of left cosets and right cosets are different.

Solution: (This problem can be solved completely computationally, without the observations that we are making in our solution. We take the opportunity to make such observations to render the solution more transparent, but they are not necessary, and were not expected from the student on first attempting the problem.)

(a) Observe that $(1357)(2468) = (12345678)^2$. Thus $\mathcal{L}_1$ consists of all even powers of (12345678).

$$\begin{aligned}
\mathcal{L}_1 I &= \{I, (1357)(2468), (15)(26)(37)(48), (1753)(2864)\} \\
&= I\mathcal{L}_1 \\
\mathcal{L}_1(12345678) &= \{(12345678), (14725836), (16385274), (18765432)\} \\
&= (12345678)\mathcal{L}_1 \\
\mathcal{L}_1(12)(38)(47)(56) &= \{(12)(38)(47)(56), (14)(23)(58)(67), \\
&\qquad (16)(25)(34)(78), (18)(47)(36)(45)\} \\
&= (12)(38)(47)(56)\mathcal{L}_1 \\
\mathcal{L}_1(28)(37)(46) &= \{(28)(37)(46), (13)(48)(57), \\
&\qquad (15)(24)(68), (17)(26)(35)\} \\
&= (28)(37)(46)\mathcal{L}_1
\end{aligned}$$

Each left coset is a right coset; this subgroup is what is called *invariant*.

(b) Since $(12)(38)(47)(56) \cdot (28)(37)(46) = (12345678)$, all powers of the rotation (123454678) are present in $\mathcal{L}_2$. But there are also other elements in this subgroup, for example $(28)(37)(46)$, which is a reflection in the axis through vertices 1 and 5. Thus the order of the subgroup is more than 8. But $\mathcal{D}_8$ contains 16 elements, and all subgroups must have, as their order, a divisor of 16. It follows that $|\mathcal{L}_2| = 16$, so $\mathcal{L}_2 = \mathcal{D}_8$. Thus there is only one coset — the entire subgroup $\mathcal{L}_2$.

(c)

$$\begin{aligned}
\mathcal{L}_3 I &= \{I, (28)(37)(46)\} \\
\mathcal{L}_3(13)(48)(57) &= \{(13)(48)(57), (1753)(2864)\} \\
\mathcal{L}_3(15)(24)(68) &= \{(15)(24)(68), (15)(26)(37)(48)\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{L}_3(17)(26)(35) &= \{(17)(26)(35), (1357)(2468)\} \\
\mathcal{L}_3(12)(38)(47)(56) &= \{(12)(38)(47)(56), (18765432)\} \\
\mathcal{L}_3(14)(23)(58)(67) &= \{(14)(23)(58)(67), (16385274)\} \\
\mathcal{L}_3(16)(25)(34)(78) &= \{(16)(25)(34)(78), (14725836)\} \\
\mathcal{L}_3(18)(27)(36)(45) &= \{(18)(27)(36)(45), (12345678)\} \\
I\mathcal{L}_3 &= \{I, (28)(37)(46)\} \\
(13)(48)(57)\mathcal{L}_3 &= \{(13)(48)(57), (1357)(2468)\} \\
(15)(24)(68)\mathcal{L}_3 &= \{(15)(24)(68), (15)(26)(37)(48)\} \\
(17)(26)(35)\mathcal{L}_3 &= \{(17)(26)(35), (1753)(2864)\} \\
(12)(38)(47)(56)\mathcal{L}_3 &= \{(12)(38)(47)(56), (12345678)\} \\
(14)(23)(58)(67)\mathcal{L}_3 &= \{(14)(23)(58)(67), (14725836)\} \\
(16)(25)(34)(78)\mathcal{L}_3 &= \{(16)(25)(34)(78), (16385274)\} \\
(18)(27)(36)(45)\mathcal{L}_3 &= \{(18)(27)(36)(45), (18765432)\}
\end{aligned}$$

Here the sets of left and right cosets are different, although there are two cosets that serve as both left and right cosets; (there is always at least one such coset — the subgroup itself).

4. Determine all positive integers m such that

   (a) $\varphi(m) = 15$

   (b) $\varphi(m) = 14$

   (c) $\varphi(m) = 6$

   Solution:

   (a) By Exercise A.6.2.9.1, the only odd value assumed by the Euler totient function is 1, which is its value at 1 and at 2 only. Thus there are no integers m where $\varphi(m) = 15$.

   (b) If $m = p_1^{r_1} p_2^{r_2} ... p_n^{r_n}$, where all r_i are positive, then 14 must be divisible by $p_i - 1$ $(i = 1, 2, ..., n)$. The only divisors of 14 are 1, 2, 7, and 14; of these only 1 and 2 are 1 less than a prime. Thus m can only be a product of 2's and 3's. But, if $m = 2^{r_1} 3^{r_2}$, where $r_1 \geq 0$ and $r_2 \geq 0$, $7 \not| \varphi(m)$, so $\varphi(m) \neq 14$. We conclude that here also there are no solutions to the equation $\varphi(m) = 14$.

   (c) The divisors of 6 are 1, 2, 3, 6, so the only primes that may divide m are in the list $1 + 1$, $2 + 1$, $3 + 1$, $6 + 1$ — and 4 is not prime. So $m = 2^{r_1} 3^{r_2} 7^{r_3}$. Since 7 is not a divisor of 6, $r_3 \leq 1$; since 2^2 is not a divisor, $r_1 \leq 2$; since 3^2 is not a divisor, $r_2 \leq 2$. The problem is now finite — there are at most

$3 \times 3 \times 2 = 18$ cases to be considered, as each exponent may be 0. We could test all 18 cases, but it is easy to dispose of the cases where $r_3 = 1$. For here $\varphi(m/7) = 1$, so $m/7 = 1$ or $m/7 = 2$ and m is either 7 or 14; in either case $\varphi = 6$. This type of analysis could be continued, but we will simply tabulate the other possible values of m and extract those for which $\varphi = 6$:

r_1	r_2	$m = 2^{r_1}3^{r_2}$	$\varphi\left(2^{r_1}3^{r_2}\right)$
0	0	1	1
0	1	3	2
0	2	9	6
1	0	2	1
1	1	6	2
1	2	18	6
2	0	4	2
2	1	12	4
2	2	36	12

In this table only $m = 9$ and $m = 18$ have $\varphi(m) = 6$. Thus the entire list of solutions is $m = 7, 9, 14, 18$.

5. Without using a calculator, and showing all your work, determine the smallest non-negative integer congruent to $5^{10,000}$ modulo 221. You may assume that $221 = 17 \cdot 13$, $10,000 = 45 \cdot 221 + 55 = 208 \cdot 48 + 16 = 52 \cdot 192 + 16$.

   Solution: [1039] Note that some of the information given in the question was irrelevant.

   Since $\varphi(221) = 16 \cdot 12 = 192$, and since $(5, 221) = 1$, we know from Euler's generalization of Fermat's "Little" Theorem that $5^{192} \equiv 1 \pmod{221}$. While the information given included the statement that $10000 = 45 \cdot 221 + 55$, this information was irrelevant; what you have to compute first is that $10000 = 52 \cdot 192 + 16$, so $5^{10000} \equiv 5^{16} \pmod{221}$.

   Of course, one could compute 5^{16} by repeatedly multiplying by 5 and reducing modulo 221; that would be very tedious, and would require working extensively with 5-digit integers. A more efficient approach would be to determine only the values of 5^{2^k} for $k = 0, 1, ..., 5$. For a general exponent n, that information could then be used to determine the residue of 5^n to the given modulus; in the present case n is a power of 2, thus all we have to do is to recursively determine the smallest non-negative residues of integers 5^{2^k}, by repeated squaring, for $k = 2, 3, 4$. So

$$5^{2^2} = \left(5^2\right)^2 = 625 \equiv 183 \pmod{221}$$

[1039] This solution has been corrected; the draft solution circulated on 7 April 2000 contained errors.

$$5^{2^3} = \left(5^{2^2}\right)^2 \equiv 183^2 \equiv 118 \pmod{221}$$
$$5^{2^4} = \left(5^{2^3}\right)^2 \equiv 118^2 \equiv 13924 \equiv 1 \pmod{221}$$

A simpler attack is to observe that $5^{16} \equiv 1 \pmod{17}$ and $5^{12} \equiv 1 \pmod{13}$. From the last congruence we have that $5^{16} \equiv 625 \equiv 1 \pmod{13}$; since $5^{16} \equiv 1$ to both (relatively prime) moduli 13 and 17, the congruence also holds to the least common multiple of the moduli, i.e. to modulus 221.

Could the fact that $5^{16} \equiv 1 \pmod{13}$ have been foreseen? The multiplicative group of the group $\mathbb{Z}_{13}^{\times}$ is cyclic, of order 12. It is generated by $\phi(12) = 4$ so-called "primitive" elements (discussed in the notes, but not in this year's syllabus); for example, one such primitive element is 2. Expressed as a power of this primitive element, $5 \equiv 2^9$; hence the 4th power of 5 satisfies the congruence $5^4 \equiv 2^{36} = (2^{12})^3 \equiv 1^3 \equiv 1$. Analysis of this type provides more information than is available from Euler's generalization of Fermat's Little Theorem, but is not expected of students in this course.

6. (a) Give, without proof, an example of each isomorphism type of group of order 6.

   (b) Find examples of all *abelian* groups of order 18. Prove that your examples are not isomorphic.

   (c) Find examples of at least 2 *non-abelian* groups of order 18, proving that each of your examples is non-abelian, and also that they are not isomorphic.

   Solution:

   (a) By the Fundamental Theorem of Abelian Groups, we know that the only abelian group of order 6 is $\mathbb{Z}_6$, or, equivalently (in the formulation given in the lectures), $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

   The only nonabelian group can be shown to be, up to isomorphism, $\mathcal{S}_3$; or, equivalently, $\mathcal{D}_3$.[1040]

   (b) We apply the Fundamental Theorem of Abelian Groups in the formulation given in the lectures. As $18 = 2^1 3^2$, the only relevant factorizations are $18 = 2 \times 3^2$, and $18 = 2 \times 3 \times 3$. We have the following two types of groups: $\mathbb{Z}_{18}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_6$. The first may also be expressed as $\mathbb{Z}_2 \oplus \mathbb{Z}_9$, and the second also as $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

[1040] A proof was not required here. One can be developed from first observing that the group will have an element x of period 3. As $\langle x \rangle$ contains exactly have of the elements of the group, it is seen that the left and right coset decompositions coincide, and the structure can be determined by examining the way in which a representative of the non-subgroup coset multiplies x on the left and the right.

(c) Following are three examples:

$\mathcal{D}_9$**:** This is the dihedral group of symmetries of the 9-gon. It contains one element of order 9, some of whose powers have orders 3 or 1; and 9 elements of order 2. This group is non-abelian since, for example, the reflections (29)(38)(47)(56) and (13)(49)(58)(67) do not commute.

$\mathcal{S}_3 \times \mathbb{Z}_3$**:** This is a group of ordered pairs, whose first elements can have orders 1, 2, or 3, and whose second element can have orders 1 or 3. An element like $((12), [1]_3)$ will have order 6. As there are no such elements in the preceding group, we know these two groups cannot be isomorphic. This group is non-abelian, since, for example, the elements $((12), [0]_3)$ and $((23), [0]_3)$ do not commute.

There exists just one other type of non-abelian group of order 18, but its structure is too complicated to describe in this course.[1041]

F 2000/2001 Problem Assignments, with Solutions

F.1 First 2000/2001 Problem Assignment

1. [4, Exercise 1.E4, p. 6] Consider the following binary relations, each denoted by $\approx$, on $\mathbb{Z}$. In each case, showing all your work briefly, decide if the relation is an equivalence relation. If so, describe the corresponding partition of $\mathbb{Z}$. If not, determine which of the properties — reflexivity, symmetry, transitivity — of an equivalence relation fail.

   (a) $a \approx b$ iff $ab \geq 0$;

   (b) $a \approx b$ iff $a - b$ is divisible by 3;

   (c) $a \approx b$ iff $ab > 0$;

   (d) $a \approx b$ iff $a + b$ is divisible by 3; and

   (e) $a \approx b$ iff $a \geq b$.

   Solution:

   (a) Reflexivity: For every integer a, $a^2 \geq 0$.

   Symmetry: By the commutativity of multiplication of integers, $ab \geq 0$ iff $ba \geq 0$. Hence

   $$\forall a \forall b((a \approx b) \Rightarrow (b \approx a)) .$$

[1041] It can be viewed as the subgroup of those permutations in $\mathcal{S}_3 \times \mathcal{S}_3$ where both elements of the ordered pair are even, or both are odd.

Transitivity: Transitivity fails. For example, $1 \approx 0$ and $0 \approx -1$, but $1 \not\approx -1$, since the product $1 \cdot (-1)$ is not positive.

(b) This is the relation of congruence modulo 3; a proof that this is an equivalence relation can be found in [35, Example 6.5.4, p. 409]. The equivalence classes are the residue classes modulo 3:

$$\begin{aligned} [0] &= \{3n | n \in \mathbb{Z}\} \\ [1] &= \{1 + 3n | n \in \mathbb{Z}\} \\ [2] &= \{2 + 3n | n \in \mathbb{Z}\} \end{aligned}$$

(c) Reflexivity: Reflexivity fails, since $0^2 \not> 0$.

Symmetry: Since the property is defined in terms of the multiplication operation on $\mathbb{Z}$, and that operation is symmetric, $\approx$ is symmetric.

Transitivity: $ab > 0$ iff a and b both are non-zero, and have the same sign. If a and b have the same sign, and b and c have the same sign, then a, b, c will all have the same sign, and $a \approx c$.

(d) Reflexivity: Reflexivity fails; for example, $1 + 1$ is not divisible by 3.

Symmetry: Symmetry holds since the relation is defined in terms of the addition operation in $\mathbb{Z}$, which is symmetric.

Transitivity: Transitivity fails. For example $1 \approx 2$ and $2 \approx 1$; but, as observed above, it is not true that $1 \approx 1$.

(e) Reflexivity and Transitivity: The relation $\geq$ on the integers is indeed reflexive and transitive, since it is known to be a partial ordering — indeed, a *total* ordering.

Symmetry: This relation is *anti*symmetric. A counterexample to symmetry is $2 \geq 1$: it is not true that $1 \geq 2$.

2. (a) [4, Exercise 3C.E5(iv)] Using Euclid's algorithm, and showing all your work neatly, find $(1001, 1309)$.

(b) Use the results of part 2a to determine integers r and s such that

$$1001r + 1309s = (1001, 1309)\,. \tag{1141}$$

(c) Determine a formula for *all* integer solutions to equation (1141).

(d) Among all solutions to equation (1141) find one for which the excess of r over 100 is positive, but as small as possible with that property.

Solution:

(a)

$$\begin{aligned} 1309 &= 1001 \cdot 1 + 308 \\ 1001 &= 308 \cdot 3 + 77 \\ 308 &= 77 \cdot 4 + 0 \end{aligned}$$

Hence $(1309, 1001) = 77$.

(b) Working upwards from the penultimate equation above,

$$\begin{aligned} 77 &= 1001 - 308 \cdot 3 = 1001 \cdot 1 - (1309 - 1001 \cdot 1) \cdot 3 \\ &= 1309 \cdot (-3) + 1001 \cdot 4 \end{aligned}$$

Thus one solution to (1141) is $r = 4$, $s = -3$.

(c) By [4, Proposition 3C.5, p. 34], the general solution to (1141) is

$$\begin{aligned} r &= 4 + n \cdot \frac{1309}{(1001, 1309)} = 4 + 17n \\ s &= -3 - n \cdot \frac{1001}{(1001, 1309)} = -3 - 13n \end{aligned}$$

where n ranges over the set $\mathbb{Z}$ of integers.

(d) We require that $4 + 17n \geq 100$, so $n \geq \frac{96}{17}$, hence $n \geq \left\lceil \frac{96}{17} \right\rceil = 6$; the smallest acceptable value will be when $n = 6$: then $r = 106$, $s = -81$.

3. In the following problems a, b, k are to be any integers, where a and b are not both zero, and k is not zero.

(a) Prove that any common divisor of a and b is also a common divisor of $a + kb$ and b.

(b) Apply the result of part 3a to prove that

$$(a, b) = (a + kb, b)\,. \tag{1142}$$

(c) You may assume the following properties of the greatest common divisor have been proved:

$$\begin{aligned} (-a, b) &= (a, b) && (1143) \\ (a, b) &= (b, a) && (1144) \\ (ka, kb) &= k(a, b). && (1145) \end{aligned}$$

Prove that, for any natural number r, $(2^r + 1, 2^r - 1) = 1$.

(d) [4, Exercise 4C.E5, p. 59, p. 486] For any natural number n prove by induction that $2^{2^n} - 1$ is divisible by at least n distinct primes. Show how this provides another proof of Euclid's theorem that there exist infinitely many primes.

Solution:

(a) Suppose that $d|a$ and $d|b$, i.e. that there exist integers u and v such that $a = du$, $b = dv$. Then $a + kb = d(u + kv)$, which is a multiple of d.

(b) Since the greatest common divisor of a and b is, in particular, a common divisor of a and b, it must also divide $a + kb$, so it is a common divisor of $a + kb$, b (and a). Thus

$$(a, b)|(a + kb, b)\,. \tag{1146}$$

Now, in (1146), take $a := a + kb$, $b := b$, $k := -k$; we find that

$$(a + kb, b)|(a, b)\,. \tag{1147}$$

Thus $(a + kb, b)$ and (a, b) are positive integers, each of which divides the other; we conclude that they are *the same* positive integer.[1042]

(c)

$$\begin{aligned}(2^r + 1, 2^r - 1) &= ((2^r + 1) + (-1)(2^r - 1), 2^r - 1) \quad \text{by (1142)}\\ &= (2, 2^r - 1) \quad \text{by 1142}\\ &= (2, 1) \quad \text{since } 2^r - 1 \text{ is odd}\\ &= 1\,.\end{aligned}$$

(d) We shall prove the proposition

$$P(n): \qquad 2^{2^n} - 1 \text{ is the product of at least } n \text{ distinct primes.}$$

by induction on n.

Base Case $n = 1$**:** $2^2 - 1 = 3$ is prime, hence it is the product of 1 prime.

Induction Step: Assume that $P(n)$ is true. Then

$$2^{2^{n+1}} - 1 = \left(2^{2^n}\right)^2 - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right)$$

where the last two factors are relatively prime. That implies that the prime factors of $2^{2^n} + 1$ are not factors of $2^{2^n} - 1$, so the product has at least one more prime factor than had $2^{2^n} - 1$. But we assumed that $2^{2^n} - 1$ has at least n distinct prime factors, and have, therefore, proved $P(n + 1)$.

[1042] Divisibility is a partial ordering of $\mathbb{N}$.

We conclude that $P(n)$ has been established for all positive n by induction(1) [4, §2A]. As $n \to \infty$, the number of distinct prime factors of $2^{2^n} - 1$ will approach infinity.

4. (cf. [4, Exercise 4A.E9, p. 52]) If $(a, b) = 24$, what are the possible values of (a^3, b^4)? You are expected to provide a careful justification of your conclusion.

   Solution: $24 = 2^3 3^1$. By the observation preceding [4, Exercise 4A.E9, p. 52], the prime decompositions of a and b consist of, with the exception of powers of 2 and 3, powers of distinct sets of primes. In one of the two cases the power of 2 must be precisely 2^3, while in the other the power must be of the form 2^k, where $k \geq 3$; similarly, one of a and b contains, in its prime decomposition, the factor 3^1, while the other contains a factor of the form 3^ℓ, where $\ell \geq 1$. There are four ways in which these events can occur; in the following table assume that $(m, n) = 1$, and that $k \geq 3$, $\ell \geq 1$.

a	b	a^3	b^4	2^r	3^s	(a^3, b^4)
$2^3 3^1 m$	$2^k 3^\ell n$	$2^9 3^3 m^3$	$2^{4k} 3^{4\ell} n^4$	9	3	$2^9 3^3$
$2^3 3^\ell m$	$2^k 3^1 n$	$2^9 3^{3\ell} m^3$	$2^{4k} 3^4 n^4$	9	$\min(4, 3\ell)$	$2^9 3^3, 2^9 3^4$
$2^k 3^1 m$	$2^3 3^\ell n$	$2^{3k} 3^3 m^3$	$2^{12} 3^{4\ell} n^4$	$\min(12, 3k)$	3	$2^9 3^3, 2^{12} 3^3$
$2^k 3^\ell m$	$2^3 3^1 n$	$2^{3k} 3^{3\ell} m^3$	$2^{12} 3^4 n^4$	$\min(12, 3k)$	$\min(4, 3\ell)$	$2^9 3^3, 2^{12} 3^3, 2^9 3^4, 2^{12} 3^4$

   It follows that, when $(a, b) = 24$, all of the following constitute the set of possible values for (a^3, b^4): $2^9 3^3, 2^{12} 3^3, 2^9 3^4, 2^{12} 3^4$. (All of these values are attained.)

F.2 Second 2000/2001 Problem Assignment

1. Give a counterexample to show that, for any composite modulus $m \geq 3$, it is not always possible to conclude from $ab \equiv ac \pmod{m}$, where $a \neq m$ that $b \equiv c \pmod{m}$.

   Solution: Suppose that m admits a non-trivial factorization $m = ab$. Take c to be 0. Then ab and ac are congruent modulo m, since both are multiples of m. But b is not congruent to 0.

2. [37, Exercise 3.1.24] Give a complete system of residues modulo 13 consisting entirely of positive odd integers not exceeding 50.

   Solution: We can begin with the system 0,1,2,...,12, and then replace the even integers by odd representatives, simply by adding 13 to each of them:

   $$13, 1, 15, 3, 17, 5, 19, 7, 21, 9, 23, 11, 25$$

   There are, of course, other solutions.

3. [37, Exercise 3.1.22] Prove by induction that, if n is a natural number,

$$4^n \equiv 1 + 3n \pmod 9 . \tag{1148}$$

Solution: Let $P(n)$ denote (1148). The base case, when $n = 1$ is obvious, since $4^1 = 1 + 3$. Suppose that $P(n)$ has been proved. Then

$$\begin{aligned} 4^{n+1} &\equiv 4(1 + 3n) \pmod 9 \\ &\equiv 4 + (3 + 9)n \pmod 9 \\ &\equiv 4 + 3n \pmod 9 \\ &\equiv 1 + 3(n + 1) \pmod 9 \end{aligned}$$

It follows by induction(1) that $P(n)$ is true for all natural numbers.

4. Determine all integer solutions to the following systems of congruences, by first transforming all congruences to systems where the moduli are only prime powers:

(a)

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 7 \pmod{16} \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 9 \pmod{16} \end{aligned}$$

(c) [4, 12A.E10, p. 200]

$$\begin{aligned} x &\equiv 1 \pmod 2 && (1149) \\ x &\equiv 2 \pmod 5 && (1150) \\ x &\equiv 5 \pmod 6 && (1151) \\ x &\equiv 5 \pmod{12} && (1152) \end{aligned}$$

Solution:

(a) Any integer which is congruent to 7 modulo 16 has the form $7 + 4(4k)$, so it is congruent to 7 modulo 4, hence also to $7 - 4 = 3$ modulo 4. Thus the second congruence implies the first, and the general solution is $x = 7 + 16k$ ($k \in \mathbb{Z}$).

(b) Any integer x congruent to 9 modulo 16 is of the form $x = 9 + 16k = 1 + 4(2 + 4k)$ and belongs to the residue class $[1]_4$. But this class is disjoint from the class $[3]_4$ of solutions to the first congruence given, so this system of congruences has no simultaneous solutions.

(c) There are several different strategies that may be followed to solve a system of this type. We will transform the system into an equivalent system where the moduli are powers of primes. Congruence (1151) is equivalent to two congruences,

$$x \equiv 5 \pmod 2 \tag{1153}$$
$$x \equiv 5 \pmod 3 \tag{1154}$$

and congruence (1152) is equivalent to two congruences,

$$x \equiv 5 \pmod 4 \tag{1155}$$
$$x \equiv 5 \pmod 3 \tag{1156}$$

Since (1156) is identical to (1154), we may suppress it. And congruence (1155) implies that $x \equiv 1 \pmod 2$, which is (1149), so we may suppress (1149); (1153) is also equivalent to (1149), and it also may be suppressed. We are left with (1150), (1154) and (1155). These congruences are now expressed to relatively prime moduli. When we reach [4, Chapter 12] we shall see that the Chinese Remainder Theorem ensures the existence of a solution, and provides an algorithm for finding it. Not having that algorithm available yet, we can proceed in an *ad hoc* way. For example, since congruences (1154) and (1155) differ only in the moduli, we can replace the two of them by the single congruence (1152), whose general solution is $x = 5 + 12m$, where $m \in \mathbb{Z}$. We can then impose (1150) to obtain $5 + 12m \equiv 2 \pmod 5$, which is equivalent to $2m \equiv 2 \pmod 5$. Since $(2, 5) = 1$, we may divide both sides by 2 (or, equivalently, we may multiply both sides by an inverse of 2 modulo 5, such as 3), to obtain

$$m \equiv 1 \pmod 5$$

which implies that $m = 1 + 5n$, where $n \in \mathbb{Z}$, and so $x = 17 + 60n$. We may verify by substitution in the original congruences that all integers of this form are solutions to the system.

5. Show that the *union* of the solution sets for the following congruences contains all of $\mathbb{Z}$. Note that this time we are not solving the congruences *simultaneously* which is equivalent to taking the *intersection* of their solution sets — we are taking the

union!

$$x \equiv 0 \pmod 2 \tag{1157}$$
$$x \equiv 0 \pmod 3 \tag{1158}$$
$$x \equiv 1 \pmod 4 \tag{1159}$$
$$x \equiv 1 \pmod 6 \tag{1160}$$
$$x \equiv -1 \pmod{12} \tag{1161}$$

Solution: Since all of the moduli are divisors of 12, it is convenient to express their solution sets in terms of that modulus; to avoid duplication, we shall use representatives from the set $\{0, 1, ..., 11\}$. The solutions to (1161) constitute the residue class $[11]_{12}$. The solutions to (1160) constitute the union of the residue classes $[1]_{12}$ and $[1+6]_{12} = [7]_{12}$. The solutions to (1159) constitute the union of the residue classes $[1]_{12}$ and $[1+4]_{12} = [4]_{12}$ and $[1+8]_{12} = [9]_{12}$. The solutions to (1158) constitute the union of the residue classes $[0]_{12}$, $[3]_{12}$, $[6]_{12}$, $[9]_{12}$. And the solutions to (1157) constitute the union of the 6 residue classes with even representatives 0, 2, 4, 6, 8, 10. The union of these sets is $\mathbb{Z}$.

6. Decide whether each of the following congruences has an integer solution. If it does not, explain why. If it has a solution, find *all* solutions.

   (a) $18x \equiv 5 \pmod{21}$

   (b) $18x \equiv 5 \pmod{19}$

   (c) $18x \equiv 5 \pmod{31}$

   Solution:

   (a) Since $(18, 21) = 3$, which does not divide 5, there can be no solution to this congruence.

   (b) Here $(18, 19) = 1$, which is a divisor of 5, so there will be solutions. We could use the Euclidean algorithm to determine an inverse, as we shall in the next problem; but there is an easier approach possible this time, since $18 \equiv -1$ to the given modulus. The congruence can be rewritten as $-x \equiv 5 \pmod{19}$; multiplying both sides by -1 yields $x \equiv -5 \pmod{19}$, which is the general solution. That is, the set of solutions are all integers in the residue class $[-5]_{19}$, or, equivalently, in the class $[14]_{19}$.

   (c) Here $(18, 31) = 1$ again. If we determine this fact by the Euclidean algorithm, we obtain

$$31 = 18 \cdot 1 + 13$$

$$\begin{aligned}
18 &= 13 \cdot 1 + 5 \\
13 &= 5 \cdot 2 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \text{; hence} \\
1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \\
&= 5 \cdot (-1) + 3 \cdot 2 = 5 \cdot (-1) + (13 - 5 \cdot 2) \cdot 2 \\
&= 13 \cdot 2 + 5 \cdot (-5) = 13 \cdot 2 + (18 - 13 \cdot 1) \cdot (-5) \\
&= 18 \cdot (-5) + 13 \cdot 7 = 18 \cdot (-5) + (31 - 18 \cdot 1) \cdot 7 \\
&= 31 \cdot 7 + 18 \cdot (-12)
\end{aligned}$$

so one inverse of 18 modulo 31 is -12. Multiplying both sides of the given congruence by this number gives $x \equiv (-12) \cdot 5 = -60 \equiv 2 \pmod{31}$; the set of solutions is $[2]_{31}$.

7. (a) Prove that the product of any two consecutive integers is even.

   (b) [37, Exercise 1.5.30] Use the preceding result to prove that the squares of all odd integers are contained in the residue class $[1]_8$.

   Solution:

   (a) In any product of two consecutive integers, one of them is even. Hence the product is even.

   (b) Any odd integer n has the form $n = 2k + 1$, where $k \in \mathbb{Z}$. Hence $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. As seen above, $k(k + 1)$ will be even, so $4k(k + 1)$ is divisible by $4 \times 2 = 8$, so $n^2 \in [1]_8$.

F.3 Third 2000/2001 Problem Assignment

1. (a) Write down the addition and multiplication tables of the ring $\mathbb{Z}/8\mathbb{Z}$.

   (b) *Using your tables* — explain how you get your information — determine the units of the ring, and their inverses.

   (c) Determine, again from your tables, which elements of the ring are zero divisors, and explain how you infer this from the tables.

   Solution:

(a)

$+$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$
$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$
$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$
$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$
$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$
$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$
$[6]_8$	$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$
$[7]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$

$\cdot$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$
$[1]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$	$[0]_8$
$[2]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$
$[3]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$	$[0]_8$
$[4]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$
$[5]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$	$[0]_8$
$[6]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$
$[7]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$	$[0]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$

(b) The units are the elements with the property that, in the rows of the multiplication table labelled by them, there is an entry of $[1]_8$. The inverse of each is the label of the *column* in which the entry $[1]_8$ is located. Thus $[1]_8^{-1} = [1]_8$, $[3]_8^{-1} = [3]_8$, $[5]_8^{-1} = [5]_8$, and $[7]_8^{-1} = [7]_8$; that is, each of the units is its own inverse! This fact has been noted before in these notes.

(c) A zero divisor is a non-zero element for which at least one of the products of it with the non-zero elements of the ring is 0. We can determine these elements by looking for zeros in the multiplication table (outside of the row or column labelled $[0]_8$). Each of $[2]_8$, $[4]_8$, $[6]_8$ is thus a zero divisor. But $[0]_8$ is not called a zero divisor.

2. (cf. [4, Exercise 8B.E5, p. 125]) Showing all your work, find, if possible, inverses for $[146]_{365}$ and $[139]_{365}$. (Since the arithmetic is messy, you should verify your answer in any case where you believe you have found an inverse.)

   Solution: We shall proceed naïvely to apply the Euclidean algorithm to each of the pairs 146, 365 and 139, 365, and allow the mathematics to tell us whether there is an inverse.

$$365 = 146 \cdot 2 + 73$$

$$\begin{aligned}
146 &= 73 \cdot 2 + 0 \\
\Rightarrow \quad & (365, 146) = 73 \\
365 &= 139 \cdot 2 + 87 \\
139 &= 87 \cdot 1 + 52 \\
87 &= 52 \cdot 1 + 35 \\
52 &= 35 \cdot 1 + 17 \\
35 &= 17 \cdot 2 + 1 \\
17 &= 1 \cdot 17 + 0 \\
\Rightarrow \quad & (365, 139) = 1 \\
1 &= 35 \cdot 1 - 17 \cdot 2 = 35 \cdot 1 - (52 - 35 \cdot 1) \cdot 2 \\
&= 52 \cdot (-2) + 35 \cdot 3 = 52 \cdot (-2) + (87 - 52 \cdot 1) \cdot 3 \\
&= 87 \cdot 3 + 52 \cdot (-5) = 87 \cdot 3 + (139 - 87 \cdot 1) \cdot (-5) \\
&= 139 \cdot (-5) + 87 \cdot 8 = 139 \cdot (-5) + (365 - 139 \cdot 2) \cdot 8 \\
&= 365 \cdot 8 + 139 \cdot (-21) \\
\Rightarrow \quad & 139 \cdot (-21) \equiv 1 \pmod{365} \\
\Leftrightarrow \quad & [139]_{365} \cdot [-21]_{365} = [1]_{365}
\end{aligned}$$

Since 146 is not relatively prime to 365, there can exist no integer a with the property that, for some integer k,

$$146a + 365k = 1$$

that is, no integer a such that $[146]_{365} \cdot [a]_{365} = [1]_{365}$. Since 139 *is* relatively prime to 365, there does exist a multiplicative inverse $[139]_{365}^{-1}$, and we can find one such integer by applying the Euclidean algorithm (a constructive implementation of Bézout's theorem):

$$1 = 365 \cdot 8 + 139 \cdot (-21) \quad \Rightarrow \quad [139]_{365}^{-1} = [-21]_{365} = [344]_{365}\,.$$

To verify this last statement, we compute the product $139 \cdot (-21) = -2919$. Dividing 365 into -2919 yields $-2919 = 365 \cdot (-8) + 1$, so

$$139 \cdot (-21) \equiv 1 \pmod{365}\,.$$

3. In each of the following cases you have two choices. If the structure described is a ring, then you should determine each of the following:

- The zero[1043] element.
- The multiplicative identity (usually denoted by 1).
- The zero divisors. (This set may not be finite: you are asked to describe precisely which ring elements are zero divisors.)
- The units. (Here again a precise description of the units is requested.)
- The elements x that have the property that $x \cdot x = x$. (These are called the *idempotents*.)
- The elements x that have the property that some power of x is 0. (These are called the *nilpotent* elements.)

If the structure is not a ring, you are to prove that fact.

(a) The underlying set is $\mathbb{R}$; the operation of addition is defined to be subtraction; the operation of multiplication is the usual operation of multiplication in $\mathbb{R}$.

(b) The underlying set consists of the integers 0, 1, 2, ..., n. The operation of addition is addition modulo n; that is, $[a] + [b]$ is defined to be the smallest non-negative remainder when $a + b$ is divided by n. Multiplication is defined by $\forall a \forall b \, a \cdot b = 0$.

(c) The underlying set is the set of vectors in $\mathbb{R}^2$, written as (x_1, x_2). The product of two vectors is defined to be the usual dot product, i.e.

$$\forall x_1 \forall x_2 \forall y_1 \forall y_1 (x_1, x_2) \cdot (y_1, y_2) = x_1 y_1 + x_2 y_2 \, .$$

(d) The underlying set is the set of 2×2 matrices whose entries are either $[0]_2$ or $[1]_2$. The sum and product of two matrices are defined in the usual way, except that all additions and multiplications of matrix entries are carred out in the ring $\mathbb{Z}/\mathbb{Z}_2$.

Solution:

(a) Subtraction is not associative. We can prove this by exhibiting an explicit counterexample: e.g., $(1 - 1) - 1 = -1 \neq 1 = 1 - (1 - 1)$. The fact that the axiom that postulates associativity of + fails in just one case is sufficient to show that this structure is not a ring, since the postulate is quantified over the universe of all ordered triples of real numbers.

[1043]By the *zero* element we mean the element which satisfies axiom (iii) in the textbook [4, p. 119]. While we usually denote that element by the symbol commonly known as *zero*, we could use another symbol for it. It is even possible to use the symbol 0 for some other purpose. The element we are calling the *zero* element is also called the *additive identity*.

(b) For $n > 0$ this is not a ring in the sense of the textbook, since it does not have a multiplicative identity.[1044] How do we know there is no multiplicative identity? We need an element — let's call it temporarily x — with the property that its product with every element y is y. Since all products yield 0, we need only observe that $x \cdot 1$ is not equal to 1, no matter what element we use for x.

But, if $n = 0$, this is indeed a ring in the sense of the textbook. The additive and multiplicative identities are the same. There are no zero divisors. The only element in this ring, being a multiplicative identity, is a unit. It is both an idempotent and a nilpotent element.

(c) This problem is deceptive. What we have called a *product* is not a binary operation on the set, since it maps ordered pairs of set elements on to a point outside the set — namely, to a real number. Thus this is not a ring.

(d) This is indeed a ring. It has $2^4 = 16$ elements. The zero element is the usual zero matrix, with all four entries equal to 0, or rather to $[0]_2$. The multiplicative identity is the identity matrix, i.e. $\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}$.

In order to determine the idempotents and the nilpotents we could proceed in a systematic way that would generalize, for example, to larger square matrices over the same ring; we could use matrix concepts familiar to students who have taken a course in linear algebra[1045]. However, we will, instead begin simply by computing powers of the 16 elements, observing whether there is, ultimately, a power which is either the zero matrix or the identity matrix. The only idempotent matrix which can be nilpotent is the zero matrix, since all powers of any other idempotent matrix will equal itself and be non-zero.

i. The matrix $\begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [1]_2 \end{pmatrix}$ has the property that its square is the zero matrix, since $[1]_2 + [1]_2 = [0]_2$. This matrix is, therefore, nilpotent. As the square is not equal to the original matrix, it is not idempotent.

ii. **Matrices with 3 entries $[1]_2$.** The matrix $\begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [1]_2 \end{pmatrix}$ has the property that its cube is equal to the identity matrix. It cannot be nilpotent, since its determinant is non-zero; a nilpotent matrix will have a determinant which is zero or a zero-divisor — here there are no zero divisors. The matrix $\begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}$ has similar properties.

[1044] We sometimes call this a *trivial* ring, since this type of structure can be obtained from any "abelian group" (where there is an operation of addition satisfying the given axioms) by defining all products to be 0.

[1045] such as 189-223 or 189-236, either of which is a prerequisite to this course

The "triangular" matrix $\begin{pmatrix} [1]_2 & [0]_2 \\ [1]_2 & [1]_2 \end{pmatrix}$ has the property that its square is the identity matrix, not itself; thus the matrix is not idempotent, and it cannot be nilpotent for the reasons stated in the preceding case. The matrix $\begin{pmatrix} [1]_2 & [1]_2 \\ [0]_2 & [1]_2 \end{pmatrix}$ has the same property.

iii. **Matrices with 2 entries** $[1]_2$**.** Where the two non-zero entries are along the diagonal the matrix is the identity, which is idempotent but not nilpotent. Where the diagonal consists of $[0]_2$'s, the square of the matrix is the identity; this matrix is neither idempotent nor nilpotent. Where the two non-zero entries are in the same column or the same row, the matrix must be singular (non-invertible), so no power will equal the identity matrix. It can be seen that, in all 4 of the cases, the matrix is idempotent, and so it is not nilpotent.

iv. **Matrices with one** $[1]_2$**.** The two triangular matrices, viz. $\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [0]_2 \end{pmatrix}$ and $\begin{pmatrix} [0]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}$, are both idempotent (and so not nilpotent). The other two matrices can be seen to have their square equal to the zero matrix, so they are nilpotent, and so not idempotent.

v. The zero matrix is both idempotent and nilpotent.

The zero divisors will include the matrices

$$\begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [1]_2 \end{pmatrix}, \quad \begin{pmatrix} [0]_2 & [1]_2 \\ [0]_2 & [0]_2 \end{pmatrix}, \quad \begin{pmatrix} [0]_2 & [0]_2 \\ [1]_2 & [0]_2 \end{pmatrix},$$

the non-zero matrices whose square is the zero matrix; the matrices

$$\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [0]_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} [0]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}$$

are also zero divisors, since their product is the zero matrix. The four matrices having precisely two $[1]_2$'s appearing in the same row, or in the same column, are all zero divisors, by virtue of the following products

$$\begin{pmatrix} [0]_2 & [1]_2 \\ [0]_2 & [1]_2 \end{pmatrix}\begin{pmatrix} [1]_2 & [1]_2 \\ [0]_2 & [0]_2 \end{pmatrix} = \begin{pmatrix} [0]_2 & [0]_2 \\ [0]_2 & [0]_2 \end{pmatrix} = \begin{pmatrix} [1]_2 & [0]_2 \\ [1]_2 & [0]_2 \end{pmatrix}\begin{pmatrix} [0]_2 & [0]_2 \\ [1]_2 & [1]_2 \end{pmatrix}$$

As for the units, each of

$$\begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [1]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [0]_2 \\ [1]_2 & [1]_2 \end{pmatrix}$$

is its own inverse; while each of the following matrices is the inverse of the other:

$$\begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}, \begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [1]_2 \end{pmatrix}.$$

4. (cf. [4, Exercise 8C.E9, p. 133]) Let $\mathcal{R}$ be any ring, and let $M_2(\mathcal{R})$ denote the ring of 2×2 matrices whose entries come from $\mathcal{R}$. In $M_2(\mathcal{R})$ addition and multiplication are defined as usual for matrices; the zero matrix, identity matrix are defined in the usual way, in terms of the zero and identity element of the ring $\mathcal{R}$; the additive inverse of a matrix is also obtained in the usual way, by replacing each of its entries by its additive inverse. Consider each of the following functions from $\mathcal{R}$ to $M_2(\mathcal{R})$. Showing all your work, determine which of these functions define a homomorphism from $\mathcal{R}$ to $M_2(\mathcal{R})$.

$$\begin{aligned} f_1(r) &= \begin{pmatrix} 0 & r \\ r & 0 \end{pmatrix} \\ f_2(r) &= \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \\ f_3(r) &= \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \\ f_4(r) &= \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \\ f_5(r) &= \begin{pmatrix} 0 & 0 \\ 0 & r \end{pmatrix} \\ f_6(r) &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ f_7(r) &= \begin{pmatrix} -r & 0 \\ 0 & r \end{pmatrix} \end{aligned}$$

Solution: (In the cases where the function is not a homomorphism, there may be other legitimate proofs different from the ones presented.)

It will be helpful if we address immediately the question of whether $0 = 1$ in $\mathcal{R}$. A consequence of this equation is that, for any $r \in \mathcal{R}$, $0 = r \cdot 0 = r \cdot 1 = r$: thus the only ring[1046] in which this can happen is the "trivial" ring consisting of only the element 0. In that special case the ring $M_2\mathcal{R}$ also consists of only its zero element, and all of the mappings given are homomorphisms. In what follows we shall assume that $0 \neq 1$.

[1046] with multiplicative identity (unity)

(a) The image of the identity in $\mathcal{R}$ is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which is not the identity in $M_2(\mathcal{R})$. Hence condition [4, (iii), p. 127] fails, and f_1 is not a homomorphism.

(b)

$$\begin{aligned} f_2(r_1 + r_2) &= \begin{pmatrix} r_1 + r_2 & 0 \\ 0 & r_1 + r_2 \end{pmatrix} \quad \text{by definition of } f_2 \\ &= \begin{pmatrix} r_1 & 0 \\ 0 & r_1 \end{pmatrix} + \begin{pmatrix} r_2 & 0 \\ 0 & r_2 \end{pmatrix} \quad \text{matrix addition} \\ &= f_2(r_1) + f_2(r_2) \quad \text{proving [4, (i), p. 127]} \\ f_2(r_1 \cdot r_2) &= \begin{pmatrix} r_1 \cdot r_2 & 0 \\ 0 & r_1 \cdot r_2 \end{pmatrix} \quad \text{definition of } f_2 \\ &= \begin{pmatrix} r_1 & 0 \\ 0 & r_1 \end{pmatrix} \cdot \begin{pmatrix} r_2 & 0 \\ 0 & r_2 \end{pmatrix} \quad \text{matrix multiplication} \\ &= f_2(r_1) \cdot f_2(r_2) \quad \text{proving [4, (i), p. 127]} \\ f_2(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{definition of } f_2 \end{aligned}$$

and this is the identity element in $M_2(\mathcal{R})$, proving [4, (iii), p. 127]. These three conditions define a homomorphism; the other conditions shown on [4, pp. 127-128] are consequences.

(c) Here also the image of the identity is not the identity of $M_2(\mathcal{R})$, since the image has at least three 0's. Thus f_3 is not a homomorphism.

(d) $f_4(0)$ is not a zero matrix, contradicting [4, (iv), p. 128].

(e) The image of $1 \in \mathcal{R}$ is not the identity matrix. This contradicts [4, (iii), p. 127], so f_5 is not a homomorphism.

(f) Here also the identity element is not mapped on to the identity matrix; so f_6 is not a homomorphism.

(g) This case is delicate. The image of the identity element $1 \in \mathcal{R}$ is $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$; if, in the ring $\mathcal{R}$, -1 and 1 are different, then f_7 is not a homomorphism. However, if $1 = -1$, it appears possible that f_7 *is* a homomorphism. Indeed, since $r + r = (1 \cdot r) + (1 \cdot r) = (1 + 1) \cdot r = 0 \cdot r = 0$ — that is, $-r = r$ — it follows that

$$f_7(r) = \begin{pmatrix} -r & 0 \\ 0 & r \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} = f_2(r)$$

so f_7 is the same as f_2. A ring with the property that $1 = -1$ is said to have *characteristic 2*; you have seen an example in an earlier problem in this assignment. What we have shown here is that f_7 is a homomorphism iff $\mathcal{R}$ has characteristic 2.

F.4 Fourth 2000/2001 Problem Assignment

1. (a) [4, Exercise 8C.E5] Let $f : \mathcal{R} \to \mathcal{S}$ be a homomorphism, where we denote the operations, zero, unity element in both rings by the same symbols. Show carefully that, for any unit $a \in \mathcal{R}$, $f(a)$ is a unit in $\mathcal{S}$, and $f(a^{-1}) = (f(a))^{-1}$.

   (b) Does the preceding result imply that f maps the set of units in $\mathcal{R}$ *onto* the set of units of $\mathcal{S}$? Expain.

   (c) Let $\mathcal{R}$ be any given ring, and let a be any fixed unit of that ring. Consider the function $f : \mathcal{R} \to \mathcal{R}$ defined by $\forall r \; f(r) = a^{-1}ra$. Show that f is a homomorphism from $\mathcal{R}$ to itself which is a bijection.

   Solution:

   (a) Since $aa^{-1} = a^{-1}a$ for all $a \in \mathcal{R}$,

   $$f(a)f\left(a^{-1}\right) = f(1) = f\left(a^{-1}\right)f(a)\,.$$

   And, since $f(1) = 1$, this implies that $f\left(a^{-1}\right) = f(a)^{-1}$.

   (b) We have proved that the image of the set of units is contained in the set of units of the codomain ring, but it may not be a surjective mapping. Here is one counterexample: let $\mathcal{R}$ be the field $\mathbb{Q}$ of rationals, and let $\mathcal{S}$ be the field $\mathbb{R}$ of reals. Then [4, Example 2, p. 129] the inclusion mapping i is a homomorphism. But it is not surjective. For example, $\sqrt{2}$ is a unit in $\mathbb{R}$ which is not in the image of i.

   (c) i. First we prove that f is a homomorphism:

   $$\begin{aligned} f(a_1 + a_2) &= a^{-1}(a_1 + a_2)a \quad \text{definition of } f \\ &= a^{-1}a_1a + a^{-1}a_2a \quad \text{distributive laws} \\ &= f(a_1) + f(a_2); \\ f(a_1a_2) &= a^{-1}(a_1a_2)a \quad \text{definition of } f \\ &= a^{-1}a_1aa^{-1}a_2a \\ &= f(a_1)f(a_2); \\ f(1) &= a^{-1}1a \\ &= a^{-1}1a = 1 \end{aligned}$$

ii. To prove f is injective we could prove from first principles that $f(x) = f(y) \Rightarrow x = y$. We will, instead, appeal to [4, Proposition 1, p. 128], which states that a homomorphism is injective iff its kernel is $\{0\}$.

$$\begin{aligned} & f(r) = 0 \\ \Rightarrow\ & a^{-1}ra = 0 \quad \text{definition of } f \\ \Rightarrow\ & a\left(a^{-1}ra\right)a^{-1} = a0a^{-1} \quad \text{“premultiply” by } a\text{, “postmultiply” by } a^{-1} \\ \Rightarrow\ & r = 0 \end{aligned}$$

iii. Any element $r \in \mathcal{R}$ is the image of ara^{-1} under f, since $f\left(ara^{-1}\right) = a^{-1}\left(ara^{-1}\right)a = \left(a^{-1}a\right)r\left(a^{-1}a\right) = r$.

2. [4, Exercise 9C.E10, p. 141] Show that if 7 does not divide n, then 7 divides $n^{12} - 1$.

   Solution: If 7 does not divide n, then, by Fermat's theorem, (7 being a prime), 7 divides $n^{7-1} - 1$. It follows that 7 also divides the product $\left(n^{7-1} + 1\right)\left(n^{7-1} - 1\right)$, which is $n^{12} - 1$.

3. [4, Exercise 9C.E16, p. 141] Let $m = 2^{15} - 1 = 32767$.

   (a) Prove that the order of 2 modulo m is 15.

   (b) Prove that 15 does not divide $m - 1$.

   (c) Explain how the preceding results imply that m is not prime.

   Solution:

   (a) Since $2^{15} = 1 + m$, $2^{15} \equiv 1 \pmod{m}$, so, by [4, Proposition 9A.2, p. 137], the order of 2 modulo m is a positive divisor of 15. The positive divisors of 15 are 1, 3, 5, 15; none of $2^1 = 2$, $2^3 = 8$, $2^5 = 32$ differs from 1 by a multiple of m, so the order must be precisely 15.

   (b) $m - 1 = 32766$. This number is not a multiple of 5, since the decimal representation of such integers must end in a 0 or a 5 [4, Fact, p. 69]; so it cannot be divisible by 15.

   (c) Suppose that m were prime; being odd prime, it would be relatively prime to 2. Then Fermat's Theorem would imply that $2^{m-1} \equiv 1 \pmod{m}$, so the order of 2 modulo m would be a divisor of $m - 1$ by [4, Proposition 9A2, p. 137]. As this contradicts the fact proved above, we conclude that m is not prime.

4. [4, Exercise 9D.E13, p. 145] Prove that, for any n, 33 divides $n^{101} - n$.

Solution: There are a number of valid approaches to solve this problem; the following is only one possibility.

We will consider four different cases, according to the value of $(n, 33)$.

Case $(n, 33) = 1$**:** First we observe that $\phi(33) = (3-1)(11-1) = 20$. Euler's theorem (i.e. Euler's generalization of Fermat's "Little" Theorem) [4, p. 142] states that $n^{20} \equiv 1 \pmod{33}$ when $(33, n) = 1$. Multiplying 5 copies of this congruence yields $n^{100} \equiv 1 \pmod{33}$, which remains true when multiplied by the congruence $n \equiv n$: $n^{101} \equiv n \pmod{33}$.

Case $(n, 33) = 3$**:** Since $(n, 11)$ must then be 1 (rather than 11), Fermat's theorem gives $n^{10} \equiv 1 \pmod{11}$, which implies that $n^{100} \equiv 1 \pmod{11}$ if we multiply 10 copies of the congruence together; and then, multiplying by $n \equiv n \pmod{11}$, we obtain $n^{101} \equiv n \pmod{11}$. Since $3|n$, $n^{101} \equiv 0 \equiv n \pmod{3}$; the two congruences to relatively prime moduli are equivalent to a single congruence

$$n^{101} \equiv n \pmod{33}\,.$$

Case $(n, 33) = 11$**:** Here Fermat's theorem for modulus 3 gives $n^2 \equiv 1 \pmod{3}$, which implies that $n^{100} \equiv 1 \pmod{3}$ and hence $n^{101} \equiv n \pmod{3}$. This time $n^{101} \equiv 0 \equiv n \pmod{11}$, so again the two congruences imply the desired result.

Case $(n, 33) = 33$**:** Here both n^{101} and n are divisible by 33, so they are both congruent to 0, and hence to each other modulo 33.

Another approach follows from [4, Exercise 9B.E7], which states that every residue class $[a]_p$ has its pth power equal to $[a]_p$. One way to prove this is to follow the hint [4, p. 489]. Another is to prove it by induction for $a = 0, 1, ..., p-1$, using the binomial theorem, where the induction step is based on the statement $(a+1)^p \equiv a^p + 1 \pmod{p}$.

5. [Students who have been reading the textbook and attending lectures should not require any additional materials to solve this problem, provided they remember what was in 189-240A. Students who would like some additional help could look at pages 343–352 in the Appendix to these notes.] Consider the group S_5 of bijections of the set $\{1, 2, 3, 4, 5\}$ with itself.

   (a) Determine the number of elements in this group.

   (b) Remember that it is possible to express each of the elements of this group as a product of "cycles" of the forms (**.**), (**..**), (**...**), (**....**), (**.....**) where the sets of symbols appearing as **.** in the various factor cycles are disjoint. Use

this fact to determine the different possible "order[1047]s" that the elements of this group may have. (Remember that there may be more than one way to represent the same element in this "disjoint cycle" notation.)

(c) Determine the number of elements of S_5 that have "order" 5.

(d) Determine the number of subgroups of S_5 that have "order"[1048] 5.

(e) Determine the subgroups of S_5 that have order 2.

(f) Determine the number of left cosets in S_5 of the subgroup S_4 which consists of all bijections of $\{2, 3, 4, 5\}$.

(g) Determine, in S_5, the members of the particular left coset of the subgroup S_3 consisting of all permutations of the points 3, 4, 5; which coset is to contain the element (12), i.e. the mapping $(1, 2, 3, 4, 5) \longrightarrow (2, 1, 3, 4, 5)$.

(h) Determine the number of elements of S_5 that have order 6.

Solution:

(a) This is the group of all permutations of the form $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$, where a, b, c, d, e are the elements of $\{1, 2, 3, 4, 5\}$ in some order. We know that the number of such orderings is $5! = 120$.

(b) We have to consider the various possible partitions of 5 into a sum of positive integers. In each case we will determine the order of the corresponding elements.

$5 = 5$: Elements of the form (•••••) have order 5.

$5 = 4 + 1$: Elements of the form (••••)(•) have order 4.

$5 = 3 + 2$: Elements of the form (•••)(••) have order 6.

$5 = 3 + 1 + 1$: Elements of the form (•••)(•)(•) have order 3.

$5 = 2 + 2 + 1$: Elements of the form (••)(••)(•) have order 2.

$5 = 2 + 1 + 1 + 1$: Elements of the form (••)(•)(•)(•) have order 2.

$5 = 1 + 1 + 1 + 1 + 1$: There is only one elements of the form (•)(•)(•)(•)(•); it is the identity, and it has order 1.

Thus the elements of this group can have orders 1, 2, 3, 4, 5, 6. Note that, among these orders, we do not find all the divisors of 5!.

(c) The elements which have order 5 are all the "5-cycles". (There are exactly 4! of these elements, since they correspond to the circular arrangements of 5 distinct objects.)

[1047]order of g = smallest positive integer n such that $g^n = e$

[1048]order of a subgroup = its cardinality

(d) If a subgroup has order 5, all of its elements must have orders that divide 5. Thus, except for the identity, each of its elements generates the subgroup, which is, therefore, cyclic. These subgroups cannot overlap, since each of the non-identity elements generates the subgroup. As observed above, there are 4!=24 5-cycles. Thus these 24 cycles are contained in $\frac{24}{5-1} = \frac{24}{4} = 6$ subgroups of order 5.

(e) The subgroups of order 2 each consist of the identity together with an element of order 2. The elements of order 2 have to be products of cycles of orders 2 and 1, hence they are of either of the forms (••)(••)(•), (••)(•)(•)(•).

(••)(••)(•): We have to count the number of ways of partitioning the set $\{1, 2, 3, 4, 5\}$ into two sets of cardinality 2 and one of cardinality 1. The element which constitutes the 1-cycle may be selected in $\binom{5}{1} = 5$ ways. After that the remaining 4 elements may be split into two *unlabelled* sets of 2 in exactly $\frac{1}{2}\binom{4}{2} = 3$ ways; in all there are $5 \times 3 = 15$ elements of this type, so there are 15 subgroups of this type having order 2.

(••)(•)(•)(•): In this case we count the number of ways of selecting the elements of the 2-cycle: $\binom{5}{2} = 10$ ways. There are 10 subgroups of this type of order 2.

So the total number of subgroups of order 2 is $15 + 10 = 25$.

(f) The subgroup has $4! = 24$ elements; the cosets are disjoint, so the total number of cosets (called the *index* of the subgroup in S_5) is $5!/4! = 5$.

(g) The coset consists of the elements of the form $(12)g$, where g is any element of the symmetric group of the set $\{3, 4, 5\}$. The subgroup consists of (3)(4)(5), (34), (35), (45), (345), (354), so the coset consists of the elements (12)(3)(4)(5), (12)(34), (12)(35), (12)(45), (12)(345), (12)(354).

(h) Elements of order 6 are — as seen above — products of a 2-cycle and a 3-cycle; i.e. they have the form (•••)(••). We can select the elements of the 2-cycle in $\binom{5}{2} = 10$ ways. Then the remaining 3 points will constitute the 3-cycle. The number of cyclical arrangements of 2 objects is $(2-1)! = 1$, while the number of cyclical arrangements of 3 objects is $(3-1) = 2! = 2$. So the total number of elements of order 6 is $10 \times 1 \times 2 = 20$.

G Some class tests from previous years, with solutions

G.1 1991 Class Test

1. [20 MARKS] Use the Chinese Remainder Theorem (no other method will be accepted) to determine 3 consecutive integers between 1 and 1000, none of which is square free.

   Solution: This is a special case of Exercise A.1.9.12.2, for which a solution is contained in these notes. We can solve a system of congruences to relatively prime moduli which are each not square free:

   $$\begin{aligned} x &\equiv 0 \pmod 4 \\ x &\equiv -1 \pmod 9 \\ x &\equiv -2 \pmod{25} \end{aligned}$$

   $M = 900$. $M_1 = 225 \equiv 1 \pmod 4$; an inverse is 1; (actually, this inverse is not required). $M_2 = 100 \equiv 1 \pmod 9$; an inverse is 1. $M_3 = 36 \equiv 11 \pmod{25}$; an inverse may be found by the Euclidean algorithm or otherwise to be 16. The general solution to the system of congruences is then the coset containing

   $$0 \cdot 1 \cdot 225 - 1 \cdot 1 \cdot 100 - 2 \cdot 36 \cdot 16$$

   modulo $4 \cdot 9 \cdot 25$, i.e. $-1252 \pmod{900}$. The member of this coset between 1 and 1000 is $-1252 + 2 \cdot 900 = 548$. Thus one solution to the problem is the consecutive integers 548, 549, 550, which are respectively divisible by 2^2, 3^2, 5^2. There are other, smaller, solutions: for example, $\{48, 49, 50\}$, $\{98, 99, 100\}$.

2. [10 MARKS] Let $\mathcal{G}$ be a permutation group operating on a set $\mathfrak{A}$. Prove carefully that $\mathcal{G}$-equivalence is an equivalence relation on $\mathfrak{A}$.

   Solution: (cf. Theorem A.3.3.9)

   reflexivity: Let $x \in \mathfrak{A}$. By hypothesis, and permutation group acting on $\mathfrak{A}$ contains the *identity* permutation I, which acts by mapping x on to x. Thus x is $\mathcal{G}$-equivalent to itself.

   symmetry: Let $x, y \in \mathfrak{A}$, and suppose that x is $\mathfrak{G}$-equivalent to y, i.e. that $\exists f \in \mathcal{G}$ such that $f(x) = y$. But f is a permutation, hence it is invertible. And, since $\mathcal{G}$ is a permutation group, it is closed under the operation of taking the inverse: i.e. $f \in \mathcal{G} \Rightarrow f^{-1} \in \mathcal{G}$. Thus there is a permutation in $\mathcal{G}$ which maps y on to x: $f^{-1}(y) = x$, so y is $\mathcal{G}$-equivalent to x.

transitivity: Suppose that x is $\mathcal{G}$-equivalent to y, and y is $\mathcal{G}$-equivalent to z. Then there exist permutations $f, g \in \mathcal{G}$ such that $f(x) = y$, $g(y) = z$. But then $(g \circ f)(x) = g(f(x)) = g(y) = z$; and, since $\mathcal{G}$ is closed under composition, $g \circ f \in \mathcal{G}$. It follows that x is $\mathcal{G}$-equivalent to z.

3. Consider the pentagonal prism graph: its vertex set is

$$\mathfrak{V} = \{a, b, c, d, e, A, B, C, D, E\}$$

and its edge set is

$$\{ab, bc, cd, de, ea, AB, BC, CD, DE, EA, aA, bB, cC, dD, eE\}$$

Among the symmetries of this graph are:

$$\text{the rotation } \alpha = (abcde)(ABCDE)$$

$$\text{the reflection } \beta = (a)(be)(cd)(A)(BE)(CD)$$

(a) [5 MARKS] Show that any permutation group acting on $\mathfrak{V}$, containing α and β, contains 4 other reflections with the same cycle type as β.

Solution:

$$\begin{aligned}
\alpha\beta\alpha^{-1} &= (b)(ca)(de)(B)(CA)(DE) \\
\alpha^2\beta\alpha^{-2} &= (c)(db)(ea)(C)(DB)(EA) \\
\alpha^3\beta\alpha^{-3} &= (d)(ec)(ab)(D)(EC)(AB) \\
\alpha^4\beta\alpha^{-4} &= (e)(ad)(bc)(E)(AD)(BC)
\end{aligned}$$

(b) [10 MARKS] Determine the smallest permutation group, $\mathcal{G}$, that contains α and β, and find its cycle index.

Solution: There certainly is a group containing α and β; for example the symmetric group on the set $\mathfrak{V}$. One group that contains these elements "resembles" the dihedral group on the set $\{a, b, c, d, e\}$. We have shown above how to express reflections in terms of these permutations; and, of course, the rotations can be expressed as powers of α. This group has 10 elements. There can be no smaller group, since each of the elements of this group is expressible as a product of α's and β's, and a group must be closed under composition. (Observe that $\alpha^5 = I$, i.e. that $\alpha^{-1} = \alpha^4$; and that $\beta = \beta^{-1}$.)

The cycle index is $\frac{1}{10}\left(x_1^{10} + 4x_5^2 + 5x_1^2x_2^4\right)$.

(c) [5 MARKS] Determine the orbits of this group.
Solution: Powers of α map each of the elements of $\{a, b, c, d, e\}$ on to the others; i.e. the group is *transitive* on this subset, i.e. these elements are together contained in an orbit. Similarly, the subset $\{A, B, C, D, E\}$ is contained in an orbit. And evidently there is no permutation that maps any of the elements of $\{a, b, c, d, e\}$ on to any of the elements of $\{A, B, C, D, E\}$. Thus the orbits containing these two subsets are disjoint; hence these two subsets are the orbits.

4. (a) [5 MARKS] List the Cayley tables of all semigroups having up to 2 elements (up to isomorphisms).
Solution: This is Exercise A.4.2.11. Students were not expected to supply proofs, simply to list the tables.

(b) [5 MARKS] Indicate which of these is a monoid.
Solution: This is Exercise A.4.3.9. (There is one monoid with 1 element, and there are 2 with 2 elements.)

(c) [10 MARKS] Prove carefully that one of the 2-element semigroups you have listed in part 4a is not a monoid.
Solution: The proof will depend on which semigroup the student selects. We must prove that no element acts as a two-sided identity. For example, in the case of the trivial semigroup, having Cayley table

$*$	a	b
a	a	a
b	a	a

, no column contains both elements, so neither of the elements can serve as a right identity. In the cases of left and right absorption, there will be one-sided identities, but no two-sided identity.

G.2 1997 Class Test

Each of the four versions of the test had four problems, chosen from the following.

1. [5 MARKS] Let $\mathbb{N}$ denote the positive integers. Determine whether the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(m, n) = m + 2n$ is an associative binary operation.
Solution: This function is not associative. For example,

$$\begin{aligned} f(f(1,2),1) &= f(1+2\cdot 2,1) = 5+2 = 7, \quad \text{but} \\ f(1,f(2,1)) &= f(1,2+2\cdot 1) = 1+8 = 9 \end{aligned}$$

For associativity

$$f(f(\ell, m), n) = f(\ell, f(m, n)) \qquad \forall \ell, m, n \in \mathbb{N}\,. \tag{1162}$$

[It is not sufficient to argue that (1162) is equivalent to

$$\ell + 2m + 2n = \ell + 2m + 4n \tag{1163}$$

or, equivalently, to

$$2n = 0\,. \tag{1164}$$

One must demonstrate that this last, equivalent, equation leads to a contradiction. For example, if the underlying set were $\mathbb{Z}_2$, then (1164) would not entail any contradictions. In the present case, however, any $n \neq 0$ will give a contradiction.]

2. [10 MARKS] Showing all your work, determine the decomposition of $S_3 \times \mathbb{Z}_2$ into right cosets of $H = \langle((1\ 3), [1]_2)\rangle$.

   Solution: (cf. [8, Problem 16.17]) We are to consider right cosets of the subgroup $H = \langle((1\ 3), [1])\rangle = \{((1\ 3), [1]), (e, [0])\}$, which has order 2. There will be $\frac{|S_3|\times|\mathbb{Z}_2|}{|H|} = \frac{6\times 2}{2} = 6$ right cosets. In describing the elements one must remember that, in the usual notation for $\mathbb{Z}_2$, the group operation is written additively, and $[1]_2 + [1]_2 = [0]_2$.

$$\begin{aligned}
H &= \langle((1\ 3), [1])\rangle = \{((1\ 3), [1]), (e, [0])\} \\
H((1\ 3), [0]) &= \{((1\ 3), [1])((1\ 3), [0]), (e, [0])((1\ 3), [0])\} = \{(e, [1]), ((1\ 3), [0])\} \\
H((1\ 2), [0]) &= \{((1\ 3), [1])((1\ 2), [0]), (e, [0])((1\ 2), [0])\} \\
&= \{((1\ 3)(1\ 2), [1]), ((1\ 2), [0])\} = \{((1\ 2\ 3), [1]), ((1\ 2), [0])\} \\
H((2\ 3), [0]) &= \{((1\ 3), [1])((2\ 3), [0]), (e, [0])((2\ 3), [0])\} \\
&= \{((1\ 3)(2\ 3), [1]), ((2\ 3), [0])\} = \{((1\ 3\ 2), [1]), ((2\ 3), [0])\} \\
H((1\ 2), [1]) &= \{((1\ 3), [1])((1\ 2), [1]), (e, [0])((1\ 2), [1])\} \\
&= \{((1\ 3)(1\ 2), [0]), ((1\ 2), [1])\} = \{((1\ 2\ 3), [0]), ((1\ 2), [1])\} \\
H((2\ 3), [1]) &= \{((1\ 3), [1])((2\ 3), [1]), (e, [0])((2\ 3), [1])\} \\
&= \{((1\ 3)(2\ 3), [0]), ((2\ 3), [1])\} = \{((1\ 3\ 2), [0]), ((2\ 3), [1])\}
\end{aligned}$$

3. [5 MARKS] Describe two non-isomorphic groups of order 8, and prove they are non-isomorphic.

   Solution: There are, in fact, 5 isomorphism types of groups of order 8. For example, $\mathbb{Z}_8$ is cyclic of order 8: it has elements (in fact, each of [1], [3], [5], [7]) of order 8. But the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 elements of order 2, and the identity, of order 1 — but no elements of order 8. Since order of elements must be preserved under isomorphism, these two groups are not isomorphic.

   Alternatively, one might take the symmetry group of the square with vertices labelled in sequence 1, 2, 3, 4; and compare it with one of the abelian groups of

order 8 (of which 2 were considered above). One need only show that the symmetry group is not abelian; this could be done, for example, by computing the two products of symmetries $(12)(34) \cdot (24) = (1234)$, $(24) \cdot (12)(34) = (1432)$.

4. (a) [7 MARKS] For the integral domain $E = \mathbb{Z}_3$, and $E' = E - \{0\}$, show how to construct the quotient field of equivalence classes of elements of $E \times E'$. Do not prove the validity of the steps carried out, but give the following information:
   i. definition of the elements of the field
   ii. definition of addition
   iii. definition of multiplication
   iv. the zero element (additive identity)
   v. the unity (multiplicative identity)
   vi. the additive inverse of any element
   vii. the multiplicative inverse of any non-zero element.

   (b) [3 MARKS] List all the elements of this quotient field without repetitions.

Solution:

(a) i. On the set $E \times E'$ of 6 ordered pairs from $\mathbb{Z}_3$ with second argument equal to [1] or to [2], we define a binary relation $\sim$ by $(a, b) \sim (c, d) \Leftrightarrow ad = bc$; this relation can be shown to be an equivalence relation. The equivalence classes of this relation form the elements of the quotient field; $[(a, b)]$ is abbreviated to $[a, b]$.
The algebraic operations on this set of equivalence classes are defined by

ii.
$$[a, b] + [c, d] = [ad + bc, bd]$$

iii.
$$[a, b] \cdot [c, d] = [ac, bd]$$

iv. The zero (additive identity) of the ring is $[0, b]$.

v. The unity is $[b, b]$.

vi. The additive inverse of $[a, b]$ is $[-a, b]$.

vii. When $[a, b]$ is not the additive identity (i.e., when $a \neq 0$) the multiplicative inverse is $[b, a]$.

(b) For convenience we shall use an abbreviated notation now — suppressing the brackets by writing $[n]_3$ simply as n. The elements of $E \times E'$ are $(0, 1)$, $(0, 2)$, $(1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 2)$. However,

$$0 \cdot 2 = 1 \cdot 0 \quad \Rightarrow \quad [0, 1] = [0, 2]$$

$$\begin{aligned} 1 \cdot 2 = 1 \cdot 2 &\Rightarrow [1,1] = [2,2] \\ 2 \cdot 2 = 1 \cdot 1 &\Rightarrow [2,1] = [1,2] \end{aligned}$$

so the elements of the quotient field are the 3 equivalence classes

$$\begin{aligned} [0,1] = [0,2] &= \{(0,1),(0,2)\} \quad \text{the zero element} \\ [1,1] = [2,2] &= \{(1,1),(2,2)\} \quad \text{the unity} \\ [2,1] = [1,2] &= \{(2,1),(1,2)\} \end{aligned}$$

(In fact, the copy of $\mathbb{Z}_3$ embedded in this field of quotients by the mapping $x \mapsto [x,1]$ is the whole of the field of quotients; i.e., the field of quotients is nothing more than (the embedded copy of) $\mathbb{Z}_3$.)

5. [5 MARKS] Showing all your work, determine whether the set $Y = \{(0,y)|y \in \mathbb{R}\}$ is a subfield of the field of complex numbers.

   Solution: This is not even a sub*ring* since it is not closed under multiplication: for example, $(0,1)(0,1) = (-1,0) \notin Y$.

6. [10 MARKS] For any $n \in \mathbb{N}$, A_n is the alternating group — the subgroup of S_n consisting of all even permutations. Showing all your work, determine the decomposition of $S_2 \times S_3$ into left cosets of $K = A_2 \times A_3$.

   Solution: The only even permutation in S_2 is the identity; i.e. $A_2 = \{e\}$; $A_3 = \{e,(123),(132)\}$. We are to consider left cosets of the subgroup $K = A_2 \times A_3$ whose elements are (e,e), $(e,(123))$, $(e,(132))$. There will be $\frac{|S_2|\times|S_3|}{|K|} = \frac{2\times(3!)}{3} = 4$ left cosets.

$$\begin{aligned} K &= A_2 \times A_3 = \{(e,e),(e,(123)),(e,(132))\} \\ (e,(12))K &= \{(e,(12))(e,e),(e,(12))(e,(123)),(e,(12))(e,(132))\} \\ &= \{(e,(12)),(e,(12)(123)),(e,(12)(132))\} \\ &= \{(e,(12)),(e,(23)),(e,(13))\} \\ ((12),e)K &= \{((12),e)(e,e),((12),e)(e,(123)),((12),e)(e,(132))\} \\ &= \{((12),e),((12),(123)),((12),(132))\} \\ ((12),(12))K &= \{((12),(12))(e,e),((12),(12))(e,(123)),((12),(12))(e,(132))\} \\ &= \{((12),(12)),((12),(12)(123)),((12),(12)(132))\} \\ &= \{((12),(12)),((12),(23)),((12),(13))\} \end{aligned}$$

7. [5 MARKS] Describe two non-isomorphic groups of order 9, and prove they are non-isomorphic.

Solution: There are, in fact, exactly 2 isomorphism types of groups of order 9. Students are not expected to know that[1049] at this stage, but you are expected to know that there are exactly 2 isomorphism types of *Abelian* groups of order 3^2: $\mathbb{Z}_3 \times \mathbb{Z}_3$, and $\mathbb{Z}_9$. The second of these, being cyclic, has elements of order 9: in fact, all elements except [0], [3], and [6] generate this group. Except for the identity, $(0, 0)$, which has order 1, the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ all have order 3. As the order of an element is preserved under an isomorphism, these two groups are not isomorphic.

8. (a) [7 MARKS] For the integral domain $L = \mathbb{Z}_2$, and $L' = L - \{0\}$, show how to construct the quotient field of equivalence classes of elements of $L \times L'$. Do not prove the validity of the steps carried out, but give the following information:
   i. definition of the elements of the field
   ii. definition of addition
   iii. definition of multiplication
   iv. the zero element (additive identity)
   v. the unity (multiplicative identity)
   vi. the additive inverse of any element
   vii. the multiplicative inverse of any non-zero element.

   (b) [3 MARKS] Showing all your work, determine the characteristic of this field.

Solution:

(a) i. On the set $L \times L'$ of 4 ordered pairs from $\mathbb{Z}_2$ with second argument equal to [1] only, we define a binary relation $\sim$ by $(a, b) \sim (c, d) \Leftrightarrow ad = bc$; this relation can be shown to be an equivalence relation. The equivalence classes of this relation form the elements of the quotient field; $[(a, b)]$ is abbreviated to $[a, b]$.
The algebraic operations on this set of equivalence classes are defined by

ii.
$$[a, b] + [c, d] = [ad + bc, bd]$$

iii.
$$[a, b] \cdot [c, d] = [ac, bd]$$

iv. The zero (additive identity) of the ring is $[0, 1]$.

v. The unity is $[1, 1]$.

vi. The additive inverse of $[a, b]$ is $[-a, b]$.

[1049]This can be proved as a consequence of a theorem of Cauchy, which states that any group whose order is a power of a prime p must contain an element of order p.

vii. When $[a, b]$ is not the additive identity (i.e., when $a \neq 0$; i.e., when $a = 1$) the multiplicative inverse is $[b, a]$.

(b) For convenience we shall use an abbreviated notation now — suppressing the brackets by writing $[n]_2$ simply as n. The elements of $L \times L'$ are $(0, 1)$, $(1, 1)$, so the elements of the quotient field are the 2 equivalence classes

$$\begin{aligned} [0, 1] &= \{(0, 1)\} \quad \text{the zero element} \\ [1, 1] &= \{(1, 1)\} \quad \text{the unity} \end{aligned}$$

(In fact, the copy of $\mathbb{Z}_2$ embedded in this field of quotients by the mapping $x \mapsto [x, 1]$ is the whole of the field of quotients; i.e., the field of quotients is nothing more than (the embedded copy of) $\mathbb{Z}_2$.) Since $[1, 1] + [1, 1] = [1 \cdot 1 + 1 \cdot 1, 1 \cdot 1] = [2, 1] = [0, 1]$, the zero element, and $[0, 1] + [0, 1] = [0, 1]$, the characteristic of this field — the smallest positive number of copies that will always yield a sum of zero — is 2.

9. [5 MARKS] Prove or disprove: For any positive integer n and any group G, the set of elements of G whose order divides n forms a subgroup of G.

Solution: False. Take $n = 2$, and consider the subset of S_3 consisting of the identity (whose order is 1, which divides 2) and the transpositions, $\binom{3}{2} = 3$ in number, whose order is exactly 2. This set is closed under the taking of inverses — indeed, every element is its own inverse. However, the set is not closed under composition: for example, $(12)(23) = (123)$, whose order is not divisible by 2.

When G is Abelian, the statement is *true*. This is why we have constructed our counterexample using the smallest non-Abelian group.

G.3 1998 Class Tests

G.3.1 Version 1

1. (a) [5 MARKS] Prove or disprove: the ring $\mathbb{Z}_2 \times \mathbb{Z}_3$, with multiplication defined by

$$([a]_2, [b]_3)([c]_2, [d]_3) = ([a]_2 \odot [c]_2, [b]_3 \odot [d]_3)\,,$$

has no zero divisors.

(b) [5 MARKS] Determine the value of the product $(123456)^2(136)(24)(5)(123456)^{-2}$ in S_6.

Solution:

(a) Two zero divisors are $([1], [0])$ and $([0], [1])$, since they are non-zero elements whose product is $([0], [0])$.

(b)

$$\begin{aligned}(123456)^2(136)(24)(5)(123456)^{-2} &= (135)(246)(136)(24)(5)(153)(264)\\ &= (1)(235)(46)\end{aligned}$$

2. (a) [3 MARKS] Prove or disprove:

$$(\forall n \in \mathbb{N} - \{0\})\ (\forall a \in \mathbb{Z})\ (\forall b \in \mathbb{Z})[(a^2 \equiv b^2 \pmod{n}) \Rightarrow (a \equiv b \pmod{n})]$$

(b) [7 MARKS] Showing all your work, determine integers a and b such that $596a + 394b = (596, 394)$.

Solution:

(a) This implication is false. For a counterexample take $n > 2$ and $a = -b = 1$.

(b) By the Euclidean algorithm,

$$\begin{aligned}596 &= 1 \cdot 394 + 202\\ 394 &= 1 \cdot 202 + 192\\ 202 &= 1 \cdot 192 + 10\\ 192 &= 19 \cdot 10 + 2\\ 10 &= 5 \cdot 2 + 0 \Rightarrow (596, 394) = 2\\ 2 &= 192 - 19 \cdot 10 = 192 - 19(202 - 1 \cdot 192)\\ &= -19 \cdot 202 + 20 \cdot 192 = -19 \cdot 202 + 20(394 - 1 \cdot 202)\\ &= 20 \cdot 394 - 39 \cdot 202 = 20 \cdot 394 - 39(596 - 1 \cdot 394)\\ &= -39 \cdot 596 + 59 \cdot 394\end{aligned}$$

3. (a) [3 MARKS] Define precisely what is meant by the statement $\theta = \psi$, where $\theta : A \to B$ and $\psi : C \to D$ are two mappings.

(b) [7 MARKS] Prove that, for any mappings $\alpha : S \to T$, $\beta : T \to U$, $\gamma : T \to U$, if α is surjective, and $\beta \circ \alpha = \gamma \circ \alpha$, then $\beta = \gamma$.

Solution:

(a) (cf. [8, p. 16]) The statement $\theta = \psi$ is equivalent to the following three facts:

- The domains are equal, i.e. $A = C$.
- The codomains are equal, i.e. $B = D$.
- The actions of the functions coincide on all points of their common domain, i.e. $\forall x \in A[\theta(x) = \psi(x)]$.

(b) (cf. [8, Problem 2.23]) As β and γ have the same domain and also the same codomain, all that remains to prove is that they have the same action.

Let t be any element of T. Since α is surjective, there exists $s \in S$ such that $\alpha(s) = t$. But then

$$\begin{aligned} \beta(t) &= \beta(\alpha(s)) \\ &= (\beta \circ \alpha)(t) \quad \text{by definition of } \circ \\ &= (\gamma \circ \alpha)(t) \quad \text{by hypothesis} \\ &= \gamma(\alpha(t)) \quad \text{by definition of } \circ \\ &= \gamma(t) \end{aligned}$$

We have proved that β and γ have the same action on their common domain, so they must be the same function.

4. [10 MARKS] Let G be any group with operation $*$ and identity e, and define, for some fixed element $g_0 \in G$, $H = \{g \in G | g_0^{-1} * g * g_0 = g\}$. Determine whether or not H is a subgroup of G.

Solution: (cf. [8, Problem 7.23]) This subset is, indeed, a subgroup, as the criteria of [8, Theorem 7.1] are satisfied.

non-empty. $g_0^{-1} * e * g_0 = e \Rightarrow e \in H$, so $H \neq \varnothing$.

closed under group operation. Suppose that $g_1, g_2 \in H$, i.e. $g_0^{-1} * g_1 * g_0 = g_1$, $g_0^{-1} * g_2 * g_0 = g_2$. Then $g_1 * g_2 = (g_0^{-1} * g_1 * g_0)(g_0^{-1} * g_2 * g_0) = g_0^{-1} * g_1 * (g_0 g_0^{-1}) * g_2 * g_0 = g_0^{-1} * g_1 * e * g_2 * g_0 = g_0^{-1} * (g_1 * g_2) * g_0$; so $g_1 * g_2 \in H$.

closed under taking inverses. The inverse of $g_0^{-1} * g * g_0$ is $g_0^{-1} * g^{-1} * \big((g_0)^{-1}\big)^{-1} = g_0^{-1} * g^{-1} * g_0$. Hence, $g \in H \Rightarrow g_0^{-1} * g * g_0 = g \Rightarrow g_0^{-1} * g^{-1} * g_0 = g^{-1} \Rightarrow g^{-1} \in H$.

H is called the *centralizer* of g_0 in G.

5. (a) [6 MARKS] Showing all your work, determine the order of each of the elements of the group A with the following Cayley table. (You must justify every step

of your argument.)

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_1	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_2	a_2	a_3	a_4	a_1	a_6	a_7	a_8	a_5
a_3	a_3	a_4	a_1	a_2	a_7	a_8	a_5	a_6
a_4	a_4	a_1	a_2	a_3	a_8	a_5	a_6	a_7
a_5	a_5	a_8	a_7	a_6	a_3	a_2	a_1	a_4
a_6	a_6	a_5	a_8	a_7	a_4	a_3	a_2	a_1
a_7	a_7	a_6	a_5	a_8	a_1	a_4	a_3	a_2
a_8	a_8	a_7	a_6	a_5	a_2	a_1	a_4	a_3

(b) [4 MARKS] Showing all your work, determine the left coset decomposition of A with respect to the subgroup $\langle a_5 \rangle$.

Solution:

(a) We observe that $a_i a_1 = a_i$ for all i (although only one of these 8 statements is needed); from this we conclude — by multiplying on the left by a_i^{-1} — that $a_1 = e$. This shows also that the order of a_1 is 1.

Now, in addition to a_1 itself, one other element has 2nd power equal to e; that is a_3; hence a_3 has order 2. (Since $a_3 \neq a_1$, 2 is the minimum power m for which $a_3^m = e$, i.e. 2 is the order of a_3.)

Scanning the main diagonal of the Cayley table, we see no other enties of e, so no other elements have order 1 or 2. However, we see that all other entries are a_3; that implies that the remaining 6 elements are such that their 1st and 2nd powers are not equal to e, but the 4th power is equal to e. We know that the 3rd power cannot be e either by computing these 3rd powers directly from the table, or from the fact that the order would then have to divide 3 (by [8, Theorem 14.3(b)]), which would imply that it was equal to 3; but then, by [8, Corollary to Lagrange's Theorem], 3|8, which is absurd.

(b) We have seen above that a_5 has order 4. This means that there will be $8/4 = 2$ cosets of $\langle a_5 \rangle$ in A. One of these will be $\langle a_5 \rangle$, whose elements are

$$\begin{aligned} a_5^1 &= a_5 \\ a_5^2 &= a_3 \quad \text{from the table} \\ a_5^3 &= a_5^2 a_5 = a_3 a_5 = a_7 \quad \text{from the table} \\ a_5^4 &= a_3^2 = a_1 \end{aligned}$$

The other coset must be disjoint from the preceding, so its elements can only be $\{a_2, a_4, a_6, a_8\}$. Thus the coset decomposition is

$$A = \{a_1, a_3, a_5, a_7\} \cup \{a_2, a_4, a_6, a_8\}\,.$$

When a coset has index 2 its left and right coset decompositions are the same!

G.3.2 Version 2

1. (a) [5 MARKS] Prove or disprove: the ring $\mathbb{Z}_3 \times \mathbb{Z}_5$, with multiplication defined by
$$([k]_3, [\ell]_5)([m]_3, [n]_5) = ([k]_3 \odot [m]_3, [\ell]_5 \odot [n]_5)\,,$$
has zero divisors.

   (b) [5 MARKS] Determine the value of the product $(123456)^{-2}(1436)(25)(123456)^2$ in S_6.

Solution:

(a) Two zero divisors are $([1], [0])$ and $([0], [1])$, since they are non-zero elements whose product is $([0], [0])$.

(b) $(123456)^{-2}(1436)(25)(123456)^2 = (153)(264)(1436)(25)(135)(246) = (1452)(36)$

2. (a) [3 MARKS] Prove or disprove:

$$(\forall n \in \mathbb{N} - \{0\})\ (\forall a \in \mathbb{Z})\ (\forall b \in \mathbb{Z})[(a^2 \equiv b^2 \pmod{n}) \Rightarrow (a \equiv b \pmod{n})]$$

   (b) [7 MARKS] Showing all your work, determine integers ℓ and m such that $165\ell + 861m = (165, 861)$.

Solution:

(a) This implication is false. For a counterexample take $n > 2$ and $a = -b = 1$.

(b) By the Euclidean algorithm,

$$\begin{aligned}
861 &= 5 \cdot 165 + 36 \\
165 &= 4 \cdot 36 + 21 \\
36 &= 1 \cdot 21 + 15 \\
21 &= 1 \cdot 15 + 6 \\
15 &= 2 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0 \Rightarrow (861, 165) = 3 \\
3 &= 15 - 2 \cdot 6 = 15 - 2(21 - 1 \cdot 15)
\end{aligned}$$

$$\begin{aligned} &= -2 \cdot 21 + 3 \cdot 15 = -2 \cdot 21 + 3(36 - 1 \cdot 21) \\ &= 3 \cdot 36 - 5 \cdot 21 = 3 \cdot 36 - 5(165 - 4 \cdot 36) \\ &= -5 \cdot 165 + 23 \cdot 36 = -5 \cdot 165 + 23(861 - 5 \cdot 165) \\ &= -120 \cdot 165 + 23 \cdot 861 \end{aligned}$$

3. (a) [3 MARKS] Define precisely what is meant by the statement $\tau = \phi$, where $\tau : B \to A$ and $\phi : C \to D$ are two mappings.

   (b) [7 MARKS] Prove that, for any mappings $\alpha : S \to T$, $\beta : T \to V$, $\gamma : T \to V$, if α is surjective, and $\beta \circ \alpha = \gamma \circ \alpha$, then $\beta = \gamma$.

   Solution:

   (a) (cf. [8, p. 16]) The statement $\tau = \phi$ is equivalent to the following three facts:

   - The domains are equal, i.e. $B = C$.
   - The codomains are equal, i.e. $A = D$.
   - The actions of the functions coincide on all points of their common domain, i.e. $(\forall x \in B[\tau(x) = \phi(x)]$.

   (b) (cf. [8, Problem 2.23]) As β and γ have the same domain and also the same codomain, all that remains to prove is that they have the same action.

   Let t be any element of T. Since α is surjective, there exists $s \in S$ such that $\alpha(s) = t$. But then

$$\begin{aligned} \beta(t) &= \beta(\alpha(s)) \\ &= (\beta \circ \alpha)(t) \quad \text{by definition of } \circ \\ &= (\gamma \circ \alpha)(t) \quad \text{by hypothesis} \\ &= \gamma(\alpha(t)) \quad \text{by definition of } \circ \\ &= \gamma(t) \end{aligned}$$

   We have proved that β and γ have the same action on their common domain, so they must be the same function.

4. (a) [6 MARKS] Showing all your work, determine the entries missing from the

following Cayley table for a group B:

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
b_1								b_8
b_2		b_3			b_6	b_7	b_8	b_5
b_3			b_1	b_2	b_7	b_8	b_5	b_6
b_4			b_2	b_3	b_8	b_5	b_6	b_7
b_5		b_8	b_7	b_6	b_3	b_2	b_1	b_4
b_6		b_5	b_8	b_7	b_4	b_3	b_2	b_1
b_7		b_6	b_5	b_8	b_1	b_4	b_3	b_2
b_8		b_7	b_6	b_5	b_2	b_1	b_4	b_3

(You must justify every step of your argument.)

(b) [4 MARKS] Showing all your work, determine the right coset decomposition of B with respect to the subgroup $\langle b_4 \rangle$.

Solution:

(a) From the fact that $b_1 b_8 = b_8$ we can conclude (by multiplying on the right by b_8^{-1}) that $b_1 = e$; this allows us to complete the first row and the first column of the table.

Now the second row of the table is missing the values for $b_2 b_3$ and $b_2 b_4$. But we know that evey element of the group must appear in this row, and the only missing values are b_1 and b_4. It is not possible that $b_2 b_4 = b_4$, as this would imply that $b_2 = e$; but we know from the foregoing that $b_1 = e$. It follows that $b_2 b_4 = b_1$, and then the only possible value for $b_2 b_3$ is b_4. The same reasoning permits the 2nd column to be completed. (The group is not abelian, but the subgroup given by the first four rows and the first four columns *is* abelian.) The completed table will be

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
b_1	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
b_2	b_2	b_3	b_4	b_1	b_6	b_7	b_8	b_5
b_3	b_3	b_4	b_1	b_2	b_7	b_8	b_5	b_6
b_4	b_4	b_1	b_2	b_3	b_8	b_5	b_6	b_7
b_5	b_5	b_8	b_7	b_6	b_3	b_2	b_1	b_4
b_6	b_6	b_5	b_8	b_7	b_4	b_3	b_2	b_1
b_7	b_7	b_6	b_5	b_8	b_1	b_4	b_3	b_2
b_8	b_8	b_7	b_6	b_5	b_2	b_1	b_4	b_3

(b) cf. solution to §G.3.1 Problem 5

$$B = \{b_1, b_2, b_3, b_4\} \cup \{b_5, b_6, b_7, b_8\}\,.$$

5. [10 MARKS] Let G be any group with operation $*$ and identity e, and define $K = \{g \in G | \forall k \in G[g^{-1} * k * g = k]\}$. Determine whether or not K is a subgroup of G.

   Solution: (cf. [8, Problem 7.24]) This subset is, indeed, a subgroup, as the criteria of [8, Theorem 7.1] are satisfied.

   non-empty. $\forall k \in G[e^{-1} * k * e = k]$; hence $e \in K$.

   closed under group operation. Suppose that $\forall k \in G[g_1^{-1} * k * g_1 = k]$ (i.e. $g_1 \in K$) and $\forall \ell \in G[g_2^{-1} * \ell * g_2 = \ell]$ (i.e. $g_2 \in K$). Then, in particular, taking $\ell = k$, we have $\forall k,\ k = g_2^{-1} * k * g_2 = g_2^{-1} * (g_1^{-1} * k * g_1) * g_2 = (g_2^{-1} * g_1^{-1}) * k * (g_1 * g_2) = (g_1 * g_2)^{-1} * k * (g_1 * g_2)$, implying that $g_1 * g_2 \in K$.

   closed under taking inverses. It follow from $\forall k \in G[g_1^{-1} * k * g_1 = k]$ by multiplying both sides of the equation on the left by g_1 and on the right by g_1^{-1}, that $\forall k \in G[g_1 * g_1^{-1} * k * g_1 * g_1^{-1} = g_1 * k * g_1^{-1}]$, i.e. $\forall k \in G[k = g_1 * k * g_1^{-1} = \left((g_1)^{-1}\right)^{-1} * k * g_1^{-1}]$, which implies that $g_1^{-1} \in K$.

   K is called the *centre* of G.

G.3.3 Version 3

1. (a) [3 MARKS] Prove or disprove:

   $$(\forall n \in \mathbb{N} - \{0\})\ (\forall a \in \mathbb{Z})\ (\forall b \in \mathbb{Z})[(a^2 \equiv b^2 \pmod{n}) \Leftrightarrow (a \equiv b \pmod{n})]$$

   (b) [7 MARKS] Showing all your work, determine integers a and b such that $a \cdot 681 + b \cdot 279 = (681, 279)$.

   Solution:

   (a) The implication $\Rightarrow$ is false. For a counterexample take $n > 2$ and $a = -b = 1$.

   (b) By the Euclidean algorithm,

   $$\begin{aligned} 681 &= 2 \cdot 279 + 123 \\ 279 &= 2 \cdot 123 + 33 \\ 123 &= 3 \cdot 33 + 24 \\ 33 &= 1 \cdot 24 + 9 \end{aligned}$$

$$\begin{aligned}
24 &= 2 \cdot 9 + 6 \\
9 &= 1 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0 \Rightarrow (681, 279) = 3 \\
3 &= 9 - 1 \cdot 6 = 9 - (24 - 2 \cdot 9) \\
&= -1 \cdot 24 + 3 \cdot 9 = -1 \cdot 24 + 3(33 - 1 \cdot 24) \\
&= 3 \cdot 33 - 4 \cdot 24 = 3 \cdot 33 - 4(123 - 3 \cdot 33) \\
&= -4 \cdot 123 + 15 \cdot 33 = -4 \cdot 123 + 15(279 - 2 \cdot 123) \\
&= 15 \cdot 279 - 34 \cdot 123 = 15 \cdot 279 - 34(681 - 2.279) \\
&= -34 \cdot 681 + 83 \cdot 279
\end{aligned}$$

2. (a) [5 MARKS] Prove or disprove: the ring $\mathbb{Z}_7 \times \mathbb{Z}_3$, with multiplication defined by

$$([d]_7, [c]_3)([b]_7, [a]_3) = ([d]_7 \odot [b]_7, [c]_3 \odot [a]_3)\,,$$

has no zero divisors.

(b) [5 MARKS] Determine the value of the product $(1234567)^2(163)(24)(1234567)^{-2}$ in S_7.

Solution:

(a) Two zero divisors are $([1], [0])$ and $([0], [1])$, since they are non-zero elements whose product is $([0], [0])$.

(b) $(1234567)^2(163)(24)(1234567)^{-2} = (1357246)(163)(24)(1642753) = (153)(2)(46)(7)$

3. [10 MARKS] Let G be any group with operation $*$ and identity e, and define, for some fixed element $g_0 \in G$, $H = \{g \in G | g_0 * g * g_0^{-1} = g\}$. Determine whether or not H is a subgroup of G.

Solution: (cf. [8, Problem 7.23]) This subset is, indeed, a subgroup, as the criteria of [8, Theorem 7.1] are satisfied.

non-empty. $g_0 * e * g_0^{-1} = e \Rightarrow e \in H$, so $H \neq \varnothing$.

closed under group operation. Suppose that $g_1, g_2 \in H$, i.e. $g_0 * g_1 * g_0^{-1} = g_1$, $g_0 * g_2 * g_0^{-1} = g_2$. Then $g_1 * g_2 = (g_0 * g_1 * g_0^{-1})(g_0 * g_2 * g_0^{-1}) = g_0 * g_1 * (g_0^{-1} g_0) * g_2 * g_0^{-1} = g_0 * g_1 * e * g_2 * g_0^{-1} = g_0 * (g_1 * g_2) * g_0^{-1}$; so $g_1 * g_2 \in H$.

closed under taking inverses. The inverse of $g_0 * g * g_0^{-1}$ is $\left((g_0)^{-1}\right)^{-1} * g^{-1} * g_0^{-1} = g_0 * g^{-1} * g_0^{-1}$. Hence, $g \in H \Rightarrow g_0 * g * g_0^{-1} = g \Rightarrow g_0 * g^{-1} * g_0^{-1} = g^{-1} \Rightarrow g^{-1} \in H$.

H is called the *centralizer* of g_0 in G.

4. (a) [6 MARKS] Showing all your work, determine the order of every element of the group L with the following Cayley table. (You must justify every step of your argument.)

	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8
ℓ_1	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8
ℓ_2	ℓ_2	ℓ_3	ℓ_4	ℓ_1	ℓ_6	ℓ_7	ℓ_8	ℓ_5
ℓ_3	ℓ_3	ℓ_4	ℓ_1	ℓ_2	ℓ_7	ℓ_8	ℓ_5	ℓ_6
ℓ_4	ℓ_4	ℓ_1	ℓ_2	ℓ_3	ℓ_8	ℓ_5	ℓ_6	ℓ_7
ℓ_5	ℓ_5	ℓ_8	ℓ_7	ℓ_6	ℓ_3	ℓ_2	ℓ_1	ℓ_4
ℓ_6	ℓ_6	ℓ_5	ℓ_8	ℓ_7	ℓ_4	ℓ_3	ℓ_2	ℓ_1
ℓ_7	ℓ_7	ℓ_6	ℓ_5	ℓ_8	ℓ_1	ℓ_4	ℓ_3	ℓ_2
ℓ_8	ℓ_8	ℓ_7	ℓ_6	ℓ_5	ℓ_2	ℓ_1	ℓ_4	ℓ_3

   (b) [4 MARKS] Showing all your work, determine the right coset decomposition of L with respect to the subgroup $\langle \ell_7 \rangle$.

Solution:

(a) cf. solution to §G.3.1, Problem 5

(b) cf. solution to §G.3.1, Problem 5

$$L = \{\ell_1, \ell_3, \ell_5, \ell_7\} \cup \{\ell_2, \ell_4, \ell_6, \ell_8\}\,.$$

5. (a) [3 MARKS] Define precisely what is meant by the statement $\lambda = \mu$, where $\lambda : K \to L$ and $\mu : M \to N$ are two mappings.

   (b) [7 MARKS] Prove that, for any mappings $\alpha : T \to U$, $\beta : S \to T$, $\gamma : S \to T$, if α is injective, and $\alpha \circ \beta = \alpha \circ \gamma$, then $\beta = \gamma$.

Solution:

(a) See the solution to §G.3.1, Problem 3a.

(b) (cf. [8, Problem 2.24]) Since β and γ have the same domain, S, and the same codomain, T, all that remains to prove is that they have the same action on their common domain S. Let s be any element of S. Since $\alpha \circ \beta = \alpha \circ \gamma$, $(\alpha \circ \beta)(s) = (\alpha \circ \gamma)(s)$; i.e., by the definition of $\circ$, $\alpha(\beta(s)) = \alpha(\gamma(s))$. But, as α is injective, this equality implies that $\beta(s) = \gamma(s)$. We have thus shown that β and γ have the same action on all points of S, so they must be the same function.

G.3.4 Version 4

1. (a) [3 MARKS] Prove or disprove:

$$(\forall n \in \mathbb{N} - \{0\})\ (\forall a \in \mathbb{Z})\ (\forall b \in \mathbb{Z})[(a^2 \equiv b^2 \pmod{n}) \Leftarrow (a \equiv b \pmod{n})]$$

   (b) [7 MARKS] Showing all your work, determine integers ℓ and m such that $841\ell + 160b = (841, 160)$.

Solution:

   (a) This implication is true. We may multiply the congruence $a \equiv b \pmod{n}$ by itself, to obtain $a^2 \equiv b^2 \pmod{n}$.

   (b) By the Euclidean algorithm,

$$\begin{aligned}
841 &= 5 \cdot 160 + 41 \\
160 &= 3 \cdot 41 + 37 \\
41 &= 1 \cdot 37 + 4 \\
37 &= 9 \cdot 4 + 1 \\
4 &= 4 \cdot 1 + 0 \Rightarrow (841, 160) = 1 \\
1 &= 37 - 9 \cdot 4 = 1 \cdot 37 - 9(41 - 1 \cdot 37) \\
&= -9 \cdot 41 + 10 \cdot 37 = -9 \cdot 41 + 10(160 - 3 \cdot 41) \\
&= 10 \cdot 160 - 39 \cdot 41 = 10 \cdot 160 - 39(841 - 5 \cdot 160) \\
&= -39 \cdot 841 + 205 \cdot 160
\end{aligned}$$

2. (a) [5 MARKS] Prove or disprove: the ring $\mathbb{Z}_5 \times \mathbb{Z}_2$, with multiplication defined by

$$([a]_5, [c]_2)([b]_5, [d]_2) = ([a]_5 \odot [b]_5, [c]_2 \odot [d]_2)\,,$$

   has zero divisors.

   (b) [5 MARKS] Determine the value of the product $(123456)^{-2}(624)(35)(1)(123456)^2$ in S_6.

Solution:

   (a) Two zero divisors are $([1], [0])$ and $([0], [1])$, since they are non-zero elements whose product is $([0], [0])$.

   (b) $(123456)^{-2}(624)(35)(1)(123456)^2 = (153)(264)(624)(35)(1)(135)(246) = (13)(246)(5)$

3. [10 MARKS] Let G be any group with operation $*$ and identity e, and define $K = \{g \in G | \forall k \in G[g * k * g^{-1} = k]\}$. Determine whether or not K is a subgroup of G.

   Solution: (cf. [8, Problem 7.24]) This subset is, indeed, a subgroup, as the criteria of [8, Theorem 7.1] are satisfied.

   non-empty. $\forall k \in G[e * k * e^{-1} = k]$; hence $e \in K$.

   closed under group operation. Suppose that $\forall k \in G[g_1 * k * g_1^{-1} = k]$ (i.e. $g_1 \in K$) and $\forall \ell \in G[g_2 * \ell * g_2^{-1} = \ell]$ (i.e. $g_2 \in K$). Then, in particular, taking $k = \ell$, we have $\forall \ell$, $\ell = g_1 * k * g_1^{-1} = g_1 * (g_2 * k * g_2^{-1}) * g_1^{-1} = (g_1 * g_2) * k * (g_2^{-1} * g_1^{-1}) = (g_1 * g_2) * k * (g_1 * g_2)^{-1}$, implying that $g_1 * g_2 \in K$.

   closed under taking inverses. It follow from $\forall k \in G[g_1 * k * g_1^{-1} = k]$ by multiplying both sides of the equation on the right by g_1 and on the left by g_1^{-1}, that $\forall k \in G[g_1^{-1} * g_1 * k * g_1^{-1} * g_1 = g_1^{-1} * k * g_1]$, i.e. $\forall k \in G[k = g_1^{-1} * k * g_1 = g_1^{-1} * k * \left((g_1)^{-1}\right)^{-1}]$, which implies that $g_1^{-1} \in K$.

   K is called the *centre* of G.

4. (a) [6 MARKS] Showing all your work, determine the missing entries in the following Cayley table for a group K. (You must justify every step of your argument.)

	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8
k_1								
k_2		k_3	k_4		k_6	k_7	k_8	k_5
k_3		k_4	k_1		k_7	k_8	k_5	k_6
k_4				k_3	k_8	k_5	k_6	k_7
k_5		k_8	k_7	k_6	k_3	k_2	k_1	k_4
k_6	k_6	k_5	k_8	k_7	k_4	k_3	k_2	k_1
k_7		k_6	k_5	k_8	k_1	k_4	k_3	k_2
k_8		k_7	k_6	k_5	k_2	k_1	k_4	k_3

   (b) [4 MARKS] Showing all your work, determine the left coset decomposition of K with respect to the subgroup $\langle k_6 \rangle$.

   Solution:

(a) cf. solution to §G.3.2, Problem 4. The completed table is

	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8
k_1	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8
k_2	k_2	k_3	k_4	k_1	k_6	k_7	k_8	k_5
k_3	k_3	k_4	k_1	k_2	k_7	k_8	k_5	k_6
k_4	k_4	k_1	k_2	k_3	k_8	k_5	k_6	k_7
k_5	k_5	k_8	k_7	k_6	k_3	k_2	k_1	k_4
k_6	k_6	k_5	k_8	k_7	k_4	k_3	k_2	k_1
k_7	k_7	k_6	k_5	k_8	k_1	k_4	k_3	k_2
k_8	k_8	k_7	k_6	k_5	k_2	k_1	k_4	k_3

(b) cf. solution to §G.3.1, Problem 5

$$K = \{k_1, k_3, k_6, k_8\} \cup \{k_2, k_4, k_5, k_7\}\,.$$

5. (a) [3 MARKS] Define precisely what is meant by the statement $\lambda = \mu$, where $\lambda : K \to L$ and $\mu : M \to N$ are two mappings.

   (b) [7 MARKS] Prove that, for any mappings $\alpha : T \to U$, $\beta : S \to T$, $\gamma : S \to T$, if α is injective, and $\alpha \circ \beta = \alpha \circ \gamma$, then $\beta = \gamma$.

   Solution:

   (a) See the solution to §G.3.1, Problem 3a.

   (b) (cf. [8, Problem 2.24]) Since β and γ have the same domain, S, and the same codomain, T, all that remains to prove is that they have the same action on their common domain S. Let s be any element of S. Since $\alpha \circ \beta = \alpha \circ \gamma$, $(\alpha \circ \beta)(s) = (\alpha \circ \gamma)(s)$; i.e., by the definition of $\circ$, $\alpha(\beta(s)) = \alpha(\gamma(s))$. But, as α is injective, this equality implies that $\beta(s) = \gamma(s)$. We have thus shown that β and γ have the same action on all points of S, so they must be the same function.

G.4 1999 Class Tests

G.4.1 Version 1

1. If $\mathfrak{A} = \{a, b\}$ $(a \neq b)$, give the Cayley table of a semigroup $(\mathfrak{A}, *)$ that is non-commutative, or *prove* that no such semigroup exists. (If the semigroup exists, you are expected to *prove* that $*$ has all the properties you claim.)

   Solution: We have seen that there are, up to isomorphism, 5 semigroups of order 2. Of these three are commutative. Either of the other 2 has the desired properties, which, however, *must be proved*.

left absorption

$*$	a	b
a	a	a
b	b	b

: The table defines a function from $\mathfrak{A} \times \mathfrak{A}$ to $\mathfrak{A}$.

(a) $*$ is associative:

$$\begin{aligned}
(a*a)*a = & \quad a*a & = a*(a*a) \\
(a*a)*b = a*b = & \quad a & = a*a = a*(a*b) \\
(a*b)*a = a*a = & \quad a & = a*b = a*(b*a) \\
(a*b)*b = & \quad a*b & = a*(b*b) \\
(b*a)*a = & \quad b*a & = b*(a*a) \\
(b*a)*b = b*b = & \quad b & = b*a = b*(a*b) \\
(b*b)*a = b*a = & \quad b & = b*b == b*(b*a) \\
(b*b)*b = & \quad b*b & = b*(b*b)
\end{aligned}$$

(b) $*$ is non-commutative:

$$a*b = a \neq b = b*a$$

right absorption

$*$	a	b
a	a	b
b	a	b

: This case is analogous to the preceding one.

2. *Showing all your work*, find the smallest non-negative integer N which gives the remainder 2 when divided by each of 3, 4, 6, and remainder 1 when divided by 5, or prove that no such integer exists. Use the Chinese Remainder Theorem where it is applicable.

   Solution: We wish to solve the congruences

$$\begin{aligned}
x &\equiv 2 \pmod 3 && (1165)\\
x &\equiv 2 \pmod 4 && (1166)\\
x &\equiv 1 \pmod 5 && (1167)\\
x &\equiv 2 \pmod 6 && (1168)
\end{aligned}$$

   The Chinese Remainder Theorem cannot be applied yet, since the moduli are not relatively prime. However (1168) is equivalent to the two congruences $x \equiv 2 \pmod 2$ and $x \equiv 2 \pmod 3$. So the system of congruences is equivalent to

$$x \equiv 2 \pmod 3 \qquad (1169)$$

$$x \equiv 2 \pmod 4 \tag{1170}$$
$$x \equiv 1 \pmod 5 \tag{1171}$$
$$x \equiv 2 \equiv 0 \pmod 2 \tag{1172}$$
$$x \equiv 2 \pmod 3 \tag{1173}$$

In this system congruences (1169) and (1173) are identical, so (1173) may be suppressed. And every solution of congruence (1170) will be even, and hence will also satisfy (1172), so (1172) may also be suppressed. The resulting system consists of congruences (1169), (1170), (1171). Only now could we use the Chinese Remainder Theorem.[1050] Applying the notation of the printed notes, we have $M = 3 \times 4 \times 5 = 60$, $M_1 = 4 \times 5 = 20$, $M_2 = 3 \times 5 = 15$, $M_3 = 3 \times 4 = 12$. Modulo 3, $d_1 = (20)^{-1} \equiv 2^{-1} \equiv 2$; modulo 4, $d_2 = (15)^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 3$; modulo 5, $d_3 = (12)^{-1} \equiv 2^{-1} \equiv 3$. Hence the general solution is $[20{\cdot}2{\cdot}2+15{\cdot}3{\cdot}2+12{\cdot}3{\cdot}1]_{3\cdot4\cdot5} = [206]_{60} = [26]_{60}$, and the smallest non-negative solution is $N = 26$.

3. *Showing all your work*, determine the Cayley Table of the smallest permutation group on the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ which contains the permutations (15)(26)(37)(48) and (15)(24)(68).

   Solution: By closure under composition, the group must contain $(15)(26)(37)(48) \circ (15)(24)(68) = (28)(37)(46)$. (Your work should have explained the advent of the new element which was not in the original list.) We begin with a 4×4 table with rows and columns labelled by e, the two given elements, and (28)(37)(46), aware that under compositions we might find the need to add additional rows and columns to the tables. This, however does not become necessary, and the set of 4 elements is closed under composition.

	e	(15)(26)(37)(48)	(15)(24)(68)	(28)(37)(46)
e	e	(15)(26)(37)(48)	(15)(24)(68)	(28)(37)(46)
(15)(26)(37)(48)	(15)(26)(37)(48)	e	(28)(37)(46)	(15)(24)(68)
(15)(24)(68)	(15)(24)(68)	(28)(37)(46)	e	(15)(26)(37)(48)
(28)(37)(46)	(28)(37)(46)	(15)(24)(68)	(15)(26)(37)(48)	e

4. *Showing all your work*, use the Euclidean algorithm to determine integers k and ℓ such that $563k + 1109\ell = (563, 1109)$, where (a, b) denotes the greatest common divisor of a and b. (Note that there is some integer arithmetic in this problem, involving integers up to 4 digits long.)

   Solution: From

$$1109 = 1 \cdot 563 + 546$$

[1050] This solution could be shortened by observing that (1169) and (1170) are together equivalent to $x \equiv 2 \pmod{12}$. The theorem could then be applied to two congruences instead of to three.

$$\begin{aligned} 563 &= 1 \cdot 546 + 17 \\ 546 &= 32 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

we know that $(563, 1009) = 1$. By backwards substitution we obtain

$$\begin{aligned} 1 &= 17 - 8 \cdot 2 = 17 - 8(546 - 32 \cdot 17) \\ &= -8 \cdot 546 + 257 \cdot 17 = -8 \cdot 546 + 257(563 - 1 \cdot 546) \\ &= 257 \cdot 563 - 265 \cdot 546 = 257 \cdot 563 - 265(1109 - 1 \cdot 563) \\ &= -265 \cdot 1109 + 522 \cdot 563 \end{aligned}$$

We may take $k = 522$ and $\ell = -265$. (Another solution is $k = 522 - 1109 = -587$ and $\ell = -265 + 563 = 298$.)

G.4.2 Version 2

1. *Showing all your work*, use the Euclidean algorithm to determine integers k and ℓ such that $1312k + 4001\ell = (1312, 4001)$, where (a, b) denotes the greatest common divisor of a and b. (Note that there is some integer arithmetic in this problem, involving integers up to 4 digits long.)

   Solution: From

$$\begin{aligned} 4001 &= 3 \cdot 1312 + 65 \\ 1312 &= 20 \cdot 65 + 12 \\ 65 &= 5 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

   we deduce that $(1312, 4001) = 1$. By backwards substitution we obtain

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) \\ &= -2 \cdot 12 + 5 \cdot 5 = -2 \cdot 12 + 5(65 - 5 \cdot 12) \\ &= 5 \cdot 65 - 27 \cdot 12 = 5 \cdot 65 - 27(1312 - 20 \cdot 65) \\ &= -27 \cdot 1312 + 545 \cdot 65 = -27 \cdot 1312 + 545(4001 - 3 \cdot 1312) \\ &= 545 \cdot 4001 - 1662 \cdot 1312 \end{aligned}$$

   We may take $k = -1662$ and $\ell = 545$.

2. *Showing all your work*, find the smallest (non-negative) integer N which gives the remainder 2 when divided by each of 4, 5, 6, and remainder 5 when divided by 7, or prove that no such integer exists.

   Solution: We wish to solve the congruences

   $$x \equiv 2 \pmod 4 \tag{1174}$$
   $$x \equiv 2 \pmod 5 \tag{1175}$$
   $$x \equiv 2 \pmod 6 \tag{1176}$$
   $$x \equiv 5 \pmod 7 \tag{1177}$$

   The Chinese Remainder Theorem cannot be applied yet, since the moduli are not relatively prime. However (1176) is equivalent to the two congruences $x \equiv 2 \pmod 2$ and $x \equiv 2 \pmod 3$. So the system of congruences is equivalent to

   $$x \equiv 2 \pmod 4 \tag{1178}$$
   $$x \equiv 2 \pmod 5 \tag{1179}$$
   $$x \equiv 2 \equiv 0 \pmod 2 \tag{1180}$$
   $$x \equiv 2 \pmod 3 \tag{1181}$$
   $$x \equiv 5 \pmod 7 \tag{1182}$$

   Every solution of congruence (1178) will be even, and hence will also satisfy (1180), so (1180) may be suppressed. The resulting system consists of congruences (1178), (1179), (1181), (1182). Only now could we use the Chinese Remainder Theorem.[1051] Applying the notation of the printed notes, we have $M = 4 \times 5 \times 3 \times 7 = 420$, $M_1 = 5{\times}3{\times}7 = 105$, $M_2 = 4{\times}3{\times}7 = 84$, $M_3 = 4{\times}5{\times}7 = 140$, $M_4 = 4{\times}5{\times}3 = 60$. Modulo 4, $d_1 = (105)^{-1} \equiv 1^{-1} \equiv 1$; modulo 5, $d_2 = (84)^{-1} \equiv (4)^{-1} \equiv 4$; modulo 3, $d_3 = (140)^{-1} \equiv 2^{-1} \equiv 2$; modulo 7, $d_4 = (60)^{-1} \equiv 4^{-1} \equiv 2$. Hence the general solution is $[105 \cdot 1 \cdot 2 + 84 \cdot 4 \cdot 2 + 140 \cdot 2 \cdot 2 + 60 \cdot 2 \cdot 5]_{4\cdot5\cdot3\cdot7} = [2042]_{420} = [362]_{420}$, and the smallest non-negative solution is $N = 362$.

3. Let $\mathfrak{C} = \{s, t\}$ where s, and t are distinct. Give the Cayley table of a monoid $(\mathfrak{C}, *, t)$ which is non-commutative, or *prove* that no such monoid exists. (If the monoid exists, you are expected to *prove* that $*$ has all the properties you claim.)

   Solution: In the monoid $(\mathfrak{C}, *, t)$ t is the identity. The Cayley table must include the following entries:

$*$	t	s
t	t	s
s	s	

   . No matter what value is assigned to $s * s$,

[1051] This solution could possibly be shortened by observing that (1178), (1179), and (1181) are together equivalent to $x \equiv 2 \pmod{60}$. The theorem could then be applied to two congruences instead of to four. However, we would have to determine 7^{-1} modulo 60; this turns out to be $[43]_{60}$ and probably has to be found using the Euclidean algorithm.

this monoid is symmetric! Thus there exists no monoid with the desired property of non-commutativity. (There is no need to investigate associativity, as we have already demonstrated non-existence.)

4. *Showing all your work*, determine the Cayley Table of the smallest permutation group on the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ which contains the permutations $(15)(26)(37)(48)$ and $(13)(48)(57)$.

   Solution: By closure under composition, the group must contain $(15)(26)(37)(48) \circ (13)(48)(57) = (17)(26)(35)$. (Your work should have explained the advent of the new element which was not in the original list.) We begin with a 4×4 table with rows and columns labelled by e, the two given elements, and $(17)(26)(35)$, aware that under compositions we might find the need to add additional rows and columns to the tables. This, however does not become necessary, and the set of 4 elements is closed under composition.

	e	$(15)(26)(37)(48)$	$(13)(48)(57)$	$(17)(26)(35)$
e	e	$(15)(26)(37)(48)$	$(13)(48)(57)$	$(17)(26)(35)$
$(15)(26)(37)(48)$	$(15)(26)(37)(48)$	e	$(17)(26)(35)$	$(13)(48)(57)$
$(13)(48)(57)$	$(13)(48)(57)$	$(17)(26)(35)$	e	$(15)(26)(37)(48)$
$(17)(26)(35)$	$(17)(26)(35)$	$(13)(48)(57)$	$(15)(26)(37)(48)$	e

G.5 2000 Class Tests

Distribution Date: **Please Note:** This is a preliminary version of the solutions. Corrections and/or additions may be required; if there are changes, they can be viewed on the Web.

The four versions of the test had 4 equally-valued questions each, numbered 1, 2, 3, 4, according to the following scheme:

	1	2	3	4
I	1		4	
II		3		4
III	2		1	
IV		4		3
V	3		2	
VI		1		2
VII	4		3	
VIII		2		1

G.5.1 Problems on monoids

I. [10 MARKS] Give a Cayley table of a finite monoid which is non-commutative; or prove that no such monoid exists.

Solution: Any non-commutative group provides an example of a non-commutative monoid. For example, the group $\mathcal{S}_3$ is the smallest non-commutative group. There are smaller examples of non-commutative monoids. For example, consider the set of 2^2 functions $\{1,2\}^{\{1,2\}}$ which map the set $\{1,2\}$ into itself. If we denote the constant functions by 1 and 2, we have that $1 \circ (12) = 1$, while $(12) \circ 1 = 2$, so composition is not commutative. The Cayley table is

$\circ$	ι	1	2	(12)
ι	ι	1	2	(12)
1	1	1	1	1
2	2	2	2	2
(12)	(12)	2	1	ι

Within this monoid we can see a smaller monoid — with 3 elements — which is also not commutative. Simply suppress the element (12), and the smaller set of 3 functions is still closed under composition. There is no monoid of order 2 which is non-commutative, as seen in the notes.

II. [10 MARKS] Give a Cayley table of a finite monoid $(\mathfrak{A}, *, e)$ in which some element a does not have an inverse; or prove that no such monoid exists.

Solution: There exists a monoid of order 2 in which some element does not have an inverse. Its Cayley table is

	e	a
e	e	a
a	a	a

One instance of this monoid is multiplication in the ring $\mathbb{Z}_2$ — take $e = [0]_2$, and $a = [1]_2$. We can see that e is the identity, since its row and column contain the label entries. That there is no entry e in the row or column for a shows that a does not have an inverse in this monoid.

G.5.2 Group homomorphisms

III. (a) [2 MARKS] Define *precisely* what is meant by a group homomorphism

$$\phi : (\mathfrak{A}, \star, e) \to (\mathfrak{B}, *, f)\,.$$

(b) [8 MARKS] Showing all your work, find a homomorphism $\phi : \mathcal{S}_3 \to \mathcal{S}_4$ such that $\phi(12) = (123)$, or prove carefully that no such homomorphism exists. Prove everything you need — do not appeal to any theorems proved in lectures or notes unless you prove them.

Solution:

(a) A function $\phi : \mathfrak{A} \to \mathfrak{B}$ is a homomorphism $\phi : (\mathfrak{A}, \star, e) \to (\mathfrak{B}, *, f)$ iff

$$\forall a_1 \in \mathfrak{A} \forall a_2 \in \mathfrak{A} \quad \phi(a_1 \star a_2) = \phi(a_1) * \phi(a_2)$$

(b) If ϕ is a homomorphism, and $\phi(12) = (123)$, then $\phi((12) \star (12) \star (12)) = (123) * (123) * (123)$, i.e. $\phi(12) = e$. Since $e \neq (123)$, this contradicts the hypothesis. We conclude that no such homomorphism ϕ may exist.

IV. (a) [2 MARKS] Define *precisely* what is meant by a group homomorphism

$$\lambda : (\mathfrak{B}, *, e) \to (\mathfrak{A}, \star, f)\,.$$

(b) [8 MARKS] Showing all your work, find a homomorphism $\lambda : \mathcal{S}_4 \to \mathcal{S}_4$ such that $\lambda(x) = x^2$ for all $x \in \mathcal{S}_4$; or prove carefully that no such homomorphism exists. Prove everything you need — do not appeal to any theorems proved in lectures or notes unless you prove them.

Solution:

(a) A function $\lambda : \mathfrak{B} \to \mathfrak{A}$ is a homomorphism $\lambda : (\mathfrak{B}, *, e) \to (\mathfrak{A}, \star, f)$ iff

$$\forall b_1 \in \mathfrak{B} \forall b_2 \in \mathfrak{B} \quad \lambda(b_1 * b_2) = \lambda(b_1) \star \lambda(b_2)$$

(b) SEE exercise A.5.2.11. The squaring function is a homomorphism iff the group is abelian. Here is a specific counterexample. (Of course, there will be specific pairs of elements which *will* satisfy the condition of the definition; but we must have that property for *all* choices of elements $(b_1, b_2) \in \mathfrak{B}^2$.)

$$\begin{aligned} \lambda((12) * (23)) &= \lambda(123) \\ &= (123)^2 \\ &= (132) \\ &\neq e = e \star e = (12)^2 \star (23)^2 \\ &= \lambda(12) \star \lambda(23) \end{aligned}$$

G.5.3 Solution of congruences

V. [10 MARKS] Prove that there is no solution to the following system of congruences; or find all solutions systematically, in a way that demonstrates that you could solve any solvable system of congruences.

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 3 \\ x &\equiv -3 \pmod 4 \end{aligned}$$

Solution: Using the notation of the notes, $M_1 = 12$, and its inverse modulo 5 is $[2]_5^{-1} = [3]_5$ (by trial and error, or by using the Euclidean algorithm), so we may take $d_1 = 3$. The inverse of $M_2 = 20$ modulo 3 is $[2]_3^{-1} = [2]$, so we may take $d_2 = 2$. And the inverse of $M_3 = 15$ modulo 4 is $[3]_4^{-1} = [3]$, so we may take $d_3 = 3$. The general solution is therefore the residue class modulo $M = 5 \cdot 3 \cdot 4 = 60$ of $12 \cdot 3 \cdot 1 + 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot (-3) = -19$, i.e., $[-19]_{60}$ or $[41]_{60}$.

VI. [10 MARKS] Prove that there is no solution to the following system of congruences; or find all solutions systematically, in a way that demonstrates that you could solve any solvable system of congruences.

$$\begin{aligned} x &\equiv -2 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 4 \pmod 6 \end{aligned}$$

Solution: Using the notation of the notes, $M_1 = 42$, and its inverse modulo 5 is $[2]_5^{-1} = [3]_5$ (by trial and error, or by using the Euclidean algorithm), so we may take $d_1 = 3$. The inverse of $M_2 = 30$ modulo 7 is $[2]_7^{-1} = [4]$, so we may take $d_2 = 4$. And the inverse of $M_3 = 35$ modulo 6 is $[5]_6^{-1} = [5]$, so we may take $d_3 = 5$. The general solution is therefore the residue class modulo $M = 5 \cdot 7 \cdot 6 = 210$ of $42 \cdot 3 \cdot (-2) + 30 \cdot 4 \cdot 1 + 35 \cdot 5 \cdot 4 = 568$, i.e., $[568]_{210}$ or $[148]_{210}$.

G.5.4 Cosets of subgroup in a group

VII. [10 MARKS] Showing all your work, determine the orbits of the group $\mathcal{S}_3$ of permutations of the symbols 1, 2, 3 under the action of the group of right translations associate with elements of the subgroup $\langle(12)\rangle$.

Solution:

$$\begin{aligned} e\langle(12)\rangle &= \{e,(12)\} \\ (23)\langle(12)\rangle &= \{(23),(23)(12)=(132)\} \\ (13)\langle(12)\rangle &= \{(13),(13)(12)=(123)\} \end{aligned}$$

VIII. [10 MARKS] Showing all your work, determine the orbits of the group $\mathcal{S}_3$ of permutations of the symbols 1, 2, 3 under the action of the group of left translations associate with elements of the subgroup $\langle(23)\rangle$.

Solution:

$$\begin{aligned} \langle(23)\rangle e &= \{e,(23)\} \\ \langle(23)\rangle(12) &= \{(12),(23)(12)=(132)\} \\ \langle(23)\rangle(13) &= \{(13),(23)(13)=(123)\} \end{aligned}$$

G.6 2001 Class Tests

Problem / Test Version	1	2	3
1	I	III	V
2	VI	II	IV
3	I	III	V
4	VI	II	IV

I. (a) Using any method you have learned in this course, solve the following system of congruences simultaneously, to find the set of *all* solutions to the system.

(b) Find the smallest non-negative solution, and the negative solution of smallest absolute value to the system.

Should you need to determine an inverse of an integer a to a given modulus, you are expected to find it *only* using the Euclidean algorithm (Bézout's theorem), except possibly in a case where $a = \pm 1$. Show all your work.

$$x \equiv 50 \pmod{11} \tag{1183}$$
$$x \equiv -37 \pmod{8} \tag{1184}$$
$$x \equiv 82 \pmod{15} \tag{1185}$$

Solution: Where symbols M, k_i, r_i, a_i are used ($i = 1, 2, 3$), we are following the

notation of the textbook. $M = 11 \times 8 \times 15 = 1320$;

i	m_i	k_i	a_i
1	11	$8 \times 15 = 120 \equiv -1 \pmod{11}$	$50 \equiv 6 \pmod{11}$
2	8	$15 \times 11 = 165 \equiv 5 \pmod{8}$	$-37 \equiv 3 \pmod{8}$
3	15	$11 \times 8 = 88 \equiv 13 \pmod{15}$	$82 \equiv 7 \pmod{15}$

An inverse of -1 modulo 11 may be taken by observation to be -1. To find inverses of 5 and 13 modulis 8 and 15 respectively we apply the Euclidean algorithm and Bézout's theorem:

$$\begin{aligned} 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ \Rightarrow 1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 5 \cdot (-1) + 3 \cdot 2 = 5 \cdot (-1) + (8 - 5 \cdot 1) \cdot 2 \\ &= 8 \cdot 2 + 5 \cdot (-3) \end{aligned}$$

$$\begin{aligned} 15 &= 13 \cdot 1 + 2 \\ 13 &= 2 \cdot 6 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ \Rightarrow 1 &= 13 - 2 \cdot 6 = 13 - (15 - 13 \cdot 1) \cdot 6 \\ &= 15 \cdot (-6) + 13 \cdot 7 \end{aligned}$$

from which calculations we may conclude that $[5]_8^{-1} = [-3]_8$, and $[13]_{15}^{-1} = [7]_{15}$. Hence the solutions to the given simultaneous system of congruences are all the integers in the residue class modulo $M = 1320$ which contains the integer

$$\sum_{i=1}^{3} k_i r_i a_i = 120 \cdot (-1) \cdot 6 + 165 \cdot (-3) \cdot 3 + 88 \cdot 7 \cdot 7 = 2107\,.$$

The smallest non-negative solution modulo $M = 1320$ is 787, and the negative solution of smallest absolute value is $2107 - 2(1320) = -533$.

The problem could also have been solved by the methods of [4, pp. 197–199].

II. (a) Using any method you have learned in this course, solve the following system of congruences simultaneously, to find the set of *all* solutions to the system.

(b) Find the smallest non-negative solution to the system.

Should you need to determine an inverse of an integer a to a given modulus, you are expected to find it *only* using the Euclidean algorithm (Bézout's theorem), except possibly in a case where $a = \pm 1$. Show all your work.

$$x \equiv -52 \pmod 9 \tag{1186}$$
$$x \equiv 37 \pmod{10} \tag{1187}$$
$$x \equiv 75 \pmod{13} \tag{1188}$$

Solution: Where symbols M, k_i, r_i, a_i are used ($i = 1, 2, 3$), we are following the notation of the textbook. $M = 9 \times 10 \times 13 = 1170$;

i	m_i	k_i	a_i
1	9	$10 \times 13 = 130 \equiv 4 \pmod 9$	$-52 \equiv 2 \pmod 9$
2	10	$13 \times 9 = 117 \equiv 7 \pmod{10}$	$37 \equiv 7 \pmod{10}$
3	13	$9 \times 10 = 90 \equiv -1 \pmod{13}$	$75 \equiv 10 \pmod{13}$

To find inverses of 4 and 7 modulis 9 and 10 respectively we apply the Euclidean algorithm and Bézout's theorem:

$$\begin{aligned} 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 + 0 \\ \Rightarrow 1 &= 9 - 4 \cdot 2 = 9 + 4 \cdot (-2) \end{aligned}$$

$$\begin{aligned} 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \\ \Rightarrow 1 &= 7 + 3 \cdot (-2) = 7 + (10 + 7 \cdot (-1)) \cdot (-2) \\ &= 10 \cdot (-2) + 7 \cdot 3 \end{aligned}$$

from which calculations we may conclude that $[4]_9^{-1} = [-2]_9$, and $[7]_{10}^{-1} = [3]_{10}$. An inverse of -1 modulo 13 may be taken by observation to be -1. Hence the solutions to the given simultaneous system of congruences are all the integers in the residue class modulo $M = 1170$ which contains the integer

$$\sum_{i=1}^{3} k_i r_i a_i = 130 \cdot (-2) \cdot 2 + 117 \cdot 3 \cdot 7 + 90 \cdot (-1) \cdot 10 = 1037\,.$$

The smallest non-negative solution modulo $M = 1170$ is 1037.

The problem could also have been solved by the methods of [4, pp. 197–199].

III. Take the defining axioms for a group $(G, *, e)$ to be the following: G is a set, and $*$ is a function from $G \times G$ to G denoted by $(x, y) \mapsto x * y$ such that

I. **Associativity.** $\forall x \in G \forall y \in G \forall z \in G[x * (y * z) = (x * y) * z]$

II. **Identity.** $\exists e \in G \forall x \in G[e * x = x = x * e]$

III. **Inverses.** $\forall x \in G \exists b \in G[x * b = e = b * x]$

You may assume that it is known, as a consequence of axioms I. and II., that e is unique. Prove that, for any x, the element b whose existence is postulated in axiom III. is unique. Justify every statement you make.

Solution: [The quantifier $\forall x$ in the axiom is to apply to the entire proof. Your proof of the uniqueness of x^{-1} is to apply to all x; you have no right to assign values to x within your proof.]

Suppose that

$$\begin{aligned} x * b &= e && (1189)\\ e &= b * x && (1190)\\ x * c &= e && (1191)\\ e &= c * x && (1192) \end{aligned}$$

Then we have

$$\begin{aligned} b &= b * e \quad \text{by II.}\\ &= b * (x * c) \quad \text{by (1191)}\\ &= (b * x) * c \quad \text{by I.}\\ &= e * c \quad (1190)\\ &= c \quad \text{by II.} \end{aligned}$$

IV. Take the defining axioms for a group $(G, *, e)$ to be the following: G is a set, and $*$ is a function from $G \times G$ to G denoted by $(x, y) \mapsto x * y$ such that

I. **Associativity.** $\forall x \in G \forall y \in G \forall z \in G[x * (y * z) = (x * y) * z]$

II. **Identity.** $\exists e \in G \forall x \in G[e * x = x = x * e]$

III. **Inverses.** $\forall x \in G \exists b \in G[x * b = e = b * x]$

You may assume that it is known, as a consequence of axioms I. and II., that e is unique; and that the element b, whose existence for a fixed x is postulated in axiom III., is unique. Let that element be called the *inverse* of x, and be denoted

by x^{-1}. Prove that, for any elements x and y, $(x * y)^{-1} = y^{-1} * x^{-1}$. Justify every statement you make.

Solution:

$$\begin{aligned}
(x * y) * \left(y^{-1} * x^{-1}\right) &= \left((x * y) * y^{-1}\right) * x^{-1} \quad \text{by I.} && (1193)\\
&= \left(x * \left(y * y^{-1}\right)\right) * x^{-1} \quad \text{by I.} && (1194)\\
&= (x * e) * x^{-1} \quad \text{by III., for } y && (1195)\\
&= (x) * x^{-1} \quad \text{by II.} && (1196)\\
&= e \quad \text{by III., for } x && (1197)
\end{aligned}$$

In a similar way it may be proved that $(y^{-1} * x^{-1}) * (x * y) = e$. Thus we have proved that $y^{-1} * x^{-1}$ has the properties of an inverse for $x * y$. But, as the inverse for $x * y$ is unique, this product must be that inverse!

A number of students attempted to apply an unacceptable method in solving this problem; one would have expected that students who had passed 189-240A would not make this mistake. It is, in general, not a valid proof technique to assume the statement you wish to prove (here, the statement $(x * y)^{-1} = y^{-1} * x^{-1}$), and, by proving that this statement would imply a true statement, conclude that the assumed statement must have been true. As an example of the fallacy in such a proof, in general, consider the following defective proof that $1 = 2$:

$$\begin{aligned}
& 1 = 2 \quad \text{hypothesis}\\
\Rightarrow\ & 0 \times 1 = 0 \times 2 \quad \text{multiply both sides by 0}\\
\Rightarrow\ & 0 = 0 \quad \text{a tautology}
\end{aligned}$$

It *is* possible to use such a method, however, if every step of the proof is reversible; that is, if the reasoning that permits the inference of one line from its predecessor is susceptible of an inverse reasoning that permits the inference of the preceding line from its successor. However, no such reasoning would be acceptable unless the logical equivalence of the two statements was very clearly stated and proved.

V. (a) State without proof the formula for the Euler totient function $\varphi(n)$, where n is a positive integer with prime decomposition $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where p_1, p_2, $\dots$, p_k are distinct primes, and $r_i > 0$ $(i = 1, 2, \dots, k)$.

(b) Showing all your work, carefully determine all positive integers n such that $\varphi(n) = 10$.

(c) Describe briefly one commutative ring that has exactly 10 units.

Solution:

(a) $\varphi\left(p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}\right) = \prod_{i=1}^{k} p_i^{r_i-1}(p_i-1)\,.$

(b) [This is not a type of problem in which the class was "drilled", although it was discussed in class briefly when the formula for the totient function was derived using Inclusion-Exclusion. The intention is that, knowing the formula, students attack this problem without advance drill, and without slick methods; but the solution should still be *correct*! There are basically two stages to such a proof: First one must show that there are only finitely many natural numbers n for which $\varphi(n)$ could have the given value. Then one must elimnate those n for which the value is not the desired one. To receive full marks students were expected to do both of these things.] If p is a prime dividing n, then $p-1$ must divide $\varphi(n) = 10$; and, in particular, $p-1 \leq 10$, so $p \leq 11$. Examining the primes with this last property — i.e. the primes 2, 3, 5, 7, 11 — we can eliminate 5 and 7 since 4 and 6 do not divide 10. Thus n has the form $n = 2^{r_1}3^{r_2}11^{r_3}$. Here r_3 cannot exceed 1, since a higher power would imply that $11|\varphi(n)$; for the same reason r_2 cannot exceed 1; but r_1 could be as great as 2, since $2^{2-1}|\varphi(n)$. This means that there are $3\times 2\times 2$ candidates for integers where the Euler function could be equal to 10. We could continue the present line of reasoning to further restrict the list of candidates; but it suffices to compute the value of φ for each of these candidates to complete the solution:

r_1	r_2	r_3	n	$\varphi(n)$
0	0	0	1	1
0	0	1	11	10
0	1	0	3	2
0	1	1	33	20
1	0	0	2	1
1	0	1	22	10
1	1	0	6	2
1	1	1	66	20
2	0	0	4	2
2	0	1	44	20
2	1	0	12	4
2	1	1	132	40

Thus 11 and 22 are the only positive integers n such that $\varphi(n) = 10$.

(c) We have proved that there are exactly 10 units in each of $\mathbb{Z}_{11}$ and $\mathbb{Z}_{22}$.

VI. (a) State without proof the formula for the Euler totient function $\varphi(n)$, where n is a positive integer with prime decomposition $n = p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$, where p_1, p_2,

$\ldots$, p_k are distinct primes, and $r_i > 0$ $(i = 1, 2, \ldots, k)$.

(b) Showing all your work, carefully determine all positive integers n such that $\varphi(n) = 4$.

(c) Find two non-isomorphic rings that both have exactly 4 units.

Solution:

(a) $\varphi\left(p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}\right) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)\,.$

(b) [This is not a type of problem in which the class was "drilled", although it was discussed in class briefly when the formula for the totient function was derived using Inclusion-Exclusion. The intention is that, knowing the formula, students attack this problem without advance drill, and without slick methods; but the solution should still be *correct*! There are basically two stages to such a proof: First one must show that there are only finitely many natural numbers n for which $\varphi(n)$ could have the given value. Then one must elimnate those n for which the value is not the desired one. To receive full marks students were expected to do both of these things.] If p is a prime dividing n, then $p - 1$ must divide $\varphi(n) = 4$; and, in particular, $p - 1 \leq 4$, so $p \leq 5$. The primes with this last property are 2, 3, 5. Thus n has the form $n = 2^{r_1} 3^{r_2} 5^{r_3}$. Here r_3 cannot exceed 1, since a higher power would imply that $5|\varphi(n)$; for the same reason r_2 cannot exceed 1; but r_1 could be as great as 3, since $2^{3-1}|\varphi(n)$. Thus there are at most $4 \times 2 \times 2 = 16$ integers that are candidates. We could reduce the number of candidates by more careful reasoning; but we will simply compile a table and read off from it the integers

having $\varphi = 4$.

r_1	r_2	r_3	n	$\varphi(n)$
0	0	0	1	1
0	0	1	5	4
0	1	0	3	2
0	1	1	15	8
1	0	0	2	1
1	0	1	10	4
1	1	0	6	2
1	1	1	30	8
2	0	0	4	2
2	0	1	20	8
2	1	0	12	4
2	1	1	60	16
3	0	0	8	4
3	0	1	40	16
3	1	0	24	8
3	1	1	120	32

Thus the solutions to the equation $\varphi(n) = 4$ are $n = 5, 8, 10, 12$.

(c) All four of the rings $\mathbb{Z}_5$, $\mathbb{Z}_8$ $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$, have exactly 4 units (respectively $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$; $[1]_8$, $[3]_8$, $[5]_8$, $[7]_8$; $[1]_{10}$, $[3]_{10}$, $[7]_{10}$, $[9]_{10}$; $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$). But these rings cannot be isomorphic, since they have different cardinalities.

G.7 2001 Homework Tests

Problem / Test Version	1	2	3
1	I	III	VI
2	II	IV	V
3	I	IV	VI
4	II	III	V

I. Consider the following binary relation, denoted by $\approx$, on $\mathbb{Z}$. Showing your work, either

- Prove that $\approx$ is an equivalence relation on $\mathbb{Z}$; or
- Prove that $\approx$ is *not* an equivalence relation on $\mathbb{Z}$. In the case where $\approx$ *is* an equivalence relation, you are also asked to describe the equivalence classes.

$$a \approx b \quad \Longleftrightarrow \quad a+b \text{ is divisible by 2.}$$

Solution: (cf. Assignment 1, Problem 1) This relation is, indeed, an equivalence relation. A sum of integers is divisible by 2 iff they are both even or they are both odd. For any integer a, $a+a$ is even; hence $\approx$ is reflexive. If $a+b$ is even, then $b+a$ has the same value and must also be even; hence $\approx$ is symmetric. And, if $a+b$ and $b+c$ are both even, then their sum, $a+2b+c$ has the same "parity" (evenness or oddness) as $a+c$ — i.e. it is congruent to $a+c$ modulo 2 — thus $a \approx c$; we have proved transitivity. There are two residue classes: the evens, $[0]_2$, and the odds, $[1]_2$.

II. Consider the following binary relation, denoted by $\approx$, on $\mathbb{Z}$. Showing your work, either

- Prove that $\approx$ is an equivalence relation on $\mathbb{Z}$; or
- Prove that $\approx$ is *not* an equivalence relation on $\mathbb{Z}$. In the case where $\approx$ *is* an equivalence relation, you are also asked to describe the equivalence classes.

$$a \approx b \quad \Longleftrightarrow \quad a^2 = b^2$$

Solution: (cf. Assignment 1, Problem 1) This relation is an equivalence relation.

(a) **Reflexivity:** Any integer a has the property that $a^2 = a^2$; hence $a \approx a$; thus $\approx$ is reflexive.

(b) **Symmetry:** Suppose that $a \approx b$, i.e. that $a^2 = b^2$. Then $b^2 = a^2$, so $b \approx a$; thus $\approx$ is symmetric.

(c) **Transitivity:** Suppose that $a \approx b$ and $b \approx c$, i.e. that $a^2 = b^2$ and that $b^2 = c^2$; then $a^2 = c^2$, so $a \approx c$; this proves that $\approx$ is transitive.

All but one of the equivalence classes are the pairs of integers having the same square. This is precisely the sets of unordered pairs of the form $\{-n, n\}$ where $n = 1, 2, \ldots$. The exception is the set $\{0\}$, which has cardinality 1.

III. If $(a, b^2) = 24$, determine the possible values of (a, b). You are expected to provide a careful justification of your conclusion.

Solution: (cf. Assignment 1, Problem 4)[1052] Since $24 = 2^3 3^1$, the primes 2 and 3 must figure in the prime decomposition of both a and b, and no other prime

[1052]The intention was that student should justify precisely every step in their proofs. Many of the solutions were defective in that some necessary justifying statements were not present. Nevertheless, it was decided to grade the question very liberally. (The purpose of this comment is to make it clear that, in many cases, full marks were awarded for a solution that was not complete.)

may appear in the decompositions of both of a and b. Hence we may assume that $a = 2^{r_2}3^{r_3}k$ and $b = 2^{s_2}3^{s_3}\ell$, where $(k,\ell) = 1$, $(k,6) = (\ell,6) = 1$. With these decompositions we find that $2^3 3^1 = (a,b^2) = 2^{\min\{r_2,2s_2\}}3^{\min\{r_3,2s_3\}}$, so $\min\{r_2,2s_2\} = 3$, $\min\{r_3,2s_3\} = 1$. In each case the second of the two integers listed is even — but the two minima are both odd. Hence $3 = r_2 < 2s_2$ and $1 = r_3 < 2s_3$; thus $s_2 \geq 2$ and $s_3 \geq 1$. It follows that $(a,b) = 2^{\min\{r_2,s_2\}}3^{\min\{r_3,s_3\}} = 2^{\min\{3,s_2\}}3^{\min\{1,s_3\}}$. Here we obtain different values when $s_2 = 2$ and $s_2 \geq 3$; all values of $s_3 \geq 1$ give the $\min(1,s_3) = 1$. The values possible are, therefore $(a,b) = 2^2 3^1$ and $(a,b) = 2^3 3^1$. For example, the first case is realized when $a = 24$, and $b = 12$, $(a,b^2) = 24$, but $(a,b) = 12$; the second case is realized when $a = 24$ and $b = 24$, where $(a,b^2) = 24$, but $(a,b) = 24$.

IV. (a) Construct a multiplication table for the units in the ring $\mathbb{Z}_9$ $(= \mathbb{Z}/9\mathbb{Z})$. For at least one row — other than the row for the multiplicative identity element — you should show your calculations in detail.

(b) For each unit, show how you can use your table to determine its inverse.

Solution: (cf. multiplication table in Assignment 3, Problem 1)

(a)

$\cdot$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

In each case the product $[a]_9 \cdot [b]_9$ is computed as $[ab]_9$; it is necessary to reduce ab modulo 9 in order to demonstrate which of the named units in the labelling row that it is equal to.

(b) The inverse of $[a]_9$ is the element $[b]_9$ heading the column in which, in the row headed by $[a]_9$, the entry is $[1]_9$. Thus we may read off from the table that

$$[1]_9^{-1} = [1]_9,\ [2]_9^{-1} = [5]_9,\ [4]_9^{-1} = [7]_9,\ [5]_9^{-1} = [2]_9,\ [7]_9^{-1} = [4]_9,\ [8]_9^{-1} = [8]_9\,.$$

V. Let $M_2(\mathbb{Z}_6)$ denote the ring of 2×2 matrices with entries from the ring $\mathbb{Z}_6$ of congruence classes modulo 6. Consider the function $\tau : M_2(\mathbb{Z}_6) \to \mathbb{Z}_6$ defined by

$$\begin{pmatrix} [a]_6 & [b]_6 \\ [c]_6 & [d]_6 \end{pmatrix} \mapsto [a]_6 + [d]_6\,.$$

Carefully showing all your work, determine whether τ is a homomorphism.

Solution: (cf. Assignment 3, Problem 4) This function is usually called the *trace*. It fails to be a homomorphism between rings with a multiplicative identity because the identity matrix maps on to $[1]_6 + [1]_6 = [2]_6$, which is not the identity of $\mathbb{Z}_6$. While there was no need to prove it here, one can observe that the addition properties of a homomorphism does hold for τ. Let $\begin{pmatrix} [a]_6 & [b]_6 \\ [c]_6 & [d]_6 \end{pmatrix}$ and $\begin{pmatrix} [a']_6 & [b']_6 \\ [c']_6 & [d']_6 \end{pmatrix}$ be any two matrices. Then

$$\begin{aligned} & \tau\left(\begin{pmatrix} [a]_6 & [b]_6 \\ [c]_6 & [d]_6 \end{pmatrix} + \begin{pmatrix} [a']_6 & [b']_6 \\ [c']_6 & [d']_6 \end{pmatrix}\right) \\ = & \begin{pmatrix} [a]_6 + [a']_6 & [b]_6 + [b']_6 \\ [c]_6 + [c']_6 & [d]_6 + [d']_6 \end{pmatrix} \quad \text{definition of sum of matrices} \\ = & ([a]_6 + [a']_6) + ([d]_6 + [d']_6) \quad \text{definition of } \tau \\ = & ([a]_6 + [d]_6) + ([a']_6 + [d']_6) \quad \text{commutativity, associativity of } + \\ = & \tau\left(\begin{pmatrix} [a]_6 & [b]_6 \\ [c]_6 & [d]_6 \end{pmatrix}\right) + \tau\left(\begin{pmatrix} [a]_6 & [b]_6 \\ [c]_6 & [d]_6 \end{pmatrix}\right) \end{aligned}$$

However, the multiplicative property does not hold:

$$\tau(I \times I) = \tau(I) = [2]_6 \neq [4]_6 = [2]_6 \times [2]_6 = \tau(I) \times \tau(I)\,.$$

VI. Let $M_2(\mathbb{Z}_3)$ denote the ring of 2×2 matrices with entries from the ring $\mathbb{Z}_3$ of congruence classes modulo 3. Consider the function $\lambda : M_2(\mathbb{Z}_3) \to \mathbb{Z}_3$ defined by

$$\begin{pmatrix} [a]_3 & [b]_3 \\ [c]_3 & [d]_3 \end{pmatrix} \mapsto [ad - bc]_3\,.$$

Carefully showing all your work, determine whether λ is a homomorphism.

Solution: (cf. Assignment 3, Problem 4) This function is usually called the *determinant*. It fails to be a homomorphism between rings with a multiplicative identity because the determinant of a sum of matrices is not always the sum of the determinants. For example, matrices $\begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [0]_3 \end{pmatrix}$ and $\begin{pmatrix} [0]_3 & [0]_3 \\ [0]_3 & [1]_3 \end{pmatrix}$ both have determinant equal to $[0]_3$; but their sum is the identity matrix, and its determinant is $[1]_3$. While there was no need to prove it here, one can observe that the other properties of a homomorphism do hold for this function. The determinant of the identity matrix is $[1 \cdot 1 - 0 \cdot 0]_3 = [1]_3$; and the determinant of a product of matrices can be shown to be the product of the determinants, using methods standard in the courses on linear algebra which are prerequisites to this course.

H Some examinations from previous years, without solutions

H.1 Final Examination, Spring, 1991

1. Where possible, give an example of each of the following; or provide a short, lucid proof that no such example can exist. [5 MARKS EACH]

   (a) [5 MARKS] five nonisomorphic semigroups, each containing exactly 2 elements

   (b) [5 MARKS] a system of congruences of the form

   $$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ x &\equiv a_4 \pmod{m_4} \end{aligned}$$

   having a solution x with the property that none of x, $x+1$, $x+2$, $x+3$, $x+4$ is square free

   (c) [5 MARKS] three distinct elements a, b, c of some monoid $(\mathfrak{A}, *, e)$ such that $|\mathfrak{A}| > 10$ and $a * b = e = c * a$

   (d) [5 MARKS] an isomorphism from some group $(\mathfrak{A}, *, e)$ to itself (i.e. an *automorphism* of $(\mathfrak{A}, *, e)$) which is not an inner automorphism

   (e) [5 MARKS] a subset $\mathfrak{S}$ of some finite non-abelian group $(\mathfrak{A}, *, e)$ which is closed under composition $(*)$, but not under the taking of inverses

   (f) [5 MARKS] a finite abelian group that is not isomorphic to a direct sum of cyclic groups

2. (a) [10 MARKS] Prove each of the following properties of the greatest common divisor:

      i. If $a = b$, $(a, b) = a$.
      ii. If a and b are both even, $(a, b) = 2\left(\frac{a}{2}, \frac{b}{2}\right)$.
      iii. If just one — say b — is even, $(a, b) = \left(a, \frac{b}{2}\right)$.
      iv. If neither a nor b is even, and $a > b$, $(a, b) = (a - b, b)$.

   (b) [5 MARKS] Explain how these properties may be applied to design an algorithm for finding the greatest common divisor, and illustrate your discussion with the pair of integers 2613, 2171.

   (c) [5 MARKS] Explain one possible advantage of the Euclidean algorithm over this method.

3. (a) [5 MARKS] Define the group $\mathcal{D}_4$, which operates on the set $\mathfrak{A} = \{1, 2, 3, 4\}$, and list all of its elements in disjoint cycle notation.

   (b) [5 MARKS] Define what is meant by the *right regular representation* R of $\mathcal{D}_4$ in $\mathcal{S}_{\mathcal{D}_4}$, and prove that it is a one-to-one homomorphism.

   (c) [5 MARKS] Let $\mathcal{G}$ denote the subgroup of $\mathcal{D}_4$ generated by (12)(34). Determine the left and right coset decompositions of $\mathcal{D}_4$ with respect to this subgroup. Determine whether or not it is true that $\mathcal{G} \trianglelefteq \mathcal{D}_4$.

   (d) [5 MARKS] Determine disjoint cycle decompositions for all elements of period 4 in the image of R in $\mathcal{S}_{\mathcal{D}_4}$.

4. (a) [5 MARKS] Prove that 3 is a primitive root modulo 4.

   (b) [10 MARKS] List the moduli in the set $\{n : n \in \mathbb{Z}, 1 \leq n \leq 12\}$ which have a primitive root, giving a reason in each case.

   (c) [10 MARKS] Prove Leibnitz's test for primality:

   $$n \quad \text{is prime iff} \quad (n-2)! \equiv 1 \pmod{n}$$

5. [20 MARKS] Explain in detail the functioning of an RSA cryptosystem.

6. Let $\mathcal{R} = (\mathfrak{A}, +, 0, *, e)$ be a ring with unity.

   (a) [5 MARKS] Define what is meant by a *(two-sided) ideal* of $\mathcal{R}$.

   (b) [10 MARKS] Let $(\mathfrak{B}, +, 0) \leq (\mathfrak{A}, +, 0)$. Show that the "definition"

   $$(a_1 + \mathfrak{B}) * (a_2 + \mathfrak{B}) = (a_1 * a_2) + \mathfrak{B}$$

   is ambiguous if and only if $\mathfrak{B}$ is not an ideal of $\mathcal{R}$.

   (c) [10 MARKS] Show that $(\mathbb{Z}, +, 0)$ is a principal ideal ring.

H.2 Final Examination, Spring, 1997

1. (a) [5 MARKS] Prove or disprove: the operation $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ defined by

   $$f(a, b) = (a + b)^2$$

   is associative.

   (b) [5 MARKS] Give the Cayley table for two non-isomorphic groups of order 6. Show from the tables — do not quote theorems — that the groups you have described are not isomorphic.

2. [10 MARKS] Determine the *left* coset decomposition of the Alternating Group A_4 with respect to the subgroup $\langle(123)\rangle$.

3. (a) [4 MARKS] Prove or disprove: The set of all square 2×2 matrices with complex entries forms a non-abelian group under the operation of matrix multiplication.

   (b) [6 MARKS] Prove or disprove: $1 - 2i$ is the square of a Gaussian integer.

4. (a) [5 MARKS] Let G be a given abelian group, with operation denoted by $+$. Show carefully that it is possible to make G into a ring R by fixing some one particular element $u \in G$, and defining $ab = u \ \forall a \forall b$. Determine the possible values that u can have.

   (b) [5 MARKS] Show briefly that there exist at least 6 non-isomorphic rings with 4 elements.

5. (a) [6 MARKS] Factorize the polynomial $a(x) = (x^5+1)^2$ into monic polynomials which are irreducible over $\mathbb{Z}_2$. You are expected to *prove* that each of your factors is irreducible.

   (b) [4 MARKS] Discuss briefly the construction of a finite field of order greater than 2, using one of the irreducible factors found in (a). List the elements of this field, and calculate, for some non-zero element u distinct from 1, u^4, and u^{15}.

6. [10 MARKS] Showing all your work, determine all integers x which satisfy all of the following conditions simultaneously:

$$\begin{aligned} x &\equiv 5 \pmod 7 \\ 2x &\equiv 11 \pmod{19} \\ x+3 &\equiv 7 \pmod 5 \end{aligned}$$

7. [10 MARKS] Showing all your work, determine the smallest positive integer x such that $3^{1024} \equiv x \pmod{77}$.

8. [10 MARKS] Determine the polynomial $f(x) \in \mathbb{C}[x]$ whose roots are *the negatives of the squares* of the roots of the polynomial $g(x) = x^2 + 2x + i \in \mathbb{C}[x]$; i.e., iff α is a root of $g(x)$, $-\alpha^2$ is a root of $f(x)$.

H.3 Supplemental/Deferred Examination, August, 1997

1. (a) [4 MARKS] Give the Cayley table for two non-isomorphic groups of order 4. Show from the tables — do not quote theorems — that the groups you have described are not isomorphic.

(b) [6 MARKS] Let A_4 be the Alternating Group on the symbols $\{1, 2, 3, 4\}$. Showing all your work, determine whether the set $\{g^2 | g \in A_4\}$ is a subgroup of A_4.

2. [10 MARKS] Determine the *left* coset decomposition of the Symmetric Group S_4 of permutations of $\{1, 2, 3, 4\}$ with respect to the subgroup $\langle (12), (34) \rangle$.

3. (a) [5 MARKS] Prove or disprove: the set of non-zero complex numbers of the form $a + b^2 i$, where a and b are rational numbers, not both zero, form a group under the operation of multiplication.

   (b) [5 MARKS] Prove or disprove: In any ring R the function that maps any element r on to $-r$ is a ring automorphism (i.e. an isomorphism of R with itself).

4. (a) [6 MARKS] Determine all rings R with the property that $ab = a$ for all $a \in R$, $b \in R$.

   (b) [4 MARKS] Give an example of a finite commutative ring with unity which is not an integral domain.

5. (a) [5 MARKS] Showing all your work, determine all polynomials of the form $x^4 + ax + 1$, where $a \in \mathbb{Z}_2$, which are irreducible over $\mathbb{Z}_2$.

   (b) Select one of the irreducible polynomials determined in part (a).

      i. [3 MARKS] Discuss briefly the construction of a finite field using this polynomial.

      ii. [2 MARKS] List the elements y of this field such that $y^4 = 1$.

6. [10 MARKS] Showing all your work, determine all integers x which satisfy all of the following conditions simultaneously:

$$\begin{aligned} x &\equiv 5 \pmod{14} \\ 2x &\equiv 11 \pmod{13} \\ x^2 + 6 &\equiv 7 \pmod{5} \end{aligned}$$

7. [10 MARKS] Showing all your work, determine the smallest positive integer x such that

$$x \equiv 7^{1000} \pmod{65}\,.$$

8. (a) [5 MARKS] Prove that, if a is rational and b is not rational, then $a + b$ is not rational.

   (b) [5 MARKS] Determine the polynomial $f(x) \in \mathbb{C}[x]$ whose roots are the excesses over 2 of each the roots of the polynomial $g(x) = x^3 - ix^2 + (1 + 2i) \in \mathbb{C}[x]$; i.e., iff α is a root of $g(x)$, $2 - \alpha$ is a root of $f(x)$.

H.4 Final Examination, Spring, 1998

1. (a) [5 MARKS] Determine the value of the product

$$(1234567)^2(3456712)^{-1}(14)(253)(76)(3456712)(1234567)^{-2}$$

in S_7.

(b) [5 MARKS] Prove or disprove: If G is any group, the subset $\{g^3 | g \in G\}$ is a subgroup of G.

2. (a) [8 MARKS] Showing all your work, use the Euclidean algorithm to determine the inverse of the polynomial $1+x+x^3$ in the field $\mathbb{Z}_2[x]/(1+x+x^2+x^3+x^4)$. You may assume it is known that $1+x+x^2+x^3+x^4$ is irreducible over $\mathbb{Z}_2$.

(b) [7 MARKS] Showing all your work, determine an integer having remainders 2, 3, 2 when divided by 5, 7, 3 respectively. Your solution should be systematic, so that the same method, with appropriate changes, could be applied to any set of 3 remainders and any set of 3 relatively prime moduli.

3. (a) [6 MARKS] Showing all your work, prove that a positive integer $n > 2$ is prime only if

$$(n-2)! - 1 \equiv 0 \pmod{n}.$$

(b) [4 MARKS] Determine all positive integers n such that $\varphi(n) = 15$, where φ is the *Euler totient function*.

4. (a) [4 MARKS] Prove that the polynomial $1+x+x^2$ is irreducible over $\mathbb{Z}_2$.

(b) [6 MARKS] Using the polynomial $1+x+x^2$ to construct the field $\mathbb{F}_4$ of order 4, show, without proof, the addition and multiplication tables of that field.

(c) [5 MARKS] One may construct the field of quotients of $\mathbb{F}_4$. Describe precisely what are the elements of that field of quotients, and show the injection that embeds $\mathbb{F}_4$ into the field of quotients.

5. (a) [7 MARKS] Prove carefully that there is no rational square root for 3.

(b) [3 MARKS] Referring to your proof in the preceding part, show precisely where your argument would break down if you attempted to apply it to the square root of 4.

6. [10 MARKS] Describe four groups of order 8, no two of which are isomorphic. You are expected to prove that no two of the groups are isomorphic.

7. (a) [5 MARKS] Prove or disprove: On any set S, a binary operation $f : S \times S \to S$ can have no more than one identity element.

(b) [5 MARKS] Suppose that $S = \{a_1, a_2, ..., a_n\}$, where $|S| = n$, and $f : S \times S \to S$ is a function such that

$$(\forall a \in S)(\forall b \in S)(\forall c \in S)[f(f(a,b),c) = f(a,f(b,c))]\,. \tag{1198}$$

Let T be a set such that $S \subset T$, where $\{a_{n+1}\} = T - S$. Show *carefully* that there exists a function $g : T \times T \to T$ such that

$$(\forall a \in T)(\forall b \in T)(\forall c \in T) \quad [g(g(a,b),c) = g(a,g(b,c))]\,, \tag{1199}$$
$$(\forall a \in S)(\forall b \in S) \quad [g(a,b) = f(a,b)]\,, \tag{1200}$$
$$(\forall a \in T) \quad [g(a_{n+1},a) = a]\,, \tag{1201}$$
$$(\forall b \in T) \quad [g(b,a_{n+1}) = b]\,. \tag{1202}$$

8. (a) [5 MARKS] Prove or disprove: There exists a positive integer n for which there is no ring R such that $|R| = n$.

   (b) [5 MARKS] Prove or disprove: If D is an integral domain of order $n \geq 2$, then the direct sum $D \times D$ cannot be an integral domain.

9. (a) [5 MARKS] Give an example of a group G and a positive integer k which divides $|G|$, such that no element of G has order k; or prove that no such example exists.

   (b) [5 MARKS] Give an example of a right coset of $\langle(23)\rangle$ in S_3 which is not a left coset of $\langle(23)\rangle$ in S_3; or prove that no such example exists.

H.5 Supplemental/Deferred Examination, August, 1998

1. (a) [5 MARKS] Determine the value of the product

$$(14)(1234567)^2(14)(253)(76)(1234567)^{-2}(76)$$

   (b) [5 MARKS] Prove or disprove: If S is any non-empty set, the set of all functions $f : S \to S$ is a subgroup of $\mathrm{Sym}(S)$.

2. (a) [8 MARKS] Showing all your work, use the Euclidean algorithm to determine the inverse of the polynomial $x^2 + x^3$ in the field $\mathbb{Z}_2[x]/(1 + x + x^2 + x^3 + x^4)$. You may assume it is known that $1 + x + x^2 + x^3 + x^4$ is irreducible over $\mathbb{Z}_2$.

   (b) [7 MARKS] Showing all your work, determine an integer having remainders 4, 1, 1 when divided by 5, 7, 3 respectively. Your solution should be systematic, so that the same method, with appropriate changes, could be applied to any set of 3 remainders and any set of 3 moduli.

3. (a) [6 MARKS] Prove or disprove: For any positive integers a and n, $a^{\varphi(n)} \equiv 1 \pmod{n}$, where φ is the *Euler totient function*.

   (b) [9 MARKS] Showing all your work, determine all positive integers n such that $\varphi(n) = 4$.

4. (a) [4 MARKS] Prove that the polynomial $1 + x^2$ is irreducible over $\mathbb{Z}_3$.

   (b) [6 MARKS] Using the polynomial $1 + x^2$ to construct the field $\mathbb{F}_9$ of order 9, show, without proof, the addition and multiplication tables of that field.

5. [10 MARKS] Describe four groups of order 12, no two of which are isomorphic, and at least 2 of which are not Abelian. You are expected to prove that no two of the groups you describe are isomorphic.

6. (a) [5 MARKS] Prove that, on any set S, a binary operation $f : S \times S \to S$ can have no more than one identity element.

   (b) [5 MARKS] Suppose that $S = \{a_1, a_2, ..., a_n\}$, where $|S| = n$, and $f : S \times S \to S$ is a given function. Let T be a set with $|S|+1$ elements, where $a_{n+1} \in T - S$. Show *carefully* that there exists a function $g : T \times T \to T$ such that

$$(\forall a \in S)(\forall b \in S) \quad [g(a, b) = f(a, b)], \tag{1203}$$

$$(\forall a \in T) \quad [g(a_{n+1}, a) = a], \tag{1204}$$

$$(\forall b \in T) \quad [g(b, a_{n+1}) = b]. \tag{1205}$$

   i.e. that a_{n+1} is an identity element for the operation g.

   (c) [5 MARKS] Prove or disprove: If the operation f described in the preceding part already has an identity element, the operation g defined on T will have two identity elements.

7. (a) [5 MARKS] Prove or disprove: For any positive prime p there exists, up to isomorphism, only one ring with p elements.

   (b) [5 MARKS] Prove or disprove: Non-singular (invertible) 2×2 matrices with entries from $\mathbb{R}$ form a ring under the usual operations of matrix addition and matrix multiplication.

8. (a) [5 MARKS] Give an example of a group G and a positive integer k which divides $|G|$, such that no subgroup of G has order k; or prove that no such example exists.

   (b) [5 MARKS] Give an example of a right coset of A_4 in S_4 which is not a left coset of A_4 in S_4; or prove that no such example exists.

H.6 Final Examination, Spring, 1999

1. (a) [5 MARKS] Prove or disprove: If $(\mathfrak{A}, *, e)$ is any group, the function $f : \mathfrak{A} \to \mathfrak{A}$ defined by $a \mapsto a^2$ is a homomorphism.

   (b) [5 MARKS] Prove or disprove: The order of every subgroup of S_5 is divisible by 5.

2. [10 MARKS] Showing all your work, determine all integer solutions to the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{74} \\ x &\equiv 19 \pmod{22} \end{aligned}$$

   (Where inverses are required to a modulus exceeding 10, they should be found using the Euclidean Algorithm — not by inspection.)

3. [10 MARKS] Showing all your work, *carefully* determine all positive integers n such that $\phi(n) = 4$, where ϕ is the Euler totient function.

4. (a) [7 MARKS] Prove that the polynomial $1 + x + x^3$ is irreducible over $\mathbb{Z}_2$.

   (b) [8 MARKS] Using the polynomial $1 + x + x^3$ to construct a field of order 8, show the multiplication table of that field.

5. Suppose that $*$ is a binary operation on a set $\mathfrak{A}$, having the following properties:

$$(\exists b)(\forall c)[c * b = c = b * c]$$

$$(\forall x)(\forall y)(\forall z)[x * (y * z) = (x * z) * y]$$

   where the universe for all quantifiers $\exists$, $\forall$ is $\mathfrak{A}$. Showing <u>all</u> your work, determine carefully

   (a) [6 MARKS] whether $*$ is associative.

   (b) [4 MARKS] whether $*$ is commutative.

6. [10 MARKS] Describe 5 groups of order 36, no two of which are isomorphic. You are expected to prove that no two of your 5 groups are isomorphic.

7. (a) [4 MARKS] Prove or disprove: $\mathbb{Z}_6$ is a field.

   (b) [6 MARKS] Prove or disprove: In the ring $\mathbb{R}\{x\}$ of formal power series with real coefficients, the only element which has no multiplicative inverse is 0 (i.e. the power series $0x^0 + 0x^1 + 0x^2 + \ldots + 0x^n + \ldots$) .

8. (a) [7 MARKS] Prove that, for any integers a and n both greater than 1, $a^{4n} + a^{2n} + 1$ is composite.

   (b) [8 MARKS] Showing all your work, determine a non-negative integer a such that $a \equiv 3^{50000} \pmod{3^4+3^2+1}$ and $0 \leq a < 100$. You are expected to carry out these calculations by hand, and to use techniques which do not require working with large integers (with the exception of the exponent 50,000).

9. (a) [5 MARKS] For the element $a = (13)$ of the permutation group whose set of elements is $\{e, (12), (13), (23), (123), (132)\}$, determine the right translation R_a and the left translation L_a, and express them both as permutations of the group elements, in disjoint cycle notation.

   (b) [5 MARKS] Give an example of a right coset of $\langle (23)(14) \rangle$ in A_4 which is not a left coset of $\langle (14)(23) \rangle$ in A_4; or prove that no such example exists.

H.7 Supplemental/Deferred Examination, Spring, 1999

1. (a) [5 MARKS] Prove or disprove: *If $(\mathfrak{A}, *, e)$ is any group, the function $f : \mathfrak{A} \to \mathfrak{A}$ defined by $a \mapsto a^{-1}$ is a homomorphism.*

   (b) [5 MARKS] Prove or disprove: *If, in any group G, a positive integer d divides the order of G, then G contains an element of period (= order) d.*

2. [10 MARKS] Showing all your work, determine all integer solutions to the system of congruences

$$\begin{aligned} x &\equiv 28 \pmod{51} \\ x &\equiv 24 \pmod{33} \end{aligned}$$

   (Where inverses are required to a modulus exceeding 10, they should be found using the Euclidean Algorithm — not by inspection.)

3. [10 MARKS] Showing all your work, *carefully* determine all positive integers n such that $\phi(n) = \phi(2n)$, where ϕ is the Euler totient function.

4. (a) [5 MARKS] Determine whether the polynomial $1 + x + x^3$ is irreducible over $\mathbb{Z}_3$.

   (b) [5 MARKS] Prove or disprove: *If a polynomial $f(x)$ is irreducible over $\mathbb{Z}_3$, then it is irreducible over $\mathbb{Z}_2$.*

5. (a) [10 MARKS] Suppose that $*$ is a commutative binary operation on a set $\mathcal{S} = \{w, x, y, z\}$, and that $\mathcal{S}$ contains an identity for $*$. Suppose also that

every element of $\mathcal{S}$ has an inverse. If it is possible, complete the following Cayley table for $*$, *justifying every entry you add to the table*; *or* prove that it is impossible to complete the table:

$*$	w	x	y	z
w	y			x
x	z	w		
y				
z				z

(b) [5 MARKS] Prove by a specific example that $*$ is not associative.

6. [10 MARKS] Describe 3 monoids which each contain 3 elements; no two of the monoids should be isomorphic. You are expected to *prove* that no two of your 3 monoids are isomorphic.

7. (a) [5 MARKS] Prove or disprove: $\mathbb{Z}_8$ is a field.

   (b) [5 MARKS] Prove or disprove: The set of 2×2 non-singular (invertible) matrices with real entries is a ring, where matrix addition and multiplication are defined in the usual way.

8. (a) [5 MARKS] Let $\mathfrak{B} = \{1, 2, 3, 4, 5\}$. For $i = 1, 2, 3, 4, 5$, define $\mathfrak{B}_i = \mathfrak{B} - \{i\}$, and let $\mathcal{G}_i$ denote the alternating group (of structure A_4) of even permutations of the set $\mathfrak{B}_i$ ($i = 1, 2, 3, 4, 5$). Prove or disprove: *If $\mathcal{G}$ is the alternating group of even permutations of the set $\mathfrak{B}$, then*

$$\mathcal{G} = \bigcup_{i=1}^{5} \mathcal{G}_i \, .$$

   (b) [5 MARKS] In the group S_5 of all permutations of $\mathfrak{B}$, give an example of a right coset of $\mathcal{G}$ which is not a left coset, or prove that no such example exists.

H.8 Final Examination, Spring, 2000

1. (a) [5 MARKS] Prove or disprove: If $(\mathfrak{A}, *, e)$ is any non-abelian group, the function $f : \mathfrak{A} \to \mathfrak{A}$ defined by $a \mapsto a^2$ is not a homomorphism.

   (b) [5 MARKS] Prove or disprove: If $(\mathfrak{A}, *, e)$ is any group, any homomorphism $f : (\mathfrak{A}, *, e) \to (\mathfrak{A}, *, e)$ has the property that, for any positive integer k, elements of period (order) k are always mapped onto elements of period (order) k.

2. [10 MARKS] Showing all your work find *all* integer solutions to the system of congruences

$$\begin{aligned} x &\equiv -7 \pmod 3 \\ x &\equiv -8 \pmod 5 \\ x &\equiv -9 \pmod{11} \end{aligned}$$

3. (a) [5 MARKS] Prove or disprove: Any semigroup which is not a monoid is non-commutative.

   (b) [5 MARKS] Prove or disprove: If elements x and y of a monoid $(\mathfrak{A}, *, e)$ are both invertible, then $x * y$ is invertible, and

$$(x * y)^{-1} = y^{-1} * x^{-1} .$$

4. (a) [4 MARKS] Prove that the polynomial $x^2 + 2x - 1$ is irreducible over $\mathbb{Z}_3$.

   (b) [6 MARKS] Determine 3 rows of the multiplication table of a field $\mathbb{F}$ of order 9 over which the polynomial $x^2 + 2x - 1$ has a root. (You may choose any 3 rows, but all entries in the rows you select must be shown.)

5. [10 MARKS] Describe 4 groups of order 12, no two of which are isomorphic. You are expected to prove that no two of your groups are isomorphic — by indicating, for every pair of your groups, some property that would be the same for two isomorphic groups, but is not the same.

6. Let $\mathcal{A}_4$ denote the alternating group of even permutations of the symbols 1, 2, 3, 4.

   (a) [5 MARKS] For the element $a = (123)$ of $\mathcal{A}_4$, determine the right translation R_a and the left translation L_a, and express them both as permutations of the group elements, in disjoint cycle notation.

   (b) [5 MARKS] Give an example of a right coset of $\langle(123)\rangle$ in A_4 which is not a left coset of $\langle(123)\rangle$ in A_4; or prove that no such example exists.

7. [10 MARKS] Showing all your work, use the Euclidean algorithm to determine the inverse of $[74]_{53}$ in the group $\mathbb{Z}_{53}^{\times}$.

8. [5 MARKS] Prove or disprove: the ring $\mathbb{Z}_6\{x\}$ of formal power series in an indeterminate x is field.

H.9 Supplemental/Deferred Examination, August, 2000

1. (a) [5 MARKS] Prove or disprove: *If* $(\mathfrak{B}, *, e)$ *is any non-abelian group, the function* $f : \mathfrak{B} \to \mathfrak{B}$ *defined by* $b \mapsto b^{-1}$ *is not a homomorphism.*

   (b) [5 MARKS] Prove or disprove: *If* $(\mathfrak{A}, *, e)$ *is any group, any homomorphism* $f : (\mathfrak{A}, *, e) \to (\mathfrak{A}, *, e)$ *has the property that the set* $\{a^2 \mid a \in \mathfrak{A}\}$ *is mapped by* f *onto a subgroup of* $(\mathfrak{A}, *, e)$.

2. [10 MARKS] Showing all your work find *all* integer solutions to the system of congruences

$$\begin{aligned} x &\equiv -9 \pmod 3 \\ x &\equiv -8 \pmod 7 \\ x &\equiv -7 \pmod{10} \end{aligned}$$

3. (a) [5 MARKS] Prove or disprove: *If* $(\mathfrak{A}, *, e)$ *is a monoid, there exists a group* $(\mathfrak{B}, \star, e)$ *such that* $a_1 * a_2 = a_1 \star a_2$ *for all* $a_1 \in \mathfrak{A}$ *and* $a_2 \in \mathfrak{A}$, *where* $\mathfrak{A} \subset \mathfrak{B}$ *and* $\mathfrak{B} - \mathfrak{A}$ *consists of exactly one element* b.

   (b) [5 MARKS] Prove or disprove: *Let* n *be an even integer,* $n > 4$. *Then there exists a ring containing exactly* n *elements.*

4. (a) [5 MARKS] Prove that the polynomial $x^4 + x^3 + x^2 + x^1 + x^0$ is irreducible over $\mathbb{Z}_2$.

   (b) [5 MARKS] Let u be any element — different from both 0 and 1 — of a 16-element field $\mathbb{F}$ over which the polynomial $x^4 + x^3 + x^2 + x^1 + x^0$ has a root. For each of the elements $a \in \mathbb{F}$ determine the product ua, showing all your work.

5. [10 MARKS] Describe 4 groups of order 18, no two of which are isomorphic. You are expected to prove that no two of your groups are isomorphic — by indicating, for every pair of your groups, some property that would be the same for two isomorphic groups, but is not the same for that pair.

6. Let $\mathcal{S}_4$ denote the symmetric group of permutations of the symbols 1, 2, 3, 4, and let $\mathcal{S}_3$ denote the subgroup consisting of all permutations of the symbols 1, 3, 4.

   (a) [5 MARKS] For the element $a = (1234)$ of $\mathcal{S}_4$, determine the right translation $R_a : \mathcal{S}_4 \to \mathcal{S}_4$, expressing it as a permutation of the group elements, in disjoint cycle notation.

(b) [5 MARKS] Give an example of a right coset of $\mathcal{S}_3$ in $\mathcal{S}_4$ which is not a left coset of $\mathcal{S}_3$ in S_4; or prove that no such example exists.

7. [10 MARKS] Showing all your work, determine *all* integers a and b such that the sum $187\,a + 289\,b$ is equal to the greatest common divisor $(187, 289)$.

8. [10 MARKS] Showing all your work, *carefully* determine all integers n such that $\phi(n) = 10$.

H.10 2000/2001 Final Examination

1. [8 MARKS] Prove or disprove:

   It is possible to define a homomorphism from $\mathbb{Z}/7\mathbb{Z}$ *to* $\mathbb{Z}/4\mathbb{Z}$ *by mapping, for all* $a \in \mathbb{Z}$, $[a]_7$ *on to* $[a]_4$.

2. [8 MARKS] Give an explicit example of a ring with at least 8 elements which has no zero divisors, or show that no such ring exists.

3. [8 MARKS] Showing all your work, determine all positive integers n such that $\varphi(n)$ is even (where φ is the Euler *totient* function).

4. [10 MARKS] Carefully showing all your work, determine all integers that satisfy all of the following congruences simlutaneously:

$$x \equiv 1 \pmod 2 \tag{1206}$$
$$x \equiv 3 \pmod 5 \tag{1207}$$
$$x \equiv 5 \pmod{12} \tag{1208}$$
$$x \equiv 8 \pmod{15} \tag{1209}$$

   (Should you require the inverse of an integer n to a given modulus, you should use a systematic method to find it, unless $n = \pm 1$.)

5. (a) [4 MARKS] Showing all your work, prove carefully that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$, but is reducible over $\mathbb{Z}_5$.

   (b) [6 MARKS] Discuss in detail how one can use the polynomial $x^4 + x^3 + x^2 + x + 1$ to construct a field $\mathbb{F}_{16}$ of order $2^4 = 16$. Show the inverses of at least 2 of the elements of the field.

   (c) [4 MARKS] Determine the order of the element x in the multiplicative group of the field that you have constructed.

6. [6 MARKS] Prove or disprove:

There exists a residue class $[a]_8$ *such that,*

$$\forall n \in \mathbb{Z}\left(n \equiv 1 \pmod 2 \Rightarrow n^2 \in [a]_8\right) .$$

7. [8 MARKS] Recall that the symmetric group S_n consists of all permutations f of the set $\{1, 2, ..., n\}$. Determine, in $\mathcal{S}_4$, all cosets of the subgroup H of all permutations of the symbols 1, 3, 4. (H is the subgroup consisting of the elements $f \in \mathcal{S}_4$ for which $f(2) = 2$.)

8. [8 MARKS] Let a relation $\sim$ on the set $\mathbb{Z} - \{0\}$ be defined as follows:

$$a \sim b \quad \Leftrightarrow \quad \begin{cases} \text{every positive prime } p \text{ which divides } a \text{ also divides } b, \\ \qquad\qquad \text{or} \\ \text{every positive prime } p \text{ which divides } b \text{ also divides } a, \\ \qquad\qquad \text{or both.} \end{cases}$$

Determine carefully whether $\sim$ is an equivalence relation.

H.11 2000/2001 Supplemental/Deferred Examination

1. Suppose that f is a homomorphism from ring $\mathcal{R}$ to ring $\mathcal{S}$, and that the *kernel* of f consists only of the zero element of $\mathcal{R}$. Prove or disprove each of the following statements:

   (a) [5 MARKS] $\mathcal{R}$ must be commutative.

   (b) [5 MARKS] f must be surjective.

2. [10 MARKS] Showing all your work, determine all positive integers n such that $\varphi(2n) = \varphi(n)$ (where φ is the Euler *totient* function).

3. [10 MARKS] Carefully showing all your work, determine all integers that satisfy all of the following congruences simlutaneously:

$$x \equiv -28 \pmod 3 \tag{1210}$$
$$x \equiv 13 \pmod 5 \tag{1211}$$
$$x \equiv 70 \pmod{11} \tag{1212}$$
$$x \equiv 1000 \pmod 8 \tag{1213}$$

(Should you require the inverse of an integer n to a given modulus, you should use a systematic method to find it, unless $n = \pm 1$.)

4. (a) [6 MARKS] Showing all your work, prove carefully that the polynomial $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$, but is reducible over $\mathbb{Z}_5$.

   (b) [6 MARKS] Discuss in detail how one can use the polynomial $x^4 + x + 1$ to construct a field $\mathbb{F}_{16}$ of order $2^4 = 16$. Show the inverses of at least 2 of the elements of the field.

   (c) [6 MARKS] Carefully determine the order of the element x^5 in the multiplicative group of the field that you have constructed.

5. [12 MARKS] Recall that the symmetric group S_n consists of all permutations f of the set $\{1, 2, ..., n\}$. Determine, in $\mathcal{S}_4$, all cosets of the subgroup H which is generated by the permutation (4321) . You are expected to show the precise membership of each of the cosets.

6. Let a relation $\sim$ on the set $\mathbb{Z} - \{0\}$ be defined as follows:

$$a \sim b \quad \Leftrightarrow \quad (\forall n \in \mathbb{Z} - \{0\})\,(n|a \Rightarrow (n+1)|b)\,.$$

   (a) [5 MARKS] Determine whether or not $\sim$ is an equivalence relation.

   (b) [5 MARKS] Determine whether or not $\sim$ is a partial ordering of $\mathbb{Z}-\{0\}$.