Abstract Algebra Cheat Sheet

16 December 2002

By Brendan Kidwell, based on Dr. Ward Heilman's notes for his Abstract Algebra class.

Notes: Where applicable, page numbers are listed in parentheses at the end of a note.

Def: A **group** is a nonempty set G together with a binary operation $*$ on $G \times G$ satisfying the following four properties:

1. G is closed under the operation $*$.
2. The operation $*$ is associative.
3. G contains an identity element, **e**, for the operation $*$.
4. Each element in G has an inverse in G under the operation $*$.

Proposition 1: A group has exactly one identity element.

Proposition 2: Each element of a group has exactly one inverse element.

Proposition 3: $(a*b)^{-1}=b^{-1}*a^{-1} \quad \forall\, a, b \in (G, *)$.

Proposition 4: $(a^{-1})^{-1}=a \quad \forall\, a \in (G, *)$.

Proposition 5: $(\mathbb{Z}_n, +_n)$ is a group $\forall\, n \in \mathbb{N}$.

Proposition 6: In a group table, every element occurs exactly once in each row and exactly once in each column.

Def: The **order of a group** $(G, *)$ is the number of elements in the set G. (Written as $|G|$.) (36)

Def: A **dihedral group** of order $2n$ is the set of symmetric transformations of a regular n-gon. (Written as D_n.) (36)

Def: An **abelian** (or **commutative**) group has the property that $a*b=b*a \quad \forall\, a, b \in (G, *)$. (37)

Def: $(H, *)$ is a **subgroup** of $(G, *)$ iff $H \in G$ and $(H, *)$ is a group under the same operation. (37) To show that $(H, *)$ is a subgroup, show that $H \in G$ and then show closure and existence of inverses.

Lagrange's Theorem: Let $(H, *)$ be a subgroup of a finite group, $(G, *)$. $|H|$ divides $|G|$.

Def: $\langle a \rangle = \{a^0, a^1, a^{-1}, a^2, a^{-2}, a^3, a^{-3} \ldots\}$ is the **cyclic subgroup** generated by a.

Def: The **order of an element**, a, is the order of $\langle a \rangle$.

Def: A **cyclic** group is a group that can be generated entirely by repeatedly combining a single element with itself. In other words, if for a cyclic group $G=\langle a \rangle$, then a is the **generator** of G.

Def: **Prime Order Proposition.** For every prime p, there is exactly one group of order p.

Proposition 8: Cancellation Laws. Let $a, b, c \in (G, *)$.

1. $(a*b=a*c) \rightarrow (b=c)$
2. $(b*a=c*a) \rightarrow (b=c)$
3. If G is abelian, $(a*b=c*a) \rightarrow (b=c)$

Proposition 9: The only solution to $a*a=a$ is $a=\boldsymbol{e}$.

Proposition 10: Let $a, b \in G$. If $a*b \neq b*a$, then $\boldsymbol{e}, a, b, a*b, b*a$ are all distinct elements. (50)

Proposition 11: Any non-abelian group has at least six elements. (51)

Def: The **center** of a group is $Z(G)=\{\text{all } g\in G \text{ such that } (g*a=a*g \quad \forall a\in G)\}$.

Proposition 12: $(Z(G), *)$ is a subgroup of *G*. (52)

Def: Two integers, *a* and *b*, are **relatively prime** iff $\gcd(a, b)=1$. (54)

Def. $\forall n\in\mathbb{N}$, the **set of units** of *n*, $\mathbf{U}(n)$, is the set of all natural numbers relatively prime to *n*. (54)

Proposition 13: $\forall n\in\mathbb{N}$, $(\mathbf{U}(n), \cdot_n)$ is a group. (54)

Def: For any set *S* and subsets $A, B\in S$, the **symmetric difference** of *A* and *B* (written as $A\,\Delta\, B$) is the set of all elements that are in *A* or *B*, but are not in both *A* and *B*. In other words, $A\,\Delta\, B=(A-B)\cup(B-A)$. (55)

Def: The **power set** of *S* (written as $P(S)$) is the set of all subsets of *S*, including $\emptyset$ and the original set *S*. (55)

Proposition 14: For any nonempty set *S*, $(P(S), \Delta)$ is a group. (55)

Def: Let $(G, *)$ and $(K, \circ)$ be two groups. Let *f* be a function from *G* to *K*. *f* is a **homomorphism** (or operation preserving function) from $(G, *)$ to $(K, \circ)$ iff $\forall a, b\in G \quad f(a*b)=f(a)\circ f(b)$. (59)

Proposition 15: Let $f\colon G\to K$ be a homomorphism. Let $\boldsymbol{e}$ be the identity of $(G, *)$ and $\boldsymbol{e}'$ be the identity of $(K, \circ)$. (60)

1. $f(\boldsymbol{e})=\boldsymbol{e}'$
2. $f(g^{-1})=(f(g))^{-1} \quad \forall g\in G$
3. $f(g^n)=(f(g))^n \quad \forall n\in\mathbb{Z}$

Def: Given nonempty sets *S* and *T*, with $x, y\in S$, and a function $f\colon S\to T$ (63)

1. *f* is a **one-to-one** (1-1) function iff $(x\neq y)\to(f(x)\neq f(y))$.
2. *f* is **onto** *T* iff $\forall z\in T \quad \exists x\in S$ such that $f(x)=z$.

Proposition 16: Let $f\colon S\to T$ be an onto function. (65)

1. $f(f^{-1}(V))=V \quad \forall V\subseteq T$
2. $W\subseteq f(f^{-1}(W)) \quad \forall W\subseteq S$

Proposition 17: Let *f* be a homomorphism from $(G, *)$ to $(K, \circ)$. (68)

1. If $(H, *)$ is a subgroup of $(G, *)$, then $(f(H), \circ)$ is a subgroup of $(K, \circ)$.
2. If $(L, \circ)$ is a subgroup of $(K, \circ)$, then $(f^{-1}(L), *)$ is a subgroup of $(G, *)$.

Def: (Using the previous example,) the **image** of *H* under *f* is $f(H)$. The **inverse image** of L under f is $f^{-1}(L)$. (68)

Proposition 18: Let *f* be a homomorphism from $(G, *)$ to $(K, \circ)$. *f* is one-to-one iff $\ker(f)=\{\boldsymbol{e}\}$. (72)

Def: Two groups, $(G, *)$ and $(K, \circ)$, are **isomorphic** iff there exists a one-to-one homomorphism *f* from $(G, *)$ *onto* $(K, \circ)$—that is, $f(G)=K$. In this case, *f* is called an **isomorphism** or **isomorphic mapping**. (73)

Proposition 19: Every finite cyclic group of order *n* is isomorphic to $(\mathbb{Z}_n, +_n)$ and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. (75)

Proposition 20: Every subgroup of a cyclic group is cyclic. (76)

Theorem: If G is a finite group, p is a prime, and p^k is the largest power of p which divides $|G|$, then G has a subgroup of order p^k.

Def: A **permutation** is a one-to-one and onto function from a set to itself. (77)

Note: See pages 78 and 81 for examples of how to notate permutations.

Def: The set of permutations on $\{1,2,3,\ldots,n\}$ is written as S_n. (79)

Theorem 21: The set of all permutations together with composition, $(S_{n,} \circ)$, is a nonabelian group $\forall n \geq 3$. (79)

Theorem 22: The set of all permutations on a set S (its symmetries), together with composition, $(\text{Sym}\, S, \circ)$, is a group. (80)

Theorem 23 (Cayley's Theorem): Every group is isomorphic to a group of permutations. (82)

Proposition 24: Every permutation can be written as a product of disjoint cycles in permutation notation. (86)

Def: The **length** of a cycle in a permutation is the number of distinct objects in it. A cycle of length 2 is a **transposition**. (86)

Proposition 25: Every cycle can be written as a product of transpositions (not necessarily distinct). (87)

Def: A permutation is **even** (or **odd**) if it can be written as a product of an even (or odd) number of transpositions. (88)

Def: The subset of S_n which consists of all the even permutations of S_n is called the **alternating group** on n and is written as A_n. (90)

Def: **Matrix multiplication**, which is not commutative, is the standard way to combine matrices. To multiply a **2×2 matrix**: (102)

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}=\begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Notes: A 2×2 matrix can be found to represent any **linear transformation**. The special matrix

$$M=\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

when mulpilied on the left with a vector in $\mathbb{R}^2$ will rotate it counterclockwise by the amount α: $M\,X_{initial}=X_{rotated}$. (100)

Def: The **inverse under multiplication of a 2×2 matrix** is computed as follows: (103)

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}=\begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}$$

Def: The **determinant of a 2×2 matrix** is computed as follows: (104)

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)=ad-bc$$

Def: A matrix is **invertible** iff its determinant is nonzero. (104)

Theorem 29: The set of all invertible 2×2 made from elements of $\mathbb{R}$, together with matrix multiplication, forms a group, called the **general linear group**, which is written as $GL(2,\mathbb{R})$. (105)

Def: The **special linear group** is the group of 2×2 matrices with determinants of 1, written as $SL(2,\mathbb{R})$. (106)

Def: To get the **transpose** of a matrix, swap each element $a_{i,j}$ with the one on the opposite side of the main diagonal, $a_{j,i}$. The transpose of a matrix *M* is written M^t. (106)

Def: A matrix *M* is **orthogonal** iff $M^t M = I$. (106)

Theorem 30: The set of orthogonal 2×2 matrices with determinant 1 together with matrix multiplication form a the **special orthogonal group**, which is written as $SO(2,\mathbb{R})$. The set of orthogonal matrices together with matrix multiplication is also a group, the **orthogonal group**, which is written as $O(2,\mathbb{R})$. $SO(2,\mathbb{R})$ is a subgroup of $O(2,\mathbb{R})$. (107)

Proposition 31: For two matrices *A* and *B*, (107)

1. $(AB)^t = B^t A^t$
2. $(A^t)^{-1} = (A^{-1})^t$
3. $\det(AB) = \det A \cdot \det B$
4. $\det(A^t) = \det A$
5. $\det(A^t A) = \det A^t \cdot \det A = \det A \cdot \det A = (\det A)^2$

Fact 32: $SO(2,\mathbb{R}) = \left\{ \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \ \forall \text{angle } \alpha \right\}$

Def: Given a set *G* and an operation $*$: (113)
G is a groupoid iff *G* is closed under $*$.
G is a semigroup iff *G* is a groupoid and $*$ is associative.
G is a semigroup with identity iff *G* is a semigroup and has an identity under $*$.
G is a group iff *G* is a semigroup and each element has an inverse under $*$.

Def: A **ring**, written $(R, *, \circ)$, consists of a nonempty set *R* and two opertaions such that (114)

- $(R, *)$ is an abelian group,
- $(R, \circ)$ is a semigroup, and
- the semigroup operation, $\circ$, distributes over the group operation, $*$.

Proposition 33: Let $(R, +, \cdot)$ be a ring. (115)

1. $0 \cdot a = a \cdot 0 = 0 \ \ \forall a \in R$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b) \ \ \forall a, b \in R$
3. $(-a) \cdot (-b) = a \cdot b \ \ \forall a, b \in R$

Def: A **ring with identity** is a ring that contains an indentity under the second operation (the multiplicative operation). (117)

Def: A **commutative ring** is a ring where the second operation is commutative. (117)

Def: A **subring** is a nonempty subset *S* of a ring $(R, +, \cdot)$ such that $(S, +, \cdot)$ is a ring (under the same operations as *R*.) (119)

Proposition 34: To prove that $(S, +, \circ)$ is a subring of $(R, +, \cdot)$ we need to prove that (119)

1. $S \subseteq R$ (set containment)
2. $\forall a, b \in S \ \ (a+b) \in S$ (closure under additive operation)
3. $\forall a, b \in S \ \ (a \cdot b) \in S$ (closer under multiplicative operation)
4. $\forall a \in S \ \ (-a) \in S$ (additive inverses exist in *S*)

Def: A ring $(R, +, \cdot)$ has **zero divisors** iff $\exists a, b \in R$ such that $a \neq 0, b \neq 0$, and $a \cdot b = 0$. (120)

Def: In a ring $(R, +, \cdot)$ with identity, an element *r* is **invertible** iff $\exists r^{-1} \in R$ such that $r \cdot r^{-1} = r^{-1} \cdot r = 1$ (the multiplicative identity). (121)

Proposition 35: Let R^* be the set of all invertible elements of *R*. If $(R, +, \cdot)$ is a ring with identity then $(R^*, \cdot)$ is a group, known as the **group of invertible elements**. (121)

Proposition 36: Let $(R, +, \cdot)$ be a ring with identity such that $R \neq \{0\}$. The elements 0 and 1 are distinct. (122)

Proposition 37: A ring $(R, +, \cdot)$ has no zero divisors iff the cancellation law for multiplication holds. (123)

Corollary 38: Let $(R, +, \cdot)$ be a ring with identity which has no zero divisors. The only solutions to $x^2 = x$ in the ring are $x = 0$ and $x = 1$. (123)

Def: An **integral domain** is a commutative ring with identity which has no zero divisors. (124)

Def: A **field** $(F, +, \cdot)$ is a set *F* together with two operations such that (125)

- $(F, +)$ is an abelian group,
- $(F - \{0\}, \cdot)$ is an abelian group, and
- $\cdot$ distributes over $+$.

In other words, a field is a commutative ring with identity in which every nonzero element has an inverse.

Back to intro and comments page: http://www.glump.net/archive/000024.php
Back to home page: http://www.glump.net/