Algebraic Structures

Abstract algebra is the study of **algebraic structures**. Such a structure consists of a set together with one or more binary operations, which are required to satisfy certain axioms. For example, here is the definition of a simple algebraic structure known as a **group**:

Definition: Group
A **group** is a set G together with a binary operation $*$ on G, satisfying the following axioms:

1. The operation $*$ is associative. That is,

   $$a * (b * c) = (a * b) * c$$

   for all $a, b, c \in G$.

2. There exists an element $e \in G$ with the property that

   $$a * e = e * a = a$$

   for all $a \in G$. (This element e is called the **identity element** of G.)

3. For each element $a \in G$, there exists an element $a^{-1} \in G$ such that

   $$a * \left(a^{-1}\right) = \left(a^{-1}\right) * a = e.$$

   (The element a^{-1} is called the **inverse** of a.)

The binary operation $*$ in this definition may be any operation at all, such as addition, multiplication, or composition of functions. Any set of elements with an operation that satisfies these axioms forms a group. For example:

- The set $\mathbb{Z}$ of integers forms a group under the operation of addition. In particular, addition is associative, the element 0 is an additive identity, and every integer has an additive inverse.
- The set $\mathbb{R} - \{0\}$ of nonzero real numbers forms a group under the operation of multiplication. Note that zero must be excluded, since it does not have a multiplicative inverse.
- The set $\mathrm{GL}(n, \mathbb{R})$ of all invertible $n \times n$ matrices forms a group under the operation of matrix multiplication. In this case, the identity element is the $n \times n$ identity matrix.

Groups are a particularly simple algebraic structure, having only one operation and three axioms. Most algebraic structures have more than one operation, and are required to satisfy a long list of axioms.

Here is a partial list of the most important algebraic structures:

- A **group** is an algebraic structure with a single operation, as defined above. Groups are closely associated with the idea of symmetry, and most groups that arise in mathematics are groups of symmetry transformations, with the operation being composition of functions.
- A **field** is an algebraic structure with addition and multiplication, which obey all of the usual rules of elementary algebra. Examples of fields include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.
- A **ring** is a more general algebraic structure with addition and multiplication. Unlike a field, a ring is not required to have multiplicative inverses, and the multiplication is not required to be commutative. A good example of a ring is the set of all $n \times n$ matrices under the operations of matrix addition and matrix multiplication. The integers $\mathbb{Z}$ also form a ring under the operations of addition and multiplication.
- A **vector space** is an algebraic structure with operations of addition and multiplication by scalars. The scalars are required to be elements of a field, such as the real numbers $\mathbb{R}$. The basic example of a vector space is the set $\mathbb{R}^n$ of all vectors with n entries.
- A **module** is similar to a vector space, except that the scalars are only required to be elements of a ring. For example, the set $\mathbb{Z}^n$ of n-dimensional vectors with integer entries forms a module, where "scalar multiplication" refers to multiplication by integer scalars.

Because algebraic structures are inherently abstract, the names for them are fairly arbitrary. Words like "group", "module", and "field" are just interchangeable collective nouns, and you should not ascribe any importance to which structure has which

name. The word "ring" is also in this category—it is meant to refer to an association or coalition, such as a smuggling ring or a ring of spies, and should not convey any sense of circularity.

The structures listed above are only a sample of the many algebraic structures of importance in mathematics. Many fields of mathematics involve their own special algebraic structures, and new algebraic structures are defined all the time. To give you a sense of scale, the online encyclopedia Wikipedia currently has articles on over a hundred different algebraic structures, and this represents only a small fraction of those that have been investigated in the mathematical literature.

Fields

The most familiar form of algebra is the elementary algebra that you learned in high school, namely the algebra of the real numbers. From an abstract point of view, this is the algebra of fields.

Definition: Field

A **field** is a set F together with two binary operations $+$ (the **addition operation**) and $\cdot$ (the **multiplication operation**), that satisfy the following axioms:

1. The addition operation is associative. That is,

   $$a + (b + c) = (a + b) + c$$

   for all $a, b, c \in F$.

2. The addition operation is commutative. That is,

   $$a + b = b + a$$

   for all $a, b \in F$.

3. There exists a special element of F called the **additive identity**, denoted by the symbol 0. This element has the property that

   $$a + 0 = a$$

   for all $a \in F$.

4. For each element $a \in F$, there is an element $-a \in F$, called the **additive inverse** of a, with the property that

$$a + (-a) = 0.$$

5. The multiplication operation is associative. That is,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

for all $a, b, c \in F$.

6. The multiplication operation is commutative. That is,

$$a \cdot b = b \cdot a$$

for all $a, b \in F$.

7. There exists a special element of F called the **multiplicative identity**, denoted by the symbol 1. This element has the property that

$$a \cdot 1 = a$$

for all $a \in F$.

8. For each element $a \in F$ other than 0, there exists an element $a^{-1} \in F$, called the **multiplicative inverse** of a, with the property that

$$a \cdot \left(a^{-1}\right) = 1.$$

9. The multiplication operation distributes over the addition operation. That is,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

for all $a, b, c \in F$.

Note that the axioms for a field are precisely the axioms for algebra on the real numbers. As a result, the real numbers $\mathbb{R}$ form a field under the usual operations of addition and multiplication. However, the real numbers are not the only possible field. Indeed, you are already familiar with a few other examples:

- The rational numbers $\mathbb{Q}$ form a field under the usual operations of addition and multiplication. In particular, we can add or multiply two elements of $\mathbb{Q}$ to obtain another element of $\mathbb{Q}$, and these operations obey all of the axioms listed above.

- The complex numbers $\mathbb{C}$ form a field under the commonly defined operations of addition and multiplication. Complex numbers do obey all of the listed axioms for a field, which is why elementary algebra works as usual for complex numbers.

The following example discusses another class of fields that we shall be using repeatedly.

EXAMPLE 1 Integers Modulo n

If $n \geq 2$, let $\mathbb{Z}_n$ denote the set $\{0, 1, \ldots, n-1\}$ under the operations of addition and multiplication modulo n. For example, here are the addition and multiplication tables for $\mathbb{Z}_5$:

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

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

It is not hard to see that $\mathbb{Z}_n$ satisfies most of the axioms for a field, but it is not clear that every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse (as is required by axiom 8). For $\mathbb{Z}_5$, we can see from the multiplication table that every element has an inverse. In particular,

$$1^{-1} = 1, \qquad 2^{-1} = 3, \qquad 3^{-1} = 2, \qquad \text{and} \qquad 4^{-1} = 4,$$

Thus $\mathbb{Z}_5$ is a field.

The same is not true for $\mathbb{Z}_6$. Here is the multiplication table modulo 6:

$\cdot$	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

As you can see from this table, $1^{-1} = 1$ and $5^{-1} = 5$ in $\mathbb{Z}_6$, but the elements 2, 3, and 4 do not have multiplicative inverses. ■

The following theorem from number theory characterizes which elements of $\mathbb{Z}_n$ have multiplicative inverses. We will not prove this theorem here:

Theorem 1 Multiplicative Inverses in $\mathbb{Z}_n$

Let $n \in \mathbb{N}$, and let $k \in \mathbb{Z}_n$. Then k has a multiplicative inverse in $\mathbb{Z}_n$ if and only if k and n are relatively prime.

Here **relatively prime** means that k and n have no common prime factors, i.e. their greatest common divisior is 1. This explains why 2, 3, and 4 have no multiplicative inverses in $\mathbb{Z}_6$ — all of these numbers have a factor in common with 6. We can immediately conclude the following:

Corollary 2 Prime Fields

$\mathbb{Z}_n$ is a field if and only if n is prime.

This gives us a large class of fields that are very different from the real numbers. However, you should be aware that we have hardly exhausted the list of fields. For example, here are the addition and multiplication tables for a field with four elements:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Note that this is not the same as $\mathbb{Z}_4$, since among other things $\mathbb{Z}_4$ is not a field. The lesson is that not every finite field comes from modular arithmetic.

There are similar fields with eight and nine elements, although surprisingly it is not possible to define a field with six or ten elements. Indeed, a famous theorem of field theory asserts that there exists a field with n elements if and only if n is a power of a prime.

Algebra of Fields

By definition, the elements of a field satisfy exactly the same algebraic axioms as the real numbers. As a result, everything you know about algebra for real numbers translates directly to algebra for the elements of any field. This includes virtually everything you know about elementary algebra, as well as basic linear algebra.

Of course, the definition of a field involves only addition and multiplication, but we usually think of algebra as involving the *four* operations of addition, subtraction, multiplication, and division. Fortunately, it is not difficult to define subtraction and division for elements of a field.

Definition: Subtraction and Division in Fields
Let F be a field, and let $a, b \in F$.

(a) The **difference** of a and b is defined by the formula

$$a - b \;=\; a + (-b),$$

where $-b$ is the additive inverse of b.

(b) If $b \neq 0$, the **quotient** of a and b is defined by the formula

$$a \div b \;=\; a \cdot (b^{-1}),$$

where b^{-1} is the multiplicative inverse of b.

For example, in the field $\mathbb{Z}_5$, we can divide 2 by 3 as follows:

$$2 \div 3 \;=\; 2 \cdot (3^{-1}) \;=\; 2 \cdot 2 \;=\; 4.$$

Now that we have subtraction and division, we can perform almost any algebraic computation in the usual way for elements of a field. Here are a few examples:

EXAMPLE 2 Solving an Equation
Solve the following equation:

$$3x + 4 \;\equiv\; 6 \pmod 7.$$

SOLUTION Since $\mathbb{Z}_7$ is a field, we can solve this equation using elementary algebra. First we subtract 4 from both sides:

$$3x \;\equiv\; 2 \pmod 7.$$

Next we must divide through by 3. A moment's thought reveals that $3^{-1} = 5$ in $\mathbb{Z}_7$, so dividing through by 3 is the same as multiplying through by 5. This gives:

$$x \;\equiv\; 5 \cdot 2 \;\equiv\; 3 \pmod 7. \qquad \blacksquare$$

EXAMPLE 3 Row Reduction

Solve the following system of equations:

$$3x + 7y \equiv 4 \pmod{11}$$
$$8x + 6y \equiv 1 \pmod{11}$$

SOLUTION Since $\mathbb{Z}_{11}$ is a field, we can solve this system in any of the usual ways. We shall use row reduction. We begin by putting the coefficients into an augmented matrix:

$$\left[\begin{array}{cc|c} 3 & 7 & 4 \\ 8 & 6 & 1 \end{array}\right]$$

The usual next step would be to divide the first row by 3. A moment's thought reveals that $3^{-1} = 4$ in $\mathbb{Z}_{11}$, so we must multiply the first row by 4:

$$\left[\begin{array}{cc|c} 1 & 6 & 5 \\ 8 & 6 & 1 \end{array}\right]$$

Continuing in this fashion, we can reduce the matrix all the way to reduced echelon form:

$$\left[\begin{array}{cc|c} 1 & 6 & 5 \\ 8 & 6 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cc|c} 1 & 6 & 5 \\ 0 & 2 & 5 \end{array}\right] \rightarrow \left[\begin{array}{cc|c} 1 & 6 & 5 \\ 0 & 1 & 8 \end{array}\right] \rightarrow \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 8 \end{array}\right]$$

So the solution is

$$x \equiv 1 \pmod{11} \qquad \text{and} \qquad y \equiv 8 \pmod{11}. \qquad \blacksquare$$

EXAMPLE 4 Inverting a Matrix

Find the inverse of the following matrix, whose entries are elements of $\mathbb{Z}_7$:

$$A = \begin{bmatrix} 5 & 2 \\ 6 & 3 \end{bmatrix}.$$

SOLUTION Since this is a 2×2 matrix, there is a simple formula for the inverse:

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

Applying this to the given matrix gives:

$$A^{-1} = 3^{-1} \begin{bmatrix} 3 & 5 \\ 1 & 5 \end{bmatrix}.$$

since $3^{-1} = 5$ in $\mathbb{Z}_7$, we conclude that

$$A^{-1} = 5 \begin{bmatrix} 3 & 5 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 5 & 4 \end{bmatrix}. \qquad \blacksquare$$