Groups, Rings, and Fields

I. Sets

Let S be a set. The Cartesian product $S \times S$ is the set of ordered pairs of elements of S,

$$S \times S = \{(x, y) \mid x, y \in S\}.$$

A *binary operation* ϕ is a function,

$$\phi : S \times S \to S.$$

A binary operation ϕ is *commutative* if

$$\phi(x, y) = \phi(y, x)$$

for all $x, y \in S$. A binary operation is *associative* if

$$\phi(\phi(x, y), z) = \phi(x, \phi(y, z))$$

for all $x, y, z \in S$.

For example, let $S = \{1, 2, 3, \dots\}$ be the set of positive integers. Then,

$$\phi(x, y) = x + y$$

is a binary operation which is both commutative and associative,

$$\phi(x, y) = (x + y)^2$$

is a binary operation which is commutative, but not associative, and

$$\phi(x, y) = x^y,$$

is a binary operation which is neither commutative nor associative. These operations are defined using the familiar operations of addition and multiplication on the positive integers.

Later, we will see examples of binary operations which are associative, but not commutative.

It will often be convenient to name binary operations on a set S by the symbols $+$ or $\cdot$ familiar from arithmetic. The operations on S may have little or nothing to do with addition or multiplication on the integers — the symbols $+$ and $\cdot$ are used simply as names. One immediate convenience: we may write $x + y$ and $x \cdot y$ instead of the cumbersome $+(x, y)$ and $\cdot(x, y)$.

II. Groups

A *group* $(G, +, 0)$ consists of a set G together with a binary operation $+$ and a distinguished element $0 \in G$ satisfying the following properties:

(i) $+ : G \times G \to G$ is associative,
(ii) for all $x \in G$,
$$x + 0 = x \quad \text{and} \quad 0 + x = x,$$
(iii) for each $x \in G$, there exists an element $y \in G$ satisfying
$$x + y = 0 \quad \text{and} \quad y + x = 0.$$

We may easily prove for each $x \in G$, the inverse element y guaranteed by (iii) is unique. If y and y' are inverses for x, then
$$y' = (y + x) + y' = y + (x + y') = y.$$
Properties (i) and (ii) are used in the above deduction. The inverse of x is usually denoted by $-x$.

The group axioms imply a useful left cancellation property: if
$$z + x = z + y,$$
then $x = y$. The cancellation property is derived as follows. Let $-z$ the inverse of z. Then, $z + x = z + y$ implies
$$-z + (z + x) = -z + (z + y).$$
By associativity,
$$(-z + z) + x = (-z + z) + y.$$
Hence,
$$0 + x = 0 + y.$$
We then conclude $x = y$ by (ii). A similar right cancellation property holds (and is proven in the same way).

Let $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ be the set of integers. Then, $(\mathbb{Z}, +, 0)$ is a group where $+$ is the usual addition. However, $(\mathbb{Z}, \cdot, 1)$, where $\cdot$ is the usual multiplication,is not a group: multiplicative inverses can not always be found in the integers, violating property (iii).

Let $\mathbb{Q}$ be the set of rational numbers. Then, $(\mathbb{Q}, +, 0)$ is a group. Let $\mathbb{Q}^*$ be the set of non-zero rational numbers. Then, $(\mathbb{Q}^*, \cdot, 1)$ is a group. You should check the problems with the (failed) example of a multiplicative group structure on the integers are fixed in $(\mathbb{Q}^*, \cdot, 1)$.

The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ also provide examples of groups:
$$(\mathbb{R}, +, 0), \ (\mathbb{R}^*, \cdot, 1),$$

$$(\mathbb{C}, +, 0),\ (\mathbb{C}^*, \cdot, 1),$$

where the superscripted $*$ denotes the non-zero elements as before.

Let n be a positive integer. Let $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$ be the set of remainders modulo n. We can define a binary operation $+$ on $\mathbb{Z}/n\mathbb{Z}$ by usual addition followed by taking the remainder modulo n. For example,

$$\overline{3} + \overline{5} = \overline{2} \ \in \mathbb{Z}/6\mathbb{Z}.$$

The bar above the elements of $\mathbb{Z}/n\mathbb{Z}$ indicates the elements are not integers, but remainder classes modulo n. You should check $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ is a group with n elements.

A group is *abelian* if the binary operation is commutative. All the above examples are abelian groups.

There are many non-abelian groups. Let $\mathbf{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices with real entries. Let $\cdot$ denote matrix multiplication, and let I_n denote the $n \times n$ identity matrix. You should check $(\mathbf{GL}_n(\mathbb{R}), \cdot, I_n)$ is a group. For $n \geq 2$, $(\mathbf{GL}_n(\mathbb{R}), \cdot, I_n)$ is not abelian.

The binary operation in a non-abelian group is associative, but not commutative.

Group theory is an old and very well developed subject. You will learn more in Math 323, the undergraduate algebra class.

III. Rings

A *ring* $(R, +, \cdot, 0, 1)$ consists of a set R together with two binary operations $+$ and $\cdot$ and two distinguished elements $0, 1 \in R$ satisfying the following properties:

(i) $(R, +, 0)$ is an abelian group,
(ii) $\cdot : R \times R \to R$ is associative,
(iii) for all $x \in R$,

$$x \cdot 1 = x \ \text{ and } \ 1 \cdot x = x,$$

(iv) for all $x, y, z \in R$,

$$x \cdot (y + z) = x \cdot y + x \cdot z \ \text{ and } \ (x + y) \cdot z = x \cdot z + y \cdot z.$$

Property (iv) consists of the left and right *distributive laws*.

The first binary operation $+$ of a ring is called addition and second $\cdot$ is called multiplication. Unless we wish to emphasize the multiplicative operation, we will often follow the usual convention of abbreviating $x \cdot y$ by xy. Sometimes rings defined by (i)-(iv) are called *unital rings* since the existence of a multiplicative unit 1 is stipulated.

The standard number systems all define rings:

$$(\mathbb{Z}, +, \cdot, 0, 1),\ (\mathbb{Q}, +, \cdot, 0, 1),\ (\mathbb{R}, +, \cdot, 0, 1),\ (\mathbb{C}, +, \cdot, 0, 1).$$

We can define multiplication $\cdot$ on the set $\mathbb{Z}/n\mathbb{Z}$ by the usual multiplication followed by taking the remainder modulo n. For example,

$$\overline{2} \cdot \overline{5} = \overline{4}, \quad \overline{2} \cdot \overline{3} = \overline{0} \ \in \mathbb{Z}/6\mathbb{Z}.$$

Then, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ is a ring with finitely many elements. The ring $(\mathbb{Z}/1\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ is degenerate since $\overline{0} = \overline{1}$.

You may ask why the addition of a ring is required to be commutative. In fact, we can *deduce* the commutativity of addition from the repeated use of properties (iii) and (iv) and the group laws for $+$.

The deduction of commutativity is as follows. First,

$$\begin{aligned} (x+y) \cdot (1+1) &= x \cdot (1+1) + y \cdot (1+1) \\ &= x \cdot 1 + x \cdot 1 + y \cdot 1 + y \cdot 1 \\ &= x + x + y + y, \end{aligned}$$

by (iii) and (iv). Next,

$$\begin{aligned} (x+y) \cdot (1+1) &= (x+y) \cdot 1 + (x+y) \cdot 1 \\ &= x \cdot 1 + y \cdot 1 + x \cdot 1 + y \cdot 1 \\ &= x + y + x + y, \end{aligned}$$

by (iii) and (iv). We have proven,

$$x + x + y + y = x + y + x + y.$$

Finally, using the cancellation property of the additive group, we can cancel the first and last terms to conclude

$$x + y = y + x.$$

So, the commutation of addition is implied by the other axioms. Hence, we may as well assume $+$ is commutative from the beginning.

However, the multiplication of a ring is *not* required to be commutative. A ring is called *commutative* if multiplication commutes. All the rings above are commutative rings.

Let $\mathbf{M}_n(\mathbb{R})$ be the set of all $n \times n$ matrices with real coefficients. Then,

$$(\mathbf{M}_n(\mathbb{R}), +, \cdot, 0, I_n)$$

is ring. If $n \geq 2$, the multiplication of $(\mathbf{M}_n(\mathbb{R}), +, \cdot, 0, I_n)$ is not commutative.

IV. Fields

A *field* $(F, +, \cdot, 0, 1)$ consists of a set F together with two binary operations $+$ and $\cdot$ and two distinguished elements $0, 1 \in F$ satisfying the following properties:

(i) $(F, +, 0)$ is an abelian group,
(ii) $\cdot : F \times F \to F$ is associative and commutative,
(iii) for all $x \in F$,

$$x \cdot 1 = x \quad \text{and} \quad 1 \cdot x = x,$$

(iv) for each $0 \neq x \in F$, there exists an element $y \in F$ satisfying

$$x \cdot y = 1 \quad \text{and} \quad y \cdot x = 1.$$

(v) for all $x, y, z \in F$,

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{and} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

We will always assume $0 \neq 1$ in F.

We can deduce many familiar properties from the field axioms. For example, for all $x \in F$,

$$x \cdot 0 = 0. \tag{1}$$

The first step of the derivation is:

$$x \cdot 0 + x \cdot 0 = x \cdot (0 + 0) = x \cdot 0,$$

using (v) and the group properties for $+$. Then, cancelling $x \cdot 0$ from both sides using the group properties for $+$, we find

$$x \cdot 0 = 0.$$

Let F^* denote the non-zero elements of a field F. If $x \in F^*$ and $x \cdot z = 0$, then $z = 0$. The proof is as follows. Let y be the multiplicative inverse of x guaranteed by (iv). Then,

$$y \cdot (x \cdot z) = y \cdot 0 = 0,$$

using property (1). Also,

$$y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z,$$

using associativity and (iii). We conclude $z = 0$.

As a consequence, we find the set F^* is closed under multiplication: for all $x, y \in F^*$, $x \cdot y \in F^*$. Also, $1 \in F^*$. The field axioms imply $(F^*, \cdot, 1)$ is an abelian group.

The field axioms (i)-(iv) above may be rewritten in a simpler form:

(i) $(F, +, 0)$ is an abelian group,
(ii) $(F^*, \cdot, 1)$ is an abelian group,
(iii) the distributive laws hold.

The standard number systems with the exception of $(\mathbb{Z}, +, \cdot, 0, 1)$ all define fields:

$$(\mathbb{Q}, +, \cdot, 0, 1),\ (\mathbb{R}, +, \cdot, 0, 1),\ (\mathbb{C}, +, \cdot, 0, 1).$$

The integers fail the field axioms since multiplicative inverses do not always exist.

Suppose n is not a prime number. Then, $pq = n$ where p and q are positive integers less than n. Hence,

$$\overline{p} \cdot \overline{q} = 0 \quad \in \mathbb{Z}/n\mathbb{Z}$$

since the product leaves 0 remainder modulo n. Since the non-zero elements are not closed under multiplication, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ is not a field if n is not prime.

If p is a prime number, then $(\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ *is* a field. The main property to verify is the existence of multiplicative inverses for non-zero elements.

Let x be a positive integer less than p corresponding to a non-zero element $\overline{x}$ of $\mathbb{Z}/p\mathbb{Z}$. Then, x and p are relatively prime (that is, they have no common factor greater than 1). Since x and p are relatively prime, there exist integers $a, b \in \mathbb{Z}$ for which

$$xa + pb = 1 \quad \in \mathbb{Z}. \tag{2}$$

Can you prove this? A proof is provided below, but you may wish to find an argument yourself.

We now establish the existence of $a, b \in \mathbb{Z}$ satisfying (2). Let $I \subset \mathbb{Z}$ denote the set of integers of the form $xs + pt$ for $s, t \in \mathbb{Z}$,

$$I = \{xs + pt \mid s, t \in \mathbb{Z}\}.$$

Since I contains both x and p, I certainly contains positive integers.

The *well-ordering* property of the integers states: every non-empty set of positive integers has a smallest element. The well-ordering property is equivalent to the principle of induction.

Let d be the *smallest positive integer* in I. Certainly $d \leq x, p$. Since $d \in I$, we see there exist $a, b \in \mathbb{Z}$ satisfying

$$xa + yb = d.$$

We prove by contradiction that d divides x. If not, we may write

$$x = md + r,$$

where $m \in \mathbb{Z}$ and r is the remainder $0 < r < d$. We see then $r \in I$ since

$$r = x(1 - ma) + y(-mb).$$

But $r \in I$ contradicts the fact that d is the smallest positive integer in I. Hence, d must divide x. Similarly, d must divide p.

Since x and p are relatively prime, the only positive integer which divides both x and p is 1. Thus, $d = 1$. We have proven the existence of (2).

Let $\overline{y}$ be the remainder of a mod p. We see (2) implies

$$\overline{x} \cdot \overline{y} = \overline{1} \in \mathbb{Z}/p\mathbb{Z}.$$

Hence, we have established the existence of multiplicative inverses of non-zero elements in

$$(\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1}).$$

All of the other field axioms are easy to check.

We can consider linear algebra over an arbitrary field F. That is, we may study systems of linear equations

$$\begin{aligned} \alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n &= y_1 \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n &= y_2 \\ \vdots &\quad \vdots \\ \alpha_{m1}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{mn}x_n &= y_m \end{aligned}$$

where the elements α_{ij}, y_i lie in F. And, we may seek solutions

$$x_1, \ldots, x_n \in F.$$

The method of elimination via row operations works without modification for any field F.

For example, we may solve the following system of equations in the field $\mathbb{Z}/11\mathbb{Z}$:

$$\begin{aligned} \overline{2}x_1 + \overline{1}x_2 &= \overline{3} \\ \overline{4}x_1 + \overline{4}x_2 &= \overline{5} \end{aligned}$$

The multiplicative inverse of $\overline{2}$ in $\mathbb{Z}/11\mathbb{Z}$ is $\overline{6}$. The additive inverse of $\overline{4}$ is $\overline{7}$. After adding a multiple of $\overline{7} \cdot \overline{6}$ of the first equation to the second, we obtain:

$$\overline{2}x_2 = \overline{10}.$$

Using the multiplicative inverse of $\overline{2}$ again, we find:

$$x_2 = \overline{5}.$$

Then, using the original system, we find:

$$x_1 = \overline{10}.$$

V. Skew-fields

By the field axioms, the multiplication of a field is required to be commutative. However, we may consider algebraic structures satisfying all the field axioms except for the commutativity of multiplication.

A *skew-field* $(F, +, \cdot, 0, 1)$ consists of a set F together with two binary operations $+$ and $\cdot$ and two distinguished elements $0, 1 \in F$ satisfying the following properties:

(i) $(F, +, 0)$ is an abelian group,
(ii) $(F^*, \cdot, 1)$ is a group,
(iii) the distributive laws hold.

The multiplication of a skew-field is allowed to be non-abelian. Sometimes skew-fields are called *division rings*.

Certainly, every field is a skew-field. It is quite difficult to find skew-fields which are not fields. In 1905, Wedderburn proved all skew-fields with only finitely many elements are actually fields (their multiplication

is actually abelian). You can find the proof in most good algebra books in the library, but some knowledge of group theory is required.

To find an example of a true skew-field, we must look for a candidate with infinitely many elements. The most fundamental example is the skew-field of quaternions discovered by Hamilton in 1843.

We will first discuss the complex numbers. Given the real numbers $(\mathbb{R}, +, \cdot, 0, 1)$, we can construct the complex numbers $(\mathbb{C}, +, \cdot, 0, 1)$ in the following way. As a set, $\mathbb{C} = \mathbb{R} \times \mathbb{R}$,

$$\mathbb{C} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

Addition in $\mathbb{C}$ is defined by addition of real components:

$$(x, y) + (z, w) = (x + z, y + w). \tag{3}$$

Multiplication in $\mathbb{C}$ is defined in terms of multiplication in $\mathbb{R}$ by:

$$(x, y) \cdot (z, w) = (xz - yw, xw + yz). \tag{4}$$

Let $0 \in \mathbb{C}$ be $(0, 0)$, and let $1 \in \mathbb{C}$ be $(1, 0)$. Then, $(\mathbb{C}, +, \cdot, 0, 1)$ is a field. From the above definition, checking the field axioms for the complex numbers takes some work.

The usual representation of complex numbers is as follows. Let $i \in \mathbb{C}$ be the element

$$i = (0, 1).$$

Then, by the definition of multiplication,

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1.$$

Complex numbers can be written as $x + yi$ where $x, y \in \mathbb{R}$. You can check the definitions of addition (3) and multiplication (4) coincide with the familiar operations for complex numbers.

The complex numbers have a norm defined by

$$||x + yi||^2 = x^2 + y^2$$

which satisfies a multiplicative property:

$$||\mu \cdot \nu||^2 = ||\mu||^2 ||\nu||^2,$$

for all $\mu, \nu \in \mathbb{C}$.

We are now prepared to describe Hamilton's quaternions $(\mathbb{H}, +, \cdot, 0, 1)$. Introduce the elements i, j, k with the multiplicative properties:

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1,$$

$$ij = k, \quad ji = -k, \tag{5}$$

$$jk = i, \quad kj = -i,$$
$$ki = j, \quad ik = -j.$$

Let $\mathbb{H}$ be set of linear combinations,

$$\mathbb{H} = \{w + xi + yj + zk \mid w, x, y, z \in \mathbb{R}\}.$$

Addition is defined on $\mathbb{H}$ by addition of the components,

$$(w + xi + yj + zk) + (w' + x'i + y'j + z'k) =$$
$$(w + w') + (x + x')\ i + (y + y')\ j + (z + z')\ k.$$

The element $0 \in \mathbb{H}$ is $0 + 0i + 0j + 0k$.

Multiplication in the quaternions is defined by the rules (5):

$$(w + xi + yj + zk) \cdot (w' + x'i + y'j + z'k) =$$
$$\begin{aligned} & (ww' - xx' - yy' - zz') \\ + \ & (wx' + xw' + yz' - zy')\ i \\ + \ & (wy' - xz' + yw' + zx')\ j \\ + \ & (wz' + xy' - yx' + zw')\ k. \end{aligned}$$

Certainly, multiplication in the quaternions is *not* commutative. The element $1 \in \mathbb{H}$ is $1 + 0i + 0j + 0k$.

Again, some work is required to check the quaternions satisfy the axioms of a skew-field. You might try to verify the axioms. Hamilton found the multiplication rules for the quaternions only after searching for 10 years. The name *quaternion* comes from the fact that i, j, and k are fourth roots of unity: $i^4 = j^4 = k^4 = 1$.

The quaternions have a norm defined by

$$||w + xi + yj + zk||^2 = w^2 + x^2 + y^2 + z^2$$

which satisfies a multiplicative property:

$$||\mu \cdot \nu||^2 = ||\mu||^2 ||\nu||^2,$$

for all $\mu, \nu \in \mathbb{H}$.

A remarkable result due to Frobenius states: the only skew-fields which are finite dimensional over the real numbers are: $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$.