CHAPTER 6

Rings & Fields

6.1. Rings

So far we have studied algebraic systems with a single binary operation. However many systems have two operations: addition and multiplication. Such a system is called a *ring.* Thus a ring is an algebraic generalization of $\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{Z}/n\mathbb{Z}$ etc.

6.1.1 Definition A *ring* R is a triple $(R, +, \cdot)$ satisfying

(a) $(R, +)$ is an abelian group,
(b) $(R, \cdot)$ is a semigroup,
(c) The distributive laws hold: for all a, b, $c \in R$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned}$$

We call $+$ *addition* and $\cdot$ *multiplication.*

If we write this out in full detail, a ring is a non-empty set R, on which are defined two binary operations $+$ and $\cdot$ satisfying for all a, b, $c \in R$

(a) $a + (b + c) = (a + b) + c$
(b) There exists element 0_R with $a + 0_R = a = 0_R + a$.
(c) For every a there exists $-a$ with $a + (-a) = 0_R = (-a) + a$
(d) $a + b = b + a$
(e) $a(bc) = (ab)c$
(f) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

From now on if there is no confusion, we just write 0 instead of 0_R.

6.1.2 Convention We give $\cdot$ higher precedence than $+$, so $a \cdot b + a \cdot c$ means $(a \cdot b) + (a \cdot c)$ not $a \cdot (b + a) \cdot c$. (This is another example of a prejudice that is heavily indoctrinated at an early age.)

Note that addition in a ring is always commutative, and there is always an additive identity, 0.

6.1.3 Definition A ring R is said to be *commutative* if multiplication is commutative, ie if $ab = ba$ for all a, $b \in R$. It has an *identity* if there is a multiplicative identity ie if there exists $1_R \in R$ with $1_R a = a = a 1_R$ for all $a \in R$.

From now on we denote the identity by 1 instead of 1_R if there is no risk of confusion.

Note: many authors require the existence of an identity in the definition of ring. There does not seem to be universal agreement on this point.

6.1.4 Example

★ $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are all commutative rings with identity.
★ $\mathbb{N}$ is not a ring. Additive inverses do not exist.
★ $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity. See theorem 2.2.8. Note that $\mathbb{Z}/n\mathbb{Z}$ is a finite ring, with n elements.

★ $M_n(\mathbb{R})$ is a non-commutative ring, with identity I.

★ The smallest possible ring is $\{0\}$, called the *zero ring* , often denoted 0 (instead of $\{0\}$). It satisfies the axioms for a commutative ring trivially (see below for another property of the 0 ring).

6.1.5 Example The set $2\mathbb{Z}$ of even integers is a commutative ring without identity element.

Proof If a and b are even, so are $a+b$ and ab, so $2\mathbb{Z}$ is closed under addition and multiplication. That is, addition and multiplication are binary operations on $2\mathbb{Z}$. Associativity and commutativity of addition and multiplication, and distributivity all hold in $\mathbb{Z}$ and hence hold in the subset $2\mathbb{Z}$. Also $0 \in 2\mathbb{Z}$, and if $n \in 2\mathbb{Z}$ then $-n \in 2\mathbb{Z}$. However there is no multiplicative identity: if e is the identity then if $ne = n$ so $e = 1 \notin 2\mathbb{Z}$.

6.1.6 Example $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ the *Gaussian integers* is a commutative ring with identity.

Proof It is easy to check that addition and multiplication of two Gaussian integers gives another Gaussian integer (exercise). Addition and multiplication are associative and commutative, since this is true in $\mathbb{C}$. Distributivity is also inherited from $\mathbb{C}$. Finally 0 and 1 are in $\mathbb{Z}[i]$, and if $z \in \mathbb{Z}[i]$ then $-z \in \mathbb{Z}[i]$.

We can also form the product of two rings.

6.1.7 Definition If R and S are rings, define[1] the *direct product* of R and S to be the set $R \times S$ with addition and multiplication given by

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2)\\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1 a_2, b_1 b_2)\end{aligned}$$

It is easy to check that $R \times S$ is a ring (compare the proof of theorem 5.1.10). This ring is denoted $R \times S$. If R and S are commutative, so is $R \times S$. If R and S have identities, so does $R \times S$: the identity will be $(1_R, 1_S)$.

Another important example of a ring is a polynomial ring.

6.1.8 Definition Let R be a commutative ring. The *polynomial ring with coefficients in* R denoted $R[x]$ consists of all polynomials in x, with the usual addition and multiplication.

Here x is a variable, not an element of R. The ring $R[y]$ consists of polynomials in the variable y etc.

Thus an element of $R[x]$ looks like

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

where the $a_i \in R$. If $q(x) = b_0 + b_1 x + \cdots + b_m x^m$ then $p(x) + q(x)$ is the polynomial

$$(a_0 + b_0) + (a_1 + b_1)x + \cdots$$

This makes sense, since each $a_i, b_i \in R$ so we can add them together.

Multiplication is a bit messy to write down, but is defined just as one would expect:

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$$

It is easy to check that $R[x]$ is a commutative ring. If R has an identity, so does $R[x]$ (namely the constant polynomial 1).

6.1.9 Example $\mathbb{Z}/3\mathbb{Z}[x]$ consists of all polynomials with coefficients in $\mathbb{Z}/3\mathbb{Z}$. For example,

$$p(x) = x^2 + 2, \quad q(x) = x^2 + x + 1 \in \mathbb{Z}/3\mathbb{Z}[x].$$

[1] $R \times S$ is also commonly called the *direct sum* of R and S, and denoted $R \oplus S$. This usage conflicts with a more general notion of sum, so ideally should be avoided.

Then

$$p(x) + q(x) = 2x^2 + x$$

and

$$p(x)q(x) = (x^2 + 2)(x^2 + x + 1) = x^4 + x^3 + 3x^2 + 2x + 2 = x^4 + x^3 + 2x + 2.$$

We have already seen that $M_n(\mathbb{R})$ is a ring. This does not rely on any special properties of the real numbers. We could also form the ring of matrices with entries in $\mathbb{C}$ or entries in $\mathbb{Z}$. All that we need to add and multiply matrices is to be able to add and multiply the corresponding entries, so we can take the entries to lie in any ring. The proofs that multiplication is associative, addition is associative and commutative etc are exactly the same as the proofs that these properties hold in $M_n(\mathbb{R})$.

6.1.10 Definition Let R be a ring. Let $M_n(R)$ denote the set of $n \times n$ matrices with entries in R. $M_n(R)$ is a ring, under matrix multiplication and addition.

$M_n(R)$ is not commutative even if R is (if $n \geq 2$). It has an identity if R does, namely the identity matrix I.

6.1.11 Example Let $\mathscr{F}$ be the set of all functions $f\colon \mathbb{R} \to \mathbb{R}$ (Example 4.1.3). Recall that if $f, g \in \mathscr{F}$ we define $f + g$ to be the function satisfying

$$(f + g)(x) = f(x) + g(x).$$

Similarly we define the product of f and g by

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

We proved in Example 4.1.3 that $\mathscr{F}$ is an abelian group under $+$. Multiplication is easily seen to be associative, and the distributive laws are easy to check. For example, to prove $f \cdot (g+h) = f \cdot g + f \cdot h$ we must check that this holds for all possible inputs. But

$$\begin{array}{rcll} f \cdot (g + h)(x) & = & f(x) \cdot (g + h)(x) & \text{Def } \cdot \\ & = & f(x) \cdot \big(g(x) + h(x)\big) & \text{Def } + \\ & = & f(x)g(x) + f(x)h(x) & \text{Distributivity in } \mathbb{R} \\ & = & (f \cdot g)(x) + (f \cdot h)(x) & \text{Def } \cdot \\ & = & (f \cdot g + f \cdot h)(x) & \text{Def } + \end{array}$$

In fact, R is a commutative ring with identity.

81 Exercise Let R be the set of all functions $f\colon \mathbb{R} \to \mathbb{R}$. Define addition as in the previous example, but define multiplication to be composition of functions: fg is defined to be $f \circ g$. Is R a ring? Explain.

82 Exercise An element x of a ring R is said to be *nilpotent* if $x \neq 0$ but $x^n = 0$ for some $n \geq 1$. Show that R has no nilpotent elements iff $x^2 = 0$ has only the solution $x = 0$ in R. Give an example of a ring with nilpotent elements.

83 Exercise Let S be any set, and let $\mathscr{P}(S)$ be the power set of S, that is, the collection of all subsets of S. Define $+$ and $\cdot$ on $\mathscr{P}(S)$ by

$$\begin{array}{rcl} A + B & = & (A \cup B) \setminus (A \cap B) \\ A \cdot B & = & A \cap B \end{array}$$

Prove that $\mathscr{P}(S)$ is a commutative ring with identity.

6.2. Subrings

6.2.1 Definition Let R be a ring. A non-empty subset $S \subseteq R$ is a *subring* if

(a) $(S, +)$ is a subgroup of $(R, +)$
(b) S is closed under multiplication: $s_1, s_2 \in S \implies s_1 \cdot s_2 \in S$.

In other words, S must satisfy: S is closed under addition, $0 \in S$, $(x \in S \implies -x \in S)$, and S is closed under multiplication. These properties ensure that S is a ring in its own right. (The distributivity laws hold in S automatically since they hold in the larger set R.)

6.2.2 Example $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$ which is a subring of $\mathbb{R}[x]$.

6.2.3 Example $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

6.2.4 Example $\mathbb{Z}/n\mathbb{Z}$ is not a subring of $\mathbb{Z}$. It is not even a subset of $\mathbb{Z}$, and the addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ are different than the addition and multiplication on $\mathbb{Z}$.

84 Exercise Show that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Prove that every subring of $\mathbb{Z}$ has this form for some n. (Hint: pick n to be the smallest non-zero element of S ...)

6.3. Basic Properties of Rings

A ring is a set with two binary operations, addition and multiplication. The operation of subtraction is not part of the definition, but it is easy to define a subtraction operation as follows.

6.3.1 Definition Let R be a ring. We define $a - b$ to be $a + (-b)$. Here $-b$ is the additive inverse of b.

In some ways this is a poor choice of notation. We use the same sign $-$ to indicate the additive inverse, and the binary operation of subtraction.[2] We should clarify that the notation works as we expect it will. The proofs of all these basic rules are very simple, although a bit notationally confusing:

6.3.2 Theorem Let R be a ring, and let $a, b, c \in R$. Then

(a) If $a + b = a + c$ then $b = c$.
(b) $a \cdot 0 = 0 = 0 \cdot a$.
(c) $a \cdot (-b) = -(ab) = (-a) \cdot b$.
(d) $-(-a) = a$.
(e) $-(a + b) = -a - b$.
(f) $-(a - b) = -a + b$.
(g) $(-a)(-b) = ab$.
(h) If R has an identity, then $(-1)a = -a$.

Proof

(a) If $a+b = a+c$ then add the additive inverse of a, $(-a)$ to both sides. Then $(-a)+a+b = (-a)+a+c$ so $0 + b = 0 + c$ so $b = c$. Note: this is a group theoretic property in the group $(R, +)$ and follows from theorem 5.3.1.

(b) $a \cdot 0 = a \cdot (0 + 0)$ 0 is the additive identity
So $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$ Definition of 0 (LHS), distributivity (RHS)

By (a), $a \cdot 0 = 0$. Similarly, $0 \cdot a + 0 = 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ so cancelling (using (a)) we get $0 \cdot a = 0$.

(c) We have to show that $a \cdot (-b)$ is the additive inverse of ab. That is, we must show $a \cdot (-b) + ab = 0$ ($+$ is commutative, so then $ab + a \cdot (-b) = 0$ also). But using the distributive property

$$a \cdot (-b) + ab = a\Big((-b) + b\Big) = a \cdot 0 = 0$$

by (b). Similarly $(-a)b + ab = \Big((-a) + a\Big)b = 0 \cdot b = 0$.

(d) This is a group theoretic result (written additively). See theorem 5.3.1.

[2] This may account many people's difficulties with operating with negative numbers: "minus times minus is plus; the reason for this we shall not discuss"; see the next theorem.

(e) We must show that $-a-b$ is the additive inverse of $(a+b)$, that is, we must show they add to 0. Here $-a-b$ stands for $(-a)+(-b)$, so we need to check that $a+b+(-a)+(-b)=0$. This is clear, since $+$ is commutative and $a+(-a)=0$ and $b+(-b)=0$.

The rest are left as exercises. □

85 Exercise Finish the Proof.

A ring can have two distinguished elements, 0 and 1. 0 is the additive identity, and 1 is the multiplicative identity. Can 0 ever be equal to 1? Recall that we write 0 for the 0 ring (the set $\{0\}$).

6.3.3 Theorem Let R be a commutative ring with identity. Then $0=1$ iff $R=0$.

Proof $\implies$ If $0=1$ then for every $a\in R$, $a=a\cdot 1=a\cdot 0=0$, so R consists only of the single element 0.

$\impliedby$ If $R=0$ then the only element of R is 0. So for every a in R, $0\cdot a=a=a\cdot 0$ (trivially), and this means 0 is the multiplicative identity. □

6.4. Units

We have talked about addition, subtraction and multiplication in rings. What about division? We can only divide under special circumstances. For example in $\mathbb{Z}$ we can divide 6 by 3 but not by 4 ($6/4\notin\mathbb{Z}$). In $\mathbb{Z}$ we can divide with impunity only by ± 1.

6.4.1 Definition Let R be a ring with identity. An element $u\in R$ is a *unit* if it has an multiplicative inverse. That is u is a unit iff there exists $v\in R$ with $uv=1=vu$. We denote v by u^{-1} and call it the *inverse* of u. The set of units of R is denoted $R^\times$.

If the inverse exists, it must be unique (theorem 4.3.2).

6.4.2 Example

- ★ $\mathbb{Z}^\times=\{\pm 1\}\quad(=\mu_2)$.
- ★ $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$, $\mathbb{R}^\times=\mathbb{R}\setminus\{0\}$.
- ★ $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of the congruence classes $[a]$ with $\gcd(a,n)=1$. This is a set with $\varphi(n)$ elements.
- ★ The units of $M_n(\mathbb{R})$ are the invertible $n\times n$ matrices (those with determinant not 0).

6.4.3 Example $\mathbb{R}[x]^\times\simeq\mathbb{R}^\times$. That is, only non-zero constant polynomials are units.

Proof Suppose $fg=1$. The degree of fg is the degree of f plus the degree of g, so $0\le\deg f+\deg g=\deg fg=\deg(1)=0$, so f and g are constant polynomials.

6.4.4 Theorem If R is a ring with identity, then $R^\times$ is a group.

Proof If u and v are units, so is uv because $(uv)^{-1}=v^{-1}u^{-1}$ by theorem 4.3.5, so $R^\times$ is closed under multiplication. Multiplication is associative, so $R^\times$ forms a semigroup. $1\in R^\times$, and if $u\in R^\times$ so is u^{-1} (because u^{-1} is invertible with inverse u again by theorem 4.3.5). □

6.4.5 Corollary This reproves that $GL_n(\mathbb{R})$ is a group inside the ring $M_n(\mathbb{R})$ (See Example 5.1.2). □

86 Exercise Show that if $u_1u_2\cdots u_n=1$ in a ring then all of the u_i are units.

87 Exercise Show that $0\in R^\times$ iff $R=0$. So if R is a non-trivial ring, the best we could hope for is that $R^\times=R\setminus\{0\}$. We discuss such rings later.

88 Exercise Show that $(A \times B)^\times = A^\times \times B^\times$. By induction,

$$(A_1 \times A_2 \times \cdots A_n)^\times = A_1^\times \times A_2^\times \times \cdots A_n^\times$$

89 Exercise Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Prove that $\mathbb{Z}[i]^\times = \pm i, \pm 1$.

[Hint: If $zw = 1$, take the complex modulus of each side. Now square. Now write $z = a + bi$, $w = c + di$. The function $a + bi \mapsto a^2 + b^2$ is called the *Norm* and is often useful in this ring.]

6.5. Homomorphisms

A ring homomorphism should respect both the additive and multiplicative structure of the ring.

6.5.1 Definition Let R and S be rings. A *ring homomorphism* $f\colon R \to S$ is a function satisfying

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \end{aligned}$$

for all a, $b \in R$. The *kernel* of f is the set of elements mapped to 0:

$$\ker f = \{x \in R \mid f(x) = 0_S\}.$$

A ring *isomorphism* is a bijective ring homomorphism. We write $R \simeq S$ and say that R and S are *isomorphic* if there exists a ring isomorphism $R \to S$.

If $R \simeq S$ then R and S are structurally identical. The elements in S are just renamed versions of the elements in R.

90 Exercise Let R, S, T be rings. Show that

(a) $R \simeq R$.
(b) $R \simeq S \implies S \simeq R$.
(c) $R \simeq S$, $S \simeq T \implies R \simeq T$.

Hint: modify the proof of theorem 5.11.3.

6.5.2 Example

★ The complex conjugation map $\mathbb{C} \to \mathbb{C}$ is a ring isomorphism.

Proof Denote the conjugate of z by $\overline{z}$. Recall that $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$, so conjugation is a ring homomorphism. (These are easy to prove directly: let $z_1 = a + bi$, $z_2 = c + di$ and expand.)

If $\overline{z_1} = \overline{z_2}$, let $z_1 = a + bi$, $z_2 = c + di$. Then $a - bi = c - di$ so $a = c$, $b = d$ so $z_1 = z_2$. Thus conjugation is injective. Finally if $m + ni \in \mathbb{C}$ then $\overline{m - ni} = m + ni$ so conjugation is surjective also. □

★ The determinant map $\det\colon M_n(\mathbb{R}) \to \mathbb{R}$ is not a ring homomorphism because $\det(A + B) \neq \det(A) + \det(B)$.

★ The function $f\colon \mathbb{Z} \to 2\mathbb{Z}$ sending $x \mapsto 2x$ is a group isomorphism (compare Example 5.11.9). However it is not a ring isomorphism because $f(xy) = 2xy$ but $f(x)f(y) = (2x)(2y) = 4xy$. This means that as groups $\mathbb{Z}$ and $2\mathbb{Z}$ are identical. But as rings, they are not. For example, $2\mathbb{Z}$ does not contain a ring identity (Example 6.1.5) while $\mathbb{Z}$ does.

91 Exercise Let $f\colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be defined by $f(x) = 4x$. Is f a well defined ring homomorphism? If so, find its kernel and image.

92 Exercise Let R be a commutative ring with identity. Let $R[x]$ denote the polynomial ring in the variable x with coefficients in R and $R[y]$ denote the polynomial ring with variable y with coefficients in R. Prove that $R[x] \simeq R[y]$. (Don't get confused—this is very easy.)

93 Exercise Show that if $\gcd(m,n)=1$ then $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/mZ \times \mathbb{Z}/n\mathbb{Z}$. Hint: we have already shown the existence of a group isomorphism. Check that it preserves multiplication. This result is often called the CRT. If we combine this with Exercise 88 we get a nice proof that φ is multiplicative. Fill in the details.

6.6. Integral Domains & Fields

6.6.1 Definition Let $R \neq 0$ be a commutative ring with identity. A non-zero element $a \in R$ is called a *zero divisor* if there exists non-zero $b \in A$ with $ab = 0$. If R has no zero divisors it is called an *integral domain.*

(The 0 ring is usually not considered to be an integral domain.)

Intuitively, an integral domain is a lot like the integers.

6.6.2 Example

- ★ $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are integral domains.
- ★ (The congruence classes of) 2 and 3 are zero divisors in $\mathbb{Z}/6\mathbb{Z}$, so $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.
- ★ A subring of an integral domain is always an integral domain (the larger ring has no zero divisors, so the smaller certainly does not).
- ★ $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain: $(1,0)\cdot(0,1) = (0,0)$ so $(1,0)$ and $(0,1)$ are zero divisors.

6.6.3 Theorem Let $n \geq 2$. Then $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime.

Proof

$\Longleftarrow$ Let $n = p$ be prime. Suppose $[a]$ and $[b]$ are zero divisors in $\mathbb{Z}/p\mathbb{Z}$, with $1 \leq a, b < p$. Then $ab \equiv 0 \pmod{p}$ so $p \mid ab$ but then $p \mid a$ or $p \mid b$ by theorem 1.7.2. Contradiction. So there are no zero divisors.

$\Longrightarrow$ If n is not prime then it has proper factors a, b with $1 < a, b < n$ and $n = ab$. So in $\mathbb{Z}/n\mathbb{Z}$, $[a], [b] \neq 0$ but $[a][b] = [ab] = [n] = [0]$. □

In integral domains cancellation holds.

6.6.4 Theorem Let A be an integral domain. If $ab = ac$ with $a \neq 0$ then $b = c$. That is, (multiplicative) cancellation holds in A.

Proof If $ab = ac$ then $0 = ab - ac = a(b-c)$. A product of two non-zero elements in an integral domain is non-zero. Hence $b - c = 0$ so $b = c$. □

This result does not hold without the integral domain hypothesis.

6.6.5 Example In $\mathbb{Z}/6\mathbb{Z}$, $2\cdot 1 \equiv 2\cdot 4$ but $1 \neq 4$. If we try the proof above, $0 \equiv 2\cdot 4 - 2\cdot 1 = 2\cdot(4-1) = 2\cdot 3$ but this does not mean that $3 \equiv 0$.

An even more special type of ring is a field.

6.6.6 Definition Let $K \neq 0$ be a commutative ring with identity. Then K is a *field* if every non-zero element is a unit.

That is, in a field we can "divide" by everything except 0.

6.6.7 Example

- ★ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields: if x is a non-zero element of one of these rings, then so is $1/x$ and $x\cdot(1/x) = 1$ so x is a unit.

★ $\mathbb{Z}$ and $\mathbb{Z}[i]$ are integral domains but not fields. For example, 2 is not a unit since $1/2$ is not in either ring.

6.6.8 Theorem

(a) Every field is an integral domain.
(b) Every finite integral domain is a field.

Proof

(a) Let K be a field. If $ab = 0$ with $a \neq 0$ then multiply each side by a^{-1} to get $a^{-1}ab = a^{-1}0$ so $b = 0$. Thus K has no zero divisors.

(b) Let A be a finite integral domain with n elements. Since $A \neq 0$ there exists $a \in A \setminus \{0\}$. Let

$$S = \{ax \mid x \in A\} \subseteq A.$$

If $ax = ay$ then $x = y$ by theorem 6.6.4. Thus S has exactly n elements. In particular it contains 1, so $ax = 1$ for some x. Thus a is a unit. □

$\mathbb{Z}$ is an integral domain but not a field. *$\mathbb{Z}/n\mathbb{Z}$ is a field if n is prime. Otherwise it is not even an integral domain.*

6.6.9 Definition We sometimes denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$ and call it the *finite field* with p elements.

Are there any other finite fields besides $\mathbb{F}_p$?

6.6.10 Theorem Let K be a finite field. Then K has p^n elements for some prime p and $n \geq 1$. Moreover there exists exactly one finite field (up to isomorphism) of order p^n for each p and n.

Proof Omitted. □

In general the unique finite field with $q = p^n$ elements is often denoted $\mathbb{F}_q$. Finite fields are extremely useful in cryptography, coding, combinatorics etc.

94 Exercise For each of the below, determine whether the given set is a ring. If it is, state whether the ring is commutative, has identity, is an integral domain and is a field.

(a) $n\mathbb{Z}$ with the usual addition and multiplication.
(b) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
(c) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

95 Exercise Let R be a ring. Show that R is commutative iff $a^2 - b^2 = (a - b)(a + b)$ for all a, $b \in R$.

96 Exercise Show that $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero divisor in the ring $M_2(\mathbb{Z}/2\mathbb{Z})$.

97 Exercise Prove: If A is an integral domain, then $A[x]$ is also an integral domain.

98 Exercise Suppose R and S are rings, and $f\colon R \to S$ is a non-zero homomorphism (that is, it is not the case that $f(x) = 0$ for all x). Suppose R has an identity and S has no zero divisors. Show that $f(1_R) = 1_S$.

99 Exercise Show that $\mathbb{Q} \not\simeq \mathbb{R}$ and $\mathbb{R} \not\simeq \mathbb{C}$. Hint: if a polynomial has a root in K and $K \simeq L$, a corresponding polynomial has a root in L.

6.7. Ideals

Ideals in ring theory play the same role that normal subgroups do in group theory. An ideal is a special type of subring.

Let R be a commutative ring and let I be an additive subgroup of $(R,+)$. Then we may form the set R/I of left cosets. Since $(R,+)$ is abelian, I is automatically normal and R/I is a group. What do we need for it to be a ring?

Recall the condition for cosets (written additively) to be equal (theorem 5.12.6):

$$a+I=b+I \iff a-b\in I.$$

We would like to define multiplication of cosets. If $a+I,\ b+I\in R/I$ we would like to define

$$(a+I)(b+I)=ab+I.$$

Does this make sense? Is multiplication well defined? If $a_1+I=a_2+I,$ so $a_1-a_2\in I$ and $b_1+I=b_2+I$ so $b_1-b_2\in I$ then we need $a_1b_1+I=a_2b_2+I$: so we need $a_1b_1-a_2b_2\in I$.

Now $a_1b_1-a_2b_2=a_1b_1-a_2b_1+a_2b_1-a_2b_2=(a_1-a_2)b_1+a_2(b_1-b_2)$. We know that a_1-a_2 and $b_1-b_2\in I$. This motivates the following definition.

6.7.1 Definition An *ideal* I of a commutative ring R is a subgroup of $(R,+)$ satisfying

$$\forall a\in R\quad \forall x\in I\quad ax\in I \text{ and } xa\in I.$$

If I is an ideal of R, we write $I\trianglelefteq R$.

The *quotient ring* or *factor ring* R/I is the ring of all *cosets* or *residue classes* $a+I$, with $a\in R$. Addition and multiplication in R/I are defined by

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)(b+I)=ab+I.$$

A subring S of R is a subgroup of $(R,+)$ that is closed under multiplication by elements in S. An ideal I of $(R,+)$ is a subgroup of $(R,+)$ that is closed not just under multiplication by elements in I, but under multiplication (on either side) by *all elements in* R.

6.7.2 Example If R is a ring, 0 and R are always ideals of R.

6.7.3 Example $3\mathbb{Z}\trianglelefteq\mathbb{Z}$.

Proof We have already seen that $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (Example 5.12.4). We have to check that if $x\in 3\mathbb{Z}$ and a is *any* integer then ax and $xa\in 3\mathbb{Z}$. This is clear because if $3\mid x$ then $3\mid ax=xa$.

The factor ring is $\mathbb{Z}/3\mathbb{Z}$. This has 3 cosets, And $1+3\mathbb{Z}=\{\ldots,-4,-1,2,5,\ldots\}$, $2+3\mathbb{Z}=\{-5,-2,1,4,\ldots\}$, and $0+3\mathbb{Z}=\{\ldots,-6,-3,0,3,6\ldots\}$ as we have already seen.

6.7.4 Example $n\mathbb{Z}\trianglelefteq\mathbb{Z}$. The proof is a generalization of the previous example. The quotient ring is $\mathbb{Z}/n\mathbb{Z}$.

6.7.5 Example Let I be the set of all polynomials in $\mathbb{Z}[x]$ with 0 constant term. Then $I\trianglelefteq\mathbb{Z}[x]$.

Proof $0\in I$, and if $p(x)$, $q(x)$ have no constant term, neither does $p(x)-q(x)$. So I is a subgroup of $\mathbb{Z}[x]$. Finally if $p(x)\in I$ and $r(x)\in\mathbb{Z}[x]$ then $p(x)=p_1x+p_2x^2+\cdots+p_nx^n$ and $r(x)=r_0+r_1x+\cdots+r_mx^m$ then $p(x)r(x)=p_1r_0x+\cdots$ has no constant term, so $p(x)r(x)\in I$. □

6.7.6 Theorem Let R be a commutative ring. Let $a\in R$, and let $\langle a\rangle=\{ab\mid b\in R\}$. Then $\langle a\rangle\trianglelefteq R$.

Proof $\langle a\rangle$ is non-empty. If $ra,\ sa\in\langle a\rangle$ then $ra-sa=(r-s)a\in\langle a\rangle$, so $\langle a\rangle$ is a subgroup. Finally if $ra\in\langle a\rangle$ and t is any element of R then $(ra)t=t(ra)=(tr)a\in\langle a\rangle$, so $\langle a\rangle\trianglelefteq R$. □

For example in $\mathbb{Z}$, $n\mathbb{Z}=\langle n\rangle$. In the previous example, the ideal $I\trianglelefteq\mathbb{Z}[x]$ is $\langle x\rangle$, the set of multiples of x.

6.7.7 Definition Let R be a commutative ring. The ideal $\langle a\rangle$ is called the *principal ideal* generated by a.

6.7.8 Theorem Let R be a commutative ring with $I \trianglelefteq R$. Then R/I is a well defined ring. The map $R \to R/I$ given by $a \mapsto a + I$ is a surjective ring homomorphism.

Proof Exercise. We already know A/I is a well defined group, and the discussion above the definition of ideal shows that multiplication is well defined. We also know $a \mapsto a+I$ gives a group homomorphism; check that it respects multiplication. □

100 Exercise Find a subring of $\mathbb{Z} \times \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \times \mathbb{Z}$.

101 Exercise Let K be a field. Show that the only ideals of K are 0 and K.

102 Exercise An element a of a commutative ring R is said to be *nilpotent* if $a \neq 0$ but $a^n = 0$ for some $n \in \mathbb{N}$. Let N be the set of nilpotent elements of R, together with 0. Show that $N \trianglelefteq R$.

103 Exercise Let R be a commutative ring and $I \trianglelefteq R$. Let $\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$. Show that $I \subseteq \sqrt{I} \trianglelefteq R$.

104 Exercise Let R be a ring. Describe the factor rings R/R and $R/0$.

105 Exercise Give an example to show that a factor ring of an integral domain may be a field. Give another example to show that a factor ring of an integral domain may not be an integral domain.

This completes the algebra section of the course.

" . . . I thought Jem and I would get grown but there wasn't much else left for us to learn, except possibly algebra."

To Kill A Mocking Bird.

Bibliography

[1] M. Artin *Algebra*, 1991.

[2] R. Crandall, C. Pomerance *Prime Numbers, A Computational Perspective*, Springer, 2001.

[3] J. Fraleigh, *A First Course in Abstract Algebra*, 7th edition, 2003.

[4] T. Hungerford, *Abstract Algebra, An Introduction*, Saunders College Publishing, 1990.

[5] T. Hungerford, *Algebra*, Graduate Texts in Mathetics 74, Springer, 1974.

[6] *Elementary Number Theory and its Applications* 3rd edition, Addison-Wesley, 1992.