In this chapter we introduce some of the concepts which are needed to study abstract rings, and prove the first theorems of the subject.

§5a Subrings and subfields

5.1 DEFINITION (i) A subset S of a ring R is called a *subring* if S is itself a ring with respect to the operations of R.

(ii) A subset S of a field F is called a *subfield* if S is itself a field with respect to the operations of F.

For example, the ring $\mathbb{Z}$ is a subring of the field $\mathbb{R}$, but not a subfield. The rational numbers, $\mathbb{Q}$, form a subfield of $\mathbb{R}$, which is in turn a subfield of $\mathbb{C}$. The even integers, $2\mathbb{Z}$, form a subring of $\mathbb{Z}$.

5.2 THEOREM *Let R be a ring and S a subset of R such that*

(i) S is nonempty,

(ii) S is closed under multiplication (that is, $ab \in S$ for all $a, b \in S$),

(iii) S is closed under addition ($a + b \in S$ for all $a, b \in S$),

(iv) S is closed under forming negatives ($-a \in S$ for all $a \in S$).

Then S is a subring of R.

Conversely, any subring of R has these four properties.

Proof. Assume first that S is a subring of R. We must prove that the four properties above are satisfied.

Since S is a ring it must have a zero element. So $S \neq \emptyset$, and the first of the properties holds. Note also that if z is the zero of S and 0 the zero of R then $z + z = z$ (by the defining property of the zero of S) and $z + 0 = z$

(by the defining property of the zero of R), so that by Theorem 2.10 (i) we must have $z = 0$.

Now let a and b be arbitrary elements of S. Since the operations of addition and multiplication in R define operations on S we must have that $a+b$ and ab are elements of S. So properties (ii) and (iii) hold. Furthermore, since a must have a negative in S there must exist $x \in S$ such that

$$a + x = z = x + a.$$

But since $z = 0$ these equations also say that x is a negative of a in R. By Theorem 2.9 it follows that $x = -a$, and we have proved that $-a \in S$, as required.

For the converse we must assume that S satisfies properties (i)–(iv) and prove that it satisfies Definition 2.2. Observe that properties (ii) and (iii) guarantee that the sum and product in R of two elements of S are actually elements of S; hence the operations of R do give rise to operations on S. It remains to prove that Axioms (i)–(vi) of Definition 2.2 are satisfied in S. In each case the proof uses the fact that since R is a ring the same axiom is satisfied in R. The hardest part is to prove that the zero element of R is actually in S; so let us do this first.

We are given that S is nonempty; hence there exists at least one element $s \in S$. By property (iv) it follows that $-s \in S$, and so by property (iii)

$$0 = s + (-s) \in S.$$

Let a, b, $c \in S$. By Axioms (i), (iv), (v) and (vi) in R we have

$$\begin{aligned}(a + b) + c &= a + (b + c)\\ a + b &= b + a\\ (ab)c &= a(bc)\\ a(b + c) &= ab + ac\\ (a + b)c &= ac + bc\end{aligned}$$

and so it follows that Axioms (i), (iv), (v) and (vi) are satisfied in S.

We proved above that $0 \in S$. Now if a is any element of S we have (by Axiom (ii) in R) that $a + 0 = a = 0 + a$, and therefore 0 is a zero element for S. Moreover by property (iv) we have that $-a \in S$; thus each element of S has a negative in S. So S satisfies Axioms (ii) and (iii). □

Comments ▷▷▷

5.2.1 In the above proof we have also shown that every subring contains the zero element of the ring.

5.2.2 The point of proving theorems is that the work which goes into proving them never has to be repeated. One has simply to check that the hypotheses of the theorem are satisfied to be able to assert that its conclusion is satisfied, without repeating the steps of the proof. In particular, if we have to prove that something is a ring we can usually contrive to use a theorem (such as the above) in whose proof the tedium of checking the axioms one by one has already been dealt with. ▷▷▷

—*Examples*—

#1 Prove that $S = \{\, a + b\sqrt{3} \mid a, b \in \mathbb{Z} \,\}$ is a subring of $\mathbb{R}$.

≫▷ By Theorem 5.2 it is sufficient to check that S is nonempty and satisfies the three closure properties.

It is obvious that S is nonempty—for example $0 = 0 + 0\sqrt{3} \in S$.

Let α, $\beta \in S$. We must show that $\alpha\beta$, $\alpha + \beta$ and $-\alpha$ are all in S. By definition of S we have $\alpha = a + b\sqrt{3}$ and $\beta = c + d\sqrt{3}$ for some a, b, c, $d \in \mathbb{Z}$. Thus

$$\begin{aligned} \alpha + \beta &= (a + c) + (b + d)\sqrt{3} \\ \alpha\beta &= (ac + 3bd) + (ad + bc)\sqrt{3} \\ -\alpha &= (-a) + (-b)\sqrt{3}. \end{aligned}$$

In each case the right hand side has the form (integer)+(integer)$\sqrt{3}$, and so $\alpha + \beta$, $\alpha\beta$ and $-\alpha$ are all in S, as required. ◁≪

#2 Prove that

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

is a subring of $\mathrm{Mat}(2, \mathbb{Z})$.

≫▷ $S \neq \emptyset$ since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$.

Let $\alpha = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $\beta = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$ be arbitrary elements of S. Then

$$\alpha + \beta = \begin{pmatrix} a+d & b+e \\ 0 & c+f \end{pmatrix} \in S,$$

$$\alpha\beta = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in S,$$

$$-\alpha = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} \in S.$$

Hence the closure properties hold. ⊲≪

#3 Let $S = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \;\middle|\; a,\, b,\, c \in \mathbb{Z} \right\}$. Prove that S is not a subring of $\mathrm{Mat}(2, \mathbb{Z})$.

≫▷ The multiplication operation on $\mathrm{Mat}(2, \mathbb{Z})$ does not yield an operation on S, since the product of two elements of S need not be in S. For example,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in S \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in S,$$

but

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S.$$

⊲≪

#4 Let $R = \mathbb{Z}_8$ and let $S \subseteq R$ be given by

$$S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}.$$

Prove that S is a subring of $\mathbb{Z}_8$.

≫▷ Observe that $S = \{\, \overline{2r} \mid r \in \mathbb{Z} \,\}$. Obviously $S \neq \emptyset$.
Since

$$\overline{2r} + \overline{2s} = \overline{2r + 2s} \in S,$$

and

$$\overline{2r}\,\overline{2s} = \overline{4rs} = \overline{2(2rs)} \in S,$$

and

$$-\left(\overline{2r}\right) = \overline{2(-r)} \in S,$$

the required closure properties hold. ⊲≪

§5c Ideals

5.7 DEFINITION A subring I of a ring R is called an *ideal* of R if $ar \in I$ and $ra \in I$ for all $a \in I$ and $r \in R$.

Comment ▷▷▷

5.7.1 If I is an ideal in R then multiplying an element of I by any element of R and must give an element of I. Note that this is a more stringent requirement than closure under multiplication, which merely says that the product of two elements of I lies in I. An ideal must be closed under multiplication by arbitrary elements of the ring. ▷▷▷

—Example—

#12 Let $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$. Then I is nonempty ($0 \in 2\mathbb{Z}$), closed under addition (the sum of two even integers is even), closed under multiplication (the product of two even integers is even), and closed under forming negatives (the negative of an even integer is even). So I is a subring of R. To observe that in fact it is an ideal it remains to show that I is closed under multiplication by arbitrary elements of R—that is, show that the product of an even integer and an arbitrary integer gives an even integer. But this is obvious.

Note that in the above example it was not really necessary to prove closure under multiplication separately since it follows from closure under multiplication by ring elements. This observation yields the following proposition:

5.8 PROPOSITION *A subset I of a ring R is an ideal if and only if the following all hold:*

(i) *I is nonempty.*

(ii) *For all x and y, if $x \in I$ and $y \in I$ then $x + y \in I$.*

(iii) *For all x, if $x \in I$ then $-x \in I$.*

(iv) *For all x and y if $x \in I$ and $y \in R$ then $xy \in I$ and $yx \in I$.*

Proof. Suppose first that I is an ideal of R. Then I is a subring of R, and by Theorem 5.2 properties (i), (ii) and (iii) above all hold. Property (iv) holds too since it is explicitly assumed in the definition of an ideal.

Conversely, assume that I satisfies properties (i)–(iv). As remarked above it follows from property (iv) that I is closed under multiplication; thus all the requirements of Theorem 5.2 are satisfied, and it follows that I is a subring of R. This together with property (iv) shows that I is an ideal. □

—Example—

#13 Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}$$

and

$$I = \left\{ \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \;\middle|\; d \in \mathbb{Z} \right\}.$$

Prove that R is a subring of $\mathrm{Mat}(2, \mathbb{Z})$ and I is an ideal of R.

≫▷ That R is a subring of $\mathrm{Mat}(2, \mathbb{Z})$ was proved in #2. Clearly I is nonempty—for instance, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$. Let x and y be arbitrary elements of I and r an arbitrary element of R. Then for some integers a, b, c, d, e,

$$x = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \qquad y = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \qquad r = \begin{pmatrix} c & d \\ 0 & e \end{pmatrix}$$

giving

$$x + y = \begin{pmatrix} 0 & a+b \\ 0 & 0 \end{pmatrix} \qquad rx = \begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix}$$

$$-x = \begin{pmatrix} 0 & -a \\ 0 & 0 \end{pmatrix} \qquad xr = \begin{pmatrix} 0 & ae \\ 0 & 0 \end{pmatrix}$$

and since these are all in I it follows that I is an ideal. ◁≪

§5d The characteristic of a ring

Let R be any ring. If $a \in R$ we define

$$\begin{aligned} 1a &= a \\ 2a &= a + a \\ 3a &= a + a + a \end{aligned}$$

and so on. In general, if m is any positive integer,

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ terms}}.$$

If m is a negative integer we define

$$ma = -\big((-m)a\big)$$

observing that $(-m)a$ has already been defined since $-m$ is positive. And for the case $m = 0$ we define $0a = 0$. We have now defined ma whenever $m \in \mathbb{Z}$ and $a \in R$. This is a method of multiplying ring elements by integers, and is not to be confused with the multiplication operation within R itself. (But—fortunately—the value $0a$ is the same whether 0 is interpreted as an integer or the zero of the ring, and the same applies to $1a$ if R has an identity element.)

Similarly we define $a^m = aa \ldots a$ (m factors) if $m \in \mathbb{Z}^+$; if R has an identity element 1 we define $a^0 = 1$ for all $a \in R$; if m is negative and $a \in R$ has an inverse we define $a^m = (a^{-1})^{-m}$. The following should be clear:

5.9 PROPOSITION *Let R be any ring, $a \in R$ and $m, n \in \mathbb{Z}$. Then*

(i) $m(na) = (mn)a$ *and* $(m+n)a = ma + na$,

(ii) $(a^m)^n = a^{mn}$ *and* $a^{m+n} = a^m a^n$.

(If either m or n is negative the second part is only applicable if a has an inverse; similarly, if either m or n is zero it is only applicable if R has an identity.)

5.10 DEFINITION Let R be a ring. If there is a positive integer n such that $na = 0$ for all $a \in R$ then the least such n is called the *characteristic* of R. If there is no such n then R is said to have characteristic 0.

—*Examples*—

#14 The characteristic of $\mathbb{Z}_2$ is 2, the characteristic of $\mathbb{Z}_3$ is 3, and so on.

#15 Let S be the subring of $\mathbb{Z}_8$ given by $S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$. Observe that

$$\bar{2} \neq \bar{0}, \quad \bar{2} + \bar{2} = \bar{4} \neq \bar{0}, \quad \bar{2} + \bar{2} + \bar{2} = \bar{6} \neq \bar{0}.$$

So the characteristic of S is not 1, 2, or 3. But

$$\begin{aligned} \bar{2} + \bar{2} + \bar{2} + \bar{2} &= \bar{8} \ = \bar{0} \\ \bar{4} + \bar{4} + \bar{4} + \bar{4} &= \overline{16} = \bar{0} \\ \bar{6} + \bar{6} + \bar{6} + \bar{6} &= \overline{24} = \bar{0} \\ \bar{0} + \bar{0} + \bar{0} + \bar{0} &= \bar{0}. \end{aligned}$$

So S has characteristic 4. (This shows that the characteristic of a subring can be less than the characteristic of the ring, since $\mathbb{Z}_8$ has characteristic 8.)

If a ring R has an identity element, 1, then $na = 0$ for all $a \in R$ if and only if $n1 = 0$. From this we can deduce the following proposition:

5.11 PROPOSITION *If R is a ring with identity element 1 then the characteristic of R is the least positive integer n such that $n1 = 0$, or zero if there is no such n.*

Proof. Define

$$H = \{\, m \in \mathbb{Z}^+ \mid m1 = 0 \,\}$$

and

$$K = \{\, m \in \mathbb{Z}^+ \mid ma = 0 \text{ for all } a \in R \,\}.$$

We prove that $H = K$.

Let $m \in H$. Then $m1 = 0$, and so for all $a \in R$ we have

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ terms}} = a(\underbrace{1 + 1 + \cdots + 1}_{m \text{ terms}}) = a(m1) = a0 = 0.$$

Hence $m \in K$.

Conversely, if $m \in K$ then $ma = 0$ for all $a \in R$, and, in particular, $m1 = 0$, whence $m \in H$. Thus $m \in K$ if and only if $m \in H$, and so $H = K$, as claimed.

By Definition 5.10 the characteristic of R is the least element of K, or zero if $K = \emptyset$. Since $H = K$ this shows that the characteristic of R is the least element of H, or zero if $H = \emptyset$, and this is precisely the assertion of Proposition 5.11. □