# Chapter 3

# Rings and Fields

We have spent a term so far studying groups. Groups occur in so many places because all that they require is a set with a binary operation which has three 'nice' properties (associativity, identity and invertible elements). These properties are held by most of the binary operations we use on a regular basis, such as addition, multiplication, composition of functions and so on. However, many of the sets, in particular number sets, that we work with, have a richer structure, with more than one binary operation on them. To investigate this structure, we deal with two more specific types of object, namely rings and fields.

## 3.1 Definitions and Examples

When we define a ring, what we have in mind is the set of integers, which has the two 'obvious' binary operations of addition and multiplication.

**Definition 3.1.1.** A *ring* is a set $R$ with two binary operations called *addition* and *multiplication* satisfying axioms R1 to R4 below. For $a, b \in R$, addition is denoted $a+b$, and multiplication is denoted $ab$ (or occasionally $a \cdot b$).

**R1** $(R, +)$ is an abelian group, with identity called 0.

**R2** For all $a, b \in R$, $ab \in R$ (multiplicative closure).

**R3** For all $a, b, c \in R$, $a(bc) = (ab)c$ (multiplicative associativity).

**R4** For all $a, b, c \in R$, $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$ (distributive laws).

The first axiom is really five axioms for the price of one, because it says that $R$ is an abelian group under addition. We do not require that $R$ be a group under multiplication though. In fact, providing it has at least two elements, $R$ can't be a group under multiplication, as Lemma 3.1.6 will show. But multiplication does need to be associative and $R$ has to be closed under multiplication. The final axiom, distributivity, is necessary to tell us how these two operations interact.

**Example 3.1.2.** The set of integers, with the usual addition and multiplication, is a ring. We already know that $(\mathbb{Z}, +)$ is an abelian group, and certainly the product $ab$ of any two integers is an integer. Multiplication is associative, and the distributive laws also hold. Proof of these facts relies on formal definitions of the integers and addition and multiplication, which is not in the remit of this module!

The definition of a ring does not completely capture all the information about $\mathbb{Z}$ though. For example, we know that although the integers do not form a group under multiplication, there is an identity

element, namely 1, for multiplication. Also, multiplication is commutative. With this in mind, we can refine the definition of a ring further by adding more properties:

**Definition 3.1.3.** Let $R$ be a ring. Then

- $R$ is a *ring with identity* if there exists an element $1 \in R$, with $1 \neq 0$, such that for all $a \in R$, $1a = a1 = a$.
- $R$ is a *division ring* if it is a ring with identity and for all $a \in R$ with $a \neq 0$, there exists $b \in R$ with $ab = ba = 1$.
- $R$ is a *commutative ring* if for all $a, b \in R$, $ab = ba$.
- $R$ is a *field* if it is a commutative division ring.

Writing $R^*$ for the set of nonzero elements of $R$, so that $R^* = R \setminus \{0\}$, we can reformulate the definition of a field as follows.

**Definition 3.1.4.** Let $R$ be a set with addition and multiplication maps defined on it. Then $R$ is a field precisely when both $(R, +)$ and $(R^*, \cdot)$ are abelian groups with distinct identity elements and the distributive axiom (R4) holds.

**Example 3.1.5.** The set of integers is a commutative ring with identity (sometimes shortened to CR-with-1). However it is certainly not a division ring (or a field) because most elements do not have a multiplicative inverse — for example there is no integer $b$ such that $2b = 1$.

**Lemma 3.1.6.** *Let $R$ be a ring. For all $a \in R$, $0a = 0$. Moreover if $R$ has at least two elements, then $R$ is not a group under multiplication.*

Lemma 3.1.6 essentially shows that a field has about as much structure as possible for two operations interacting nicely with each other — by which I mean obeying the distributive laws.

*Proof.* Let $a \in R$. Because 0 is the additive identity, $0 + 0 = 0$. Therefore $(0 + 0)a = 0a$. But, from the distributive law, $(0 + 0)a = 0a + 0a$. So we have

$$0a = 0a + 0a.$$

Hence

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

Therefore

$$0 = 0a + 0.$$

So

$$0 = 0a.$$

(Note, we have implicitly used associativity here.) Therefore $0a = 0$. This means that if $a$ is any other element of $R$ then $0a \neq a$, so 0 is not a multiplicative identity and if there is a multiplicative identity other than 0, then 0 has no multiplicative inverse. Therefore $R$ cannot be a group under multiplication. □

Notice that, in the last proof, we effectively cancelled one $0a$ from each side by adding the additive inverse of $0a$, namely $-0a$, to each side. This will always work, so in future we will happily cancel like this without bothering to write the intermediate steps every time. Lemma 3.1.6 shows that, provided it has at least two elements, a ring $R$ cannot be a group under multiplication. In some cases though, the ring has a multiplicative identity and every nonzero element is invertible with respect to multiplication.

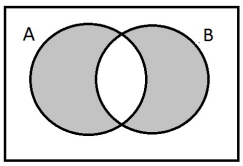
**Example 3.1.7.** Let $R$ be $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Each of these sets is an abelian group under addition, and in addition $\mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ are all abelian groups under multiplication. Furthermore the distributive laws hold in each case. Therefore $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are not only rings, but in fact are fields under the usual addition and multiplication.

**Example 3.1.8.** Consider the set $\mathcal{M}_2(\mathbb{R})$ of $2 \times 2$ real matrices. This is an abelian group under matrix addition. Moreover under matrix multiplication (which is associative) it is closed, and the distributive laws hold. Therefore $\mathcal{M}_2(\mathbb{R})$ is a ring. It is a ring with identity because the usual identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity element for matrix multiplication. It is not a division ring because not all the nonzero elements are invertible — the invertible elements comprise precisely the proper subset $GL_2(\mathbb{R})$. So, for example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is not invertible. Nor is $\mathcal{M}_2(\mathbb{R})$ commutative, as for example $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

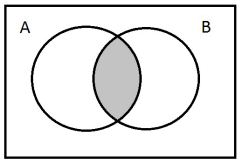
**Exercise 3.1.** Let $R$ be a ring. Define $\mathcal{M}_2(R)$ to be the set of $2 \times 2$ matrices with entries in $R$. Show that $\mathcal{M}_2(R)$ is a ring (you may assume without proof that the associative and distributive laws hold for matrix addition and matrix multiplication). Under what criterion for $R$ is $\mathcal{M}_2(R)$ a ring with identity? Is $\mathcal{M}_2(R)$ ever a commutative ring? a division ring? a field?

The definition of a ring, while more proscriptive than the definition of a group, is sufficiently loose that examples crop up in wider arenas than those of numbers and matrices. Here is an example from set theory, called a Boolean Ring.

**Example 3.1.9.** Let $\mathcal{E}$ be a set, and consider the collection $R$ of all subsets of $\mathcal{E}$ (that is, the power set of $\mathcal{E}$). There are several binary operations that can be defined on $R$. The most obvious are union $\cup$ and intersection $\cap$. Unfortunately $R$ is not a group under either of these, but we can modify $\cup$ slightly so that things work. Define $A + B$ to be $(A \cup B) \setminus (A \cap B)$. This is known as the *symmetric difference* of $A$ and $B$. In other words, $A + B$ is the set of elements lying in exactly one of $A$ and $B$, as shown in the Venn diagram below left. We also define $A \cdot B$ as just $A \cap B$, shown below right.

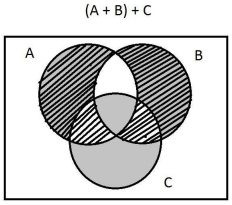


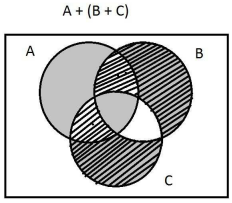

$A + B$




$A \cdot B$

To prove $R$ is a ring, we need to establish that the axioms hold. First, we'll show that $(R, +)$ is an abelian group. Since $A + B$ is a subset of $\mathcal{E}$, and $R$ is the collection of all subsets of $\mathcal{E}$, certainly $A + B \in R$, so $R$ is closed under $+$. Next, associativity. This can be proved with Venn diagrams. The diagram on the left over the page shows $A + B$ indicated by diagonal lines, and $(A + B) + C$ (shaded grey), is the elements lying in exactly one of $(A + B)$ and $C$. The diagram on the right shows $(B + C)$ indicated by diagonal lines and $A + (B + C)$ shaded grey.



From the diagram we can see that the two shaded regions are the same and hence

$$(A + B) + C = A + (B + C).$$

Thus + is associative. The identity element for + is clearly $\emptyset$ as $A + \emptyset = \emptyset + A = A$ for all $A$. Finally, each $A$ is self inverse, as $A + A = A \cup A \setminus A \cap A = A \setminus A = \emptyset$. Also from the definition + is clearly commutative. Therefore $(R, +)$ is an abelian group.

Next, we note that $A \cap B \in R$ for all $A, B \in R$, and that $\cap$ is associative — this is Exercise 3.2. Finally, we can check, again using Venn diagrams, that the distributive laws hold — this is Exercise 3.3. Therefore $R$ is a ring, called a Boolean ring, after the mathematician and logician Boole — see the historical notes at the end of the chapter.

**Exercise 3.2.** Show, using Venn diagrams, that $\cap$ is associative — that is, for all sets $A, B, C$, we have $(A \cap B) \cap C = A \cap (B \cap C)$.

**Exercise 3.3.** Show, using Venn diagrams, that the distributive laws hold for the Boolean ring described in Example 3.1.9. Namely, show that for all $A, B, C \in R$, we have $(A + B) \cap C = (A \cap C) + (B \cap C)$ and $C \cap (A + B) = (C \cap A) + (C \cap B)$.

**Exercise 3.4.** Let $R$ be the Boolean ring described in Example 3.1.9. Is $R$: a ring with identity? a division ring? a commutative ring? a field? Justify your answers in each case.

If $\mathcal{E}$ is finite, then the Boolean ring associated with it is also finite. For more examples of finite rings, we can look at integers modulo a positive integer $n$.

**Exercise 3.5.** Let $n$ be a positive integer. Consider $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Let the addition operation be $\oplus_n$ and multiplication be $\otimes_n$. Show that $\mathbb{Z}_n$ is a ring with these operations. Show further that $\mathbb{Z}_n$ is a commutative ring with identity.(You may use any properties of $\oplus_n$ and $\otimes_n$ given in Chapter 1.) From now on, we refer to the ring $\mathbb{Z}_n$ without specifying the operations: they will always be $\oplus_n$ and $\otimes_n$, unless otherwise stated. I also reserve right to drop the $n$ subscript where our choice of $n$ is clear, and just write $\oplus$ and $\otimes$.

**Example 3.1.10** (Polynomials)**.** One very useful type of ring is a ring of polynomials. We know that we can add and multiply polynomials together, and subtract one from another, but we cannot usually divide one polynomial by another and still end up with a polynomial. In a situation like this, a ring is the perfect structure. Let $R$ be any ring (but nearly always it will be a ring of numbers, such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$). An $R$ polynomial (or polynomial over $R$) in $x$ is simply a formal sum

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where each $a_i \in R$ and $n \geq 0$ is an integer, and either $a_i = 0$ for all $i$ (the zero polynomial) or $a_n \neq 0$. So we may speak of integer polynomials, real polynomials and so on. If we are dealing with $\mathbb{Z}_n$ we tend to speak of 'polynomials over $\mathbb{Z}_n$' rather than $\mathbb{Z}_n$ polynomials. The zero element is just the zero polynomial $0(x) = 0$. Let the set of all $R$ polynomials in $x$ be called $R[x]$. Suppose that $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_n \neq 0$. Then the *degree* of $f(x)$ is $n$, written $\deg(f(x)) = n$. If $R$ is a ring with identity 1, we say $f(x)$ is a *monic* polynomial if $a_n = 1$.

**Example 3.1.11.** Addition and multiplication in $R[x]$ is inherited from the addition and multiplication in the underlying ring. So, for example, in $\mathbb{Z}[x]$,

$$(3x + 2) + (4x + 1) = (3 + 4)x + (2 + 1) = 7x + 3$$

and

$$(3x + 2)(4x + 1) = (3 \times 4)x^2 + ((3 \times 1) + (2 \times 4))x + (2 \times 1) = 12x^2 + 11x + 2.$$

However in $\mathbb{Z}_5[x]$,

$$(3x+2)+(4x+1) = (3 \oplus_5 4)x + (2 \oplus_5 1) = 2x+3$$

and

$$(3x+2)(4x+1) = (3 \otimes_5 4)x^2 + ((3 \otimes_5 1) \oplus (2 \otimes_5 4))x + (2 \otimes_5 1) = 2x^2 + x + 2.$$

**Exercise 3.6.** Show that $R[x]$ is a ring for all rings $R$. Is $R[x]$: a ring with identity? a division ring? a commutative ring? a field? Justify your answers in each case. If the answer is 'sometimes', try and categorise for which $R$ the answer is yes, and for which the answer is no.

**Exercise 3.7.** Consider the set $R$ of all real-valued functions on $\mathbb{R}$. That is, the set of functions $f$ from $\mathbb{R}$ to $\mathbb{R}$. The operations of addition and multiplication of real-valued functions are the same ones as those used in $\mathbb{R}[x]$. With these operations, it can be shown that $R$ is a ring (feel free to check as many of the axioms as you wish). Is $R$: a ring with identity? a division ring? a commutative ring? a field?

Next we consider two natural questions; what is the smallest possible ring, and given any abelian group, is there some definition of multiplication that will make it into a ring?

**Example 3.1.12** (The Trivial Ring)**.** Certainly any ring is at least a group. The smallest group is the trivial group $\{e\}$, which just contains one element, the identity. Since we are after an abelian group, let's write this as $R = \{0\}$, and the operation as $+$, and we have $0+0=0$. If there is going to be a multiplication on this, there is only one possible definition that makes $R$ closed under multiplication, namely $0 \cdot 0 = 0$. Since the outcome of all additions and multiplications is 0, it is clear that by default addition and multiplication are commutative, associative, distributive and in fact that all the axioms for a ring hold. Therefore the smallest possible ring has exactly one element, and is known as the trivial ring. This cannot be a field because as part of the definition of a field we have a multiplicative identity element which is required to be distinct from the additive identity element, so any field must in particular have at least two elements.

**Exercise 3.8.** We proved in Exercise 3.5 that both $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are commutative rings with identity. Show that $\mathbb{Z}_2$ is a field and that $\mathbb{Z}_4$ is not a field.

**Example 3.1.13.** Let $R$ be any abelian group, call the operation $+$ (even if it isn't actually addition), and the identity element 0 (even if it isn't actually the number zero!). Then we can define a rather boring multiplication: for all $a, b \in R$, define $a \cdot b = 0$. Since $0 \in R$, certainly $R$ is closed under this operation, and since the result of any multiplication is the same, 0, the associative and distributive laws must hold. Therefore, under this rather dull operation, $R$ is a ring. It is called a *zero ring*. Any abelian group is therefore a ring, though we hope to be working with rather more interesting examples than this!

Finally in this section, we define the terms $na$ and $a^n$, for $n \in \mathbb{Z}$ and $a$ in a ring $R$.

**Definition 3.1.14.** Let $R$ be a ring, let $a \in R$, and let $n$ be a positive integer. Then $na$ denotes $\underbrace{a + \cdots + a}_{n \text{ times}}$. If $n = 0$ then define $na = 0$ (the zero element of $R$). The term $(-n)a$ denotes $n(-a)$; that is, $(-n)a = n(-a) = \underbrace{(-a) + \cdots + (-a)}_{n \text{ times}}$. Moreover $a^n$ denotes $\underbrace{aa \cdots a}_{n \text{ times}}$. If $R$ is a ring with identity, then define $a^0 = 1$. If $a$ has a multiplicative inverse $a^{-1}$, we define $a^{-n}$ to be $(a^{-1})^n$.

**Example 3.1.15.** For $a \in R$ we have $4a = a+a+a+a$ and $a^4 = aaaa$. In many examples the integers will themselves be elements of the ring. So $na$ actually means something in the ring already. Luckily it corresponds to our new definition!

**Exercise 3.9.** Let $\mathcal{E}$ be a set, and $R$ be the collection of all subsets of $\mathcal{E}$. This is the Boolean Ring defined in Example 3.1.9. Let $A \in R$. Find $0A$, $1A$, $2A$, $3A$, $(-2)A$, $(-3)A$. What is $nA$, in general (this will depend on $n$)?

**Exercise 3.10.** Let $R$ be the collection of subsets of a set $\mathcal{E}$ as in Example 3.1.9, let $A \in R$ and let $n \in \mathbb{Z}$. Determine $A^n$ for all $n$ such that $A^n$ is defined. This will depend on whether $R$ is a ring with identity, which was decided in Exercise 3.4, and on whether $A$ is invertible.

**Exercise 3.11.** (Revision) To prepare yourself for later sections, revise the Euclidean algorithm for the positive integers — this can be found for example in the Proof and Structure in Mathematics notes, which are available on the Algebra 2 website. It is an algorithm that, given any pair $(a, b)$ of positive integers, returns the greatest common divisor $\gcd(a, b)$ of $a$ and $b$. It can be reversed to find integers $r, s$ such that $ar + bs = \gcd(a, b)$.

## 3.2 Subrings

In this section we look at subrings, which have the obvious definition. In general it is much easier to show a set is a ring by showing it is a subring of a known ring.

**Definition 3.2.1.** Let $R$ be a ring. A *subring* of $R$ is a subset $S$ of $R$ which is itself a ring under the same addition and multiplication as $R$.

As with subgroups, we do not need to check all the axioms — things such as associativity are inherited from $R$. In fact, really we only need to check that the subset is closed under addition, multiplication and taking (additive) inverses:

**Proposition 3.2.2** (The Subring Criterion)**.** *Let $R$ be a ring. A subset $S$ of $R$ is a subring if $S$ is non-empty and for all $a, b \in S$ we have:*

*(i)* $a + b \in S$;

*(ii)* $-a \in S$;

*(iii)* $ab \in S$.

*Proof.* Suppose $S$ is a non-empty subset of $R$ which satisfies conditions (i)–(iii). We must work through the axioms for a ring to show that $S$ is a ring:

**R0 ($S$ is an abelian group):** We apply the Subgroup Criterion to show that $S$ is a subgroup of $R$. The set $S$ is non-empty. By (i) it is closed and by (ii) the inverse of every element of $S$ is in $S$. Furthermore any subgroup of an abelian group is abelian, so $S$ is abelian.

**R1 ($S$ is closed under multiplication)**: this is just (iii).

**R2 (multiplication on $S$ is associative):** inherited from $R$.

**R3 (distributive laws hold on $S$):** Since the laws hold over all of $R$, and $S \subseteq R$, certainly they hold in $S$. Therefore $S$ is a ring. □

There is also a finite subring criterion, corresponding to the finite subgroup criterion, but since we will mostly be working with infinite rings, I have not included it here. We should remark though, that because subrings are subgroups under addition, Lagrange's Theorem tells us that in a finite ring, the order of any subring divides the order of the ring.

**Definition 3.2.3.** A *number ring* is a subring of the ring $\mathbb{C}$, with the usual addition and multiplication.

**Example 3.2.4.** Define the set $\mathbb{Z}[\sqrt{2}]$ to be $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. We will show $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{C}$ and hence a number ring, using the subring test. Clearly, it is nonempty. Let $x = a+b\sqrt{2}$ and $y = c + d\sqrt{2}$ be arbitrary elements of $\mathbb{Z}[\sqrt{2}]$ (so $a, b, c, d \in \mathbb{Z}$).

$$\begin{aligned} x + y &= (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]. \\ -x &= -(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]. \\ xy &= (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]. \end{aligned}$$

Therefore, by the subring criterion, $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{C}$ and hence it is a number ring.

The previous example has shown that it is much easier to prove that something is a ring by showing it is a subring of a known ring, than to start from scratch and prove that it is an abelian group (5 things to check) plus three more axioms.

**Definition 3.2.5.** The *Gaussian integers* are the set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

This is one of the few examples of number rings that we may not have encountered before.

**Exercise 3.12.** Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and hence a number ring.

**Example 3.2.6.** Let us look at some subrings of our 'favourite' ring, $\mathbb{Z}$. Let $n$ be any non-negative integer, and consider the set $S = n\mathbb{Z} = \{nt : t \in \mathbb{Z}\}$. In other words, this is just the set of all integer multiples of $n$. Now $S$ is certainly nonempty. Let $a, b \in S$. Then $a = nk, b = nl$ for some $k, l \in \mathbb{Z}$. So: (i) $a + b = nk + nl = n(k + l) \in S$; (ii) $-a = -nk = n(-k) \in S$; and (iii) $ab = (nk)(nl) = n(knl) \in S$. Therefore $S$ is a subring, by the subring criterion. This works for negative $n$ too, but would just duplicate examples already seen, as $(-n)\mathbb{Z} = n\mathbb{Z}$ for all $n \in \mathbb{Z}$. There are two important special cases here: if $n = 0$ we get the trivial subring $\{0\}$, and if $n = 1$ we get the whole of $\mathbb{Z}$.

**Example 3.2.7.** We will now classify all the subrings of $\mathbb{Z}$. Suppose $S \neq \{0\}$ is a nontrivial subring. Then $S$ contains an integer $a$, and because $S$ is a subgroup, $-a \in S$. Therefore $S$ contains a positive integer (as exactly one of $a, -a$ is positive). Let $n$ be the smallest positive integer in $S$. Since $(S, +)$ is a group, we have $-n \in S$ and $0 \in S$. Therefore, for all integers $k$, it is certainly the case that $nk \in S$. Hence $n\mathbb{Z} \subseteq S$. Now let $b$ be any element of $S$. By the Division Theorem, there exist integers $q, r$ with $0 \leq r < n$ such that $b = qn + r$. Clearly $qn \in S$, since all multiples of $n$ are elements of $S$. Therefore, $b - qn \in S$. But $b - qn = r$ and $0 \leq r < n$. Now $n$ was the smallest positive integer in $S$. So to avoid a contradiction, we must have $r = 0$. Hence $b = qn + r = qn + 0 = qn$. Therefore every element of $S$ is an integer multiple of $n$. That is, $S \subseteq n\mathbb{Z}$. But we already know $n\mathbb{Z} \subseteq S$. Therefore $S = n\mathbb{Z}$. We have therefore shown that the only subrings of $\mathbb{Z}$ are precisely the subrings $n\mathbb{Z}$ discovered in Example 3.2.6.

**Exercise 3.13.** Let $\mathbb{R}[x]$ be the ring of polynomials with real coefficients (see Example 3.1.10). For any real number $a$, let $R_a = \{f(x) \in \mathbb{R}[x] : f(a) = 0\}$, in other words, the set of polynomials for which $a$ is a root. Show that $R_a$ is a subring of $\mathbb{R}[x]$.

## 3.3 Units and Zero Divisors

Consider the linear equation $ax + b = c$ where $a, b, c$ are elements of our favourite ring and $a \neq 0$ — if $a = 0$ we would not have a linear equation. How might we solve this? Well of course every element in the ring has an additive inverse, so our first step is:

$$\begin{aligned} ax + b &= c \\ ax + b + (-b) &= c + (-b) \\ ax + 0 &= c - b \\ ax &= c - b. \end{aligned}$$

Then to find $x$ we would like to 'divide by $a$'. But this does not necessarily have a meaning in our ring. If we have a ring with identity [that is, a multiplicative identity element], then each element may or may not have a multiplicative inverse.

**Definition 3.3.1.** Let $R$ be a ring with identity 1, and $a \in R$. Then $a$ is a *unit* if it has a multiplicative inverse, that is, there exists $a' \in R$ with $aa' = a'a = 1$.

As with groups, the multiplicative inverse, if it exists, is unique, for, supposing $a_1$ and $a_2$ are both inverses of $a$, then $a_2 = 1a_2 = (a_1a)a_2 = a_1(aa_2) = a_11 = a_1$. Therefore we can refer without ambiguity to *the* (multiplicative) inverse of $a$ as $a^{-1}$. Now we may proceed with our calculation. Assume $R$ is a ring with identity. If $a$ is a unit, then:

$$\begin{aligned} ax &= c - b \\ a^{-1}ax &= a^{-1}(c-b) \\ 1x &= a^{-1}(c-b) \\ x &= a^{-1}(c-b). \end{aligned}$$

So we have solved the equation, and in fact proved the following lemma.

**Lemma 3.3.2.** *Let $R$ be a division ring. Then every linear equation has a unique solution.*

*Proof.* A division ring is precisely a ring with identity in which every nonzero element is a unit. Hence the unique solution of $ax + b = c$ (with $a \neq 0$) is $x = a^{-1}(c - b)$. □

Note that every field is a division ring, and so linear equations in fields are always solvable.

**Exercise 3.14.** Find the units of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

**Example 3.3.3.** Consider the ring $\mathbb{Z}_n$ of integers modulo $n$, where $n \geq 2$. This is a ring with identity, because $1 \in \mathbb{Z}_n$. We will find the units. (We have done this before in a different guise.) Let $a \in \mathbb{Z}_n$. Suppose that $a$ is a unit. Then there exists $b \in \mathbb{Z}_n$ such that $a \otimes_n b = 1$. That is, $ab \equiv 1 \pmod{n}$. In other words, $ab - 1$ is divisible by $n$. So for some integer $k$ we have $ab + kn = 1$. Now, if $\gcd(a, n) = d$, then $d$ divides $ab$ and $d$ divides $kn$, which implies that $d$ divides $ab + kn = 1$. But the only positive integer that divides 1 is 1, forcing $d = 1$. So far, we have shown that if $a$ is a unit, then $\gcd(a, n) = 1$. Conversely suppose $\gcd(a, n) = 1$. Then we recall a fact from first year algebra (which you were asked to revise in Exercise 3.11) — we can use the Euclidean algorithm to show that there exist integers $b, k$ such that $ab + kn = \gcd(a, n) = 1$. Therefore $ab \equiv 1 \pmod{n}$ and hence $a \otimes_n b = 1$. Therefore $ab = 1$ in $\mathbb{Z}_n$ and so $a$ is a unit, with inverse $b$ (or actually the element of $\mathbb{Z}_n$ that is congruent to $b$ modulo $n$). Hence the units of $\mathbb{Z}_n$ are precisely the elements coprime to $n$. We use the notation $U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ for the set of units of $\mathbb{Z}_n$. Last term we showed this was a group under $\otimes_n$.

**Exercise 3.15.** Let $R$ be a ring with identity and $U = U(R)$ be the set of units of $R$. Show that $U$ is a group under the multiplication defined for $R$. We call $U$ the 'group of units of $R$' or the 'multiplicative group of $R$'.

**Exercise 3.16.** Consider $\mathcal{M}_n(\mathbb{R})$. It is a ring with identity, as the usual matrix identity element $I_n$ is contained in $\mathcal{M}_n(\mathbb{R})$. Find the group of units of $\mathcal{M}_n(\mathbb{R})$. By what name have we encountered this group before?

**Lemma 3.3.4.** *Let $p$ be prime. Then $\mathbb{Z}_p$ is a field.*

**Exercise 3.17.** Prove Lemma 3.3.4 by showing the slightly stronger result that $\mathbb{Z}_n$ is a field if and only if $n$ is prime. (Note that, unless otherwise specified, the addition and multiplication in $\mathbb{Z}_n$ are always $\oplus_n$ and $\otimes_n$.)

**Example 3.3.5.** Let $F$ be a field. Write $F^*$ for the group of units of $F$. Then $F^* = F \setminus \{0\}$, because $F$ is a division ring. (This extends our notation $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ for the nonzero elements of these sets.) By the previous exercise, $F^*$ is a group. We will show later that, surprisingly, if $F$ is finite then $F^*$ is always cyclic.

**Theorem 3.3.6** (Fermat's Little Theorem)**.** *Let $p$ be prime and $a$ be a positive integer not divisible by $p$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

*Proof.* Since $\mathbb{Z}_p$ is a field, the group of units $U_p$ of $\mathbb{Z}_p$ has order $p-1$. Therefore the order of every $u \in U_p$ divides $p-1$. Hence $u^{p-1} = 1$ in $U_p$. Now $a$ is not divisible by $p$, so $a$ is congruent to some $u \in U_p$. Therefore $a^{p-1} \equiv u^{p-1} \equiv 1 \pmod{p}$. □

**Example 3.3.7.** The Gaussian integers $\mathbb{Z}[i]$ were shown to be a ring in Exercise 3.12. Recall that $\mathbb{Z}[i] = \{a + bi : a, b, \in \mathbb{Z}\}$. So clearly $1 = 1 + 0i \in \mathbb{Z}[i]$ and thus the Gaussian integers form a commutative ring with identity. At first glance one might think that every nonzero element of this ring is a unit: after all, every nonzero element $z$ of $\mathbb{C}$ is a unit, (because $\frac{1}{z}$ is also in $\mathbb{C}$ and is the inverse of $z$), but of course there is no guarantee that for $z = a + ib \in \mathbb{Z}[i]$, the inverse $1/z$ will be in $\mathbb{Z}[i]$. To find which elements really are units, we can use a clever trick. Suppose $z$ is a unit of $\mathbb{Z}[i]$. Then there exists $w \in \mathbb{Z}[i]$ such that $zw = 1$. This implies that $|z|^2|w|^2 = 1$ (where $|z|$ is just the standard modulus of a complex number). Now in $\mathbb{Z}[i]$, writing $z = x + iy$ for integers $x$ and $y$, we have $|z|^2 = x^2 + y^2 \in \mathbb{Z}$. Therefore, if $z, w \in \mathbb{Z}[i]$, the squares of the moduli $|z|^2$ and $|w|^2$ are always (non-negative) integers. So $|z|^2|w|^2 = 1$ forces $|z|^2 = 1$. Therefore $x^2 + y^2 = 1$. Now $x$ and $y$ are integers. So the only solutions are $x = \pm 1, y = 0$ and $y = \pm 1, x = 0$. That is, $z = 1, -1, i$ or $-i$. Each of these really is a unit, because $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$, $i \cdot (-i) = 1$ and $(-i) \cdot i = 1$. Therefore the units of $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$. Note that this implies the set $\{1, -1, i, -i\}$ of complex numbers is a group under multiplication: we encountered this group in an exercise last term.

**Exercise 3.18.** Define $\mathbb{Z}[\sqrt{2}i] = \{a + b\sqrt{2}i : a, b, \in \mathbb{Z}\}$.

(a) Show that $\mathbb{Z}[\sqrt{2}i]$ is a ring with identity.

(b) Use the trick from Example 3.3.7 to find the units of $\mathbb{Z}[\sqrt{2}i]$.

When we work with units we must have rings with identity. In the example of Gaussian Integers, the ring in question was a subring of the ring $\mathbb{C}$ that happened to contain the identity. Subrings do not necessarily inherit all the properties of the ring that contains them. For example, $\mathbb{Z}$ is a subring of $\mathbb{C}$, but $\mathbb{Z}$ is not a field or a division ring, even though $\mathbb{C}$ is both. It is, however, a ring with identity. But as we have seen with, for example, the ring $2\mathbb{Z}$, another subring of $\mathbb{C}$, subrings of rings with identity do not have to be themselves rings with identity. In fact there is only one property a subring can be sure to inherit: the proof is trivial.

**Lemma 3.3.8.** *Every subring of a commutative ring is itself commutative.*

In an even stranger turn of events, there are rings with no multiplicative identity element which contain subrings that are rings with identity, as shown in the following exercise. The moral of all this is that we must be cautious about the assumptions we make.

**Exercise 3.19.** Consider the following subset $R$ of $\mathcal{M}_2(\mathbb{R})$ (the ring of $2 \times 2$ real matrices).

$$R = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in \mathbb{R} \right\}.$$

(a) Show that $R$ is a ring. Show further that $R$ is a ring with identity. This is unexpected because the element that we might normally hope to be the identity, namely $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, is not even in $R$. However there is an identity element nonetheless, and you must find it.

(b) Find the units of $R$ (again these are units only in $R$, with respect to the multiplicative identity element of $R$). Is $R$ a commutative ring? a division ring? a field?

We now move on to zero divisors, and to see the motivation, let us return to our linear equation. Recall that we have a ring $R$ and a linear equation $ax + b = c$, where $a, b, c \in R$, $a \neq 0$ and we are trying to determine the solutions $x$, if any, in $R$. We can simplify by writing $d = c - b$, so that $ax = d$. We know we can solve this if $a$ is a unit. But what about when $a$ is not a unit, how can we proceed? What about the special case when $d = af$ for some $f \in R$. Can we solve $ax = af$ by concluding $x = f$?

**Example 3.3.9.** Consider the ring $\mathbb{Z}_{10}$. Here, $2x = 2 \cdot 2 = 4$ does have a solution $x = 2$, but it also has the solution $x = 7$. So we cannot conclude from $2x = 2f$ that $x = f$.

**Exercise 3.20.** Let $R = \mathcal{M}_2(\mathbb{R})$. Let $a = \begin{pmatrix} 3 & 1 \\ 6 & 2 \end{pmatrix}$ and $f = \begin{pmatrix} 5 & 4 \\ 3 & 1 \end{pmatrix}$. Show that the equation $ax = af$ has infinitely many solutions.

The number 2 in Example 3.3.9 and the matrix $a$ in Exercise 3.20 have something in common: they are what is known as *zero divisors*.

**Definition 3.3.10.** Let $R$ be a ring. An element $a \in R$ is known as a zero divisor if $a \neq 0$ and there exists a nonzero $z \in R$ such that $az = 0$.

This is not something we are used to when working with everyday numbers. In fact we all know that if $a, b$ are numbers then $ab = 0$ implies either $a = 0$ or $b = 0$. This means that in any number ring there are no zero divisors. This motivates the following definition.

**Definition 3.3.11.** A commutative ring with identity that has no zero divisors is called an *integral domain*.

Therefore all number rings containing 1 are integral domains. Another class of integral domains follows from the next result.

**Lemma 3.3.12.** *Let $R$ be a ring with identity and $a \in R$. If $a$ is a unit, then $a$ is not a zero divisor.*

*Proof.* Suppose $a$ is a unit and a zero divisor. Then $a$ has an inverse $a^{-1}$ and there is a nonzero element $z$ such that $az = 0$. But now $a^{-1}az = a^{-1}0$. So $1z = 0$, and hence $z = 0$, contradicting the choice of $z$. Therefore $a$ cannot be both a unit and a zero divisor. □

Lemma 3.3.12 shows that all fields are integral domains (division rings are not necessarily, because they do not have to be commutative). This therefore includes, for example, $\mathbb{Z}_p$ for any prime $p$. The reason we care about integral domains is because of the following fact.

**Lemma 3.3.13.** *(Cancellation) Let $R$ be a ring and $a, x, y \in R$. Suppose $ax = ay$, where $a$ is neither 0 nor a zero divisor. Then $x = y$.*

*Proof.* We have $ax + (-ay) = ay + (-ay) = 0$, and hence $ax - ay = 0$. Therefore, using the distributive axiom, $a(x - y) = 0$. Now $a$ is not zero, nor is it a zero divisor. Therefore $x - y = 0$, and so $x = y$. □

Therefore, at least in an integral domain, if we have $ax = af$ for some nonzero $a$, then we can solve and say $x = f$.

**Exercise 3.21.** Show that, in $\mathbb{Z}_n$, the zero divisors are precisely the nonzero elements $a$ which are not units.

**Exercise 3.22.** Let $R$ be an integral domain. Show that $R[x]$, the ring of polynomials over $R$, is an integral domain.

**Exercise 3.23.** Let $R$ be an integral domain. Find the units of $R[x]$.

**Exercise 3.24.** Let $R$ be an integral domain. It was shown in Exercise 3.1 that $\mathcal{M}_2(R)$, the set of $2 \times 2$ matrices with entries in $R$, is a ring. Since $R$ is a ring with identity, $\mathcal{M}_2(R)$ is also a ring with identity, because it contains $I_2$, the $2 \times 2$ identity matrix. What are the units in $\mathcal{M}_2(R)$? (**Hint:** the answer will involve determinants!)

### The Field of Fractions

Recall that fields are commutative rings with identity in which every nonzero element is invertible. The ring of integers fails to be a field because division by an integer does not result in another integer in general. If we are to allow division by (nonzero) integers, we must extend our ring of integers to the field of fractions, or rational numbers. This trick can be generalised to any integral domain as follows. Let $R$ be an integral domain. Then a field $F$ is a *field of fractions* of $R$ if $R$ is (isomorphic to) a subring of $F$, and every element of $F$ can be thought of as $ab^{-1}$ for some $a, b \in R$, $b \neq 0$ (where $b^{-1}$ is defined in $F$). Our motivating example is $F = \mathbb{Q}$ and $R = \mathbb{Z}$. Then every nonzero $b \in \mathbb{Z}$ has an inverse $\frac{1}{b}$ in $\mathbb{Q}$, and every $x \in \mathbb{Q}$ is of the form $\frac{a}{b}$ for some $a, b \in \mathbb{Z}$. So $\mathbb{Q}$ is a field of fractions of $\mathbb{Z}$.

**Theorem 3.3.14.** *Any integral domain has a field of fractions.*

The proof of this theorem is sketched in Appendix B.1.

## 3.4 Ideals

In this section we will introduce a special kind of subring called an ideal. It turns out that ideals of rings are in some sense the analogues of normal subgroups of groups.

**Definition 3.4.1.** Let $R$ be a ring and $S$ a subring of $R$. Then $S$ is an *ideal* of $R$ if for all $r \in R$, $s \in S$, we have $rs \in S$ and $sr \in S$.

Not every subring of a ring is an ideal, as the following example shows.

**Example 3.4.2.** Consider the ring $\mathbb{R}$. Although $\mathbb{Z}$ is a subring of $\mathbb{R}$, it is certainly not an ideal, because it is not the case that for all $r \in \mathbb{R}$ and $s \in \mathbb{Z}$, $rs \in \mathbb{Z}$ — let $r = \sqrt{5}$ and $s = 2$ for instance. $2\sqrt{5}$ is certainly not an integer!

**Example 3.4.3.** In a ring $R$ both the trivial ring $\{0\}$ and $R$ itself are ideals.

**Example 3.4.4.** In $\mathbb{Z}$, in fact every subring *is* an ideal. The reason for this is as follows (and doesn't require our classification of the subrings). Suppose $S$ is a subring, and let $s \in S$, $r \in \mathbb{Z}$. Then $r$ is an integer. If $r = 0$, then certainly $0s = s0 = 0 \in S$, as $S$ is a ring. If $r > 0$, then $rs = sr$ is simply $s$ added to itself $r$ times, and so must be an element of $S$, because $S$ is closed under addition. If $r < 0$, then write $t = -r$, so $t$ is a positive integer. Then $ts = st$ is $s$ added to itself $t$ times, and so $ts \in S$. But $rs = -ts \in S$, since $S$ is closed under additive inverses. Therefore $rs = sr \in S$ for all $r \in \mathbb{Z}$. Hence $S$ is an ideal. So every subring of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$. We showed earlier that the subrings are precisely the sets $n\mathbb{Z}$, for $n \in \mathbb{Z}$.

**Example 3.4.5.** Let $F$ be a field and $I$ an ideal of $F$. Suppose there exists a nonzero $s \in I$. Then, since $F$ is a field, $s$ is a unit, and so there exists $t \in F$ with $st = 1$. By the definition of an ideal, this implies that $1 \in I$. Let $x \in F$. Then by the definition of an ideal, $x = x1 \in I$. Therefore every element of $F$ is contained in $I$. This shows that the only ideals in a field are the trivial ideal and the field $F$. More generally the same argument would show that in a ring $R$ with identity, any ideal containing a unit is equal to $R$.

The following criterion for an ideal is very similar to the Subring Criterion, and its validity is clear from the definition of an ideal. The only difference is that part (iii) is strengthened.

**Lemma 3.4.6** (The Ideal Criterion)**.** *Let $R$ be a ring. A subset $S$ of $R$ is an ideal if $S$ is non-empty and for all $x, y \in S$ and $r \in R$ we have:*

*(i)* $x + y \in S$;

*(ii)* $-x \in S$; *and*

*(iii)* $xr \in S$ *and* $rx \in S$.

**Exercise 3.25.** Show that if $S$ and $T$ are ideals of $R$, then $S \cap T$ is also an ideal.

The fact that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ leads us to a new definition. For a ring $R$ and $a \in R$, we define $\langle a \rangle$ to be the smallest ideal containing $a$, and call it the *ideal generated by a*. By 'smallest' we mean that if $I$ is an ideal with $a \in I$, then $\langle a \rangle \subseteq I$. Given that the intersection of any ideals is also an ideal, in fact $\langle a \rangle$ is the intersection of all ideals of $R$ that contain $a$. By definition, any ring containing $a$ must at least contain $ar$ for all $r \in R$. It turns out (see the next exercise) that in a commutative ring with identity the collection of all these elements $ar$ is itself an ideal. Hence we can write $\langle a \rangle = aR = \{ar : r \in R\}$.

**Exercise 3.26.** Let $R$ be a commutative ring with identity and let $a \in R$. Show that the set $aR$ is an ideal which contains $a$ and hence that $\langle a \rangle = aR$.

For the next definition remember that an integral domain is a commutative ring with identity and no zero divisors.

**Definition 3.4.7.** Let $R$ be a commutative ring with identity and $a \in R$. We say that an ideal $I$ of $R$ is a *principal ideal* if $I = \langle a \rangle = aR$ for some $a \in R$. If $R$ is an integral domain and *every* ideal of $R$ is a principal ideal, then $R$ is called a *principal ideal domain*.

**Example 3.4.8.** $\mathbb{Z}$ is a principal ideal domain. This is because we showed in Example 3.4.4 that every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

**Example 3.4.9.** Consider the ring $\mathbb{Z}_{12}$ of integers modulo 12. Let $S = \{0, 4, 8\}$, the cyclic subgroup (under $\oplus_{12}$) generated by 4. Therefore for all $a, b \in S$ we have $a \oplus_{12} b \in S$ and $(-a) \in S$. Hence conditions (i) and (ii) of the Ideal Criterion apply. Finally, for any $x \in \mathbb{Z}_{12}$ and $a \in S$, we have $a = 4k$ for some integer $k$. Now $ax = xa = 4xk$. By the division theorem, $xk = 3q + r$ for some integers $q, r$ with $0 \leq r < 3$. So $ax = 4(3q + r) = 12q + 4r$. Hence $a \otimes_{12} x = 4r \in S$. Therefore $a \otimes_{12} x \in S$ for all $a \in S, x \in \mathbb{Z}_{12}$. This is part (iii) of the Ideal Criterion. Hence $S$ is an ideal of $\mathbb{Z}_{12}$.

**Exercise 3.27.** Let $n$ be a positive integer, and consider $\mathbb{Z}_n$, the ring of integers modulo $n$. Now $(\mathbb{Z}_n, \oplus_n)$ is a group of order $n$ and so any subgroup, in particular any subring, has order dividing $n$. Let $k$ be a (positive) divisor of $n$, and let $a = \frac{n}{k}$. Write $R_a = \{0, a, 2a, \ldots, (k-1)a\}$. Show that $R_a$ is a subring of order $k$. Hence for all positive integers $k$, show that $\mathbb{Z}_n$ has a subring of order $k$ if and only if $k$ divides $n$. Is $R_a$ always an ideal? Explain your answer.

**Exercise 3.28.** Show that every field is a principal ideal domain.

I have said that ideals are the analogue of normal subgroups. Recalling our group theory, normal subgroups correspond to kernels of group homomorphisms. If we define the notion of a ring homomorphism, we might expect that the kernels of these would be ideals, and the images would be subrings, and indeed this is so.

**Definition 3.4.10.** Let $R$ and $S$ be rings. A map $\theta : R \to S$ is a (ring) homomorphism if for all $a, b \in R$:

$$\theta(a + b) = \theta(a) + \theta(b) \qquad \text{and} \qquad \theta(ab) = \theta(a)\theta(b).$$

If $\theta$ is also injective and surjective, then we say $\theta$ is a ring isomorphism, and that $R$ and $S$ are isomorphic rings (written $R \cong S$).

Being a ring homomorphism tells us that the map $\theta$ is behaving nicely with respect to the operations in the rings. If $\theta$ is an isomorphism, then, as with groups, the structure is completely preserved. More is required of ring homomorphisms than group homomorphisms, so there are in some sense fewer of them. This is hinted at by the next lemma.

**Lemma 3.4.11.** *Suppose $R$ and $S$ are number rings with identity, and $\theta : R \to S$ is a homomorphism. Then either $\theta$ is the zero homomorphism ($\theta(a) = 0$ for all $a \in R$), or $\theta(1) = 1$.*

*Proof.* Since $\theta$ is a homomorphism, we have $\theta(1) \cdot \theta(1) = \theta(1 \cdot 1) = \theta(1)$. Thus $\theta(1)$ is a number $x$ satisfying $x^2 = x$. Hence $\theta(1) = 0$ or 1. If $\theta(1) = 0$, then for all $a \in R$ we have

$$\theta(a) = \theta(a1) = \theta(a)\theta(1) = \theta(a) \cdot 0 = 0.$$

Hence $\theta$ is the zero homomorphism. Therefore, either $\theta$ is the zero homomorphism, or $\theta(1) = 1$. □

If $\theta$ is a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$, for any number ring $S$, then

$$\theta(2) = \theta(1 + 1) = \theta(1) + \theta(1) = 2\theta(1),$$

and it's not hard to see that in general $\theta(n) = n\theta(1)$, for all integers $n$. This means the homomorphism is completely determined by $\theta(1)$. In fact it is either the zero homomorphism or the identity map.

**Exercise 3.29.** Explore the possibilities for ring homomorphisms from: (a) $\mathbb{Z}$ to $\mathbb{Q}$; (b) $\mathbb{Q}$ to $\mathbb{Q}$.

**Definition 3.4.12.** Let $\theta : R \to S$ be a ring homomorphism.

(i) The *image* of $\theta$ is $\mathrm{im}(\theta) = \{\theta(a) : a \in R\}$.

(ii) The *kernel* of $\theta$ is $\ker(\theta) = \{a \in R : \theta(a) = 0\}$.

**Lemma 3.4.13.** *If $\theta : R \to S$ is a ring homomorphism, then $\mathrm{im}(\theta)$ is a subring of $S$ and $\ker(\theta)$ is an ideal of $R$. Moreover, $\theta$ is injective if and only if $\ker(\theta) = \{0\}$ and surjective if and only if $\mathrm{im}(\theta) = S$.*

**Exercise 3.30.** Prove Lemma 3.4.13.

Much of the same theory that we covered for groups with relation to homomorphisms, isomorphisms, normal subgroups and quotient groups can be developed for rings and ideals. Here I will give a brief indication of the path to follow. For example there is a ring analogue of the homomorphism theorem for groups. It deals with quotient rings. It can be shown that for any ideal $I$ of a ring $R$, the quotient group $R/I$ is in fact a ring, and there is a 'ring homomorphism theorem' based on the group homomorphism theorem we studied last term. I have put the basic theory, statement and proof in Appendix B.2 to the notes. You are not required to know it for the exam, but you may find it interesting nonetheless.

## 3.5 Factorisation

Throughout this section we will work only with integral domains (commutative rings with identity and no zero divisors): this includes all number rings containing 1 and all polynomial rings $R[x]$ for which $R$ is an integral domain. The main question we want to ask is whether there is any analogue of the fact that every integer can be factorised into a product of prime numbers in only one way. (This is known as the fundamental theorem of arithmetic.)

The key steps in proving the fundamental theorem of arithmetic involve the Euclidean algorithm, so a closely related question will be to determine whether there is an analogue of the Euclidean algorithm. We shall define two classes of rings: those where the there is an analogue of the Euclidean algorithm and those where there is an analogue of the fundamental theorem of arithmetic. We shall see that the latter class contains the class of Principal Ideal Domains which, in turn, contains the former.

In seeking an analogue of the fundamental theorem of arithmetic, we need to be slightly careful, because, for example

$$10 = 2 \times 5 = 5 \times 2 = (-2) \times (-5) = (-5) \times (-2).$$

Normally, to get round this, the theorem is stated for positive integers and then we can define primes as positive integers with exactly two divisors, or similar, and state that the order in which they appear in the factorisation is irrelevant. However, note now that we have the appropriate language, that the units of $\mathbb{Z}$ are 1 and $-1$, and the only difference in the factorisations of 10, apart from the order in which the factors are written, is possible multiplication of factors by a unit (i.e. 2 and $-2$ differ only by multiplication by a unit). This will be a crucial step in defining 'uniqueness' of factorisations.

**Definition 3.5.1.** Two elements $r, s$ of $R$ are said to be *associates* if there is a unit $u$ such that $s = ru$.

In these terms, the only difference between factorisations of an integer is that factors may be replaced by their associates. To generalise unique factorisation, we need an analogue of prime numbers.

**Definition 3.5.2.** Let $R$ be an integral domain, and $p \in R$ with $p \neq 0$ and $p$ not a unit. We say that $p$ is *irreducible* if $p = ab$ (with $a, b \in R$) implies either $a$ or $b$ is a unit. Otherwise we say $p$ is reducible.

Thus if $p = ab$, and $p$ is irreducible, then either $a$ or $b$ is an associate of $p$. Note that if $R$ is a field there are no irreducibles, because every element is either zero or a unit.

**Example 3.5.3.** The units of $\mathbb{Z}$ are $\pm 1$. The irreducibles are the numbers $p$ and $-p$ for each prime $p$.

The analogue of unique prime factorisation will be factorisation as a product of irreducibles in essentially only one way. In the absence of a neat classification of rings that have such a property, we can at least give them a name.

**Definition 3.5.4.** Let $R$ be an integral domain. We say that $R$ is a unique factorisation domain (UFD) if all elements other than zero and units can be factorised into irreducibles, and moreover that if $p_1 \cdots p_m = q_1 \cdots q_n$, where each $p_i$ and $q_j$ is irreducible, then $m = n$ and the factors can be reordered so that for $1 \leq i \leq m = n$, $p_i$ and $q_i$ are associates.

**Example 3.5.5.** We already know that $\mathbb{Z}$ is a UFD. However in fact we will soon re-prove this in a more general context.

Let's look at some more irreducible elements in different rings.

**Example 3.5.6.** Consider $\mathbb{Z}_2[x]$, the polynomials with coefficients in $\mathbb{Z}_2$. This is a commutative ring with identity being the constant polynomial 1. We first find the units. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ be nonzero elements of $\mathbb{Z}_2[x]$, so we can assume $a_n \neq 0$ and $b_m \neq 0$. But the only nonzero element of $\mathbb{Z}_2$ is 1, so $a_n = 1 = b_m$. Now the coefficient of $x^{m+n}$ in $f(x)g(x)$ is $a_n b_m = 1$. Therefore if $f(x)g(x) = 1$, then $m = n = 0$ and $f(x) = g(x) = 1$. So the only unit in $\mathbb{Z}_2[x]$ is 1. Let us try to find irreducible elements. The only constant polynomials are 0 and 1, and they are not irreducible. The polynomials of degree 1 are $x$ and $x + 1$. Clearly they are both irreducible, because they could only be factored into polynomials of degree 1 or less. Now $xx = x^2, (x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$ because $2 = 0$ in $\mathbb{Z}_2$, and $x(x+1) = x^2 + x$. Thus these degree 2 polynomials are reducible. The only other degree 2 polynomial is $x^2 + x + 1$. It is irreducible, as we have already looked at all possible products of lower degree polynomials, and it is not equal to any of them.

**Example 3.5.7.** Consider the Gaussian integers $\mathbb{Z}[i]$. (These were shown to be a ring in Exercise 3.12, and the units were found in Exercise 3.3.7.) The units are $\pm 1$ and $\pm i$. These are exactly the elements $z$ satisfying $|z|^2 = 1$. Let $n \neq 0$ be an integer. Then $n = n + 0i \in \mathbb{Z}[i]$. Under what circumstances is $n$ irreducible? Certainly if $n$ is composite, say $n = km$ for integers $k, m \neq \pm 1$, then $n = (k+0i)(m+0i)$ is reducible. So assume $\pm n$ is a prime $p$, and suppose $p = wz$ where $w = u + iv$, $z = x + iy$. Then $p^2 = |w|^2|z|^2 = (u^2 + v^2)(x^2 + y^2)$. Assume this is a non-trivial factorisation, so that neither $z$ nor $w$ is a unit. Then $x^2 + y^2 > 1$, and $u^2 + v^2 > 1$. Since $p$ is prime, the only possibility is that $x^2 + y^2 = p$ and $u^2 + v^2 = p$. We have shown that if a prime number $p$ is reducible, then $p$ must be of the form $x^2 + y^2$ for some integers $x$, $y$, Suppose $p$ is of this form. Then clearly $p = (x + iy)(x - iy)$ is reducible. It is a theorem in number theory (proved in the Number Theory and Geometry course) that a prime number $p$ is expressible as the sum of two squares if and only if $p = 2$ or $p$ is congruent to 1 modulo 4. Therefore, we have shown that in the ring of Gaussian integers, the only elements $n \in \mathbb{Z}$ which are irreducible are $\pm p$ where $p$ is a prime number congruent to 3 modulo 4. There are some other irreducible elements, of $\mathbb{Z}[i]$: they are of the form $a + ib$ where $a^2 + b^2$ is a prime integer, but it is harder to show that these are the only other examples.

Since $\mathbb{Z}$ is a unique factorisation domain, in our search for others it is helpful to pick apart some of the properties of the integers that are required to prove unique factorisation. A vital step in the argument is that if a prime $p$ divides a product $ab$, then $p$ divides at least one of $a$ and $b$. The proof of this is that if $p$ doesn't divide $a$, then we can reverse the Euclidean algorithm to find integers $x$ and $y$ for which $ax + py = 1$. (So we have the idea of greatest common divisors here, as well as some algorithm for finding them.) Then $abx + pby = b$. Since $p$ divides the left hand side, it must also divide the right hand side, and we're done. OK so which rings have a 'Euclidean algorithm'? Again we don't know, but we give such rings a name anyway. It will turn out that such rings are always UFDs.

**Definition 3.5.8.** Let $R$ be an integral domain. A Euclidean norm on $R$ is a non-negative integer valued function $N$ on the nonzero elements of $R$ such that for all $a, b \in R$:

(i) if $a, b \neq 0$, then $N(ab) \geq N(a)$;

(ii) if $b \neq 0$, then there exist $q, r \in R$ with $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

If $R$ is equipped with such a function, then we say $R$ is a *Euclidean domain.*

**Example 3.5.9.** $\mathbb{Z}$ is a Euclidean domain. To see this, first note that $\mathbb{Z}$ is an integral domain. For the norm, simply define $N(a) = |a|$. Then for all nonzero $a, b \in \mathbb{Z}$, $|ab| = |a||b| \geq |a|$, so part (1) holds. And by the Division Theorem we know that for all integers $a, b$ with $b \neq 0$, there exist integers $q, r$ with $a = bq + r$ and $0 \leq |r| < |b|$. Hence either $r = 0$ or $N(r) < N(b)$, which is part (2).

**Theorem 3.5.10** (The Division Theorem for Polynomials)**.** *Let $f(x)$ and $g(x)$ be polynomials over a field $F$, and suppose $g(x) \neq 0$. Then there exist polynomials $q(x)$ and $r(x)$ with $f(x) = q(x)g(x) + r(x)$ and either $r(x)$ is the zero polynomial or* $\deg(r(x)) < \deg(g(x))$.

Note that every nonzero polynomial $f(x)$ can be written in the form $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ for some $a_i$ with $a_n \neq 0$. The degree of the polynomial $\deg(f(x))$, is just this $n$. In fact the polynomials $q(x)$, $r(x)$ are unique, but we do not need to prove uniqueness for our purposes, just existence.

*Proof.* If $f(x)$ is the zero polynomial, then clearly setting $q(x) = r(x) = 0$ will work. We will proceed by induction on $\deg(f(x))$. If $\deg(f(x)) < \deg(g(x))$, then set $q(x) = 0$ and $r(x) = f(x)$. So suppose $n = \deg(f(x)) \geq \deg(g(x)) = m$. Suppose the leading term of $f(x)$ is $a_nx^n$, and the leading term of $g(x)$ is $b_mx^m$. Write $h(x) = \frac{a_n}{b_m}x^{n-m}g(x)$. Now $f(x) - h(x)$ is a polynomial of strictly smaller degree than $f(x)$. Hence, inductively, there exist polynomials $q_1(x)$ and $r_1(x)$ with either $r_1(x) = 0$ or $\deg(r_1(x)) < \deg(g(x))$ such that

$$f(x) - h(x) = q_1(x)g(x) + r_1(x).$$

But now, recalling the definition of $h(x)$:

$$f(x) = q_1(x)g(x) + \tfrac{a_n}{b_m}x^{n-m}g(x) + r_1(x) = \left(q_1(x) + \tfrac{a_n}{b_m}x^{n-m}\right)g(x) + r_1(x).$$

Now we just set $q(x) = q_1(x) + \frac{a_n}{b_m}x^{n-m}$ and $r(x) = r_1(x)$, and we are done. By induction, the theorem holds. □

**Corollary 3.5.11.** *If $F$ is a field, then $F[x]$ is a Euclidean domain.*

*Proof.* The fact that $F[x]$ is an integral domain was Exercise 3.22. Now, for any nonzero polynomial $f(x)$, define $N(f) = \deg(f)$. Then property (1) of a Euclidean norm is obviously true, and property (2) follows from the Division Theorem for polynomials. □

**Exercise 3.31.** Consider $\mathbb{Z}[i]$, the ring of Gaussian integers. We will show that $\mathbb{Z}[i]$ is a Euclidean domain. For $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, suppose $\frac{a}{b} = x + iy$. Define $s$ to be $x$ rounded to the nearest integer, and $t$ to be $y$ rounded to the nearest integer. So, for example, if $x + iy = \frac{1}{3} + \frac{2}{3}i$, then $s = 0$ and $t = 1$. Now set $q_{a,b} = s + ti$ and $r_{a,b} = a - bq_{a,b}$. Finally, for $a = m + in \in \mathbb{Z}[i]$, define $N(a) = m^2 + n^2$, so that $N(a) = |a|^2$.

(a) Explain why $\mathbb{Z}[i]$ is an integral domain.

(b) Show that if $a, b$ are non-zero elements of $\mathbb{Z}[i]$, then $N(ab) \geq N(a)$.

(c) Show that if $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, then $q = q_{a,b}$ and $r = r_{a,b}$ are elements of $\mathbb{Z}[i]$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

Recall from earlier that an ideal is a subring $I$ with the property that for all $a \in I$ and $r \in R$, we have $ar \in I$ and $ra \in I$. Principal ideals in a commutative ring with identity are precisely the sets of the form $aR = \{ar : r \in R\}$. And a Principal Ideal Domain is an integral domain in which every ideal is principal.

**Proposition 3.5.12.** *Let $R$ be a Euclidean domain. Then $R$ is a Principal Ideal Domain.*

*Proof.* Let $I$ be an ideal of $R$. If $I = \{0\}$, then clearly $I = 0R$ is a principal ideal. So suppose $I$ contains non-zero elements. Choose a non-zero $m \in I$ such that $N(m)$ is as small as possible. In other words, for any nonzero $a \in I$, we have $N(m) \leq N(a)$. I claim that $I = mR$. Certainly, since $I$ is an ideal, we have $mr \in I$ for all $r \in R$. So $mR \subseteq I$. For the reverse inclusion, let $x \in I$. Now because $R$ is a Euclidean domain, there exist $q, r \in R$ such that $x = mq + r$ and either $r = 0$ or $N(r) < N(m)$. So $r = x - mq$. Now $x$ and $m$ are elements of the ideal $I$. Thus $x - mq \in I$. Hence $r \in I$. But $N(m)$ is minimal in $I$. Therefore $N(r) < N(m)$ is impossible. We are forced to conclude that $r = 0$ and hence $x = mq$. So $x \in mR$. Hence $I \subseteq mR$. We have shown that $I = mR$. Therefore $I$ is a principal ideal, and $R$ is a principal ideal domain. □

The following definition generalises the idea of greatest common divisors.

**Definition 3.5.13.** Let $R$ be an integral domain. For $a, d \in R$ we say that $d$ *divides* $a$, or is a *divisor of* $a$, if there is some $c \in R$ for which $cd = a$. We write $d|a$ for $d$ *divides* $a$.

The element $D \in R$ is a *greatest common divisor* of $a$ and $b$ (or gcd) if

- $D$ divides $a$ and $D$ divides $b$; and
- for any $d \in R$, if $d$ divides $a$ and $d$ divides $b$, then $d$ divides $D$.

In this wider context then, both 4 and $-4$ are greatest common divisors of 12 and $-20$. Of course 4 and $-4$ only 'differ' by a unit: in other words they are associates.

**Lemma 3.5.14.** *Let $R$ be an integral domain. If two nonzero elements $a$ and $b$ have a greatest common divisor $d$, then any greatest common divisor $e$ of $a$ and $b$ is an associate of $d$.*

**Exercise 3.32.** Prove Lemma 3.5.14.

**Proposition 3.5.15.** *Any two non-zero elements $a$, $b$ of a Principal Ideal Domain $R$ have a greatest common divisor $d$. Moreover there exist $r, s \in R$ such that $d = ar + bs$.*

*Proof.* The set $I = \{ar + bs : r, s \in R\}$ is an ideal of $R$ (proof of this is Exercise 3.33). Since $I$ is a principal ideal, $I = dR$ for some $d \in R$. Therefore, in particular, $d \in I$. So there exist $r, s$ such that $d = ar + bs$. Now $a = a \cdot 1 + b \cdot 0 \in I$ and similarly $b \in I$, so there exist $x, y \in R$ with $a = dx, b = dy$ (because $I = dR$). Thus $d|a$ and $d|b$. Now let $c$ be any common divisor of $a$ and $b$. Then $c$ divides $ar + bs = d$. Therefore $d$ is a greatest common divisor of $a$ and $b$. □

**Exercise 3.33.** Let $R$ be a commutative ring, and let $a, b \in R$. Show that the set $\{ar + bs : r, s \in R\}$ is an ideal.

**Proposition 3.5.16.** *Any two non-zero elements $a$, $b$ of a Euclidean Domain $R$ have a greatest common divisor $d$. Moreover there exist $r, s \in R$ such that $d = ar + bs$.*

*Proof.* Every Euclidean Domain is a Principal Ideal Domain (Proposition 3.5.12). And now we just apply Proposition 3.5.15. □

This is all very well but doesn't actually help you to find a gcd. The reason for defining Euclidean domains (and for naming them thus) is that the definition gives exactly the circumstances under which the Euclidean algorithm works. Recall that the Euclidean algorithm for positive integers gives the greatest common divisor (gcd) of two positive integers, and it can be reversed to express the gcd as a linear combination of those integers.

**The Euclidean algorithm:** Let $a, b \in R$. If $b = 0$, then set $\gcd(a, b) = a$. If $b \neq 0$, then there exist $q, r \in R$ with $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$. Set $\gcd(a, b) = \gcd(b, r)$.

Why does this work? Well, to work out $\gcd(a, b)$ we will need to follow the algorithm repeatedly. For every $s \in R$, $0s = 0$ and hence $s|0$. Hence $s$ is a greatest common divisor of $s$ and 0 for every $s \in R$. So if $r = 0$ in the algorithm above, then $\gcd(b, r) = \gcd(b, 0) = b$. If not then we repeat the algorithm with $b, r$. At each stage the 'remainder' is either 0 and we can stop, or has strictly lower norm than the previous step. So the algorithm is guaranteed to stop. The full proof that the Euclidean algorithm always gives a gcd is analogous to the proof of this for positive integers. I have put some more detail in Appendix B.3. Here we will content ourselves with a couple of examples.

**Example 3.5.17.** Consider $17, 5 \in \mathbb{Z}$. Now

$$17 = 3 \times 5 + 2, \qquad 5 = 2 \times 2 + 1 \qquad \text{and} \qquad 2 = 2 \times 1 + 0.$$

The last remainder is 0, so we deduce that $\gcd(17, 5) = \gcd(5, 2) = \gcd(2, 1) = \gcd(1, 0) = 1$.

**Exercise 3.34.** Find $\gcd(294, 216)$ in the Euclidean domain $\mathbb{Z}$.

We know that if $F$ is a field, then $F[x]$ is a Euclidean domain, (where the degree of a polynomial supplies the requisite Euclidean norm) so that any two nonzero polynomials have a greatest common divisor, any two greatest common divisors are associates (meaning they differ only by multiplication by a unit) and that it is possible to find a greatest common divisor using the Euclidean algorithm. In practice, in questions about polynomials in Euclidean domains, we will always work with $\mathbb{R}[x]$, but what we're about to do applies for any field, so $\mathbb{C}[x], \mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ for $p$ prime and so on.

Here is a simple algorithm to follow. It is a slight variant on the Euclidean algorithm, the main advantage being that for this variant we do not have to do long division of polynomials. Let $f(x), g(x)$

be nonzero polynomials with $\deg(f(x)) = n$ and $\deg(g(x)) = m$. We wish to find $\gcd(f(x), g(x))$. Since certainly $\gcd(f(x), g(x)) = \gcd(g(x), f(x))$, we can assume without loss of generality that $m \leq n$. Suppose the leading term of $f(x)$ is $a_n x^n$, and the leading term of $g(x)$ is $b_m x^m$. Then calculate $p(x)$ as follows:

$$f(x) - \tfrac{a_n}{b_m} g(x) = p(x).$$

If $p(x) = 0$, then $\gcd(f(x), g(x)) = g(x)$, because this means $g(x)$ divides $f(x)$. Otherwise, we observe that $\gcd(f(x), g(x)) = \gcd(g(x), p(x))$. And we repeat this process with $g(x)$ and $p(x)$. Continue until we get 0. This must happen because at each stage either $p(x) = 0$ or $\deg(p(x)) < \deg(f(x))$. At that point the gcd we obtain will also be $\gcd(f(x), g(x))$.

Note that the true Euclidean algorithm would produce a remainder term $r(x)$ of degree strictly less than $\deg(g(x))$, rather than $\deg(f(x))$. However since $\deg(g(x)) + \deg(p(x))$ is strictly less than $\deg(f(x)) + \deg(g(x))$, we know that the total degree decreases at each step, so again this variant algorithm is guaranteed to finish eventually.

**Example 3.5.18.** Find $\gcd(f(x), g(x))$ in $\mathbb{R}[x]$, in each of the following cases.

(i) $f(x) = x^3 + 3x^2 + 2x + 6$, $g(x) = x^2 + 2$;

(ii) $f(x) = 2x^2 + 4x + 7$, $g(x) = x^2 + 2$;

(iii) $f(x) = 6x^3 + 3x^2 + 1$, $g(x) = 2x^2 + x$.

**Solutions:** The solutions are as follows:

(i) The leading term of $f(x)$ is $1x^3$, the leading term of $g(x)$ is $1x^2$, so our first step is to find $p(x) = f(x) - \frac{1}{1}x^{3-2}g(x) = f(x) - xg(x)$. Now

$$f(x) - x(g(x)) = x^3 + 3x^2 + 2x + 6 - x(x^2 + 2) = x^3 + 3x^2 + 2x + 6 - x^3 - 2x = 3x^2 + 6 = p(x).$$

So

$$f(x) = xg(x) + (3x^2 + 6)$$

and our remainder term $p(x)$ is $3x^2 + 6$. This tells us that

$$\gcd(f(x), g(x)) = \gcd(g(x), p(x)) = \gcd(p(x), g(x)) = \gcd(3x^2 + 6, x^2 + 2).$$

Of course we may well notice at this point that $g(x)$ and $p(x)$ are associates but let's continue for practice. The leading term in $p(x)$ is $3x^2$, that of $g(x)$ is $1x^2$, so we find

$$p(x) - \frac{3}{1}x^{2-2}g(x) = p(x) - 3g(x) = (3x^2 + 6) - 3(x^2 + 2) = 0.$$

That is,

$$p(x) = 3g(x) + 0.$$

Thus $\gcd(f(x), g(x)) = \gcd(p(x), g(x)) = g(x) = x^2 + 2$.

(ii) The leading term of $f(x)$ is $2x^2$, the leading term of $g(x)$ is $1x^2$, so $p(x) = f(x) = 2x^0 = 2$. Thus

$$p(x) = f(x) - 2g(x) = 2x^2 + 4x + 7 - 2(x^2 + 2) = 2x^2 + 4x + 7 - 2x^2 - 4 = 4x + 3.$$

Thus $\gcd(f(x), g(x)) = \gcd(g(x), p(x)) = \gcd(x^2 + 2, 4x + 3)$. We find

$$(x^2 + 2) - \tfrac{1}{4}x(4x + 3) = x^2 + 2 - x^2 - \tfrac{3}{4}x = -\tfrac{3}{4}x + 2.$$

So $\gcd(f(x), g(x)) = \gcd(4x + 3, -\frac{3}{4}x + 2)$. Next we calculate

$$(4x + 3) + \frac{16}{3}\left(-\frac{3}{4}x + 2\right) = 3 + \frac{32}{3} = \frac{41}{3}.$$

So $\gcd(f(x), g(x)) = \gcd\left(-\frac{3}{4}x + 2, \frac{41}{3}\right)$. We could carry on until the bitter end, but $\frac{41}{3}$ is a unit, and units divide everything! Here, for example $-\frac{3}{4}x + 2 = \frac{41}{3} \cdot \frac{3}{41}\left(-\frac{3}{4}x + 2\right)$. Hence $\gcd(f(x), g(x)) = \gcd\left(-\frac{3}{4}x + 2, \frac{41}{3}\right) = \frac{41}{3}$. Since any associate of $\frac{41}{3}$ is also a gcd, then also 1 is a gcd. So we can say that $\gcd(f(x), g(x)) = 1$ (although obviously $\frac{41}{3}$ is also a correct answer).

(iii) Finally, in this last example the leading term of $f(x)$ is $6x^3$, the leading term of $g(x)$ is $2x^2$, so we find $p(x) = f(x) - \frac{6}{2}x^{3-2}g(x) = f(x) - 3xg(x)$:

$$f(x) - 3xg(x) = 6x^3 + 3x^2 + 1 - 3x(2x^2 + x) = 6x^3 + 3x^2 + 1 - 6x^3 - 3x^2 = 1.$$

Therefore $\gcd(f(x), g(x)) = \gcd(g(x), 1)$. Now, again, it is clear that 1 divides $g(x)$. Hence $\gcd(f(x), g(x)) = \gcd(g(x), 1) = 1$.

**Exercise 3.35.** Find the greatest common divisor of $x^3 + x^2 + 5x + 5$ and $x^2 + 5x + 4$ in $\mathbb{R}[x]$.

**Exercise 3.36.** Find $\gcd(x^3 + 3x^2 + 3x + 2, x^2 - x - 6)$ in the Euclidean domain $\mathbb{R}[x]$.

**Exercise 3.37.** Find $\gcd(7-i, 5-5i)$ in the Euclidean domain $\mathbb{Z}[i]$. (See Exercise 3.31 for the relevant Euclidean norm and how to express $a, b$ as $a = bq + r$.)

As with the algorithm for the positive integers, we can 'reverse' the algorithm to produce an expression for $\gcd(a, b)$ in terms of $a$ and $b$: I've again relegated this to Appendix B.3. We already know that such expressions exist from Proposition 3.5.16. This fact allows us to prove the following lemma, which is a crucial tool in proving the 'uniqueness' part when we show that Euclidean domains are Unique Factorisation domains.

**Lemma 3.5.19.** *Suppose $R$ is a Euclidean domain. Let $p \in R$ be irreducible. If $p$ divides $ab$, then $p$ divides $a$ or $p$ divides $b$.*

*Proof.* If $p$ divides $a$, then we are happy. So suppose $p$ does not divide $a$. The only divisors of $p$ are $p$, associates of $p$ and units. But $p$ (and its associates) do not divide $a$. Therefore $\gcd(p, a) = u$ for some unit $u$. So (by Proposition 3.5.16) there exist $r, s \in R$ with $pr + as = u$. Multiply through by $u^{-1}b$ to get $prbu^{-1} + absu^{-1} = buu^{-1} = b$. Now $p$ divides $prbu^{-1}$ and $(ab)su^{-1}$. Hence $p$ divides $b$. □

**Exercise 3.38.** Using Lemma 3.5.19 as the starting point, prove by induction on $n$ that if $p$ is irreducible and $p$ divides $a_1 \cdots a_n$, then $p$ divides at least one of $a_1, \ldots, a_n$.

**Theorem 3.5.20.** *Suppose that $R$ is a Euclidean domain, and that for some $a \in R$ we have $a = p_1 p_2 \cdots p_m$ and $a = q_1 q_2 \cdots q_n$ for some irreducibles $p_i$ and $q_j$. Then $m = n$ and the factors can be reordered so that for $1 \leq i \leq m = n$, $p_i$ and $q_i$ are associates.*

*Proof.* Since $p_m$ divides $a$, $p_m$ divides at least one of the $q_j$. Reordering if necessary, we can assume $p_m$ divides $q_n$. But the only divisors of $q_n$, since it is irreducible, are units and associates of $q_n$. Now $p_m$ is not a unit. Therefore $p_m$ is an associate of $q_n$, say $q_n = up_m$ for some unit $u$. Thus

$$p_1 \cdots p_m = q_1 \cdots q_{n-2} q_{n-1} u p_m.$$

We are in an integral domain so we may cancel the $p_m$ on both sides. We now proceed by induction on $m$. If $m = 1$, then we end up with $1 = q_1 \cdots q_{n-2} q_{n-1} u$. Since irreducibles are not units, they do not divide 1, and so $n - 1 = 0$. Hence $n = 1$, $q_1$ is an associate of $p_1$ and we are done. Now assume $m > 1$. Then the cancelling of $p_m$ results in

$$p_1 \cdots p_{m-1} = q_1 \cdots q_{n-2}(q_{n-1} u).$$

This is a shorter product of irreducibles. By induction then, $n-1 = m-1$ and the $q_j$ can be re-ordered so that $p_i$ is an associate of $q_i$ for $1 \leq i \leq m-1$. We already know $p_m$ is an associate of $q_n$, and now that we have $n = m$, this completes the proof by induction. So $n = m$ and the $q_j$ can be re-ordered so that $p_i$ is an associate of $q_i$ for all $1 \leq i \leq m$. □

Before we show the existence of a factorisation, we will need a lemma.

**Lemma 3.5.21.** *Let $a$, $b$, $c$ be nonzero elements of a Euclidean domain. If $a = bc$ and $N(b) = N(a)$, then $c$ is a unit.*

*Proof.* Suppose $N(b) = N(a)$. Then there exist $q, r$ such that $b = aq + r$ and $r = 0$ or $N(r) < N(a) = N(b)$. But now $b = bcq + r$, so $r = b(1 - cq)$. If $r \neq 0$, then (by 1. of the definition for a Euclidean Norm), it must be the case that $N(r) \geq N(b)$, contradicting $N(r) < N(b)$. Therefore $r = 0$ and $0 = b(1 - cq)$. Certainly $b \neq 0$. But $R$ is an integral domain, so has no zero divisors. Thus we must have $cq = 1$. Hence $c$ is a unit. □

**Theorem 3.5.22.** *Every Euclidean domain is a unique factorisation domain (UFD).*

Recall the definition of a UFD, that every element other than zero and units can be expressed as a product $p_1 \cdots p_m$ of irreducibles, and furthermore any other such expression contains the same $p_i$ or associates of them.

*Proof.* Let $R$ be a Euclidean domain. By Theorem 3.5.20, if $a$ has a factorisation into irreducibles, then that factorisation is unique up to associates. So all we need to do is show that every nonzero non-unit element has a factorisation.

Let $a \in R$ be nonzero. We show by induction on $N(a)$ that $a$ is either a unit has a factorisation as a product of irreducibles.

First, suppose $N(a)$ is minimal in $R$. Suppose $a = bc$ for some $b, c \in R$. Then by definition of a Euclidean norm, we know $N(b) \leq N(a)$. But $N(a)$ is minimal. Therefore $N(b) = N(a)$ and by Lemma 3.5.21, $c$ is a unit. Hence $a$ is either a unit or is irreducible. We do not need to consider units, as the theorem does not apply, and if $a$ is irreducible then there is nothing to prove (set $m = 1$, $p_1 = a$) and we are done. Now suppose $N(a)$ is not minimal. Assume inductively that for any non-zero non unit $t$ for which $N(t) < N(a)$, there is a factorisation of $t$. Again if $a$ is irreducible there is nothing to prove. So assume $a$ is reducible. Then there are $b, c \in R$, neither of which is zero or a unit, such that $a = bc$. By the definition of Euclidean norm, $N(b) \leq N(a)$ and $N(c) \leq N(a)$. If $N(b) = N(a)$ then by Lemma 3.5.21, $c$ is a unit, a contradiction. So $N(b) < N(a)$, and similarly $N(c) < N(a)$. By the inductive hypothesis then, $c$ and $b$ can both be factorised. The product of these factorisations gives a factorisation of $a$. Hence, by induction on $N(a)$, every nonzero, non unit element of $R$ has a factorisation into irreducibles. □

**Example 3.5.23.** Since $\mathbb{Z}$ is a Euclidean domain, $\mathbb{Z}$ is a unique factorisation domain. Moreover, for all fields $F$, the polynomial ring $F[x]$ is a Euclidean domain. Therefore $F[x]$ is a UFD.

**Exercise 3.39.** Consider the set $R = \mathbb{Z}[\sqrt{-5}] = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$. Recall that for a complex number $z = x + iy$, the modulus $|z|$ is given by $|z|^2 = x^2 + y^2$, and that for $z, w \in \mathbb{C}$, we have $|zw|^2 = |z|^2|w|^2$. You should also check that for $z = a + bi\sqrt{5} \in R$, we have $|z|^2 = a^2 + 5b^2$.

(a) Show that $R$ is a ring, and further that $R$ is an integral domain.

(b) Suppose $z = a + bi\sqrt{5} \in R$ is a unit with multiplicative inverse $w = c + di\sqrt{5} \in R$, so that $zw = 1$. From the fact that $|z|^2|w|^2 = 1^2 = 1$, show that $a^2 = 1$ and $b^2 = 0$. Hence show that the units of $R$ are 1 and $-1$.

(c) Suppose $2 = zw$ for some $z, w \in R$. Show, by considering the equation $4 = 2^2 = |z|^2|w|^2$, that either $z$ or $w$ is a unit. Hence show that 2 is irreducible in $R$.

(d) Show, similarly, that 3, $(1 + i\sqrt{5})$ and $(1 - i\sqrt{5})$ are irreducible in $R$.

(e) By factorising 6 in two different ways in $R$ (eg using part (d)), show that $R$ is not a unique factorisation domain.

In fact it is possible to prove a slightly sharper version of Theorem 3.5.22. The proof is a little more difficult and lengthy, so it is excluded.

**Theorem 3.5.24.** *Let $R$ be a Principal Ideal Domain. Then $R$ is a Unique Factorisation Domain.*

Thus every Euclidean Domain is a Principal Ideal Domain and every Principal Ideal Domain is a Unique Factorisation Domain. Both of these inclusions are strict, in the sense that there is a Unique Factorisation Domain that is not a Principal Ideal Domain and there is a Principal Ideal Domain that is not a Euclidean Domain.

We finish off this section with a couple of results about polynomial rings which can help to determine whether a given polynomial is irreducible, and are also useful in our work on finite fields.

**Lemma 3.5.25.** *Let $F$ be a field, $f(x)$ a polynomial in $F[x]$, and suppose $a \in F$ is a root of $f(x)$. Then $(x-a)$ divides $f(x)$ in $F[x]$.*

*Proof.* By the Division Theorem for Polynomials, there are polynomials $q(x), r(x)$ with $r = 0$ or $\deg(r) < \deg(x-a) = 1$ such that $f(x) = (x-a)q(x) + r(x)$. Setting $x = a$, and noting that $f(a) = 0$, this implies $r(a) = 0$. But $\deg(r) = 0$, so $r$ is constant. Hence $r = 0$. Therefore $f(x) = (x-a)q(x)$ for some polynomial $q(x)$, meaning $(x-a)$ divides $f(x)$. □

**Theorem 3.5.26.** *Let $F$ be a field and $f(x)$ a nonzero polynomial of degree $n$ in $F[x]$. Then $f$ has at most $n$ distinct roots in $F$.*

*Proof.* It follows inductively from Lemma 3.5.25 that if $a_1, \ldots, a_m$ are $m$ distinct roots in $F$ of $f(x)$, then $g(x) := (x-a_1)(x-a_2)\cdots(x-a_m)$ divides $f(x)$ (because, for example, we may write $f(x) = (x-a_1)q_1(x)$ for some $q_1(x)$, and then since $x - a_2$ does not divide $x - a_1$, it must divide $q_1(x)$. So $f(x) = (x-a_1)(x-a_2)q_2(x)$ for some $q_2$ and so $(x-a_1)(x-a_2)$ divides $f(x)$, and so on). Hence $m = \deg(g) \leq \deg(f) = n$. Hence there are at most $n$ roots of $f(x)$ in $F$. □

Of course there may be no roots in $F$: for example the polynomial $x^2 + 1$ has no roots in $\mathbb{R}$, but two in $\mathbb{C}$. The fundamental theorem of algebra, which we won't prove in this course, states that every complex polynomial of degree $n$ has $n$ roots (some possibly repeated) in $\mathbb{C}$: in other words it can be factorised completely into a product of linear factors. This implies that there are no irreducible quadratic polynomials in $\mathbb{C}[x]$.

**Exercise 3.40.** Find the irreducible polynomials of degree 3 and 4 in $\mathbb{Z}_2[x]$. (Since $1 = -1$ in $\mathbb{Z}_2$, note that by Lemma 3.5.25 $x + 1$ is a factor of $f(x)$ precisely when $f(1) = 0$.)

**Exercise 3.41.** Let $R$ be an integral domain, and let $f(x) = x^2 - 2$. Determine whether or not $f(x)$ is reducible in $R[x]$ when $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$.

**Exercise 3.42.** Consider $\mathbb{Z}_{11}$. Find all values of $k \in \mathbb{Z}_{11}$ for which $g(x) = x^2 - k$ is irreducible.

**Exercise 3.43.** (a) Let $p$ be an odd prime, and $m \in \mathbb{Z}_p$. Show that $m \otimes_p m = (p-m) \otimes_p (p-m)$. Hence show that the map $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $\phi(m) = m^2$ is not surjective.

(b) Using part (a) or otherwise, show that there always exists an irreducible quadratic polynomial in $\mathbb{Z}_p$, for any odd prime $p$.

## 3.6 Finite Fields

It turns out that the orders of finite fields are very restricted. To show this, we need to make a definition.

**Definition 3.6.1.** Let $F$ be a field. If there is a positive integer $n$ such that $n1 = 0$, then the *characteristic* of $F$ is defined to be $\text{char}(F) = \min\{n \in \mathbb{Z}^+ : n1 = 0\}$. Otherwise, we define $\text{char}(F)$ to be zero.

**Example 3.6.2.** We have $\text{char}(\mathbb{C}) = 0$ because $n1 = n \neq 0$ for any positive integer $n$. However $\text{char}(\mathbb{Z}_3) = 3$ because $3 \cdot 1 = 1 \oplus 1 \oplus 1 = 0$.

**Lemma 3.6.3.** *Let $F$ be a field. Then either* $\text{char}(F) = 0$ *or* $\text{char}(F)$ *is prime.*

*Proof.* Suppose $\text{char}(F) = n \neq 0$. Then $n \cdot 1 = 0$. If $n$ is composite, so $n = ab$ for some positive integers $a < n, b < n$, then $ab \cdot 1 = 0$ implies $(a \cdot 1)(b \cdot 1) = 0$. But a field has no zero divisors, so at least one of $a \cdot 1 = 0$ or $b \cdot 1 = 0$ holds. But $n$ is the least positive integer with this property, a contradiction. Therefore $n$ must be prime. □

**Proposition 3.6.4.** *The order of a finite field $F$ is $p^k$ for some prime $p$ and positive integer $k$, and every nonzero element of $F$ has (additive) order $p$.*

*Proof.* Let $F$ be a finite field of order $n$. Then $(F, +)$ is a finite abelian group, and the order of any element divides $n$. Hence $n \cdot 1 = 0$. Therefore $\text{char}(F)$ is certainly non-zero, and is therefore prime. Say $\text{char}(F) = p$, where $p$ is prime. Let $a$ be a nonzero element of $F$. Then $p1 = 0$ implies $p1a = 0a$ and hence $pa = 0$. Therefore the order of $a$, as an element of $(F, +)$ is at most $p$. Suppose $ta = 0$ for some $0 < t < p$. Then $t1 = taa^{-1} = 0a^{-1} = 0$, so $t1 = 0$. But the smallest positive integer $m$ satisfying $m1 = 0$, is $p$, a contradiction. Therefore $p$ is the smallest positive integer for which $pa = 0$. Hence $o(a) = p$. Now let $q$ be a prime divisor of $|F|$. In Chapter 2 of the notes we proved Cauchy's Theorem, which stated that for every prime divisor $q$ of the order of a group $G$, there is an element of order $q$. Therefore $F$ has an element of order $q$. We have seen that every nonzero element of $F$ has order $p$, and of course 0 is the additive identity element, and so has order 1. Hence $q = p$. In other words, the only prime divisor of $|F|$ is $p$. Thus $|F| = p^k$ for some positive integer $k$ and every nonzero element $a$ of $F$ has additive order $p$, meaning that $pa = 0$. □

So there can be no field of order 10, for example. It can be shown that for any prime $p$ and positive integer $n$, there exists a field of order $p^n$. This fact follows from a theorem of Galois that there is always an irreducible polynomial of degree $n$ over $\mathbb{Z}_p$. If $f(x)$ is such a polynomial, then it turns out that the quotient ring $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field of order $p^n$. The proof of this is in appendix B.4. It can also be shown that two finite fields of the same order are isomorphic (as fields not just as groups).The 'unique' field of order $p^n$ is called the *Galois Field* of order $p^n$. In fact this is even stronger a result than at first it seems, as the next result shows.

**Lemma 3.6.5.** *Every finite integral domain is a field.*

*Proof.* Let $R$ be a finite integral domain and let $a$ be a nonzero element of $R$. Consider the set $a, a^2, a^3, \ldots$ of all positive powers of $a$. Now $R$ is closed under multiplication, so each of these powers is contained in $R$. But $R$ is finite, so at some point in the list, we must see an element we have encountered before. That is, there must exist integers $m$ and $n$ with $m < n$ for which $a^n = a^m$. But now, by the cancellation property of integral domains (Lemma 3.3.13), this implies $a^{n-m} = 1$. Now let $b = a^{n-m-1}$ (this is well defined because $n - m - 1 \geq 0$). Then $ab = a^{n-m} = 1$. Hence $a$ has a multiplicative inverse. This holds for every nonzero element $a$ of $R$ and so $R$ is a field. □

Next we will prove an interesting fact about the multiplicative groups of finite fields. First we need a bit of notation.

**Definition 3.6.6.** Let $G$ be a finite group. The exponent $\exp(G)$ is the least common multiple of the orders of the elements of $G$.

Since the order of elements of $G$ always divides $|G|$, certainly $\exp(G)$ divides $G$, but certainly does not always equal $|G|$.

**Example 3.6.7.** The group $(\mathbb{Z}_{12}, \oplus_{12})$ is cyclic and has an element of order 12 (namely 1), so the exponent is certainly at least 12. The order of every element divides 12, the order of the group, so the exponent is at most 12. Hence $\exp(\mathbb{Z}_{12}) = 12$.

**Example 3.6.8.** The group $(U_{12}, \otimes)$ (the group of units of $\mathbb{Z}_{12}$), consists of the integers in $\mathbb{Z}_{12}$ which are coprime to 12. So $U_{12} = \{1, 5, 7, 11\}$. Now $5 \otimes 5 = 1, 7 \otimes 7 = 1, 11 \otimes 11 = 1$. Hence every element of $U_{12}$ has order 1 or 2. Thus the exponent of $U_{12}$ is 2.

**Example 3.6.9.** The group $S_3 = \{e, (12), (13), (23), (132), (123)\}$ has elements of order 1, 2 and 3. Hence the exponent of $S_3$ is $\operatorname{lcm}(1, 2, 3) = 6$.

This example shows that $G$ does not necessarily have an element of order $\exp(G)$. However when $G$ is abelian, there is guaranteed to be such an element.

**Lemma 3.6.10.** *Suppose $G$ is a finite abelian group. Then $G$ contains an element of order $\exp(G)$.*

*Proof.* Write $\varepsilon = \exp(G)$. Suppose $p$ is a prime divisor of $\varepsilon$. Then we can write $\varepsilon = p^k m$ for some positive integers $k, m$ with $\gcd(p, m) = 1$. Let $|G| = n$ and write $G = \{g_1, \ldots, g_n\}$. Then for each $i$ there is a positive integer $m_i$, coprime to $p$, and a non-negative integer $a_i$ such that $o(g_i) = p^{a_i} m_i$. Now

$$p^k m = \varepsilon = \operatorname{lcm}(p^{a_1} m_1, \ldots, p^{a_n} m_n) = p^{\max(a_1, \ldots, a_n)} \operatorname{lcm}(m_1, \ldots, m_n).$$

Therefore $k = \max(a_1, \ldots, a_n)$. In other words, for some $i$ we have $a_i = k$. Hence $g_i$ has order $p^k m_i$. Set $g = g_i^{m_i}$. Then $g^{p^k} = g_i^{p^k m_i} = 1$. Hence $g$ has order $p^k$. We can extend this to any prime divisor of $\varepsilon$. Let the prime factorisation of $\varepsilon$ be $\varepsilon = p_1^{k_1} \cdots p_t^{k_t}$. For $j = 1, \ldots, t$ let $h_j$ be an element of $G$ with order $p_j^{k_j}$. Then define $h = h_1 h_2 \cdots h_t$. Since $G$ is abelian, we have $h^r = h_1^r h_2^r \cdots h_t^r$ for all positive integers $r$. So if $h^r = 1$, then $p_j^{k_j}$ divides $r$ for all $j$. Hence $\varepsilon \leq r$. But certainly $h^\varepsilon = 1$ by definition of exponent. Hence $o(h) = \varepsilon$ and we have found the appropriate element of $G$. □

**Theorem 3.6.11.** *Let $F$ be a field. Then any finite subgroup of the multiplicative group of $F$ is cyclic.*

*Proof.* Recall that the multiplicative group of $F$ is $F - \{0\} = F^*$. Note that $F^*$ is abelian. Let $G$ be any finite subgroup of $F^*$. Then certainly $G$ is also abelian. Let $\varepsilon$ be the exponent of $G$. Then $a^\varepsilon = 1$ for any $a \in G$, so $a$ is a root of the polynomial $x^\varepsilon - 1$. But by Theorem 3.5.26 there are at most $\varepsilon$ roots of this polynomial, as it has degree $\varepsilon$. Hence $|G| \leq \varepsilon$. We have already noticed that for any finite group $G$, $\exp(G) \leq |G|$. Therefore $\varepsilon \leq |G|$ and hence $\varepsilon = |G|$. But now we can apply Lemma 3.6.10 and deduce that $G$ has an element $g$ of order $\varepsilon = |G|$. Therefore $G$ is cyclic, generated by $g$. □

**Corollary 3.6.12.** *The multiplicative group of any finite field is cyclic.*

*Proof.* The multiplicative group of a finite field is certainly finite. Hence it is cyclic, by the theorem. □

**Corollary 3.6.13.** *Every finite subgroup of $(\mathbb{C}^*, \times)$ is cyclic.*

*Proof.* This follows immediately from the fact that $\mathbb{C}^*$ is the multiplicative group of the field of complex numbers. □

**Exercise 3.44.** By considering $\mathbb{Z}_{12}$ or otherwise, show that the multiplicative group of a finite ring is not always cyclic.

**Exercise 3.45.** Find a generator of the multiplicative group of $\mathbb{Z}_{11}$.

## Exam-Style Questions

### Section A

**Exercise 3.46.** The set $\mathcal{M}_2(\mathbb{R})$ of $2 \times 2$ real matrices is a ring. Let $R$ be the following subset of $\mathcal{M}_2(\mathbb{R})$.

$$R = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}.$$

(a) Show that $R$ is a subring of $\mathcal{M}_2(\mathbb{R})$.

(b) Is $R$ a ring with identity? Is $R$ a division ring? Justify your answers.

**Exercise 3.47.** Let $R$ be a commutative ring with identity.

(a) Define the terms 'zero divisor' and 'unit' of $R$.

(b) Find the zero divisors of $\mathbb{Z}_{15}$ and the units of $\mathbb{Z}_{15}$.

**Exercise 3.48.** Let $R$ be a ring.

(a) What does it mean for a subset $I$ of $R$ to be an *ideal* of $R$?

(b) Suppose $R$ is a commutative ring with identity, and let $a \in R$. Show that the set $aR = \{ar : r \in R\}$ is an ideal of $R$ that contains $a$.

**Exercise 3.49.** Find all the irreducible monic quadratic polynomials of $\mathbb{Z}_3[x]$ (that is, the irreducible polynomials $x^2 + bx + c$, where $b, c \in \mathbb{Z}_3$).

### Section B

**Exercise 3.50.** This question is about the set $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$.

(a) (i) Show that $\mathbb{Z}[\sqrt{3}]$ is a ring (you may assume without proof that $\mathbb{R}$ is a field and use the subring test).

(ii) Show further that $\mathbb{Z}[\sqrt{3}]$ is an integral domain.

(b) Show that if $u$ is a unit of an integral domain, then $u^{-1}$ is a unit and that $u^n$ is a unit for all positive integers $n$.

(c) Suppose $a + b\sqrt{3}$ is a unit of $\mathbb{Z}[\sqrt{3}]$ with inverse $c + d\sqrt{3}$.

(i) Show that $a - b\sqrt{3}$ is a unit with inverse $c - d\sqrt{3}$.

(ii) Show that $(a + b\sqrt{3})(a - b\sqrt{3})(c + d\sqrt{3})(c - d\sqrt{3}) = 1$ and hence that if $a + b\sqrt{3}$ is a unit, then $a^2 - 3b^2 = \pm 1$.

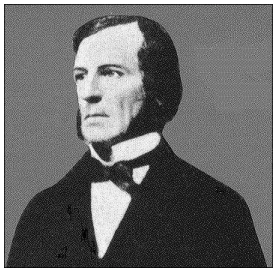
(iii) Use part (ii) to show that there are infinitely many elements of $\mathbb{Z}[\sqrt{3}]$ which are not units.

(d) Show that if $m^2 - 3n^2 = \pm 1$, then $m + n\sqrt{3}$ is a unit of $\mathbb{Z}[\sqrt{3}]$. Hence or otherwise find three units of $\mathbb{Z}[\sqrt{3}]$.

(e) Using your answers to parts (b) and (d), or otherwise, find two further units of $\mathbb{Z}[\sqrt{3}]$.

**Note.** Exam questions, particularly Section B and C questions, often combine elements from different chapters.

## Historical Notes



**George Boole** (2 November 1815 – 8 December 1864)

As a boy, Boole's real interest was in languages. He learnt Latin, then taught himself Greek, French and German. He became a teacher when his father went bankrupt. In fact he opened his own school when he was only 19. He continued teaching, but started studying mathematics on the side. He published several papers and finally got a university position aged 35. Boole met his future wife in 1850, and romance blossomed (obviously) when he taught her differential calculus.

Boole managed to fit a lot into his short career; he is most famous for his work on Logic. His death was probably wholly preventable. One day he walked to college in the pouring rain and gave his lecture still in his wet clothes. He developed a fever and unhappily for him, his wife put into practice her theory that the way to cure a disease is to replicate its cause. So she tucked him up in bed and proceeded to throw buckets of cold water over him until he got better. Which he didn't. He died soon after, aged 49.

**Emmy Noether** (23 March 1882 – 14 April 1935)
Emmy Noether is famous in mathematics for her pioneering work in ring theory. A *Noetherian ring* is a generalisation of a principal ideal domain; it satisfies the property that every ideal is generated by a finite number of elements. This is a weaker requirement than that every ideal should be a principal ideal, but it is enough to guarantee that every nonzero element is either a unit or can be factorised as a product of irreducibles. Emmy Noether grew up just at the point when women were starting to be allowed to study mathematics at university. In fact as late as 1898 the University of Erlangen's academic senate passed a resolution stating that the admission of women students would '*overthrow all academic order*'. However women students were finally admitted there in 1904, and Noether was among the first cohort of that year. Hilbert recognised her talent and fought to get her an academic position at Göttingen University. As he famously argued in a faculty meeting: '*I do not see that the sex of the candidate is an argument against her admission [as an academic]. After all, we are a university, not a bathing establishment!*' Noether's best work was done in her forties, most importantly the 1921 paper introducing the concept later named in her honour as a Noetherian ring. In 1933 the Nazis seized power in Germany and Noether (who was Jewish) was removed from her university position. She moved to America but sadly died just two years later.

**Learning Outcomes**

*After studying this chapter, and the related exercises, the following is an indicative list of what you*

*should be able to do.*

- Give the definition of a ring, and determine whether or not a given set is a ring.
- Know what is meant by the terms 'trivial ring' and 'zero ring'.
- Work with familiar examples of rings, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$, number rings (including the Gaussian integers $\mathbb{Z}[i]$), matrix rings and polynomial rings.
- Give the definition of the following terms: ring with identity, commutative ring, division ring, field, and be able to determine whether a given ring is one of these special types of ring.
- Work with subrings and ideals; know and apply the subring test and ideal test.
- Define zero divisor, unit, integral domain and irreducible elements, and work with these terms. Be aware of the properties of integral domains, such as the cancellation property. Be aware that every integral domain has a field of fractions, and that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.
- Be familiar with the term 'the ideal generated by $a$', and 'principal ideal domain'.
- Know the definitions of ring homomorphisms, kernels and images. Be aware that the kernel of a ring homomorphism is an ideal, and the image is a ring.
- Give the definition of a Euclidean domain and a unique factorisation domain, and know the main properties of Euclidean domains, for example that every Euclidean domain is a principal ideal domain and a unique factorisation domain.
- Determine whether a given map on a set is a Euclidean norm, and hence whether that set is a Euclidean domain.
- Use the Euclidean algorithm in a Euclidean domain to find a greatest common divisor of two nonzero elements (in particular where the Euclidean domain is $F[x]$ for a field $F$, or $\mathbb{Z}$, or $\mathbb{Z}[i]$).
- Determine whether or not an element of an integral domain is irreducible (in particular where the integral domain is $F[x]$ for a field $F$).
- Define the characteristic of a field; be able to show that every finite field has characteristic $p$, and be aware that every finite field has prime power order.
- Know what is meant by the exponent of a finite group, and be aware that if $G$ is a finite abelian group, then $G$ contains an element of order $\exp(G)$. Be able to use this fact to show that any finite subgroup of the multiplicative group of a field is cyclic.