Notes in ring theory

Paul Martin

Dec 11, 2009 (printed: May 18, 2011)

Contents

Chapter 1

Foreword

Ring theory is generally perceived as a subject in Pure Mathematics. This means that it is a subject of intrinsic beauty. However, the idea of a ring is so fundamental that it is also vital in many applications of Mathematics. Indeed it is so fundamental that very many other vital tools of Applied Mathematics are built from it. For example, the crucial notion of linearity, and linear algebra, which is a practical necessity in Physics, Chemistry, Biology, Finance, Economics, Engineering and so on, is built on the notion of a *vector space*, which is a special kind of *ring module*.

At Undergraduate Level Three and beyond, one typically encounters many applications of ring theory (either explicitly or implicitly). For example, many fundamental notions about information and information transmission (not to mention information protection) are most naturally described in the setting of ring theory. In particular, a *field* is a special kind of ring, and the theory of *Coding* — one of the main planks of modern information technology and Computer Science — makes heavy practical use of the theory of fields, which lives inside the theory of rings.

So, there are countless applications of ring theory ahead (not to mention countless amazing open problems). But here we shall concentrate, for now, on the first point: ring theory is "a subject of intrinsic beauty".

Ring theory appears to have been among the favourite subjects of some of the most influential Scientists of the twentieth century, such as Emmy Noether (discoverer both of Noether's Theorem — one of the most important theorems in modern Physics; and of Noetherian rings[1]); and Alfred Goldie (author of Goldie's Theorem, and founder of the University of Leeds Algebra Group).

But perhaps more important than any of these points is that ring theory is a core part of the subject of Algebra, which forms the *language* within which modern Science can be put on its firmest possible footing.

[1] Also someone who helped to defeat the terrible sexism that afflicted European academia in the 20th century.

Chapter 2

Rings, Polynomials and Fields

This Chapter is based partly on the undergraduate lecture course notes of Bill Crawley-Boevey, and sections from the textbooks of Serge Lang and Nathan Jacobson. It is intended as an undergraduate exposition.

2.1 Introduction

As we shall see later, a *ring* is a set with two binary operations (usually called *addition* and *multiplication*) satisfying certain axioms. The most basic example is the set $\mathbb{Z}$ of integers. Another familiar example is the set $\mathbb{Z}[x]$ of polynomials in an indeterminate x, with integer coefficients.

(**2.1.1**) Example. Make sure you can add and multiply polynomials, by trying a few examples.

(**2.1.2**) Example. Suppose $n \in \mathbb{Z}$ is not a square and define $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$. Check that you can add and multiply in this case, and that these operations are closed.

(**2.1.3**) Let us start by thinking about the integers before we go any further. They are (hopefully) familiar, and 'familiarity breeds contempt'.[1] But what aspects of their behaviour should we *not* be contemptuous of? What we need to do, for a moment, is forget the familiarity, and consider the integers as an example of an algebraic structure. What can we say about them in this light?

Addition and multiplication mean that, given $a, b \in \mathbb{Z}$ we have solutions $x, y \in \mathbb{Z}$ to the equations

$$x = a + b, \qquad y = ab$$

Continuing to regard a, b as given, this does *not* automatically mean that we have a solution x to

$$xa = b \tag{2.1}$$

It also does not *automatically* mean that we have a solution x to $x + a = b$, but of course if $a, b \in \mathbb{Z}$ then this problem *does* have a solution. On the other hand equation (2.1) does not always have a solution. It depends on a, b. For this reason, we say a *divides* b if $xa = b$ has a solution $x \in \mathbb{Z}$. If a divides b we may write this as $a|b$.

[1] According to Charles Dickens.

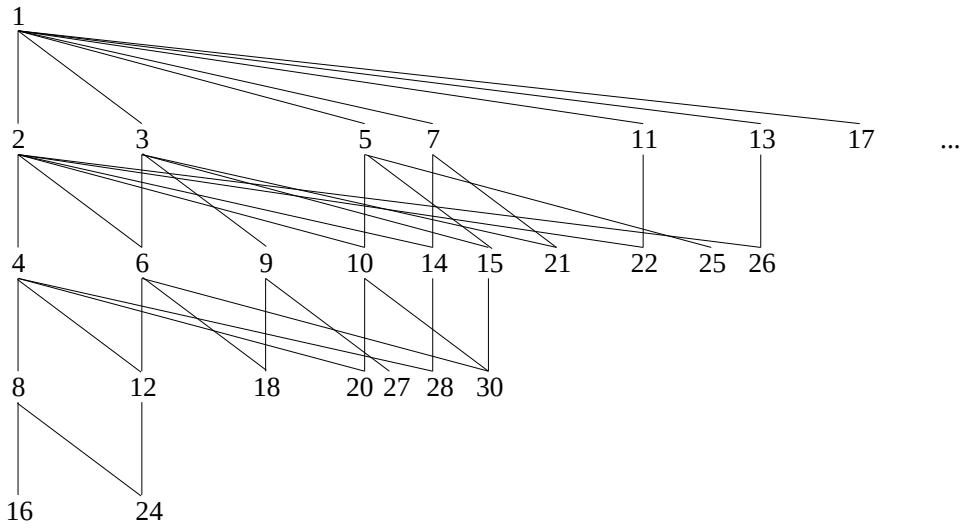


Figure 2.1: The start of the 'divides' Hasse diagram

(**2.1.4**) Recall that a *poset* is a set S together with a transitive, reflexive and antisymmetric relation on S. If $\geq$ is such a relation we write $a > b$ if $a \geq b$ and $a \neq b$.

A *transitive reduction* of a poset $(S, \geq)$ is a simple directed graph with vertex set S and an edge (a, b) if $a > b$ and there does not exist $a > c > b$.

A *lattice* is a poset such that for any pair of elements (a, b) there is a least upper bound (LUB) and a greatest lower bound (GLB).

(**2.1.5**) We define a relation on $\mathbb{N}$ by $a \sim b$ if $a|b$. This is evidently transitive, reflexive and antisymmetric. Thus it makes $\mathbb{N}$ into a poset (different from the obvious but very important total order $(\mathbb{N}, \geq)$). Indeed $(\mathbb{N}, |)$ is a (complete distributive) lattice. In $(\mathbb{N}, |)$ the GLB is the GCD.

(**2.1.6**) Example. The GCD of 6 and 8 is 2. A *lower bound* of 6 in this case is a number that divides 6 (thus 6,3,2 or 1). A lower bound of 8 is any of 8,4,2,1. Thus a lower bound of $\{6, 8\}$ is an element of $\{1, 2\}$. Since $1|2$ but $2 \not| 1$ we have the GCD of 2.

(**2.1.7**) We say that a, b are *coprime* if their GCD is 1.

(**2.1.8**) Exercise. Draw the begining of the Hasse diagram for $(\mathbb{N}, |)$. (See Figure 2.1.)

2.2 Factorisation of integers

(**2.2.1**) A *prime number* is an integer $p > 1$ such that $p|ab$ implies $p|a$ or $p|b$.

(**2.2.2**) Theorem. (Fundamental theorem of arithmetic) Any integer $n > 1$ can be written as a product of prime numbers:

$$n = p_1 p_2 ... p_k$$

And if $n = q_1 q_2 ... q_l$ is another product of primes then $k = l$ and indeed the factorisations are the same up to reordering.

Proof. First we show that such a factorisation is always possible (then later we will show the uniqueness up to reordering).

Suppose, for a contradiction, that there is an n that *cannot* be factorised into prime numbers. Then there is a *least* such n (note that we are using an *ordering* property of the integers here that goes beyond just arithmetic — in fact we have already used the $>$ ordering repeatedly!). Of course any such n cannot itself be prime (else $n = n$ would already be an acceptable prime factorisation). Since it is not prime, it has a divisor d (say), that is $d|n$ and $1 < d < n$. So $n = dm$, with $1 < m < n$. But since n was the least integer without a factorisation, both d and m have one. But then the combination of these is a factorisation of n — a contradiction.

To show uniqueness, we work again for a contradiction. Let n be the lowest integer with *distinct* factorisations, and let them be $n = p_1 ... p_k$ and $n = q_1 ... q_l$. If $k = 1$ then n is prime, so $l = 1$ and $p_1 = q_1$ giving a contradiction, so $k > 1$. But in this case note that $p_1 | q_1 ... q_l$. Thus by definition $p_1 | q_i$ for some i. That is, $p_1 = q_i$ and $n = mp_1 = mq_i$ for some m. Cancelling p_1 from each factorisation we get two factorisations for m. But $1 < m < n$, so m has a unique factorisation — a contradiction. □

(**2.2.3**) THEOREM. (Euclid) There are infinitely many prime numbers.

Proof. Exercise. Hint: Suppose $p_1 p_2 ... p_n$ is a product of primes. Then $p_1 p_2 ... p_n + 1$ is coprime to them all. Now suppose, for a contradiction, that there are only finitely many primes.

(**2.2.4**) Perhaps it is strange that the integers contain this special prime structure, whereas the larger sets such as the rationals $\mathbb{Q}$ and the reals $\mathbb{R}$ do not (it is too easy to solve $xa = b$ in these cases).

2.3 Rings

(**2.3.1**) A *monoid* is a set with a closed associative binary operation, with an identity element.

(**2.3.2**) EXAMPLE. $(\mathbb{Z}, \times)$ is a monoid — so this is an even simpler thing than a ring, because we only use *one* binary operation.

(**2.3.3**) A *group* is a monoid $(G, *, 1)$ with the property that every element $g \in G$ has an inverse (i.e. there is an element $g' \in G$ such that $g * g' = 1$).

A group is *abelian* if $a * b = b * a$.

(**2.3.4**) A ring is a set R with two binary operations, $+$ and $\times$ such that $(R, +, 0)$ is an abelian group; $(R, \times, 1)$ is a monoid; and

$$a \times (b + c) = a \times b + a \times c, \qquad (b + c) \times a = b \times a + c \times a$$

for all a, b, c.
(When there is no ambiguity we often write ab for $a \times b$.)

(**2.3.5**) EXAMPLE. Can a set with one element be a ring? Yes.

(**2.3.6**) EXAMPLE. Fix an integer m. Integers modulo m, written $\mathbb{Z}_m$, form a ring — the ring of modular arithmetic.

(**2.3.7**) EXAMPLE. Let R be a ring. Then the $n \times n$ matrices with entries in R, denoted $M_n(R)$, form a ring via the usual matrix algebra rules.

(**2.3.8**) EXERCISE. For S a set, let $P(S)$ denote the power set. Note that the binary operations of intersection and union are closed on $P(S)$. In fact if S is finite, then $(P(S), \cup, \cap)$ is a ring (with $\cap$ playing the role of $\times$; and $\cup$ the role of $+$). Prove this, in case $S = \mathbb{Z}_2$.

(**2.3.9**) Some workers do not require a ring to have an identity of multiplication. Both Lang and Jacobson consider rings with 1, however.

Special elements in a ring

(**2.3.10**) The identity of the operation $+$ in a ring is usually written 0 and called *zero*, even if the ring does not contain $\mathbb{Z}$.

(**2.3.11**) A *unit* in a ring is an invertible element.

(**2.3.12**) A *zero-divisor* in a ring is a nonzero element a such that there is another nonzero element b with $ab = 0$.

Ring homomorphisms

(**2.3.13**) A ring homomorphism is a map

$$f : R \to S$$

between two rings such that $f(ab) = f(a)f(b)$, $f(a + b) = f(a) + f(b)$ and $f(1) = 1$.

(**2.3.14**) EXAMPLE. There is a map $f : \mathbb{Z} \to \mathbb{Q}$ given by $f(n) = n$.

(**2.3.15**) EXAMPLE. There is a map $g : \mathbb{Z} \to M_2(\mathbb{C})$ given by $g(n) = n1_2$.

(**2.3.16**) EXAMPLE. The set map $g' : \mathbb{Z} \to M_2(\mathbb{C})$ given by $g(n) = \ diagonal(n, 0)$ is not a ring homomorphism.

(**2.3.17**) EXAMPLE. For any ring R there is a *trivial* homomorphism $1_R : R \to R$ given by $1_R(r) = r$ for all $r \in R$.

(**2.3.18**) If for a ring homomorphim $f : R \to S$ there is also a ring homomorphim $f' : S \to R$ such that $f' \circ f = 1_R$ and $f \circ f' = 1_S$, then f is a ring *isomorphism*.
If there is an isomorphism between two rings ($f : R \to S$, say) then the rings are said to be *isomorphic*. We write $R \cong S$.

(**2.3.19**) A ring isomorphism from a ring R to itself is called an *automorphism*.
Note that the set of automorphisms of a ring R forms a group under composition of maps, denoted $\mathrm{Aut}(R)$.

(**2.3.20**) EXAMPLE. The map $-^* : \mathbb{C} \to \mathbb{C}$ given by $a + ib \mapsto a - ib$ is a ring automorphism.

(**2.3.21**) REMARK. It is an exercise to construct some simple examples of isomorphisms and automorphisms. We will give some 'interesting' examples later, when we have constructed a few more rings.

(**2.3.22**) The *kernel* of a ring homomorphism $f : R \to S$ is the set

$$\ker f \ := \ \{r \in R \mid f(r) = 0\}$$

(**2.3.23**) EXAMPLE. The map $f : \mathbb{Z} \to \mathbb{Z}_m$ given by $n \mapsto n' = [n]$ (the class of n) is a ring homomorphism, and $\ker f = m\mathbb{Z}$.

(**2.3.24**) If a ring homomorphism $f : R \to S$ is an inclusion of sets, and the operations are the same, then R is a *subring* of S.

(**2.3.25**) EXAMPLE. For $d \in \mathbb{Z}$ the subset of $M_2(\mathbb{Z})$ given by

$$M_2^d(\mathbb{Z}) := \{\begin{pmatrix} a & db \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$$

is a subring.

(**2.3.26**) A subset R is a subring of ring S iff (i) the operations close in R; (ii) $1 \in R$; and (iii) R is closed under additive inverse.
Exercise: check this.

(**2.3.27**) REMARK. An interesting way of constructing new rings from old is suggested by our kernel example. Suppose $r \in R$ and consider the set of all finite sums of elements of R of form arb:

$$RrR := \{\sum_i a_i r b_i \mid a_i, b_i \in R\}$$

(This is just  an extension of our notation $m\mathbb{Z}$.)

Notice that RrR behaves a bit like a ring itself: For $x, y \in RrR$ we have $x + y, xy \in RrR$. But note that $1 \in R$ may not be in RrR. (In fact if it is, then $RrR = R$.)

(**2.3.28**) Picking R and $r \in R$ we can define an equivalence relation on R by

$$[x] = \{y \in R \mid x - y \in RrR\}$$

We claim that the set of classes (denoted R/RrR) inherits a ring structure from R.

(**2.3.29**) In other words, for every R and $r \in R$ we have another new ring R/RrR. (Although this might often be the zero ring of course.) We automatically have a ring homomorphism

$$f : R \to R/RrR$$

given by $f(r) = [r]$. The kernel of this f is RrR.

(**2.3.30**) There is a very useful *abstraction* of this idea RrR as follows.

(**2.3.31**) An *ideal* in a ring R is a subset I such that $(I, +)$ is a subgroup; and $rx, xr \in I$ for all $x \in I$ and $r \in R$.

(**2.3.32**) EXAMPLE. $3\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

(**2.3.33**) EXAMPLE. RrR is an ideal in R.

(**2.3.34**) Let I be an ideal of ring R. Then we define $[r] \subset R$ as the set of elements of the form $r+x$, where $x \in I$. We define a relation on R by $r \sim^I s$ if $r - s \in I$. Note that this is an equivalence relation. Thus each $[r]$ is an equivalence class. (It is sometimes also useful to write $r + I$ for $[r]$.)

We write R/I for the set of equivalence classes.
Note that if $rs = t$ then

$$(r + x)(s + y) = rs + ry + xs + xy = t + L$$

where $L = ry + xs + xy$, so that if $x, y \in I$ then $L \in I$. It follows that we have a well-defined multiplication on R/I given by $[r][s] = [rs]$.
Also $(r + x) + (s + y) = (r + s) + (x + y)$ so $[r] + [s] = [r + s]$ is a well-defined addition. Thus R/I is a ring.

(**2.3.35**) THEOREM. [First ring isomorphism theorem] Let R be a ring. If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R, $\phi(R)$ is a subring of S, and $R/\ker(\phi) \cong \phi(R)$.

(**2.3.36**) EXAMPLE. Consider the set $M^\sigma(\mathbb{Z})$ of 2×2 matrices of the form $a_1 1_2 + a_2\sigma$ where $a_i \in \mathbb{Z}$ and

$$1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Does this form a subring of $M_2(\mathbb{Z})$?
Is $f : M^\sigma(\mathbb{Z}) \to \mathbb{Z}$ given by $f : a_1 1_2 + a_2\sigma \mapsto a_1 + a_2$ a ring homomorphism? If so, what is the kernel? (...And in the form RrR?)
Is f_2 given by $f_2(a_1 1_2 + a_2\sigma) = a_1 - a_2$ a ring homomorphism?
Can we 'learn' anything about $M^\sigma(\mathbb{Z})$ from this exercise?!

(**2.3.37**) We will study ideals further in Section 2.10.

Special kinds of ring

(**2.3.38**) A ring is an *integral domain* if it is commutative, has more than one element, and no zero-divisors.

(**2.3.39**) EXAMPLE. $\mathbb{Z}_4$ is not an integral domain, since $2 \times 2 = 0$; but $\mathbb{Z}$ is an integral domain.

(**2.3.40**) A *field* is a commutative ring that has more than one element, and such that every nonzero element is invertible.

(**2.3.41**) THEOREM. A finite integral domain is a field.

Proof. Let $R = \{r_1, r_2, ..., r_l\}$ be a finite integral domain. For any $r_i \neq 0$ and $j \neq k$ we have $r_i(r_j - r_k) \neq 0$, since $r_j \neq r_k$ and there are no zero-divisors. Thus $\{r_i r_1, r_i r_2, ..., r_i r_l\} = R$ and in particular one of these is $r_i r_j = 1$. □

(**2.3.42**) THEOREM. $\mathbb{Z}_n$ is a field iff n is prime.

Proof. (Only if): Suppose $n = p_1 p_2$. Then p_1, p_2 pass to zero-divisors in $\mathbb{Z}_n$.
(If): See later.

(**2.3.43**) A matrix ring over a field is not in general a field. For example, the matrix ring $M_2(\mathbb{Z}_2)$ is not a field.

(**2.3.44**) EXERCISE. (i) The matrix ring $M_2(\mathbb{Z}_2)$ is finite. What is its order? Give an algorithm for writing out all the elements; then do it.
(ii) Find a subring of $M_2(\mathbb{Z}_2)$ that is a field, and which properly contains the natural image of $\mathbb{Z}_2$.

Hints: Consider the subset

$$F_4 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

(**2.3.45**) Suppose $n \in \mathbb{Z}$ is not a square. Then

$$\mathbb{Z}[\sqrt{n}] \;=\; \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

This is a subring of $\mathbb{C}$; and an integral domain.

The norm function

(**2.3.46**) Any element of $\mathbb{Z}[\sqrt{n}]$ above can be written in a unique way as $\gamma = a + b\sqrt{n}$ with $a, b \in \mathbb{Z}$. We define the *norm*

$$N(\gamma) \;=\; |a^2 - nb^2|$$

(**2.3.47**) Lemma. (i) $N(\gamma) = 0$ iff $\gamma = 0$; (ii) $N(\gamma\delta) = N(\gamma)N(\delta)$.

Proof. (i) $a^2 - nb^2 = 0$ implies $a^2 = nb^2$ and hence $n = \frac{a^2}{b^2}$. But this requires that n is a square. (ii): Exercise. (Possible hint: cf. (2.3.25).)
Hereafter, when we omit a proof without comment, it is to be treated as an exercise.

(**2.3.48**) Lemma. γ is a unit in $\mathbb{Z}[\sqrt{n}]$ iff $N(\gamma) = 1$.

(**2.3.49**) Example. In $\mathbb{Z}[\sqrt{3}]$ we have $N(7 \pm 4\sqrt{3}) = 1$ so $7 \pm 4\sqrt{3}$ are units.

2.4 Factorisation in integral domains

(**2.4.1**) Suppose R is an integral domain. Once again we define $a|b$ to mean that $ac = b$ has a solution $c \in R$.

(**2.4.2**) Example. In $\mathbb{Z}[i]$ we have $(1 + i)(2 - i) = 3 + i$, so $1 + i|3 + i$.

(**2.4.3**) $a, b \in R$ are *associates* if $a = ub$ for u some unit. Association is an equivalence relation.

(**2.4.4**) $p \in R$ is *irreducible in* R iff (i) p is not zero and not a unit; (ii) $p = ab$ implies a or b a unit.

(**2.4.5**) $p \in R$ is *prime in* R iff (i) p is not zero and not a unit; (ii) $p|ab$ implies $p|a$ or $p|b$.

(**2.4.6**) Example. In $\mathbb{Z}$ an element is irreducible iff it is prime iff it is a prime number up to sign.

(**2.4.7**) Remark. In light of the case $R = \mathbb{Z}$, we might like to suppose that the notions of primeness and irreducibility are always interchangeable in an integral domain. In the next few paragraphs, though, we shall see that this is asking to much, in general. Although they are indeed related...

(**2.4.8**) Lemma. In an integral domain R, prime implies irreducible.

Proof. Suppose for a contradiction that some prime $p \in R$ obeys $p = ab$ with a, b nonunits in R. Then by primeness $p|a$ or $p|b$ — say $p|a$ WLOG. Then $a = pc$ for some $c \in R$, so $a = abc$, thus $a(1 - bc) = 0$. Since $a \neq 0$ we have $bc = 1$, which contradicts that b is a nonunit. □

(**2.4.9**) If $a|b$ in $R = \mathbb{Z}[\sqrt{n}]$ then $N(a)|N(b)$ as integers.
If $a \in \mathbb{Z}[\sqrt{n}]$ and $N(a)$ is a prime number then a must be irreducible.

(**2.4.10**) Example. In $\mathbb{Z}[\sqrt{-5}]$ the element $\gamma = 1 + \sqrt{-5}$ is irreducible but not prime.
To see that γ is irreducible, note that $N(\gamma) = 6$, thus any nonunit factorisation $\gamma = \alpha\beta$ would have to obey $N(\alpha)N(\beta) = 6$. Thus the two norms are 2,3. But it will be clear that $a^2 + 5b^2 = 2$ has no solution for $a, b \in \mathbb{Z}$.
Exercise: show γ is not prime.

(**2.4.11**) Theorem. In $\mathbb{Z}[\sqrt{-2}]$ every irreducible element is prime.

Before we prove this, we will need to parallel some more of the machinery we have for $\mathbb{Z}$ in this more general setting.

(**2.4.12**) A *GCD* of $a, b \in R$ is a common divisor $c \in R$ such that if d is another common divisor then $d|c$.

(**2.4.13**) Remark. It is not clear that GCDs exist in R in general, and indeed they may not.
But if a pair a, b have *two* GCDs then note that they are associates.

(**2.4.14**) Theorem. Suppose $R = \mathbb{Z}[\sqrt{-2}]$. Then any pair $a, b \in R$ has a GCD. If γ is this GCD then it can be written in the form $\gamma = ax + by$ for some $x, y \in R$.

Proof. This is an analogue of the situation for $\mathbb{Z}$. There is an algorithm for computing the unknowns starting from a, b in either case, called *Euclid's algorithm*. In the $\mathbb{Z}$-case this starts from the familiar observation that $a = qb + r$ has a solution with $0 \leq r < |b|$, where q is called the quotient, and r the remainder. If course this just says that for every b there is an element r of the class of a in $\mathbb{Z}_{|b|}$ in the interval $[0, |b|)$.

Here, with $n = -2$, we express $b = l + m\sqrt{n}$ and define $b_- = l - m\sqrt{n}$ and $M = bb_- = l^2 - (n)m^2$. Thus

$$\frac{a}{b} = \frac{ab_-}{bb_-} = \frac{ab_-}{M}$$

Write $ab_- = t + s\sqrt{n}$, so that

$$\frac{a}{b} = \frac{t}{M} + \frac{s}{M}\sqrt{n}$$

Now let X, Y be the integers closest to the two ratios on the right, that is $|\frac{t}{M} - X| \leq 1/2$ and similarly for Y. Next set

$$q = X + Y\sqrt{n}$$

and $r = a - qb$. We have

$$rb_- = ab_- - qbb_- = ab_- - qM = (t + s\sqrt{n}) - (X + Y\sqrt{n})M = (t - MX) + (s - MY)\sqrt{n}$$

so

$$N(rb_-) = (t - MX)^2 - (n)(s - MY)^2$$

so

$$N(r) = \frac{N(rb_-)}{N(b_-)} = \frac{N(rb_-)}{M} = M((\frac{t}{M} - X)^2 - (n)(\frac{s}{M} - Y)^2)$$

$$\leq M((1/2)^2 - n(1/2)^2) \leq \frac{3}{4}M = \frac{3}{4}N(b) < N(b)$$

(Note well how this parallels the $\mathbb{Z}$-case.)
(Note that this argument works also for $n = -1, 2, 3$, but not for $n = -3$.)

Using this idea we run an algorithm, first defining q_1, r_1 by:

$$a = q_1 b + r_1$$

then q_2, r_2 by

$$b = q_2 r_1 + r_2$$

then q_i, r_i by

$$r_1 = q_3 r_2 + r_3$$

and so on. Note that $N(r_1) > N(r_2) > ....$ Thus eventually some $N(r_k) = 0$. Let γ be the last nonzero remainder $\gamma = r_{k-1}$. Evidently $\gamma | r_{k-2}$, so $\gamma | r_{k-3}$ and so on, so $\gamma | b$, so $\gamma | a$. Now if δ is another common divisor then it divides all the remainders, so it divides γ. □

(**2.4.15**) THEOREM. In $\mathbb{Z}[\sqrt{-2}]$, if $d|ab$ and the GCD of d and a is a unit, then $d|b$.

Proof. By (2.4.14) we can write a unit $u = dx + ay$. Thus $b = buu^{-1} = dbxu^{-1} + abyu^{-1}$. Evidently d divides the RHS, so it divides b. □

(**2.4.16**) Proof of (2.4.11): Say d is irreducible and $d|ab$ in $\mathbb{Z}[\sqrt{-2}]$. (We require to show, then, that $d|a$ or $d|b$.) Now let x be a GCD of d, a (recall that such a thing exists, by the Euclid algorithm argument). Indeed set $d = xe$. By irreducibility of d, either x or e is a unit. If x is a unit then $d|b$ by (2.4.15). If e is a unit then $d|x$, and since $x|a$ we have $d|a$. □

UFDs

(**2.4.17**) A ring R is a *unique factorisation domain* (UFD) if it is an integral domain and
(i) every nonzero nonunit can be written as a product of irreducibles

$$x = p_1 p_2 ... p_k$$

and (ii) if $x = q_1 q_2 ... q_l$ is another such factorisation then $k = l$ and there is an ordering so that p_i, q_i are associates for all i.

(**2.4.18**) EXAMPLE. $\mathbb{Z}$ is a UFD: we can write $-45 = (-3).3.5 = 3.3.(-5) = (-5).(-3).(-3)$, and -1 is a unit.

(**2.4.19**) THEOREM. $\mathbb{Z}[\sqrt{-2}]$ is a UFD.

Proof. The idea of this proof is to use the norm function to upgrade the proof of the Fundamental Theorem of Arithmetic for use in this case.

To show factorisation, suppose for a contradiction that there is a nonzero, nonunit element α that cannot be written as a product of irreducibles. Then there is, in particular, such an element with smallest norm $N(\alpha)$ (among all such elements). Obviously α is not irreducible, so $\alpha = \beta\gamma$ with β, γ also nonunits. Thus $N(\alpha) = N(\beta)N(\gamma)$ with $N(\beta), N(\gamma) > 1$. Thus $1 < N(\beta) < N(\alpha)$ and $1 < N(\gamma) < N(\alpha)$. But then by assumption we can write β, γ as products of irreducibles. Thus we can do this for α too — a contradiction.

The proof of uniqueness is analogous to the case for $\mathbb{Z}$, using Theorem (2.4.11) to allow us to treat irreducibles as primes. □

(**2.4.20**) REMARK. The same argument shows that $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\sqrt{3}]$ are UFDs. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD since $2.3 = (1+\sqrt{-5}).(1-\sqrt{-5})$ are alternative factorisations of 6.

(**2.4.21**) EXAMPLE. Let us write $30 \in \mathbb{Z}[i]$ as a product of irreducibles. We have $30 = 2.3.5$ for starters, but also $2 = (1+i)(1-i)$, so we can go further...
How can we be systematic about this?
If an integer can be written as a norm in $\mathbb{Z}$ (i.e. in the form $n = a^2+b^2$), then $n = (a+ib)(a-ib)$. The factorisation of 2 above comes from $2 = 1^1+1^2$; and we also have $5 = 2^2+1^2 = (2+i)(2-i)$. Thus

$$30 = (1+i)(1-i).3.(2+i)(2-i)$$

Can we go further? (No.)

(**2.4.22**) EXERCISE. What happens if we form the quotient $\mathbb{Z}[\sqrt{n}]/r\mathbb{Z}[\sqrt{n}]$ for r a unit; r an irreducible; or r a prime?

2.5 Polynomials

See for example Kelarev[2] [**?**, §3.4], or Anderson–Fuller[3] [**?**, §1 Exercise 16], for a more general setting for the following.

(**2.5.1**) Let R be a ring. A *polynomial* in indeterminate x, with coefficients in R, is a formal expression of the form

$$f(x) \;=\; a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \;=\; \sum_{i=0}^{n} a_ix^i$$

(any $n \in \mathbb{N}$) with $a_i \in R$. We say $f(x) = g(x)$ if the 'coefficients' a_i agree for all i. We write $R[x]$ for the set of all such polynomials.

(**2.5.2**) REMARK. Note that this is somewhat like $\mathbb{Z}[\sqrt{d}]$, except that we do not know d, so we cannot eliminate x^2 from expressions.

(**2.5.3**) We assume that you are familiar with real polynomial arithmetic. We define sum and product on polynomials in the usual way (treating the symbol + above as the usual + for polynomials), making use of the operations in R in place of real arithmetic. For example

$$(a_0 + a_1x) \times (b_0 + b_1x) \;=\; a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2$$

One sees that $(R[x], +, 0)$ is an abelian group; and that $(R[x], \times, 1)$ is a monoid. The operations 'distribute' appropriately, and so $R[x]$ is a ring.

(**2.5.4**) Define $R[x,y] = (R[x])[y]$ and so on.

(**2.5.5**) LEMMA. If R is a field then $R[x]$ is an integral domain. The units are the nonzero constant polynomials. Every nonzero polynomial is associated to a unique monic polynomial (a polynomial with leading coefficient $a_n = 1$).

[2] Ring constructions and applications. By Andrei V. Kelarev.
[3] Rings and categories of modules. By F W Anderson and K R Fuller.

Proof. Note that $R[x]$ is a commutative ring, and that it is not the zero ring, and that the constant polynomial 1 is the identity of multiplication. Suppose $f(x) = \sum_{i=1}^{n} a_i x^i$ and $g(x) = \sum_{i=1}^{m} b_i x^i$, of maximal degree. We have

$$fg = a_n b_m x^{n+m} + ...$$

Since R is an integral domain $a_n b_m \neq 0$. Thus $fg \neq 0$.

We leave the checking of units and associates as an exercise. □

(**2.5.6**) THEOREM. Let R be a field and $f, g \in R[x]^*$. Then there are $q, r \in R[x]$ such that $f = qg + r$ with either $r = 0$ or degree r less than degree g.

Proof. Use polynomial division.

(**2.5.7**) THEOREM. If R is a field then any pair $f, g \in R[x]$ have a GCD $h \in R[x]$; and we can write $h = fu + gv$ for some $u, v \in R[x]$.

Proof. A direct analogy of the Euclid algorithm from before. Note that it terminates this time because the *degree* is decreasing. □

The following are proved essentially as for the $\mathbb{Z}[\sqrt{-2}]$ case.

(**2.5.8**) THEOREM. Suppose R is a field and consider $R[x]$. If the GCD of $f(x), g(x)$ is a constant polynomial, and $f(x)|g(x)h(x)$ then $f(x)|h(x)$.

(**2.5.9**) THEOREM. If R is a field then every irreducible polynomial in $R[x]$ is prime.

(**2.5.10**) THEOREM. If R is a field then $R[x]$ is a UFD.

2.6 Polynomials over $\mathbb{Z}$

Now what about $R[x]$ when R is *not* a field?

(**2.6.1**) LEMMA. $\mathbb{Z}[x]$ is an integral domain. The units are ± 1.

Proof. $\mathbb{Z}$ is not a field, but in fact the same argument works here as in the case $R[x]$ for R a field.

(**2.6.2**) If $f = \sum_i a_i x^i \in \mathbb{Z}[x]$ the *content* of f (denoted c_f) is the GCD of the coefficients. Polynomial f is *primitive* if its content is 1.

(**2.6.3**) EXAMPLE. Let $f = 4x - 6$ and $g = 10x^2 + 15$. We have $c_f = 2$ and $c_g = 5$.

(**2.6.4**) REMARK. If $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ is irreducible then it is primitive, since any non-constant f can be expressed in the form $c_f f'$ where f' is non-constant primitive.

(**2.6.5**) THEOREM. (Gauss's Lemma) If $f, g \in \mathbb{Z}[x]$ are primitive then so is fg.

Proof. Hint: One can set this up as a proof by contradiction.

(**2.6.6**) Corollary: For any $f, g \in \mathbb{Z}[x]$ the content of fg is $c_f c_g$.

(**2.6.7**) EXAMPLE. From our example (2.6.3) above we have $c_{fg} = 10$. (Check this by brute force!)

(**2.6.8**) REMARK. Note that each prime number p is an irreducible element in $\mathbb{Z}[x]$; but no such p is irreducible in $\mathbb{Q}[x]$. OTOH, an element of the form $x + a$ ($a \in \mathbb{Z}$) is also irreducible in $\mathbb{Z}[x]$. (How about in $\mathbb{Q}[x]$?) What other irreducibles are there in $\mathbb{Z}[x]$? Is $x^2 + 1$ irreducible? Is $x^2 - 1$? Is $x^2 - 2$?

(**2.6.9**) THEOREM. If $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ is irreducible in $\mathbb{Z}[x]$ then it is also irreducible in $\mathbb{Q}[x]$.

Proof. Hint: Aim for a contradiction.

(**2.6.10**) THEOREM. (A) The irreducible elements of $\mathbb{Z}[x]$ are the numbers $\pm p$ with p a prime number; and the primitive polynomials that are irreducible in $\mathbb{Q}[x]$.
(B) Every irreducible element in $\mathbb{Z}[x]$ is prime.
(C) $\mathbb{Z}[x]$ is a UFD.

Proof. Non-examinable.

2.7 Irreducible polynomials

(**2.7.1**) THEOREM. (Factor theorem) Suppose R a field. If $f \in R[x]$ and $a \in R$ then $(x-a)$ is a factor of f iff $f(a) = 0$.

Proof. The (only if) part is trivial. The (if) part uses polynomial division. □

(**2.7.2**) Corollary: If R is a field then $f \in R[x]$ of degree n has at most n roots in R.

(**2.7.3**) THEOREM. (Fundamental theorem of algebra) Every $f \in \mathbb{C}[x]$ of degree > 0 has a root in $\mathbb{C}$.

Proof. Interestingly, this one is easier to prove using Analysis. □

(**2.7.4**) Corollary: The irreducible polynomials in $\mathbb{C}[x]$ are the linear polynomials $ax+b$ (note that $ax+b$ and $x+\frac{b}{a}$ are associates).
The irreducible polynomials in $\mathbb{R}[x]$ are the linear polynomials $ax+b$ and the quadratics ax^2+bx+c without real roots.

(**2.7.5**) LEMMA. If R is a field and $f \in R[x]$ has degree 2 or 3 and has no root in R, then it is irreducible.

Proof. If $f = gh$ one of g, h must have degree 1, giving a root in R. □

(**2.7.6**) EXAMPLE. Let $f \in \mathbb{Z}_3[x]$ be $f = x^3 + x^2 + 2'$. For $x = 0', 1', 2'$ we have $f(x) = 2', 1', 2'$ respectively. Thus f is irreducible.

(**2.7.7**) THEOREM. (The rational root test) If $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and r/s is a rational root (with r, s coprime integers), then $r|a_0$ and $s|a_n$.

Proof. Hint: Consider $s^n f(r/s) = 0$.

(**2.7.8**) EXAMPLE. Any rational root of $f = x^3 + x + 9$ must be of form r/s with $r|9$ and $s|1$. That is, $r = \pm 1, \pm 3, \pm 9$ and $s = \pm 1$. Trying all six cases one quickly finds that none gives a root. Since the degree is 3, we deduce that f is irreducible in $\mathbb{Q}[x]$.

(**2.7.9**) THEOREM. (Eisenstein's criterion) Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Assume that there is a prime number p such that
(i) $p \not| a_n$
(ii) $p|a_i$ $(i \neq n)$
(iii) $p^2 \not| a_0$.
Then f is irreducible in $\mathbb{Q}[x]$.

Proof. By (2.6.9) it is enough to show f irreducible in $\mathbb{Z}[x]$. Suppose (aiming for a contradiction) that $f = gh$ with $g = \sum_i b_i x^i$ of degree $s > 0$ and $h = \sum_i c_i x^i$ with degree $t > 0$. Thus $n = s + t$, and $a_i = \sum_{j=0}^{i} b_j c_{i-j}$. Now $p|a_0$ so $p|(b_0 c_0)$, so $p|b_0$ or $p|c_0$ (but not both, since $p^2 \not| a_0$) — say $p|b_0$.

Now $p|a_1$ so $p|(b_0 c_1 + b_1 c_0)$ so $p|b_1 c_0$; and $p \not| c_0$ so $p|b_1$. Similarly $p|b_i$ for all i. But then $p|a_n$, giving a contradiction. □

(**2.7.10**) EXAMPLE. Taking $p = 3$ we see that $7x^4 - 36x^3 - 6x^2 + 18x - 12$ is irreducible.

(**2.7.11**) EXERCISE. Is $f = x^{10} + x^9 + x^8 + ... + x + 1$ irreducible?
Obviously we cannot apply Eisenstein directly here (why not?). But note that $f = f(x)$ is irreducible if $f(x + 1)$ is irreducible... (Now consider $p = 11$.)

2.8 Fields of fractions

A commutative ring that is not a field fails to be a field by lacking inverses. Recently we have been thinking about extending rings and fields by adding elements to them from rings which contain them. Could we extend a ring to a field by 'adding inverses'? What if we do not have to hand a larger ring from which to get these inverses?...

(**2.8.1**) Let R be an integral domain and consider the set $R \times (R \setminus \{0\})$. Define an *additive* binary operation on this set by $(r, s) + (t, u) = (ru + ts, su)$. This is closed and commutative. Is it associative? Is there an identity element? An identity element would be an element (e_n, e_d) such that $(e_n, e_d) + (t, u) = (e_n u + te_d, e_d u) = (t, u)$ for all t, u. Such an element is $(0, 1)$.
Define a *multiplicative* binary operation on this set by $(r, s)(t, u) = (rt, su)$. This is closed and commutative. Is it associative? Is there an identity element? An identity element would be an element (i_n, i_d) such that $(i_n, i_d)(t, u) = (i_n t, i_d u) = (t, u)$ for all t, u. Such an element is $(1, 1)$.

(**2.8.2**) The *field of fractions* of an integral domain R is the quotient of $R \times (R \setminus \{0\})$ by $(r, s) \sim (t, u)$ if $ru = st$. Addition is represented by $(r, s) + (t, u) = (ru + ts, su)$ and multiplication by $(r, s)(t, u) = (rt, su)$.
One needs to check that these are well-defined on classes.

Example: The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

(**2.8.3**) EXERCISE. We have seen that $\mathbb{R}[x]$ is an integral domain. What is the field of fractions of $\mathbb{R}[x]$?

(**2.8.4**) EXERCISE. A field is an integral domain. What is the field of fractions of a field?

2.9 Extension Fields

(**2.9.1**) To say a field F *extends* a field R is just to say that R is a subfield of F (i.e. it is a subring that is a field).

(**2.9.2**) EXAMPLE. $\mathbb{R}$ is an extension field of $\mathbb{Q}$.

(**2.9.3**) Let F be an extension field of a field R, and $a_1, a_2, ..., a_n \in F$. Define $R(a_1, a_2, ..., a_n)$ to be the set of all elements of F obtained from elements of R and $a_1, a_2, ..., a_n$ by repeatedly applying the field operations: addition, multiplication, negation and multiplicative inverse.

This is a subfield of F (possibly all of it). It is called the subfield of F *generated* by R and $a_1, a_2, ..., a_n$.

(**2.9.4**) We assume familiarity with real and complex vector spaces, bases and so on. (But please *do* ask for a refresher if you like.) We note that these ideas all extend to vector spaces over a field.

(**2.9.5**) EXERCISE. Define the term *basis* of a vector space. How would this work over an arbitrary field (e.g. $\mathbb{Z}_2$)? What would go wrong if we tried to make it work over an arbitrary commutative ring?

(**2.9.6**) The *degree* of a field extension $F \supseteq R$, denoted $[F : R]$, is the dimension of F as a vector space over R.

(**2.9.7**) EXAMPLE. $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ is a basis for $\mathbb{C}$ regarded as a real vector space. For d non-square we have $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ since $\{1, \sqrt{d}\}$ is a basis.
It can be shown that $[\mathbb{R} : \mathbb{Q}] = \infty$, that is, $\mathbb{R}$ can be regarded as a vector space over $\mathbb{Q}$, but there is no finite basis.

(**2.9.8**) THEOREM. (Tower Law) Let $L \supset F \supset R$ be field extensions. Then

$$[L : R] = [L : F].[F : R]$$

Proof. The idea is to show that if $\{v_1, ..., v_n\}$ is a basis for F over R and $\{w_1, ..., w_m\}$ is a basis for L over F then $\{v_i w_j\}_{i,j}$ is a basis for L over R. □

(**2.9.9**) EXAMPLE. Consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, i)$. One can check that $\{1, \sqrt{2}, i, i\sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$.

2.9.1 Extending a field by algebraic elements

(**2.9.10**) Let $F \supset R$ be a field extension. Element $a \in F$ is *algebraic* over R if there is a non-zero polynomial $f \in R[x]$ with $f(a) = 0$ in F.
Otherwise a is *transcendental* over R.

(**2.9.11**) EXAMPLE. (I) $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, since it is a root of $f = x^2 - 2 \in \mathbb{Q}[x]$.
(II) $\sqrt[5]{2}$ is algebraic over $\mathbb{Q}$, since it is a root of $f = x^5 - 2 \in \mathbb{Q}[x]$.
(III) $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, since it is a root of $f = x^2 + 1 \in \mathbb{Q}[x]$.
(IV) $a = \sqrt{\sqrt{7} - 1}$ is algebraic over $\mathbb{Q}$, since it is a root of $f = x^4 + 2x^2 - 6 \in \mathbb{Q}[x]$.
(V) $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (Lindemann, 1882). How might you prove this?

(**2.9.12**) EXERCISE. What can we say about algebraic extensions of the field $\mathbb{Z}_2$?

(**2.9.13**) If a is algebraic over R then the *minimal polynomial* of a over R is the unique monic polynomial $f \in R[x]$ of least degree with $f(a) = 0$.

(**2.9.14**) EXAMPLE. Element $\sqrt{2}$ is a root of $x^4 - 4$ and $2x^3 - 4x$, but its minimal polynomial is $x^2 - 2$.

(**2.9.15**) REMARK. Note that the minimal polynomial exists since by the algebraic assumption there *is* a polynomial $g \in R[x]$ with $g(a) = 0$. But if the leading coefficient is g_n then $(1/g_n)g$ is monic with the same root. Among such polynomials will be at least one with least degree. If it is

not unique then there are two of this degree, but then $g - g'$ also has root a and lower degree — leading to a contradiction.

(**2.9.16**) LEMMA. Suppose $F \supset R$ is a field extension, and $a \in F$ algebraic over R with minimal polynomial f. Then (i) f is irreducible in $R[x]$; (ii) If $g \in R[x]$ and $g(a) = 0$ then $f|g$.

Proof. (i) If f factorises as gg' then one of $g(a), g'(a)$ must be zero. Rescaling leads to a polynomial of smaller degree — a contradiction.
(ii) Division gives $g = qf + r$. Then $r(a) = 0$, so in fact $r(x) = 0$ (else it contradicts the minimality of f. □

(**2.9.17**) THEOREM. Suppose $F \supset R$ is a field extension, and $a \in F$ algebraic over R with minimal polynomial f. Then f is the unique monic irreducible polynomial in $R[x]$ with $f(a) = 0$. (I.e. irrespective of degree.)

Proof. Suppose g has these properties. Then $f|g$, so $g = fh$ for some h. But then h is constant by irreducibility, and this constant is 1 since f and g are both monic. □

(**2.9.18**) EXAMPLE. $\sqrt[n]{2}$ is algebraic over $\mathbb{Q}$ since a root of $x^n - 2$. This polynomial is monic irreducible in $\mathbb{Q}[x]$ (by Eisenstein with $p = 2$, for example), so it is the corresponding minimal polynomial.

(**2.9.19**) PROPOSITION. *Suppose $F \supset R$ is a finite field extension. Then every element of F is algebraic over R.*

Proof. Let $a \in F$. Then all powers of a are in F. But these can't all be linearly independent over R. □

(**2.9.20**) THEOREM. Suppose $F \supset R$ is a field extension, and $a \in F$ algebraic over R with minimal polynomial f_a of degree n. Then $R(a)$ has basis $\{1, a, ..., a^{n-1}\}$ as a vector space over R.
In particular $[R(a) : R] = n$, so $R(a)$ is a finite extension field of R.

(**2.9.21**) EXAMPLE. $a = \sqrt[3]{2}$ has $f_a = x^3 - 2$ over $\mathbb{Q}$. Thus $\mathbb{Q}(a)$ has basis $1, a, a^2$ over $\mathbb{Q}$. Thus $\mathbb{Q}(a) = \{\alpha + \beta a + \gamma a^2 \ : \ \alpha, \beta, \gamma \in \mathbb{Q}\}$ and $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.

Proof. Let $f_a = x^n + a_{n-1}x^{n-1} + ... + a_0x^0$. The powers $1, a, a^2, ..., a^{n-1}$ are linearly independent over R by the minimal condition. Let E be the R-subspace of F spanned by these. We will next show by induction that $a^{n+k} \in E$ for all $k \geq 0$.

We have $f_a(a) = a^n + a_{n-1}a^{n-1} + ... + a_0a^0 = 0$, so the base case $k = 0$ is true. Now suppose true up to level $k - 1$ (the inductive assumption). Multiplying by a^k we have

$$a^{n+k} \ = \ -a_{n-1}a^{n+k-1} - a_{n-2}a^{n+k-2} - ... - a_0a^k$$

But everything on the right is in E by assumption, and hence so is a^{n+k}.
Thus E contains all positive integral powers of a.

It follows from this that E is closed under products, so it is a subring of F. Next we show that it is a subfield. Suppose $b \in E^*$. Then let $b = b_0a^0 + ... + b_{n-1}a^{n-1}$ be an expansion in the spanning set. Thus $b = g(a)$ where $g = b_0x^0 + ... + b_{n-1}x^{n-1}$. Since $g(a) \neq 0$ we know that $f_a \not| g$. As f_a is irreducible, it and g have a GCD which is a unit. Thus there are polynomials u, v such that $f_au + gv = 1$. Thus $g(a)v(a) = 1$. Thus $b^{-1} = v(a) \in E$.

Finally we show that $E = R(a)$. The inclusion $E \subseteq R(a)$ follows from the definition, and the reverse inclusion holds since E is a field which contains R and a. □

Throughout this section we have had the assumption that $F \supset R$ is a field extension, and we have considered the nature of elements of F in relation to R. This contrasts with our earlier construction of fields of fractions, where we wanted to extend a (certain kind of) ring *without* having a pre-existing structure to extend it into.

If our subfield is a subfield of the complex numbers then of course every polynomial over the subfield has a root over $\mathbb{C}$, so extending the subfield by a root of a polynomial is the same as extending by a concrete complex number. In general though, we could start with a field and a polynomial f over that field, and it is not a 'given' that there is an extension field containing a root of f.
Except that...

(**2.9.22**) THEOREM. (Kronecker's Theorem) A polynomial f in a field F has a root in an extension field.

Proof. We may assume that $f = f(x)$ does not have a linear factor in $F[x]$ since otherwise that factor would give the root. Let $g(x)$ denote a factor of $f(x)$ which is irreducible. Let $E = F[x]/gF[x]$. Since g is irreducible this ring is a field containing F, and hence an extension field of F. The representative $x \in F[x]$ of the element $x' \in E$ satisfies $f(x) = h(x)g(x) \equiv 0 \pmod{g(x)}$, as it were), so $f(x') = h(x')\, g(x') = 0'$. □

(If the learning curve is a bit steep here, first recall that the basic model for something like $F[x]/gF[x]$ is $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (p prime); and then have a look at some of the exercises and hints in section 2.11, such as Theorem (2.11.2).)

(**2.9.23**) EXERCISE. (Optional) Show that the smallest extension field of $\mathbb{Z}_2$ in which $p_1(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ has a zero is isomorphic to the smallest extension field of $\mathbb{Z}_2$ in which $p_2(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ has a zero.

2.9.2 Remarks on Kronecker

(**2.9.24**) Recall the fundamental theorem of algebra. From this we see that, while there are lots of non-algebraically closed fields, the fields $\mathbb{Q}$ and so on contained in $\mathbb{C}$ can be extended to an algebraically closed field.

We now see that the Kronecker Theorem says something similar (but more general). If we start with an arbitrary field F and form polynomials, then either F is algebraically closed or eventually we will find a polynomial without a root in F. But then we can form an extension field of F, via this polynomial, which does contain a root of F. Iterating this process to 'closure' (i.e. exhaustively) we will extend F to an algebraically closed field.

On the other hand note (cf. e.g. Fulton [**?**]):

(**2.9.25**) Let F be any field. Let $f_1, f_2, ..., f_n$ be a set of irreducible monic polynomials in $F[x]$. Then $f_1 f_2, ...f_n + 1$ is not divisible by any of these. Thus there are infinitely many distinct irreducible monic polynomials.

(**2.9.26**) It follows that the algebraic closure of any field F is infinite.

2.9.3 Geometric constructions

(**2.9.27**) We say a real number a is *constructible* if starting with two marked points in the plane at distance 1 apart, we can construct two marked points with distance $|a|$ between them, using only the following operations:
(i) draw line through any pair of marked points;
(ii) add the distance between these to our set of constructed constructible distances;
(iii) draw a circle of constructed radius centred at a marked point (e.g. the circle defined by that point and another marked point);
(iv) mark any point of intersection of lines and circles.

(**2.9.28**) Example. Any number in $\mathbb{Q}$ is constructible. $\sqrt{2}$ is constructible.

(**2.9.29**) Exercise. (Optional) What other kinds of real numbers are constructible?

(**2.9.30**) Lemma. The set S_c of constructible numbers is a subfield of $\mathbb{R}$. If $a \in S_c$ then so is $\sqrt{|a|}$.

Proof. Optional exercise. (The key point is that we have embedded the real line in the real plane.)

(**2.9.31**) Theorem. (Wantzel 1837) If a constructible, then it is algebraic over $\mathbb{Q}$ and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2.

Proof. Optional exercise.

2.10 Ideals

Let R be a ring. We can partially order the ideals of R by inclusion. Obviously R itself is the top of this order, but if we restrict the order to the *proper* ideals then there could be many maximal elements in the order.

For example, $36\mathbb{Z} \subset 18\mathbb{Z} \subset 6\mathbb{Z} \subset 3\mathbb{Z}$, but we can't go any further without hitting $\mathbb{Z}$, so $3\mathbb{Z}$ is a maximal element among the proper ideals of $\mathbb{Z}$. Indeed $p\mathbb{Z}$ is a maximal element iff p prime.

(**2.10.1**) In general we call the maximal elements of this order the maximal ideals of a ring.

(**2.10.2**) A proper ideal P in a commutative ring R is a *prime ideal* if whenever $ab \in P$ then either $a \in P$ or $b \in P$.
(We will give a definition for *prime ideal in an arbitrary ring* in (2.10.21).)

(**2.10.3**) Example. The maximal ideals of $\mathbb{Z}$ are also prime. (We will see later that maximal ideal implies prime ideal in any commutative ring R.)

Ideal 'arithmetic', towards Principal ideal domains

(**2.10.4**) Exercise. Show that the intersection of two subgroups of a group is a group.

Answer: Let $H, H' \subseteq G$ be groups. If $g, f \in H \cap H'$ then $g, f \in H, H'$ so $gf \in H, H'$, so $gf \in H \cap H'$. Thus multiplication closes in $H \cap H'$. Evidently the identity element e of G lies in H and H' and hence in $H \cap H'$. Finally if $g \in H, H'$ then $g^{-1} \in H, H'$ so $H \cap H'$ also has inverses. □

(**2.10.5**) Let R be an abelian group and S a subset. Let us write $\langle S \rangle = \langle S \rangle_R$ for the intersection of all subgroups of R containing S. This is called the *abelian group generated by* S in R.

(**2.10.6**) The group $\langle S\rangle$ is the set of finite sums of elements of S and their additive inverses.
Example: $\langle 3\rangle_{\mathbb{Z}} = 3\mathbb{Z} = \langle 3, -6\rangle_{\mathbb{Z}}$.

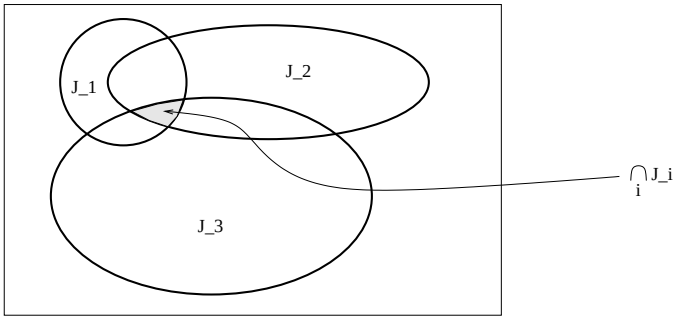
(**2.10.7**) Recall that an ideal in a ring R is a subgroup J such that $rar' \in J$ for all $r, r' \in R$ and $a \in J$.

(**2.10.8**) Note that if J is an ideal of R then $J = \langle J\rangle_R$.

(**2.10.9**) Lemma. The intersection of two R-ideals is an R-ideal.

Proof. If A, B ideals and $x \in A, B$ then $rx \in A, B$ (and so on). Closure under addition is also clear. □

(**2.10.10**) Note that if $\{J_i\}_{i\in T}$ is a set of R-ideals then $\cap_i J_i$ is an R-ideal.



(**2.10.11**) Example. Let $S \subseteq R$ a subset, and let $\{J_i\}_{i\in T(S)}$ be the subset of ideals of R such that $J_i \supseteq S$. Then

$$(S) := \cap_i J_i$$

is an ideal.

(**2.10.12**) This (S) is the smallest R-ideal containing S. It is called the *ideal generated by* S.

(**2.10.13**) Let $S = \{s_1, s_2, ..., s_n\} \subset R$. Elements of $(S) = (s_1, s_2, ..., s_n)$ take the following form. Firstly we have all constructs of form rs_ir'. Then we have all finite sums of such constructs:

$$(s_1, s_2, ..., s_n) = \{\sum_i \sum_{j_i} r_{ij_i} s_i r'_{ij_i} \mid r_{ij_i}, r'_{ij_i} \in R;\ s_i \in S\}$$

That is, $(S) = \langle \{rar' \mid r, r' \in R;\ a \in S\}\rangle_R$.

(**2.10.14**) Let R be a ring. For A, B subsets of R we define another subset of R by

$$AB\ := \{a_1b_1 + a_2b_2 + ... + a_nb_n \mid n \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$$

(where the empty sum is zero). Note that this is the finite additive closure of the set of elements of the form ab with $a \in A$ and $b \in B$.

(**2.10.15**) Note that if A, B are ideals then so is AB. (See e.g. Jacobson I §2.5.)

(**2.10.16**) Suppose A, B are R-ideals. What is $(AB)A$?

(**2.10.17**) Exercise. Whats is $A(BA)$? How are they related?
(Answer: $(AB)C = A(BC)$ — see e.g. Jacobson I §2.5.)

(**2.10.18**) Let R be a ring and S a subset of R. The subset of R *generated* by S is the set RSR.

(**2.10.19**) Let R be a ring. For A, B subsets of R we define another subset of R by

$$A + B := \{a + b \mid a \in A,\ b \in B\}$$

If A, B are R-ideals then so is $A + B$. (See also, e.g., Zariski–Samuel [**?**, §III.7].)

(**2.10.20**) Exercise. What are $A \cap B$, $A + B$ and AB in each of the following cases?:
(i) $A = 2\mathbb{Z}$ and $B = 3\mathbb{Z}$;
(ii) $A = 2\mathbb{Z}[x]$ and $B = x\mathbb{Z}[x]$;
(iii) $A = 2\mathbb{Z}[x]$ and $B = 2x\mathbb{Z}[x]$.

(**2.10.21**) A proper ideal P in an arbitrary ring R is a *prime ideal* if, for ideals A, B, whenever $AB \subseteq P$ then either $A \subseteq P$ or $B \subseteq P$.
(Note that this definition contains the commutative case.)

Principal ideal domains

(**2.10.22**) An ideal in a commutative ring R is *principal* if it can be expressed in the form dR for some $d \in R$.

(**2.10.23**) We have repeatedly used the construction dR for ideals in commutative rings. For example $3\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

(**2.10.24**) Lemma. Every ideal in $\mathbb{Z}$ is principal.

Proof. Let I be an ideal in $\mathbb{Z}$ and d the smallest positive element. Suppose for a contradiction that $I \setminus d\mathbb{Z} \neq \emptyset$, and let d' be the smallest positive element. Then $d' - ld \in [1, d-1]$ for some l. But $d' - ld \in I$, contradicting that d is smallest. □

(**2.10.25**) A *principal ideal domain* (PID) is an integral domain such that every ideal is principal.

(**2.10.26**) Exercise. Show that every ideal in $\mathbb{Z}[\sqrt{2}]$ is principal.

(**2.10.27**) Exercise. Show that we can choose a d so that $\mathbb{Z}[\sqrt{d}]$ is not principal.

(**2.10.28**) Exercise. Show that the ideal of $\mathbb{Z}[x]$ generated by 2 and x (i.e. the smallest ideal containing these two elements) is not principal.

(**2.10.29**) Lemma. If r is an irreducible element in a PID R then rR is a maximal ideal.

Proof. Else $rR \subset aR \subset R$ for some a, so $r = ab$ for some nonunit b, a contradiction. □

(**2.10.30**) Lemma. A maximal ideal M in a PID R has the property that $ab \in M$ implies a or $b \in M$.

Proof. For, suppose $ab \in M$ but $a, b \notin M$. Then $M + aR = \{m + ar \mid m \in M,\ r \in R\}$ and $M + bR$ are both ideals properly containing M. Since M is maximal this says that $M + aR = R = M + bR$. We have $aRbR \subseteq abR \subseteq M$, so $R = R^2 = (M + aR)(M + bR) \subseteq M^2 + aRM + MbR + aRbR \subseteq M$ — a contradiction. □

(**2.10.31**) LEMMA. A PID is a UFD.

Proof. First we show that any element x of a PID R can be factorised into a list of irreducible factors. Clearly if x cannot be factorised then it is irreducible, so the only obstruction is if in fact it can be factorised but this process does not terminate! We rule this out as follows:

Suppose R is an integral domain, and $(x =)r_1, r_2, r_3, ...$ is a sequence of elements such that $r_i | r_{i-1}$.
(The example one might have in mind here is something like 100, 50, 10, 5, 2, 1.)
It follows that $r_i R \supseteq r_{i-1} R$. Let I be the union of all these ideals.
(This union might be over infinitely many ideals, but every element of I is an element of some $r_i R$. Just as $\mathbb{Z}$ is infinite, but every element is a finite number.)
If R is a PID then there is an r such that $rR = I$. Thus there is some i with $r \in r_i R$. At this point $I = rR = r_i R$ (we have just shown that $rR \subseteq r_i R$, and $rR \supseteq r_i R$ by construction), and $r_j R = rR$ for all $j \geq i$ (so that all subsequent r_js are associates).
In particular, it is not possible to have an *infinite* sequence of r_is as above that are all non-associate.
(In our example this just says that every such positive integer sequence must terminate.)
But an infinite irreducible factorisation $x = p_1 p_2 ...$ would give rise to an infinite sequence $r_1 = x = p_1 p_2 ...$, $r_2 = p_2 p_3 ...$, with $r_i | r_{i-1}$. Thus there can be no such factorisation.

Now we set out to show uniqueness. We will need to note a couple of facts.

(**2.10.32**) LEMMA. In a PID, irreducible implies prime.

Proof. First note that r irreducible implies rR maximal, by Lemma 2.10.29. But any maximal ideal M has the property that $ab \in M$ implies a or $b \in M$, by Lemma 2.10.30.

Since rR is maximal it has this 'prime ideal' property. [4] That is, whenever $r|ab$, then $r|a$ or $r|b$. Thus r is prime.

□

(**2.10.33**) (Now back to complete the proof of (2.10.31))
Suppose $p_1 p_2 ... p_r = q_1 q_2 ... q_s$ are two irreducible (hence prime) factorisations of $x \in R$. By primeness p_1 must divide some q_i. Hence $p_1 = u q_i$ for some unit u (by irreducibility). Reorder so that $q_1 = q_i$. We then have $u q_1 p_2 ... p_r = q_1 q_2 ... q_s$ so $u p_2 ... p_r = q_2 ... q_s$. Up to the unit, this is analogous to the initial equality except with one fewer irreducible on each side, so we can iterate, pairing each p_i with a q_i up to a unit. This establishes uniqueness. □

(**2.10.34**) EXAMPLE. Since $\mathbb{Z}$ is a PID, it is a UFD. (But of course we already knew this.)

(**2.10.35**) EXERCISE. Can you think of a UFD that is not a PID?
(Hint: Think about $\mathbb{Z}[x]$.)

2.11 More Exercises

(**2.11.1**) For what nonsquare values of d is the set

$$I_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z};\ a - b \ even\}$$

[4] An ideal M is *prime* if whenever A and B are ideals and AB is a subideal of M then either A or B is a subideal of M.

an ideal in $\mathbb{Z}[\sqrt{d}]$?

HINTS: Suppose $\alpha = a + b\sqrt{d}$ and $\beta = e + f\sqrt{d}$ both in I_d. We have $(a + b\sqrt{d}) + (e + f\sqrt{d}) = (a + e) + (f + b)\sqrt{d}$ and $a + e - f - b = (a - b) + (e - f)$, so we have closure under addition for any d.
Now for $\alpha \in I_d$ and $\beta \in \mathbb{Z}[\sqrt{d}]$ we have $(a + b\sqrt{d})(e + f\sqrt{d}) = ae + dbf + (af + be)\sqrt{d}$ and $ae + dbf - (af + be) = e(a - b) + f(db - a)$ The first part is even for any e, and the second part is even for any f provided that d is odd.

(**2.11.2**) THEOREM. Let F be a field. Then $F[x]/gF[x]$ is a field if g is an irreducible polynomial in $F[x]$.

Prove it. (What about the *only if* version?)

HINTS: Let $h \in F[x]$ be a representative of $h' \in F[x]/gF[x]^*$. Since g is irreducible, the GCD $(g, h) = 1$. Thus there is a u, v such that $gu + hv = 1$ in $F[x]$. But the image of this in the quotient is $h'v' = 1'$, so there is an inverse v' of h'.

(**2.11.3**) CLAIM: Let F be a field and g a nonconstant polynomial in $F[x]$. The map $F \to\to F[x] \to F[x]/gF[x]$ given by $f \mapsto fx^0 + 0x^1 + ... \mapsto f'$ is an injection.

Prove it.

HINTS: Suppose $g = 1 + x^2$ for example. Then $1' = \{1, 1 + g, 1 + 2g, ..., 1 + (2 + x)g, ...\}$ Note that no other constant polynomial besides 1 occurs.

2.12 More revision exercises

(**2.12.1**) Find a GCD of $a = 5 + 14i$ and $b = -4 + 7i$ in $\mathbb{Z}[i]$.

HINTS: We could start by trying to find a quotient-remainder formula: $a = bq + r$ (say). Noting that a has the bigger norm, we compute a/b, which will *eventually* give us $a/b = q + r/b$:

$$\frac{a}{b} = \frac{5 + 14i}{-4 + 7i}\frac{-4 - 7i}{-4 - 7i} = \frac{78 - 91i}{65} = \frac{6}{5} - \frac{7i}{5}$$

This is $a/b = (1 - i) + (1 - 2i)/5$ (by first rounding to the nearest integers, then computing the correction) so

$$a = (1 - i)b + ((1 - 2i)/5)b$$

The second summand (the 'remainder') is $\frac{1}{5}(1 - 2i)(-4 + 7i) = \frac{1}{5}(-4 + 14 + 8i + 7i) = 2 + 3i$ (of course we knew the denominator would cancel, since $a - (1 - i)b \in \mathbb{Z}[i]$).

The norms are $N(2 + 3\sqrt{-1}) = |2^2 - (-1)3^2| = 13$, and $N(5 + 14i) = |5^2 - (-1)14^2|$ =big, and $N(-4 + 7i) = |(-4)^2 - (-1)7^2|$ =big-ish. This just checks that the remainder has small enough norm (as the rounding method is designed to ensure — have a think about how it does this).

We next compute

$$\frac{b}{2 + 3i} = \frac{-4 + 7i}{2 + 3i}\frac{2 - 3i}{2 - 3i} = \frac{13 + 26i}{13} = 1 + 2i$$

Normally we would have to keep going, but since this quotient is in $\mathbb{Z}[i]$ there is no remainder, and we see that $2 + 3i|b$. Thus $2 + 3i$ also divides a and is a common divisor.

(**2.12.2**) Find as many subrings as possible of $\mathbb{Q}$.

(**2.12.3**) If $\theta : R \to S$ is a ring homomorphism, what can we say about $\theta(0)$?

(**2.12.4**) Determine which of the following mappings are ring homomorphisms:
(1) $\theta : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ defined by $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$ for $a, b \in \mathbb{Z}$.
(2) $\theta_2 : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ defined by $\theta_2(a + b\sqrt{2}) = b + a\sqrt{2}$ for $a, b \in \mathbb{Z}$.
(3) $\theta_3 : \mathbb{Z}[\sqrt{2}] \to M_7(\mathbb{Z}[\sqrt{2}])$ defined by $\theta_3(a + b\sqrt{2}) = (a + b\sqrt{2})1_7$ for $a, b \in \mathbb{Z}$ (where 1_7 is the identity matrix).

(**2.12.5**) (I) Let I be an ideal in a ring R. Show that the multiplication in the factor ring R/I is well-defined.
(II) Give the multiplication table for the factor ring $\mathbb{Z}/3\mathbb{Z}$.

(**2.12.6**) For $y \in \mathbb{R}$ define $A_y = \{f \in \mathbb{Q}[x] \mid f(y) = 0\}$. Under what circumstances is A_y an ideal in $\mathbb{Q}[x]$?

(**2.12.7**) Write $x^4 - 2$ as a product of irreducible polynomials over each of $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.

(**2.12.8**) Determine which of the following polynomials are irreducible over $\mathbb{Q}$:
(a) $2x^3 + 5x^2 - 2x + 3$.
(b) $x^4 + 55x^2 + 1210x$.

2.13 Homework exercises

Here we write $\det M$ for the determinant of a square matrix M.

(**2.13.1**) Show that a sufficient condition for a matrix M in the ring $M_2(\mathbb{Z})$ to be a unit in $M_2(\mathbb{Z})$ is $\det M = \pm 1$.

(**2.13.2**) Consider the subset S^x of matrices in $M_2(\mathbb{Z})$ such that all four matrix entries are nonzero. Give an example of an element of S^x:
(i) that is a unit in $M_2(\mathbb{Z})$;
(ii) that is a non-unit in $M_2(\mathbb{Z})$ but a unit in $M_2(\mathbb{Q})$; and
(iii) that is a non-unit in $M_2(\mathbb{Z})$ and in $M_2(\mathbb{Q})$.

(**2.13.3**) Show that for any unit U in the ring $R = M_2(\mathbb{Z})$ the map

$$f_U : R \to R$$

given by $f_U(X) = UXU^{-1}$ is a ring homomorphism from R to itself.
Construct an inverse map to f_U.

(**2.13.4**) There are infinitely many elements X of $M_2(\mathbb{Z})$ with $\det X = 0$. Recall from lectures that for each choice of $d \in \mathbb{Z}$ we have a subring

$$M_2^d(\mathbb{Z}) = \{\begin{pmatrix} a & db \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$$

(i) Prove carefully that, for any choice of d, $M_2^d(\mathbb{Z})$ *is* a ring.
(ii) For what choices of d does the ring $M_2^d(\mathbb{Z})$ contain nonzero elements X with $\det X = 0$?
(iii) For what choices of d is $M_2^d(\mathbb{Z})$ a commutative ring?

(**2.13.5**) Consider a fixed but arbitrary $d \in \mathbb{Z}$, and consider the ring $R = \mathbb{Z}[\sqrt{d}]$. Suppose $x \in R$ obeys $x = a + \sqrt{d}b$ with $a, b \in \mathbb{Z}$. For what values of d does x determine a *unique* values for the

pair (a, b) in this way? In the *other* cases, what can be said about the set of pairings (a, b) such that $x = a + \sqrt{d}b$, for any given x.

(**2.13.6**) For each d determine whether the map

$$f_d : M_2^d(\mathbb{Z}) \to \mathbb{Z}[\sqrt{d}]$$

given by $\begin{pmatrix} a & db \\ b & a \end{pmatrix} \mapsto a + \sqrt{d}b$ is a ring homomorphism.

(**2.13.7**) Prove that $M_2^{-2}(\mathbb{Z})$ is a UFD.

Answers

1. The inverse of M if it exists is easily verified to be the transpose of the matrix of cofactors 'divided' by $\det M$. The transpose of the matrix of cofactors is integral by construction. ± 1 divide every integer.

2. Examples: (i) $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

3. $f_U(a + b) = U(a + b)U^{-1} = U(a)U^{-1} + U(b)U^{-1} = f_U(a) + f_U(b)$ (via distributivity);
$f_U(a.b) = U(a.b)U^{-1} = U(a)U^{-1}.U(b)U^{-1} = f_U(a).f_U(b)$

Inverse is $f_{U^{-1}}$.

4. (i) Observe that it is a subset. Now check closure and inverses.
(ii) d a perfect square.
(iii) any.

5. (i) d not a perfect square;
(ii) There are infinitely many (with a, b related by a simple formula).

6. Yes. To see this check $f_d(ab) = f_d(a)f_d(b)$ and $f_d(a + b) = f_d(a) + f_d(b)$ for each d (routine calculations, which you should do!, with d left as an arbitrary but fixed number).

Homework exercises 2

(**2.13.8**) For $n > m$ consider the set map

$$\psi : M_n(\mathbb{Z}) \to M_m(\mathbb{Z})$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2m} & \dots & a_{2n} \\ \vdots & & & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} & \dots & a_{mn} \\ \vdots & & & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} & \dots & a_{nn} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}$$

For which values of n, m is this a ring homomorphism (if any)? Give reasons for your answer.

(**2.13.9**) Show that the intersection of two subgroups of a group is a group.

(**2.13.10**) For R a ring and A a subset of R, let $s(A)$ denote the set of all subrings of R that contain A (including R itself). Show that the intersection of all these subrings is itself a subring of R.

This intersection subring is called the ring *generated* by A in R.

Suppose that $0 \neq 1$ in R. Show that the sets $\emptyset$, $\{0\}$ and $\{1\}$ all generate the same ring in R.

Construct a ring R with $0 \neq 1$ such that the ring generated by $\emptyset$ in R is

(i) isomorphic to $\mathbb{Z}$;

(ii) *not* isomorphic to $\mathbb{Z}$.

(**2.13.11**) Consider the polynomial $f = x^2 + 1$. Regarded as a polynomial over which of the following coefficient rings is this polynomial irreducible? (i) $\mathbb{Z}$; (ii) $\mathbb{R}$; (iii) $\mathbb{C}$; (iv) $\mathbb{Z}_2$. Give reasons for your answers.

(**2.13.12**) Explain why the polynomial $x^4 - 7$ is irreducible over $\mathbb{Q}$, quoting any theorems you use.

(**2.13.13**) Give the multiplication table for the ring $\mathbb{Z}/4\mathbb{Z}$.

Answers

8. Define $A \in M_n(\mathbb{Z})$ (any $n > 1$) by $a_{1n} = a_{n1} = 1$ and all other entries zero. Then $\Psi(A) = 0$ (any $m < n$) but $\Psi(A^2) \neq 0$. Thus never a homomorphism. (Other formulations are possible.)

9. Let G, G' be the subgroups. If $a, b \in G \cap G'$ then $a, b \in G, G'$ so ab in G, G' (since they are groups), so $ab \in G \cap G'$, so the operation is closed in $G \cap G'$. It is associative by restriction similarly. The identity lies in both, hence in the intersection. Inverses lie in the intersection similarly.

10. Suppose elements a, b lie in the intersection. Then they lie in every subring. Now proceed similarly to above.

The smallest subring containing $\emptyset$ is simply the smallest subring. But every ring contains $0, 1$, so this subring does. Thus it is the same as the subring generated by 0, or 1.

(i) $\mathbb{R}$ (other answers are possible);

(ii) $\mathbb{Z}_2$.

11. This is a quadratic, so it is irreducible iff it had no root in the ring. Thus: (i) irreducible, since every element of $f(\mathbb{Z})$ is positive; (ii) irreducible, since every element of $f(\mathbb{R})$ is positive; (iii) not irreducible (i is a root); (iv) not irreducible (1 is a root).

12. Use Eisenstein's criterion with $p = 7$. (Or could determine a complete factorisation over $\mathbb{C}$, and note that none of the roots lie in $\mathbb{Q} \subset \mathbb{C}$.)

13. Elements of $\mathbb{Z}/4\mathbb{Z}$ are $\{[0], [1], [2], [3]\}$. Multiplication is then just as in the usual mod.4 arithmetic.

Homework exercises 3

(**2.13.14**) Determine if the map $X : \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $f(x) \mapsto f(x+3)$ is a ring homomorphism.

(**2.13.15**) Explain what is meant by $\mathbb{Q}(\sqrt{7})$.

(**2.13.16**) Suppose $K \supset F$ is a field extension Explain what it means for $a \in K$ to be *algebraic* over F.

(**2.13.17**) Prove that $\sqrt{7}$ is irrational.

(**2.13.18**) Determine a basis of $\mathbb{Q}(\sqrt{\sqrt{5}-11})$ over $\mathbb{Q}$.

(**2.13.19**) Construct an irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ (where $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$).

(**2.13.20**) Let $f(x) = 2x^3 + 3x^2 + 9x + 12 \in \mathbb{Z}[x]$. Is this polynomial primitive? State Eisenstein's criterion, and use it to determine if $f(x)$ is irreducible over $\mathbb{Q}$.

Compute the polynomial $x^3 f(1/x)$. Can Eisenstein's criterion be applied directly to this polynomial? Is it irreducible (give reasons for your answer)?

(**2.13.21**) Let $g(x) = x^3 + 3x + 9 \in \mathbb{Z}[x]$. This polynomial is irreducible over $\mathbb{Q}$, but why can we *not* use Eisenstein's criterion to show this directly?

(**2.13.22**) Determine which of the following polynomials are irreducible over $\mathbb{Q}$, explaining your method in each case.
(i) $f_0(x) = 3x^4 + 15x^2 + 10$;
(ii) $f_1(x) = 3x^9 + 15x^6 + 10$;
(iii) $f_2(x) = x^2 + x + 2$;
(iv) $f_3(x) = f_4(x + 3)$, where $f_4(x)$ is an irreducible polynomial.

(**2.13.23**) Let R be a ring and I, I' ideals of R. Show that $I \cap I'$ is an ideal of R.

Answers

14. We need to check that $X(fg) = X(f)X(g)$, and $X(f + g) = X(f) + X(g)$. We have

$$X(fg) = X(f(x)g(x)) = X((fg)(x)) = (fg)(x + 3) = f(x + 3)g(x + 3) = X(f(x))X(g(x))$$

$$X(f+g) = X(f(x)+g(x)) = X((f+g)(x)) = (f+g)(x+3) = f(x+3)+g(x+3) = X(f(x))+X(g(x))$$

(Note also that $X(1) = 1$ and $X(0) = 0$.)
15. $\mathbb{Q}(\sqrt{7})$ is the field of elements of form $a + b\sqrt{7}$ $(a, b \in \mathbb{Q})$. This is the smallest field extension of $\mathbb{Q}$ containing $\sqrt{7}$.
16. $a \in K$ is algebraic over F if there is a polynomial in the ring $F[x]$ with root a.
17. Suppose for a contradiction that $\sqrt{7} = a/b$ with $a, b \in \mathbb{Z}$ coprime. Then $7b^2 = a^2$. But then $7|a^2$ and hence $7|a$, since 7 is prime. But then 7^2 divides a^2 and hence 7 divides b^2. So, similarly, 7 divides b, contradicting coprimeness.
18. Write $a = \sqrt{\sqrt{5}-11}$. Then $a^2 = \sqrt{5} - 11$ and $(a^2 + 11)^2 = 5$ so a is algebraic with minimal polynomial $f_a = (a^2 + 11)^2 - 5 = a^4 + 22a^2 + 116$ (note that this is irreducible: there is no rational root, or indeed real root, since the coefficients are positive; thus the only possibility is a factorisation into two quadratics; but the roots over $\mathbb{C}$ are $a_i = \pm\sqrt{\pm\sqrt{5} - 11}$ and one readily

checks that no quadratic factor is integral).
A basis is therefore $\{1, a, a^2, a^3\}$.
19. Try $f(x) = x^2 + x + 1$. Since it is quadratic, it is enough to show that it has no roots in $\mathbb{Z}_2$. We have $f(0) = f(1) = 1$, so done.
20. The polynomial is primitive since the first two coefficients are coprime. Eisenstein's criterion says $f = \sum_{i=0}^{n} c_i x^i$ is irreducible over $\mathbb{Q}$ if there is a prime p such that $p \not| a_n$ and $p|a_i$ otherwise and $p^2 \not| a_0$.
Thus f is irreducible by Eisenstein with $p = 3$.
$g = x^3 f(1/x) = 12x^3 + 9x^2 + 3x + 2$ and Eisenstein cannot show irreducibility directly since there is no suitable prime.
g is irreducible since if it factorised this would induce a factorisation of f, contradicting its irreducibility.
21. There is no suitable prime.
22. (i) irreducible by Eisenstein with $p = 5$
(ii) ditto
(iii) irreducible by rational root test (Suppose r/s a root, with r, s coprime: then $(r^2+rs+2s^2)/s^2 = 0$, so $r^2 = -s(r+2s)$ so $s = \pm 1$ (else contradicts coprimeness), giving possible roots $\pm 1, \pm 2$. These all fail.)
(iv) irreducible since any factorisation induces a factorisation of f_4.
23. Need to show $J = I \cap I'$ an abelian group closed under the R action. Suppose $j, k \in J$. Then $j, k \in I$ so $j + k \in I$, and similarly for I', so $j + k \in J$. For $r \in R$ we have $rj \in I, I'$ (since these are R-ideals) so $rj \in J$. Similarly for jr.

2.14 More (Optional) Rings and Exercises

(**2.14.1**) Let R_1, R_2 be rings. Define operations on $R_1 \times R_2$ by

$$(r_1, r_2).(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$$

Show that $R_1 \times R_2$ can be made into a ring using these operations.
(The new ring is called the *direct product* or *direct sum* of R_1, R_2.)

(**2.14.2**) To form a product of three rings, R_a, R_1, R_α say, we need to address some practicalities of notation. For one thing the 'indexing set' $I = \{a, 1, \alpha\}$ is not necessarily ordered (that is, we may not be *given* an order on the set, and there may not be a natural way to assign one). For another, the Cartesian product is not strictly associative. Thus the underlying set of the product is not strictly $R_a \times R_1 \times R_\alpha$ (indeed it is not necessarily clear what this means). A convenient resolution is to consider $R = \times_{i \in I} R_i$ to be the set of 'indexed triples' of elements from the three rings. That is, if $r \in R$ then it contains, for each $i \in I$, a component r_i; and the collection of these components determines r.

(**2.14.3**) Show that the above direct product construction extends in the obvious way to any finite set of rings $\{R_i \mid i \in I\}$ (with I a finite indexing set).

(**2.14.4**) The construction may be extended still further to infinite indexing sets I (we write $R = \prod_{i \in I} R_i$), but where R is such that $r \in R$ implies that only finitely many of the r_i are

different from the zero element of the ring R_i. Explain why the given 'pointwise' addition and multiplication close on R constructed in this way.

2.14.1 Group rings and skew group rings

(**2.14.5**) If R is a ring and S a semigroup (resp. monoid, group) then the semigroup (resp. monoid, group) ring $R[S]$ is defined as follows. The underlying set is the set of all formal sums $\sum_{s\in S} r_s s$ where $r_s \in R$ and only finitely many of these are nonzero. (See e.g. Kelarev [**?**, §3.2].) Addition is

$$(\sum_{s\in S} r_s s) \ + \ (\sum_{s\in S} r'_s s) \ = \ \sum_{s\in S} (r_s + r'_s)s$$

and

$$(\sum_{s\in S} r_s s) \, . \, (\sum_{s'\in S} r'_{s'} s') \ = \ \sum_{s,s'\in S} (r_s r'_{s'})ss'$$

(**2.14.6**) Suppose R is a ring and G a group of automorphisms on R; and write r^g for the image of $r \in R$ under automorphism $g \in G$. The *skew group ring* $R * G$ is the same set and additive structure as $R[G]$; this time made into a ring by

$$(rg).(r'g') = \ ((r(r')^{g^{-1}})(gg'))$$

(**2.14.7**) The *fixed subring* of G on R is

$$R^G \ := \ \{r \in R \mid r^g = r \ \forall \ g \in G\}$$

2.14.2 Monoid-graded algebras

(See e.g. Karpilovsky [**?**, §22].)

(**2.14.8**) An algebra A over a commutative ring K is a ring R together with a choice of subring K from its centre.

(**2.14.9**) If M is a monoid then an algebra A over K is said to be M-graded if

$$A = \oplus_{m\in M} A_m$$

is a direct sum decomposition of A as a K-module; and

$$A_m A_{m'} \subseteq A_{mm'}$$

(When the latter is replaced by an equality A is *strongly* graded.)

(**2.14.10**) Note that if A is a K-algebra, and hence a ring, then $A * G$ as above is a strongly G-graded K-algebra. In particular

$$(A * G)_g = Ag$$