Part A Algebra II Notes

Tim Hosgood*
contact@timhosgood.co.uk

September 15, 2014

Abstract

These notes summarise the contents of a second-year algebra course at the University of Oxford. Because of this, there are many references to certain proofs being 'non-examinable', though the contents are still intended to be as self contained as possible.

Please email any corrections to contact@timhosgood.co.uk.

Contents

*Based on K. McGerty's 2014 University of Oxford lecture notes.

Starting definition

Basics

DEFINITION Rings: (1.1)
A *ring with 1* is an algebraic object $(R, +, \times, 0, 1)$, where R is a set, $+$ and $\times$ are binary operations on R, and $0, 1 \in R$, such that

1. $(R, +, 0)$ is an abelian group;
2. $(R, \times, 1)$ is a monoid;
3. $\times$ distributes over $+$:

$$x \times (y + z) = (x \times y) + (x \times z)$$
$$(y + z) \times x = (y \times x) + (z \times x)$$

LEMMA Subring criterion: (1.2)
Let R be a ring and $S \subseteq R$. Then S is a subring of R if and only if $1 \in S$ and for all $x.u \in S$ we have $xu.x - u \in S$.

Proof. Since $1 \in S$ we know that S is non empty. Then the condition that $x - y \in S$ implies that S is an additive subgroup by the subgroup test. The other conditions for being a subring can be checked directly. □

DEFINITION Units of a ring: (1.3)
Let R be a ring. The subset

$$R^\times := \{r \in R \mid \exists s \in R,\ rs = 1\}$$

is called the group of *units* of R. Note that is the group of all elements in R with multiplicative inverses.

Characteristic

There is an important concept in rings, which arises for noting that any ring R has a smallest subring: for $n \in \mathbb{Z}_{\geqslant 0}$ set $n_R := 1 + \ldots + 1$ (that is, 1 added to itself n times), and for $n \in \mathbb{Z}_{<0}$ set $n_R := -(-n)_R$. In one of the problem sheets we are asked to prove that $\{n_R | n \in \mathbb{Z}\} \leqslant R$ is a subring of R, and indeed tht the map $n \mapsto n_R$ gives a ring homomorphism $\phi\colon \mathbb{Z} \to R$. Since a ring homomorphism is, in particular, a homomorphism of the underlying additive abelian groups, using the First Isomorphism Theorem for abelian groups we see that $\{n_R | n \in \mathbb{Z}\} \cong \mathbb{Z}/d\mathbb{Z}$ (that is, they are isomorphic as groups) for some $d \in \mathbb{Z}_{\geqslant 0}$.

Now, any subring of R must contain 1 and hence, since it is closed under addition, must also contain n_R for all $n \in \mathbb{Z}$. Hence any subring contains $\mathrm{im}\phi$, so $\mathrm{im}\phi$ is the smallest subring of R.

DEFINITION Characteristic: (1.4)
The integer d defined as above is called the *characteristic* of R.

Evaluation of polynomial rings

In general, polynomials with coefficients in a ring cannot be viewed as functions, so one might be confused as to what such a polynomial actually is. It turns out, however, that there is a natural idea of an 'evaluation' homomorphism: to specify a homomorphism from a polynomial ring $R[t]$ to a ring S you only need to specify what happens to the elements of R and what happens to t.

LEMMA Evaluation homomorphisms: (1.5)
Let R, S be rings and $\phi\colon R \to S$ a ring homomorphism. If $s \in S$ then there is a unique ring homomorphism $\Phi\colon R[t] \to S$ such that $\Phi \circ \iota = \phi$ and $\Phi(t) = s$ (where $\iota\colon R \to R[t]$ is the inclusion of R into $R[t]$).

Proof. Any element of $R[t]$ has the form $\sum_{i=0}^{n} a_t t^i$ (where $a_i \in R$). Hence if Θ is any homomorphism satisfying $\Theta \circ \iota = \phi$ and $\Theta(t) = s$, we see that

$$\Theta\left(\sum_{i=0}^{n} a_i t^i\right) = \sum_{i=0}^{n} \Theta(a_i t^i) = \sum_{i=0}^{n} \Theta(a_i)\Theta(t^i) = \sum_{i=0}^{n} \phi(a_i) s^i$$

and so Θ is uniquely determined. To check that there is indeed such a homomorphism we just have to check that this definition of Θ satisfies the conditions, which is immediate from the definition. □

Ideals and quotients

Ideals and homomorphisms

LEMMA (2.1)
If $f : R \to S$ is a homomorphism then $\ker(f)$ *is an ideal.*

Proof. This is immediate from the definitions (and also, since the kernel was our motivation for defininining ideals, it would be rather strange if a kernel weren't an ideal...). □

REMARK (2.2)
Note that, if I is an ideal of R with $1 \in I$, then $I = R$.

LEMMA (2.3)
Let R be a ring, and I, J ideals of R. Then both

$$I + J := \{i + j \mid i \in I, j \in J\}$$

and

$$IJ := \left\{\sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J, n \in \mathbb{N}\right\}$$

are ideals. Moreover, we have that

$$IJ \subseteq I \cap J \quad \text{and} \quad I, J \subseteq I + J$$

REMARK (2.4)
Note that $I + J = \langle I \cup J \rangle$.

Quotients

THEOREM Quotient rings and the quotient map: (2.5)
Let R be a ring and I an ideal of R. Then we can define the quotient R/I and the quotient map $q\colon R \to R/I$, which is a surjective ring homomorphism.

Proof. Just checking that cosets behave well under addition and multiplication etc. □

COROLLARY (2.6)
Any ideal is the kernel of some ring homomorphism

LEMMA (2.7)
Let R be a ring, I an ideal of R, and $q\colon R \to R/I$ the quotient map. If J is an ideal of R then $q(J)$ is an ideal of R/I, and if K is an ideal of R/I then $q^{-1}(K)$ is an ideal of R, which contains I. (Note that q^{-1} is simply the preimage of q). Further, these correspondences give a bijection between the ideals in R/I and the ideals in R that contain I.

Proof. Long winded... □

Three isomorphism theorems

THEOREM First isomorphism theorem: (2.8)
Let $f\colon R \to S$ be a ring homomorphism, and $I = \ker(f)$. Then f induces an isomorphism, $\bar{f}\colon R/I \to \mathrm{im}(f)$, given by $\bar{f}(r + I) = f(r)$. That is,

$$\frac{R}{\ker(f)} \cong \mathrm{im}(f)$$

Proof. First, $r - s \in I \implies f(r - s) = 0 \implies f(r) = f(s)$, so $\bar{f}$ takes a unique value on each coset, regardless of representative (i.e. it is well defined). Clearly from the definition of the quotient structure, it is a ring homomorphism, and surjectivity onto the image of f is also clear. To check that it is injective, it is enough to check that $\bar{f}(0) = 0$, which is also clear. □

THEOREM Second isomorphism theorem: (2.9)
Let R be a ring, A a subring of R, and B an ideal of R. Then $A + B$ is a subring of R, and the natural map $R/(I \cap J) \to R/I$ induces an isomorphism

$$\frac{A}{A \cap B} \cong \frac{A + B}{B}$$

Proof. We can check that $A \cap B$ is an ideal of A, and that B is an ideal in $A + B$, so these two quotients exists at the least. Let $q\colon R \to R/B$ be the quotient map. It restricts to a homomorphism $p\colon A \to R/B$, whose image is clearly $(A + B)/B$, so by the first isomorphism theorem it is enough to check that $\ker(p) = A \cap B$, but this is clear from definitions. □

THEOREM Universal property of quotients: (2.10)
Let $f\colon R \to S$ be a ring homormorphism, and $I \subseteq \ker(f)$ an ideal. Then there is a unique homomorphism $\bar{f}\colon R/I \to S$ such that $f = \bar{f} \circ q$, where q is the quotient map.

Proof. Since q is surjective, the requirement $\bar{f}(q(r)) = f(r)$ uniquely defines $\bar{f}$ if it exists. But if $x, y \in I$ then, since $I \subseteq \ker(f)$, we have that $0 = f(x-y) = f(x) - f(y)$, and hence $f(x) = f(y)$. It follows that f is constant on the I-cosets, and so does indeed induce a unique map $\bar{f} : R/I \to S$ such that $\bar{f} \circ q = f$. (This is really more of a statement about general sets with an equivalence relation and thus a partition into equivalence classes). It is then immediate from the definitions on the ring structure on R/I that $\bar{f}$ is a homomorphism. □

THEOREM Third isomorphism theorem: (2.11)
Let $I \subseteq J$ be ideals of R. Then $J/I = \{j + I \mid j \in J\}$ is an ideal in R/I, and

$$\frac{R/I}{J/I} \cong (R/J)$$

Proof. Let $q_i\colon R \to R/I$ and $q_j\colon R \to R/J$ be the two quotient maps. By the universal property for q_j we see that there is a homomorphism $\bar{q}_i\colon R/J \to R/I$ induced by the map q_i, and such that $\bar{q}_i \circ q_j = q_i$. Clearly $\bar{q}_i$ is surjective (since q_i is), and if $\bar{q}_1(r + J) = 0$ then, since $r + J = q_j(r)$ so that $\bar{q}_1(r + J) = q_i(r)$, we have $r \in I$, so that $\ker(\bar{q}_i) = I/J$. The result then follows from the first isomorphism theorem. □

Chinese Remainder Theorem

The direct sum of rings, denoted by $R \oplus S$, is the ring of ordered pairs (that is, $\{(r, s) \mid r \in R, s \in S\}$) where addition and multiplication are defined componentwise.

THEOREM Abstract Chinese Remainder Theorem: (2.12)
Let R be a ring, and I, J ideals of R such that $I + J = R$. Then

$$\frac{R}{I \cap J} \cong (R/I) \oplus (R/J)$$

Proof. We have quotient maps q_i, q_j, which map R to R/I, R/J respectively. Define $q\colon R \to (R/I) \oplus (R/J)$ by $q(r) = (q_i(r), q_j(r))$. By the first isomorphism theorem it is enough to show that q is surjective and that $\ker(q) = I \cap J$. The latter is immediate. To see that q is surjective, suppose that $(r + I, s + J) \in (R/I) \oplus (R/J)$. Then, since $R = I + J$, we may write $r = i_1 + j_1$ and $s = i_2 + j_2$ (where the $i_k \in I$ and $j_k \in J$). But then $r + I = j_1 + I$ and $s + J = i_2 + J$, so that $q(j_1 + j_2) = (r + I, s + J)$. □

REMARK Clarification of direct sum: (2.13)
The usual use of the symbol $\oplus$ is when we have two ideals, say I and J, of a ring R, such that $R = I + J$ and $I \cap J = \{0\}$. We then write $R = I \oplus J$, just as for vector space direct sums. Also, just as for direct sums in vector spaces, we can write any element in R uniquely as some $i + j$, for $i \in I, j \in J$.

However, in the construction of a new ring, say $R := S_1 \oplus S_2$, for two other rings, S_1 and S_2, where we define this 'sum' to be the set of ordered tuples with addition and multiplication defined componentwise. Then the copies of S_1 and S_2 in R, denoted by S_1^R and S_2^R respectively, are simply those sets $S_1^R = \{(x, 0) \mid x \in S_1\}$ and $S_2^R = \{(0, x) \mid x \in S_2\}$. But since these copies don't contain the multiplicative identity for R, they aren't subrings, but instead ideals.

Thus the 'external' notation of direct sums that we use to define new rings is compatible with the 'internal' notation that we are used to

Principal, prime, and maximal ideals

Principal ideals

DEFINITION Principal ideals: (2.14)
A *principal ideal* is an ideal that is generated by a single element.

DEFINITION Associates: (2.15)
Two elements, $a, b \in R$, are said to be *associates* if there is a unit $u \in R^\times$ such that $a = ub$. (Note that this is an equivalence relation on the elements of R).

LEMMA (2.16)
Let R be an integral domain and I a principal ideal. Then the generators of I are associates, and any associate of a generator is itself a generator. Thus the generators of a principal ideal in an integral domain form a single equivalence class of associate elements of R.

Prime ideals

DEFINITION Prime ideals: (2.17)
An ideal I of R is *prime* if, first of all, $I \neq R$, and secondly, for all $a, b \in R$, whenever $ab \in I$, either $a \in I$ or $b \in I$.

LEMMA (2.18)
An ideal I in a ring R is prime if and only if R/I is an integral domain.

Maximal ideals

DEFINITION Maximal ideals: (2.19)
An ideal I of R is *maximal* if it is not contained in any proper ideal of R.

LEMMA (2.20)
An ideal I in a ring R is maximal if and only if R/I is a field.

COROLLARY (2.21)
A maximal ideal is prime.

Polynomial rings, fields, and field extensions

LEMMA Division algorithm for polynomials over a ring: (3.1)
Let R be a ring and $f = \sum_{i=0}^{n} a_i t^i \in R[t]$, where $a_n \in R^\times$, and let $g \in R[t]$ be any polynomial. Then there exist unique $q, r \in R[t]$ such that either $r = 0$ or $\deg(r) < \deg(f)$ and $g = qf + r$.

Proof. This follows by induction on $\deg(g)$. Since the leading coefficients are in $R^\times$ we can see that, for any $f, g \in R[t]\backslash\{0\}$, we have $\deg(fg) = \deg(f)+\deg(g)$. It follows that if $\deg(g) < \deg(f)$, we must take $q = 0$ and thus $r = g$. Let $m = \deg(g) \geqslant n = \deg(f)$, then if $g = \sum_{j=0}^{m} b_j t^j$, where $b_m \neq 0$, the polynomial

$$h = g - (a_n^{-1} b_m t^{m-n}) f$$

has $\deg(h) < m = \deg(g)$, and so (by the induction hypothesis) there are unique q', r' with $h = q'f + r'$. Setting $q = a_n^{-1} b_m t^{m-n} + q'$ and $r = r'$ it follows that $g = qf + r$. Uniqueness of q and r follows from the fact that they are uniquely determined by q' and r'. □

COROLLARY (3.2)
We have the division algorithm for all non-zero polynomials in $\mathbb{F}[t]$.

Polynomials over a field

LEMMA (3.3)
Let I be a non-zero ideal in $\mathbb{F}[t]$. Then there is a unique monic polynomial $f \in \mathbb{F}[t]$ such that $I = \langle f \rangle$. Thus all ideals in $\mathbb{F}[t]$ are principal.

Proof. Existence of such an f comes from the division algorithm: since I is non zero, choose some $f \in I$ with minimal degree. By the division algorithm, for any $g \in I$, we can write $g = qf + r$, but rearranging we see that $r \in I$, and since $\deg(r) < \deg(f)$ we must have $r = 0$ so as not to contradict the minimality of f. Thus $g = qf$.

For uniqueness, if $I = \langle f \rangle = \langle f' \rangle$, then there exist $a, b \in \mathbb{F}[t]^\times = \mathbb{F}[t] \setminus \{0\}$ such that $f = af'$ and $f' = bf$. Then $f = (ab)f$, so a, b must have degree zero, and thus $a, b \in \mathbb{F}$. Since we require f and f' to be monic, $a = b = 1$. □

LEMMA Greatest common divisor: (3.4)
Let $f, g \in \mathbb{F}[t]$ be non-zero polynomials. Then there exists a unique monic polynomial $d \in \mathbb{F}[t]$ such that d divides both f and g, and there exist $a, b \in \mathbb{F}[t]$ such that $af + bg = d$. We call d the greatest common divisor *of f and g since, if c also divides f and g, then c divides $af + bg = d$ too.*

Proof. Let $I = \langle f, g \rangle$. Since all ideals in $\mathbb{F}[t]$ are principal, it follows that there exists some unique monic polynomial d such that $\langle d \rangle = I$. Then, certainly, $f \in \langle f \rangle \subseteq I = \langle d \rangle$, so that d divides f, and similarly for g. Since $I = \langle f, g \rangle = \{rf + sg \mid r, s \in \mathbb{F}[t]\}$ and

$d \in I$ it's clear that we can find $a, b \in \mathbb{F}[t]$ such that $d = af + bg$. □

LEMMA (3.5)
Let $\mathbb{F}$ be a field and $I = \langle f \rangle$ a non-zero ideal in $\mathbb{F}[t]$. Then I is prime if and only if $f \in \mathbb{F}[t]$ is an irreducible polynomial. Moreover, every such ideal is maximal, and all maximal ideals are of this form. That is, the non-zero prime ideals are exactly the maximal ideals

Proof. If $\langle f \rangle$ is a non-zero prime ideal (so that $f \neq 0$) and $f = gh$, then $f|g$ or $f|h$, say $f|g$. But then $g = fk$, and so $f = (fk)h$, thus $f(1 - kh) = 0$. Since $\mathbb{F}[t]$ is an integral domain (has no zero divisors) it follows that $kh = 1$, and h is a unit. Thus f is irreducible as claimed.

Conversely, suppose that f is irreducible and that f divides a product gh. We must show that f divides one of g and h. But if f does not divide g then the highest common factor of f and g must be 1. Then by Bezout's Lemma we have that $1 = af + bg$ for some $a, b \in \mathbb{F}[t]$, and so

$$h = h.1 = h(af + bg) = f(ah) + b(gh)$$

so that f clearly divides h as required.

To see the moreover part, suppose that M is a maximal ideal. Then it is certainly prime, and so the f such that $M = \langle f \rangle$ is irreducible by the above. On the other hand, if $I = \langle f \rangle$ is a prime ideal, then suppose that $I \subset J$ for some proper ideal J. Then, since all ideals in $\mathbb{F}[t]$ are principal, there exists some g such that $J = \langle g \rangle$. But then $f = gh$ for some $h \in \mathbb{F}[t]$ where, since J is proper, $\deg(g) > 0$. Since f is irreducible, we must have $h \in \mathbb{F}$, and so h is a unit, and $I = J$, as required. □

Quotients of polynomial rings (an introduction)

We now consider what the quotients of $\mathbb{F}[t]$ look like. We know that any ideal I is of the form $\langle f \rangle$ for some monic irreducible $f \in \mathbb{F}[t]$. Say that $\deg(f) = d$. Then by the division algorithm we can write any polynominal $g \in \mathbb{F}[t]$ as $g = qf + r$, for some unique $q, r \in \mathbb{F}[t]$ with $\deg(r) < \deg(f) = d$. Thus the polynomials of degree strictly less than d form a complete set of representatives for the I-cosets.

Since $\{1, t, \ldots, t^{d-1}\}$ forms an $\mathbb{F}$-basis for the vector space of polynomials degree less than d, this means that, letting $q\colon \mathbb{F}[t] \to \mathbb{F}[t]/I$ be the quotient map, and $\alpha = q(t)$, the set $\{1, \alpha, \ldots, \alpha^{d-1}\}$ forms an $\mathbb{F}$-basis for the quotient $\mathbb{F}[t]/I$. We are left with the question of how to define α^d in $\mathbb{F}[t]/I$, but there is a naturally arising solution for this: let $\alpha^d = -\sum_{i=0}^{d-1} a_i \alpha^i$, where the right hand side comes from $f(t) = t^d + \sum_{i=0}^{d-1} a_i t^i$. So in particular, $\mathbb{F}[t]/I$ is an $\mathbb{F}$-vector space of dimension d.

We can therefore view the quotient $\mathbb{F}[t]/I$ as a way of building a new ring out of $\mathbb{F}$ and a single element, α, which satisfies the relation $f(\alpha) = 0$. Or, rather, the quotient construction gives us a rigorous way of doing this. For example, to build $\mathbb{C}$ out of $\mathbb{R}$, we know that all we really need to do is to 'add in' i, which satisfies $i^2 + 1 = 0$. Via the quotient construction, this simply says that we want to set $\mathbb{C} = \mathbb{R}[t]/\langle t^2 + 1 \rangle$, which is indeed a field, since $t^2 + 1$ is irreducible in $\mathbb{R}[t]$ (which we can easily check).

In fact, with a little more care (by using the general division algorithm), it is straight forward to check that if R is a ring and $f \in R[t]$ is a monic polynomial of degree d, and we let $Q = R[t]/\langle f \rangle$ and $\alpha = q(t)$ (where q is the quotient map, as before), then any element of Q can be written as a linear combination of powers less than d of α. That is, $Q = \{a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1} \mid a_i \in R\}$, where multiplication in Q is given by the same rules as above (α^d is found by rearranging $f(\alpha)$).

So, to recap one important motivating point, if $\mathbb{F}$ is a field and f is any monic irreducible polynomial, then $\mathbb{F}[t]/\langle f\rangle$ is a field, but in particular, an $\mathbb{F}$-vector space of dimension $\deg(f)$.

Field extensions

DEFINITION Field extensions and dimension: (3.6)
If E and F are fields with $F \subset E$, then we may view E as an F-vector space. Then E, thought of in this way, is called the *field extension* E/F. If E is finite dimensional as such a vector space, then we write $[E : F] = \dim_F(E)$ for this dimension, and call it the *degree of the field extension* E/F.

Since the definition of the characteristic of a ring and the embedding property of the field of fractions (to be covered later, nearer the end of the notes) show that any field contains either a copy of $\mathbb{F}_p$ for some prime p or a copy of $\mathbb{Q}$, we will focus on finite extensions of these fields. That is, fields that are finite dimensional when viewed as either $\mathbb{Q}$- or $\mathbb{F}_p$-vector spaces.

LEMMA (3.7)
Let E/F be a field extension and $[E : F] < \infty$. Then if V is an E-vector space, we may also view it as an F-vector space, and V is finite dimensional as an F-vector space if and only if it is finite dimensional as an E-vector space. Moreover, $\dim_F(V) = [E : F] \dim_E(V)$.

Proof. Clearly if V is an E-vector space then, by restricting scalar multiplication to F, it follows that V is an F-vector space. Moreover, if V is finite dimensional as an F-vector space then, since a finite F-spanning set will also be a finite E-spanning set, then it is also finite dimensional as an E-vector space.

Conversely, suppose that V is a finite-dimensional E-vector space. Let $\{x_1, x_2, \ldots, x_d\}$ be an F-basis of E, and $\{e_1, e_2, \ldots, e_n\}$ an E-basis for V. To finish the proof it is enough to check that $\{x_i e_j \mid 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n\}$ is an F-basis of V. Indeed, if $v \in V$ then, since $\{e_1, \ldots, e_n\}$ is an E-basis of V, there are $\lambda_i \in E$ such that $v = \sum_{i=1}^n \lambda_i e_i$. Moreover, since $\{x_1, \ldots, x_d\}$ is an F-basis for E, then for each λ_i there are μ_j^i (where the i is simply a label, not repeated multiplication) such that $\lambda_i = \sum_{j=1}^d \mu_j^i x_j$. Thus

$$v = \sum_{i=1}^{n} \lambda_i e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{d} \mu_j^i x_j \right) e_i = \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant d}} \mu_j^i (x_j e_i)$$

and so $\{x_j e_i\}$ spans V as an F-vector space. To see linear independence, and hence establish the dimension formula, simply note that $v = 0$ if and only if each $\lambda_i = 0$ if and only if each $\mu_j^i = 0$. □

COROLLARY Tower Law: (3.8)
Let $F \subset E \subset K$ be fields. Then $[K : F]$ is finite if and only if both degrees $[K : E]$ and $[E : F]$ are finite. If this is the case, then we have that $[K : F] = [K : E][E : F]$

DEFINITION Algebraic and simple extensions: (3.9)
Let $\alpha \in \mathbb{C}$. We say that α is *algebraic over* $\mathbb{Q}$ if there is a field E containing α such that $[E : \mathbb{Q}]$ is finite. Otherwise, we say that α is *transcendental*.

Since the intersection of subfields is again a subfield, we can, as per usual, talk about the smallest subfield containing a set, and thus the idea of a field generated by a set. Given a set $T \subseteq \mathbb{C}$, we write $\mathbb{Q}(T)$ for the field generated by T (since any subfield of $\mathbb{C}$ contains $\mathbb{Z}$ and thus, by the inclusion of the field of fractions (which, again, will be discussed later), also contains $\mathbb{Q}$). If the set T consists of a single element α then we write $\mathbb{Q}(\alpha)$ rather than $\mathbb{Q}(\{\alpha\})$, and we say that the extension is *simple*. Note that α being algebraic is equivalent to $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ being finite.

Slightly more generally, if F is any subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$, we let $F(\alpha) = \mathbb{Q}(F \cup \{\alpha\})$ be the smallest subfield of $\mathbb{C}$ containing both F and α, and one says that α is algebraic over F if $[F(\alpha) : F]$ is finite.

Quotients of polynomial rings (properly)

Going back to quotients of polynomial rings, but using what we have just learnt about general field extensions, we discover that simple extensions are exactly the types of fields that we have been building with our quotient construction.

LEMMA (3.10)
Suppose that E/F is a finite field extention, with both E and F subfields of $\mathbb{C}$, say, and let $\alpha \in E \setminus F$. Then there exists a unique irreducible monic polynomial $f \in F[t]$ such that $F(\alpha) \cong F[t]/\langle f \rangle$.

Proof. The field $F(\alpha)$ is a finite extension of F, since it is a subfield of E (and thus a sub-F-vector space of the F-vector space E/F). Let $d = [F(\alpha) : F] = \dim_F(F(\alpha))$. Since the set $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ has $d + 1$ elements, it must be linearly dependent, and thus there exist $\lambda_i \in F$, not all zero, such that $\sum_{i=0}^{d} \lambda_i \alpha^i = 0$. But then if $g = \sum_{i=0}^{d} \lambda_i t^i \in F[t] \setminus \{0\}$, we see that $g(\alpha) = 0$. It follows that the kernel I of the homomorphism $\phi\colon F[t] \to E$ given by $\phi(\sum_{j=0}^{m} c_j t^j) = \sum_{j=0}^{m} c_j \alpha^j$ is non zero.

Now any non-zero ideal in $F[t]$ is generated by a unique monic polynomial, thus $I = \langle f \rangle$ for some f. By the First Isomorphism Theorem, the image S of ϕ is isomorphic to $F[t]/I$. Since S is a subring of a field, so certainly an integral domain, we must have that $\langle f \rangle$ is a prime ideal, and by our previous description of prime ideals in $F[t]$, it must also be maximal, so that therefore S is a field.

Finally, any subring of $\mathbb{C}$ containing F and α must clearly contain S (as the elements of S are F-linear combinations of powers of α), and so it follows that $F[t]/\langle f \rangle \cong S = F(\alpha)$. □

DEFINITION Minimal polynomial: (3.11)
Given $\alpha \in \mathbb{C}$, the polynomial f associated to α by the previous lemma, that is, the irreducible f such that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[t]/\langle f \rangle$, is called the *minimal polynomial of α over* $\mathbb{Q}$. Note that our description of the quotient $\mathbb{Q}[t]/\langle f \rangle$ shows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$, hence the degree of the simple field extension $\mathbb{Q}(\alpha)$ is simply the degree of the minimal polynomial of α.

EXAMPLE (3.12)
Consider $\sqrt{3} \in \mathbb{C}$. There is a unique ring homomorphism $\phi\colon \mathbb{Q}[t] \to \mathbb{C}$ such that $\phi(t) = \sqrt{3}$. Clearly the ideal $\langle t^2 - 3\rangle$ lies in $\ker(\phi)$, and since $t^2 - 3$ is irreducible in $\mathbb{Q}[t]$ so that $\langle t^2 - 3\rangle$ is a maximal ideal, we see that $\ker(\phi) = \langle t^2 - 3\rangle$, and hence, by the First Isomorphism Theorem, $\mathrm{im}(\phi) \cong \mathbb{Q}[t]/\langle t^2 - 3\rangle$. But the fact that $t^2 - 3$ is irreducible also tells us that the quotient $\mathbb{Q}[t]/\langle t^2 - 3\rangle$ is a field, and thus so too is $\mathrm{im}(\phi)$. Moreover, any subfield of $\mathbb{C}$ containing $\sqrt{3}$ clearly contains $\mathrm{im}(\phi)$, so we see that $\mathrm{im}(\phi) = \mathbb{Q}(\sqrt{3})$.

In particular, since the images of $\{1, t\}$ form a basis of the quotient $\mathbb{Q}[t]/\langle t^2 - 3\rangle$ by our description of quotients of polynomial rings in the previous section, and under the isomorphism induced by ϕ these map to 1 and $\sqrt{3}$ respectively, we see that $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, a degree two extension of $\mathbb{Q}$. (Note that we could also check that the right hand side of this equality is a field instead, but this method is more enlightening concerning the existence of the isomorphism with $\mathbb{Q}[t]/\langle t^2 - 3\rangle$).

Commutative rings

Integral Domains

From now on, every ring that we deal with in this chapter shall be an integral domain, unless otherwise explicitly stated.

DEFINITION Zero divisors: (4.1)
Let R be a ring. Then an element $a \in R \setminus \{0\}$ is said to be a *zero divisor* if there is some $b \in R \setminus \{0\}$ such that $ab = 0$.

DEFINITION Integral domains: (4.2)
An non-zero ring is an *ID* if it has no zero divisors, or, equivalently, $ab = 0 \iff a = 0$ or $b = 0$.

LEMMA (4.3)
Let R be an ID. Then $R[t]$ is an ID, and any subring $S \leqslant R$ is also an ID. Moreover, the characteristic of R is either 0 or p, for some prime $p \in \mathbb{Z}$.

Proof. The proof that $R[t]$ is an ID can be found on one of the problem sheets, and it is clear from the definition of a subring that S is also an ID. Now, from the definition of the characteristic, if $\mathrm{char}(R) = n > 0$ then $\mathbb{Z}/n\mathbb{Z}$ is a subring of R. Clearly if $n = ab$ where $a, b \in \mathbb{Z}$ are both greater than 1, then $a_R b_R = 0$ in R, with neither being zero, and thus both are zero divisors. It follows that if R is to be an integral domain then we require n to be prime, or zero. □

Primes, irreducibles, and factors

Note: we are still assuming that every ring is an ID.

DEFINITION Prime elements: (4.4)
A non-zero element $a \in R \setminus \{0\}$ is said to be *prime* if aR is a prime ideal. That is, $aR \neq R$, and whenever a divides rs it also divides at least one of r and s. Note that $aR \neq R = 1R$ says that a and 1 are not associates, i.e. a is not a unit. Note also that it follows by induction on m that if p is prime and $p | a_1 a_2 \dots a_m$ then $p | a_j$ for some $1 \leqslant j \leqslant m$.

DEFINITION Irreducible elements: (4.5)
A non-zero element $a \in R\backslash\{0\}$ is said to be *irreducible* if it is not a unit, and whenever $a = bc$, either b or c is a unit.

LEMMA (4.6)
If R is an ID then any prime element is also irreducible.

Proof. Suppose that $p = ab$ is prime. Then p divides ab, so p must divide one of a and b, say a. But then $a = rp$ for some r, and thus $p = (rb)p$, so cancelling (since we are in an ID) gives $1 = rb$, and so b is a unit. □

DEFINITION Factors, and the highest common factor: (4.7)
Let $a, b \in R$. We say that a *divides* b, or a is a *factor* of b, and write $a|b$, if there is some $c \in R$ such that $b = ac$. Note that we can also write this in terms of ideals: $a|b$ if and only if $bR \subseteq aR$.

We say that c is a *common factor* of $a, b \in R$ if c divides both a and b. If c is a common factor of a and b, and further any other common factor d is such that $d|c$, then we say that c is the *highest common factor*, or *greatest common divisor* of a and b.

In the same way, a *common multiple* of two elements $a, b \in R$ is an element k such that both a and b divide k. If a common multiple is a factor of every other common multiple, then it is called the *least common multiple*.

Note that these definitions can be rephrased in terms of ideals:

- c is a common factor of a, b if and only if $\{a, b\} \in cR$;
- c is the highest common factor of a, b if and only if cR is minimal amongst principal ideals containing $\{a, b\}$;
- k is the least common multiple of a, b if and only if kR is maximal amongst principal ideals lying in $aR \cap bR$.

LEMMA (4.8)
In an ID, if $\gcd\{a, b\}$ *exists then it is unique up to units. Similarly for* $\mathrm{lcm}\{a, b\}$.

LEMMA (4.9)
Let R be an ID and $a \in R$. Then a is irreducible if and only if the ideal $\langle a\rangle$ is maximal amongst proper principal ideals in R. That is, if and only if whenever $aR \subseteq bR$, either b is a unit so that $bR = R$, or $bR = aR$ so that b and a are associates.

Proof. If $a \in R$ and $aR \subseteq bR$ then we have $a = bc$ for some $c \in R$. If c is a unit then $aR = bR$, otherwise we have $aR \subset bR$. Now if $a \in R$ is irreducible it clearly follows that any principal ideal containing aR is either aR or all of R.

Conversly, if aR is maximal amongst proper principal ideals and $a = bc$, then aR is contained in bR and cR. Since a is not a unit, one of b and c must also not be a unit, say b. But then $aR \subseteq bR \neq R$, and by maximality $aR = bR$, whence $a = bu$ for some unit $u \in R$. Thus $bc = bu$, and hence $c = u$ is a unit. □

Unique Factorisation Domains

DEFINITION Unique factorisations domains: (4.10)
A integral domain R is a *UFD* if every non-zero element in R is either a unit, or can be written as a product of prime elements, and moreover the factorisation into primes is unique up to reordering and units.

LEMMA (4.11)
Suppose that R is an ID and that every $a \in R \setminus \{0\}$ can be written as a product of prime elements, say $a = p_1 p_2 \dots p_k$. Then this factorisation is unique up to reordering and units.

Proof. The lemma could be restated by saying that, if $a = p_1 p_2 \dots p_k$ and $a = q_1 q_2 \dots q_l$ are two factorisations into primes, then $k = l$ and there exist units $u_i \in R^\times$ such that, after reordering the q_i, we have $p_i = u_i q_i$. We prove by induction on the minimal number $M(a)$ of primes in a factorisation of $a \in R$. □

So by the above, if an element has *some* factorisation into prime elements then such a factorisation is unique (up to reordering and units).

Principal Ideal Domains

DEFINITION Principal ideal domains: (4.12)
A ring is a *PID* if every ideal is principal.

LEMMA (4.13)
Let R be a PID. Then for any $a, b \in R$, we have $\gcd\{a, b\} \in R$.

Proof. We prove the stronger statement: for $a_1, a_2, \dots, a_n \in R$, we have $\gcd\{a_1, \dots, a_n\} \in R$. Consider $I = \langle\{a_1, \dots, a_n\}\rangle$. Since R is a PID there exists some d such that $I = \langle d\rangle$. Then we can check that this d is indeed the greatest common divisor of the a_i by checking the two parts of the definition (and noting that $d = \sum r_i a_i$ for some $r_i \in R$). □

LEMMA (4.14)
If R is a PID then irreducible elements are prime and all non-zero prime ideals are maximal.

Proof. If $a \in R$ is irreducible then $\langle a\rangle$ is maximal, and hence prime. Moreover, any non-zero prime ideal in R is of the form $\langle p\rangle$ for some prime element $p \in R \setminus \{0\}$. But since R is an ID, prime elements are irreducible, and hence $\langle p\rangle$ is maximal. □

LEMMA (4.15)
Let R be a PID and suppose that $\{I_n \mid n \in \mathbb{N}\}$ is a sequence of ideals such that $I_n \subseteq I_{n+1}$. Then the union $I = \bigcup_{n\in\mathbb{N}} I_n$ is an ideal, and there exists an $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geqslant N$.

Proof. Given any two elements $p, q \in I$, we may find $k, l \in \mathbb{N}$ such that $p \in I_k$ and $q \in I_l$. It follows that, for any $r \in R$, we have $rp \in I_k \subset I$, and by taking $n = \max\{k, l\}$ we see that $r, s \in I_n$, so that $r + s \in I_n \subset I$. It follows that I is an ideal. Since R is a PID, there exists some $c \in R$ such that $I = \langle c\rangle$. But then there must be some N such that $c \in I_N$, and hence $I = \langle c\rangle \subseteq I_N \subseteq I$, so that $I = I_N = I_n$ for all $n \geqslant N$ as

required. □

LEMMA (4.16)
If R is a PID then it is a UFD.

Proof. In a PID, an element is irreducible if and only if it is prime, and, more generally, any prime factorisation is unique up to reordering and units. So all that remains to show is that any element in R has a factorisation into irreducibles.

Suppose, for a contradiction, that there is some $a = a_1 \in R$ that is not a product of irreducible elements. Clearly a cannot be irreducible, so we may write it as $a = bc$, where neither b nor c is a unit. If both b and c can be written as a product of prime elements, then multiplying these expressions together we see that a is also prime, hence at least one of b or c cannot be written as a product of prime elements, say b. Then let $a_2 = b$. Note that, if we set $I_k = \langle a_k \rangle$ (for $k = 1, 2$) then $I_1 \subsetneq I_2$. As before, a_2 cannot be irreducible, so we may find an a_3 such that $I_2 = \langle a_2 \rangle \subsetneq \langle a_3 \rangle = I_3$. Continuing in this fashion, we get a nested sequence of ideals I_k, each strictly bigger than the previous one. By the above lemma, this cannot happen if R is a PID, thus no such a exists. □

Euclidean Domains

DEFINITION Euclidean domains: (4.17)
A ring is an *ED* if there exists a function $N \colon R \setminus \{0\} \to \mathbb{N}$ (called the *norm*) such that, given any $a \in R, b \in R \setminus \{0\}$ there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

LEMMA (4.18)
If R is an ED then it is a PID.

Proof. Let I be an ideal. If I is the zero ideal then there is nothing to show, otherwise pick $a \in I$ with $N(a)$ minimal. The claim is that $I = \langle a \rangle$. Using the property of the norm (almost exactly as we used the division algorithm to show that $R[t]$ was a PID) we can see that any element $s \in I$ must be such that $a | s$, and thus $I \subseteq \langle a \rangle$ Then since $\langle a \rangle \subseteq I$, clearly, we have that the two are equal. □

Fields

DEFINITION Fields: (4.19)
A ring is a *field* if it is

- a finite integral domain;
- an integral domain consisting only of units;
- an integral domain with the only ideals being the two trivial ideals.

Field of fractions

It is possible to have infinite integral domains that are not fields, e.g. $\mathbb{Z}$. However, we can generalise the construction of the rationals from the integers to any ID R to build a field $F(R)$: the *field of fractions of* R. This field has the property that it is the smallest field into which we can embed R.

We formally define this field by defining first an equivalence relation on $R \times R \setminus \{0\}$, where (a,b) (c,d) if $ad = bc$ (which we need to check is an equivalence relations). Next we define binary operations in the expected sense:

$$+\colon ((a,b),(c,d)) \mapsto (ad+bc, bd)$$
$$\times\colon ((a,b),(c,d)) \mapsto (ac, bd)$$

and we start to write $\frac{a}{b}$ to represent the equivalence class of (a,b). Then $F(R)$ is a field under these operations, with the obvious additive and multiplicative identities. Moreover, there is a unique injective homomorphism sending $a \mapsto \frac{a}{1}$.

Finally, we make clear what we mean by the statement that this field of fractions $F(R)$ is the smallest field containing R: Let $\mathbb{F}$ be a field and $\theta\colon R \to \mathbb{F}$ be an injective homomorphism (an *embedding*). Then we claim that there is a unique injective homomorphism $\tilde{\theta}\colon F(R) \to \mathbb{F}$ extending θ (that is, it agrees with θ in the sense that $\tilde{\theta}(\frac{a}{1}) = \theta(a)$). To prove this we note that, if $\tilde{\theta}$ is such a homomorphism, then $\tilde{\theta}(\frac{a}{1}$ forces us to have $\tilde{\theta}(\frac{1}{a}) = \theta(a)^{-1}$. But then $\tilde{\theta}(\frac{a}{b}) = \tilde{\theta}(\frac{a}{1})\tilde{\theta}(\frac{1}{b}) = \theta(a)\theta(b)^{-1}$. So if $\tilde{\theta}$ exists, then it is uniquely determined by this formula.

To check existence, it is simply a matter of checking that this recipe indeed works.

REMARK (4.20)
This implies that any field $\mathbb{F}$ of characteristic zero contains a unique copy of the rationals, since by the definition of the characteristic, the unique homomorphism $\mathbb{Z} \to \mathbb{F}$ is an embedding, and the above shows that it therefore extends uniquely to an embedding of $\mathbb{Q}$ into $\mathbb{F}$, as claimed.

Integer polynomials ($\mathbb{Z}[t]$)

DEFINITION Content: (5.1)
Let $f \in \mathbb{Z}[t]$. Then the *content*, $c(f)$, of f is the highest common factor of the coefficients of f. That is, if $f = \sum_{i=0}^{n} a_i t^i$, then $c(f) = \gcd\{a_0, \ldots, a_n\}$. We further insist that $c(f) > 0$, so that it is unique (as opposed to simply being unique up to units).

LEMMA Gauss' Lemma: (5.2)
Let $f, g \in \mathbb{Z}[t]$. Then $c(fg) = c(f)c(g)$.

Proof. Suppose first that f, g have content 1, and let $p \in \mathbb{N}$ be prime. We have for each such p a homomorphism $\phi_p\colon \mathbb{Z}[t] \to \mathbb{F}_p[t]$ given by simply computing the coefficients modulo p. It is immediate that $\ker \phi_p = p\mathbb{Z}[t]$, so that $p|c(f)$ if and only if $\phi_p(f) = 0$. But since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[t]$ is an ID, and so, since ϕ_p is a homomorphism, we see that

$$\begin{aligned} p|c(fg) &\iff \phi_p(fg) = 0 \iff \phi_p(f)\phi_p(g) = 0 \\ &\iff \phi_p(f) = 0 \quad \text{or} \quad \phi_p(g) = 0 \iff p|c(f) \quad \text{or} \quad p|c(g) \end{aligned}$$

whence it is clear that $c(fg) = 1$ (if $c(f) = c(g) = 1$).

Now let $f, g \in \mathbb{Z}[t]$, and write $f = af'$, $g = bg'$, for some $f', g' \in \mathbb{Z}[t]$ with content 1, and $a, b \in \mathbb{Z}$. Then $c(f) = a$ and $c(g) = b$, so clearly $fg = (ab)f'g'$, and since $c(f'g') = 1$, it follows that $c(fg) = c(f)c(g)$. □

LEMMA (5.3)
Suppose that $f \in \mathbb{Q}[t]$ is non zero. Then there is a unique $\alpha \in \mathbb{Q}_{>0}$ such that $f = \alpha f'$, where $f' \in \mathbb{Z}[t]$ has content 1. We then write $c(f) = \alpha$. Moreover, if $f, g \in \mathbb{Q}[t]$, then $c(fg) = c(f)c(g)$.

Proof. Let $f = \sum_{i=0}^{n} a_i t^i$ where $a_i = \frac{b_i}{c_i}$ for $b_i, c_i \in \mathbb{Z}$ with $\gcd\{b_i, c_i\} = 1$. Then pick $d \in \mathbb{Z}_{>0}$ such that $da_i \in \mathbb{Z}$ for all i, so that $df \in \mathbb{Z}[t]$ (e.g. let $d = \operatorname{lcm}\{c_0, \ldots, c_n\}$). Let $\tilde{f} = df$, so that $f\frac{1}{d}\tilde{f}$. Now consider $c = c(\tilde{f})$. Then $f' = \frac{1}{c}\tilde{f} = \frac{d}{c}f$ has content 1. Rearranging gives $f = \frac{c}{d}f'$, where $\alpha = \frac{c}{d} \in \mathbb{Q}_{>0}$ and $c(f') = 1$.

To show uniqueness, suppose that $f = \alpha g = \beta h$, where $\alpha, \beta \in \mathbb{Q}_{>0}$ and $g, g \in \mathbb{Z}[t]$ with content 1. Then $\alpha\beta^{-1}h = g \in \mathbb{Z}[t]$. But now write $\alpha\beta^{-1}$ as $\frac{m}{n}$, where $m, n \in \mathbb{Z}$ have highest common factor 1, so $mg = nh$. Assume that $m > 1$, then since m doesn't divide n, it must divide every coefficient in h. But h is primitive, and so $m = 1$, and similarly for $n = 1$. Thus also $g = h$.

The moreover part follows immediately from Gauss' Lemma: writing $f = \alpha f'$ and $g = \beta g'$ we see that $fg = (\alpha\beta)(f'g')$, and $c(f'g') = 1$, so that $c(fg) = \alpha\beta = c(f)c(g)$. □

LEMMA (5.4)
1. *Suppose that $f \in \mathbb{Z}[t] \subset \mathbb{Q}[t]$ is non zero, and that $f = gh$, where $g, h \in \mathbb{Q}[t]$. Then there exists $\alpha \in \mathbb{Q}$ such that $\alpha g, \frac{h}{\alpha} \in \mathbb{Z}[t]$. Thus $f = (\alpha g)(\frac{h}{\alpha})$ is a factorisation of f in $\mathbb{Z}[t]$.*

2. *Suppose that $f \in \mathbb{Q}[t]$ is irreducible and that $c(f) = 1$. The f is a prime element of $\mathbb{Z}[t]$.*

3. *Let $p \in \mathbb{Z}$ be a prime number. Then p is a prime element in $\mathbb{Z}[t]$.*

Proof.
1. By the above lemma, we may write $g = cg'$ and $h = dh'$, where $g', h' \in \mathbb{Z}[t]$ have content 1. Then $c(f) = cd$, so that, since $f \in \mathbb{Z}[t]$, we must have $cd \in \mathbb{Z}[t]$. Setting $\alpha = d$ we see that $f = (\alpha g)(\alpha^{-1}h) = cdg'h'$ is the required factorisation, with both factors lying in $\mathbb{Z}[t]$.

2. Note that if $f \in \mathbb{Q}[t]$ has content 1, then by definition $f \in \mathbb{Z}[t]$. To see that such an f is prime, we need to show that if $g, h \in \mathbb{Z}[t]$ are such that $f|gh$ in $\mathbb{Z}[t]$, then $f|g$ or $f|h$ in $\mathbb{Z}[t]$. Now, if $f|gh$ in $\mathbb{Z}[t]$ then it also does so in $\mathbb{Q}[t]$. Since $\mathbb{Q}[t]$ is a PID, irreducibles are prime, and so either $f|g$ or $f|h$, say $f|g$. Then we have that $g = fk$ for some $k \in \mathbb{Q}[t]$. By the above lemma, we may write $k = c(k)k'$, where $k' \in \mathbb{Z}[t]$. Moreover, by the same lemma, $c(h) = c(f)c(k) = c(k)$, and since $h \in \mathbb{Z}[t]$, so $c(h) = c(k) \in \mathbb{Z}[t]$, we have that $k \in \mathbb{Z}[t]$, so that $f|g$ in $\mathbb{Z}[t]$ as required.

3. The homomorphism $\phi_p \colon \mathbb{Z}[t] \to \mathbb{F}_p[t]$ has kernel $p\mathbb{Z}[t]$, and so, since $\mathbb{F}_p[t]$ is an ID, the ideal $p\mathbb{Z}[t]$ is prime, which is equivalent to saying that p is a prime element of $\mathbb{Z}[t]$.

□

THEOREM (5.5)
The ring $\mathbb{Z}[t]$ is a UFD.

Proof. Since $\mathbb{Z}[t]$ is an ID, we simply have to show that any element of $\mathbb{Z}[t]$ is a product of primes. Let $f \in \mathbb{Z}[t]$. We may write $f = af'$, where $c(f') = 1$, and since $\mathbb{Z}$ is a UFD we may factorise a into a product of prime elements of $\mathbb{Z}$, which we have just seen are also prime in $\mathbb{Z}[t]$. Thus we may assume that $c(f) = 1$. But then, by thinking

of f as an element of $\mathbb{Q}[t]$, we can write it as a product of prime elements in $\mathbb{Q}[t]$, say $f = p_1 p_2 \dots p_k$. Now each p_i can be written as $a_i q_i$, where $a_i \in \mathbb{Q}$ and $q_i \in \mathbb{Z}[t]$ with $c(q_i) = 1$. By the above lemma, each q_i is prime in $\mathbb{Z}[t]$ and $f = (a_1 \dots a_k) q_1 \dots q_k$. But then by comparing contents we see that $(a_1 \dots a_k)$ must be a unit in $\mathbb{Z}$, and so we are done. □

REMARK (5.6)
In summary: the primes in $\mathbb{Z}[t]$ are exactly either the primes in $\mathbb{Z}$ or the primes in $\mathbb{Q}[t]$ that have content 1.

Irreducibility of polynomials in $\mathbb{Q}[t]$

Here we now try to develop some techniques for showing that a polynomial $f \in \mathbb{Q}[t]$ is irreducible. By what we have done in the previous chapter, if $f \in \mathbb{Q}[t]$ is irreducible then we can write $f = c(f)g$, where $g \in \mathbb{Z}[t]$ has content 1 and is a prime in $\mathbb{Z}[t]$. Since f and g are associates in $\mathbb{Q}[t]$ it follows that to understand irreducible elements in $\mathbb{Q}[t]$ it is enough to understand prime elements in $\mathbb{Z}[t]$ of positive degree (or, equivalently, the irreducibles $f \in \mathbb{Q}[t]$ with content 1).

This is useful, since for any prime $p \in \mathbb{Z}$ we have the homomorphism $\phi_p \colon \mathbb{Z}[t] \to \mathbb{F}_p[t]$. This allows us to turn questions about factorisation in $\mathbb{Z}[t]$ into similar questions in $F_p[t]$: clearly if $f \in \mathbb{Z}[t]$ is reducible in $\mathbb{Z}[t]$ and its image in $\mathbb{F}_p[t]$ is non zero (which will always be the case if $c(f) = 1$, say), then it will be reducible in $\mathbb{F}_p[t]$.

EXAMPLE (6.1)
Suppose that $f = t^3 - 349t + 19 \in \mathbb{Z}[t]$. If f is reducible in $\mathbb{Q}[t]$, then it is reducible in $\mathbb{Z}[t]$, and hence its image under ϕ_p will also be reducible in $\mathbb{F}_p[t]$. But since f has degree 3 it follows that it is reducible if and only if it has a degree 1 factor, and similarly for its image in $\mathbb{F}_p[t]$. So it is enough to search for a root in $\mathbb{F}_p[t]$. By taking $p = 2$ we see that $\phi_2(f) = \bar{f} = t^3 + t + 1 \in \mathbb{F}_2[t]$, and so it's easy to check that $barf(0) = \bar{f}(1) = 1 \in \mathbb{F}_2$, and so $\bar{f}$ doesn't have a root, and so f must be irreducible in $\mathbb{Q}[t]$.

Note that the converse of the latter implication does not always hold though: t^2+1 is irreducible in $\mathbb{Z}[t]$ but in $\mathbb{F}_2[t]$ we have $t^2 + 1 = (t + 1)^2$.

LEMMA Eisenstein's Criterion: (6.2)
Suppose that $f \in \mathbb{Z}[t]$ and $f = t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0$. Then if there exists a prime $p \in \mathbb{Z}$ such that $p|a_i$ for all $0 \leqslant i \leqslant n-1$ but p^2 does not divide a_0 then f is irreducible in both $\mathbb{Z}[t]$ and $\mathbb{Q}[t]$.

Proof. Clearly $c(f) = 1$, so irreduciblibility in $\mathbb{Z}[t]$ and $\mathbb{Q}[t]$ are equivalent. Suppose that $f = gh$ were a factorisation of f in $\mathbb{Z}[t]$ where say $\deg(g) = k > 0$. Then we have $\phi_p(f) = \phi_p(g)\phi_p(h)$. By assumption, $\phi_p(f) = t^n$, hence, since $\mathbb{F}_p[t]$ is a UFD and t is irreducible, we must have $\phi_p(g) = t^k$ and $\phi_p(h) = t^{n-k}$. But then it follows that the constant terms of both g and h must be divisible by p, and hence a_0 must be divisible by p^2, contradicting our assumption. □

EXAMPLE (6.3)

Suppose that $p \in \mathbb{N}$ is prime, and $f = 1 + t + \ldots + t^{p-1} \in \mathbb{Z}[t]$. Then we claim that f is irreducible. Let $g = f(t+1)$. Then if g were reducible, say $g = h_1 h_2$, then it would follow that $f(t) = g(t-1) = h_1(t-1)h_2(t-1)$ be reducible, and similarly if g were irreducible so then would be f. Thus f is irreducible if and only if g is. But as $f = \frac{t^p-1}{t-1}$ we see that

$$g = \frac{(t+1)^p - 1}{t} = \sum_{i=0}^{p-1} \binom{p}{i+1}$$

Now it is easy to see that p divides $\binom{p}{i+1}$ for any $0 \leqslant i \leqslant p-2$, while the constant term $\binom{p}{1} = p$ is not divisible by p^2, so by Eisenstein's Criterion we see that g, and hence f, is irreducible.