Mathematics and Algorithms for Computer Algebra

Part 1 © 1992 Dr Francis J. Wright – CBPF, Rio de Janeiro

July 9, 2003

2a: Introduction to Abstract Algebra (continued)

1 Ideals and quotient rings

1.1 Quotient algebras

Homomorphic images provide simpler models of algebras, and quotient algebras provide a technique for constructing homomorphic images. The quotienting is by a congruence relation.

Definition 1 *A* congruence relation *E on an Ω-algebra A is an equivalence relation on A such that for any operation $\omega \in \Omega$ of arity n*

$$a_i \, E \, b_i \text{ for } i = 1, \ldots, n \;\Rightarrow\; \omega(a_1, \ldots, a_n) \, E \, \omega(b_1, \ldots, b_n).$$

That is, if the operands of any operator are equivalent then so are the corresponding values.

Example: Equivalence mod m on $\mathbb{Z}$ generalizes immediately to *congruence* mod m on an arbitrary commutative ring R, thus:

$$a \equiv_m b \iff a - b = km \iff m \,|\, (a - b), \quad a, b, k, m \in R.$$

Theorem 1 (Quotient algebras) *Let A be an Ω-algebra and E a congruence relation on A. Then:*

1. *the quotient set A/E is an Ω-algebra if $\omega \in \Omega$ is defined on A/E by*

$$\omega([a_1], \ldots, [a_n]) = [\omega(a_1, \ldots, a_n)]$$

(i.e. $\omega : A/E \to A/E$ maps equivalence classes to equivalence classes);

2. A/E is a homomorphic image of A under the natural map

$$\nu : a \mapsto [a].$$

Hence we have a source of homomorphic images. But do all homomorphic images of algebras have this form? Essentially, yes, as follows.

Lemma 2 *Let $\phi : A \to A'$ be a morphism of Ω-algebras. Then the kernel relation E_ϕ, defined by*

$$a\, E_\phi\, b \iff \phi(a) = \phi(b),$$

is a congruence relation on A.

Theorem 3 (Universal Isomorphism Theorem) *Let A and A' be Ω-algebras, with A' a homomorphic image of A under $\phi : A \to A'$. Then $A' \cong A/E_\phi$, where $\psi : [a] \mapsto \phi(a)$ is an isomorphism $A/E_\phi \to A'$, thus*

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "\substack{\nu :\\ a \mapsto [a]}"'] & A' \\
A/E_\phi \arrow[ur, "\psi : [a] \mapsto \phi(a)"'] &
\end{tikzcd}$$

[This is essentially the Decomposition Theorem for Functions applied to algebras instead of sets.]

1.2 Ideals

Let R be a ring. Then all homomorphic images of R are given up to isomorphism by quotient rings R/E for some congruence relation E on R. Ideals provide congruence relations.

Definition 2 *An* ideal *I in a ring R is a nonempty subset of R such that:*

1. $a, b \in I \;\Rightarrow\; a - b \in I$;

2. $a \in I,\; r \in R \;\Rightarrow\; ar, ra \in I$.

Requirement (1) makes I an additive subgroup of R. However:

Remark A proper ideal $I \subset R$ is not a subring because it does not contain 1_R. If $1_R \in I$ then $I = R$.

The equivalence relation E_I induced by I is defined by

$$a\,E_I\,b \iff a-b\in I.$$

This is also written as $a \equiv b \pmod I$ ("a is congruent to b mod I").

1.2.1 Principal ideals

If R is a commutative ring and $m \in R$ then

$$(m) = \{km \mid k \in R\}$$

is the smallest ideal of R containing m, called the principal ideal generated by m (principal because it is generated by a single element).

Examples: $(2) \subset \mathbb{Z}$ is the principal ideal of *even* integers, $\not\ni 1$; $(x) \subset R[x]$ is the principal ideal of all polynomials containing x as a factor, i.e. with zero constant term, $\not\ni 1$.

The equivalence relation $a\,E_{(m)}\,b \iff a-b \in (m)$ induced by (m) is the same as congruence mod m, $\equiv_m$, defined above, and is normally written "mod m" rather than "mod (m)".

1.2.2 Ideal generators

More generally, let $a_1, a_2, \ldots, a_n \in R$, a commutative ring. Then

$$(a_1, a_2, \ldots, a_n) = \{\textstyle\sum_{i=1}^n r_i a_i \mid r_i \in R\}$$

is the smallest ideal of R containing $\{a_i\}_{i=1}^n$, called the *ideal generated by* $\{a_i\}_{i=1}^n$. (It is principal iff $\exists b \in R$ such that $(a_1, a_2, \ldots, a_n) = (b)$.)

Theorem 4 *Let R be a ring and I an ideal in R. Then the equivalence relation E_I induced by I ($a\,E_I\,b \iff a-b\in I$) is a congruence relation on R.*

Hence ideals generate homomorphic images via their equivalence relations.

1.3 Quotient rings

First we need a notion from group theory.

Definition 3 *For any element a of a ring R regarded as an additive group and any additive subgroup I, the (left)* coset *of I by a is defined to be*

$$a + I = \{a + i \mid i \in I\}.$$

Since an additive group is commutative, the right coset $I + a = a + I$.

Denote by R/I ("R mod I") the set of all cosets of I by elements of R:

$$R/I = \{a + I \mid a \in R\}.$$

Because the coset $a + I$ is the same as the equivalence class $[a]_{E_I}$, R/I and R/E_I are just different notations for the same set.

Theorem 5 (Quotient rings) *Let I be an ideal in a ring R. Then*

1. *$R/I = R/E_I = \{a + I \mid a \in R\}$, the set of all additive cosets of I in R, is a quotient ring under the following "mod I" operations:*

$$\begin{aligned} (a+I)+(b+I) &= (a+b)+I, \\ -(a+I) &= -a+I, \\ 0_{R/I} &= 0_R + I = I, \\ (a+I)(b+I) &= ab+I, \\ 1_{R/I} &= 1_R + I; \end{aligned}$$

2. *R/I is a homomorphic image of R under the natural map $\nu : a \mapsto a+I$;*

3. *R/I is a ring (commutative if R is).*

Let us consider some examples.

1.3.1 The quotient ring $\mathbb{Z}/(m)$

This is identical to $\mathbb{Z}/{\equiv_m}$, and each element $a + (m)$ has a unique representative $r_m(a)$ in $\mathbb{Z}_m$.

1.3.2 The quotient ring $R[x]/(m(x))$

Let $m(x)$ be a polynomial in $R[x]$, R commutative (and assume $\deg m(x) > 0$). Then $(m(x))$ is an ideal in $R[x]$, and by the quotient ring theorem

$$R[x]/(m(x)) = \{a(x) + (m(x)) \mid a(x) \in R[x]\}$$

is a ring – the "quotient ring of polynomials mod $m(x)$" – and a homomorphic image of $R[x]$ under the (natural) map

$$a(x) \mapsto a(x) + (m(x)).$$

Moreover, $R[x]/(m(x))$ and $R[x]/\equiv_{m(x)}$ are the same sets and the coset $a(x) + (m(x)) \in R[x]/(m(x))$ is the equivalence class $[a(x)] \in R[x]/\equiv_{m(x)}$.

Each coset or equivalence class has a unique representative having degree $< \deg m(x)$, namely $r_{m(x)}(a(x))$, because:-

Theorem 6

1. *For any* $a(x) + (m(x)) \in R[x]/(m(x))$,

$$a(x) + (m(x)) = r_{m(x)}(a(x) + (m(x))).$$

2. *If* $\deg a(x), \deg b(x) < \deg m(x)$ *then*

$$a(x) \neq b(x) \;\Rightarrow\; a(x) + (m(x)) \neq b(x) + (m(x)).$$

Corollary 7 *If the number of elements in the set* R*, denoted* $|R|$*, is* k *and* $\deg m(x) = n$*, then*

$$|R[x]/(m(x))| = k^n$$

(whereas $|R[x]|$ *is infinite because there is no limit on the degrees of the polynomials in* $R[x]$*).*

1.3.3 The quotient ring $R[[x]]/(x^m)$

For fixed positive m,

$$\begin{aligned} a(x) \equiv_{x^m} b(x) \quad &\iff \quad a(x) - b(x) \in (x^m) \\ &\iff \quad a_i = b_i \;\; (i = 0, \ldots, m-1) \end{aligned}$$

and each element has a unique *polynomial* representative having degree $< m$.

1.4 Principal ideal domains

A *principal ideal domain* (PID) is an integral domain D in which every ideal I is principal, i.e. $I = (a) = \{ra \mid r \in D\}$ for some $a \in D$.

Examples: $\mathbb{Z}$, $F[x]$ and $F[[x]]$ are PIDs, but $F[x, y]$ is not, because (x, y) is not principal. More generally:

Theorem 8 *A Euclidean domain is a PID.*

Proof Let D be a Euclidean domain with degree function d, and let I be an ideal in D. If $I = \{0\}$ then I is the principal ideal (0), so assume $I \neq \{0\}$. Let $m \neq 0$ be an element of I having *minimum* degree; then we claim that $I = (m)$. $(m) \subseteq I$ trivially by the definition of ideal. To prove that $I \subseteq (m)$, perform a Euclidean division of any $a \in I$ by m to give

$$a = mq + r, \quad d(r) < d(m) \quad \text{or} \quad r = 0.$$

Then $a, m \in I \;\Rightarrow\; r = a - mq \in I$. But $d(r) \not< d(m)$ because m has minimum degree by assumption, so $r = 0 \;\Rightarrow\; a = mq \in (m)$. □

Generally in an integral domain D the generator of a principal ideal is determined only up to associates, i.e.

$$(a) = (b) \iff a \sim b,$$

because $a \in (m) \iff au \in (m)$ if u is a unit in D from the definition of ideal. Hence $\mathbb{Z}$ is a PID in which *every* ideal has the form (m) where $m \geq 0$ and $F[x]$ is a PID in which every ideal $\neq (0)$ has the form $(m(x))$ where $m(x))$ is monic, because both are Euclidean domains. Although $F[[x]]$ is not a Euclidean domain is can be proved to be a PID in a similar way to the proof for Euclidean domains, in which every ideal $\neq (0)$ has the form (x^m) for some $m \geq 0$.

Because any homomorphic image of a ring R must be isomorphic to R modulo an ideal, and a PID has only one class of ideals, the conclusion is that the *only* non-trivial homomorphic image of $\mathbb{Z}$ is $\mathbb{Z}_m$, of $F[x]$ is $F[x]_{m(x)}$ (polynomials mod $m(x)$) and of $F[[x]]$ is $F[[x]]_{x^m}$ (truncated power series under truncated arithmetic) – hence the importance of those image rings.

1.5 Simple rings

Any ring R has two *improper* ideals, the zero ideal $(0) = \{0\}$ and the unit ideal $(1) = R$, with corresponding *improper* homomorphic images

$$R/(0) \cong R \quad \text{and} \quad R/(1) \cong \{0\}$$

(and their isomorphs).

A ring whose only ideals are improper is called *simple*. It has no proper homomorphic images and so cannot be abstracted or further simplified.

Theorem 9 *Let R be a nontrivial commutative ring. Then*

$$R \textit{ is simple} \iff R \textit{ is a field.}$$

Proof

($\Leftarrow$) Let $I \neq (0)$ be an ideal in a field R. Then there exists $x \neq 0$ in I, hence $x^{-1}x = 1 \in I$, so $r1 \in I$ for all $r \in R \Rightarrow I = R$.

($\Rightarrow$) Let R be a simple ring and $x \neq 0$ be in R. Since $x \in (x)$, $(x) \neq (0)$. But R is simple, hence $(x) = R$ and so $1 \in (x)$. Thus $1 = ax$ for some $a \in R \Rightarrow a = x^{-1}$. □

Hence fields are trivial PIDs, since their only ideals are (0) and (1), and they have no proper homomorphic images. This means that fields cannot be modelled by homomorphic images, hence it is often preferable to work with rings that are not fields – for example, to regard elements of $\mathbb{Q}[x]$ as elements of $Q(\mathbb{Z}[x])$ with trivial denominators in $\mathbb{Z}$. Thus, to factorize a polynomial over $\mathbb{Q}$ express it as a quotient of a polynomial over $\mathbb{Z}$ and an integer, factorize the polynomial over $\mathbb{Z}$ by factorizing (several) homomorphic images of it and lifting back to $\mathbb{Z}$, and finally divide by the denominator to return to $\mathbb{Q}[x]$ (in some preferred way, e.g. with an overall numeric factor and monic polynomial factors).

Finally, it may be useful to know the following:

Theorem 10 *A PID is a gcd domain.*

1.6 Unital subrings

Whilst (0) is the smallest *ideal* in any ring R, the smallest *subring* is $[1] = [0]$. The nature of $[1]$ is determined by the *characteristic* of R as follows:

Theorem 11 *Let R be a ring. Then*

1. $[1] \cong \mathbb{Z}$ *if char* $R = 0$*;*
2. $[1] \cong \mathbb{Z}_m$ *if char* $R = m$*.*

1.7 Prime subfields

The smallest (with respect to inclusion) subfield of a field E is called the *prime subfield* of E, which can be proved always to exists and to be unique. It is determined by the characteristic of the field E as follows:

Theorem 12 *Let E be a field and P the prime subfield of E. Then*

1. $P \cong \mathbb{Z}_p$ *if char* $E = p$*;*

2. $P \cong \mathbb{Q}$ if char $E = 0$.

Note that p must be prime for E to be a (finite) field, hence the name "prime subfield", even though it is not entirely appropriate and "unital subfield" might be better, since P is the smallest subfield containing 1 (or 0).

1.8 Prime and maximal ideals

In this subsection R will always denote a commutative ring. A homomorphic image of R is isomorphic to a quotient ring R/I by an ideal I in R. So what kind of ideal I makes R/I (1) an integral domain, or (2) a field?

Definition 4 *An ideal P in R is* prime *if $ab \in P \;\Rightarrow\; a \in P$ or $b \in P$.*

This is motivated by the fact that if p is a prime in an integral domain then

$$p \,|\, ab \;\Rightarrow\; p \,|\, a \text{ or } p \,|\, b.$$

Example: (6) is not prime in $\mathbb{Z}$ because $3 \times 2 \in (6)$ but $3 \notin (6)$ and $2 \notin (6)$. However, (7) is prime because $ab \in (7) \;\Rightarrow\; 7 \,|\, ab \;\Rightarrow\; 7 \,|\, a$ or $7 \,|\, b$ (since 7 is prime), and hence either $a \in (7)$ or $b \in (7)$.

Definition 5 *An ideal M in R is* maximal *if $M \subset I \subset R$ for* no *ideal I in R.*

This is the largest non-trivial ideal in the ring.

Example: (x) is not maximal in $\mathbb{Z}[x]$ because $(x) \subset (x, 2) \subseteq \mathbb{Z}[x]$. However, $(x, 2)$ is maximal, as I will prove below.

Theorem 13 *R/P is an integral domain $\iff$ P is prime.*

Theorem 14 *R/M is a field $\iff$ M is maximal.*

Corollary 15 *A maximal ideal is a prime ideal.*

Proof A field is an integral domain, hence M maximal $\Rightarrow$ R/M is a field $\Rightarrow$ R/M is an integral domain $\Rightarrow$ M is prime. □

Example: Now we can prove that $(x, 2)$ is the maximal ideal in $\mathbb{Z}[x]$.

Proof We show that $\mathbb{Z}[x]/(x, 2)$ is a field and appeal to Theorem 14 above. To prove that $\mathbb{Z}[x]/(x, 2)$ is a field we use the Ring Isomorphism Theorem, which is the Universal Isomorphism Theorem for Ω-algebras given earlier specialized to rings, starting from the ring $\mathbb{Z}[x]$.

Consider the "0-evaluation mod 2" map

$$\phi : a(x) \mapsto r_2(a(0)),$$

which is easily shown to be an *epi*morphism: $\mathbb{Z}[x] \to \mathbb{Z}_2$. (In fact, ϕ is the composition of two familiar epimorphisms: 0-evaluation, $a(x) \mapsto a(0)$, and reduction mod 2, $b \mapsto r_2(b)$.) Then by the Ring Isomorphism Theorem

$$\mathbb{Z}[x]/\ker\phi \cong \mathbb{Z}_2,$$

and because $\mathbb{Z}_2$ is a field (2 is prime) so is $\mathbb{Z}[x]/\ker\phi$.

It remains to show that $\ker\phi = (x, 2)$.[1] By definition, $(x, 2) = \{rx + 2s \mid r, s \in \mathbb{Z}[x]\}$ and $\phi(rx + 2s) = r_2(2s(0)) = 0$, so $rx + 2s \in \ker\phi \Rightarrow (x, 2) \subseteq \ker\phi$.

On the other hand, if $a(x) = a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{Z}[x]$ then $\phi(a(x)) = r_2(a_0) = 0 \Rightarrow a_0 = 0 + 2k$, $k \in \mathbb{Z}$, so

$$\phi(a(x)) = 0 \Rightarrow a(x) = 2k + xr, \quad k \in \mathbb{Z},\ r \in \mathbb{Z}[x],$$

and hence

$$\ker\phi = \{rx + 2k \mid r \in \mathbb{Z}[x],\ k \in \mathbb{Z}\} \subseteq (x, 2).$$

Therefore $\ker\phi = (x, 2)$. □

Finally, we return to the connection between prime elements and prime ideals.

Theorem 16 *In any integral domain,*

$$(p) \text{ prime} \Rightarrow p \text{ prime}.$$

Corollary 17 *In an integral domain D,*

$$m \text{ composite} \Rightarrow D/(m) \text{ is a ring with zerodivisors}.$$

[1] The ring-theoretic definition of *kernel* is

$$\ker\phi = \{a \in R \mid \phi(a) = 0\},$$

which specializes the general set-theoretic definition.

Proof m composite $\Rightarrow$ (m) is not prime by Theorem 16 $\Rightarrow$ $D/(m)$ is not an integral domain by Theorem 13. □

Generally, the converse to Theorem 16 is false, but:-

Theorem 18 *In a PID (and hence in a Euclidean domain),*

$$p \text{ prime} \Rightarrow (p) \text{ maximal (and hence prime).}$$

Corollary 19 *In a PID,*

$$p \text{ prime} \Rightarrow D/(p) \text{ is a field.}$$

Proof Apply Theorem 18 and Theorem 14. □

Examples: $\mathbb{Z}$ and $F[x]$ are Euclidean domains and hence PIDs, so from Corollary 19:-

1. $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ is a field $\iff$ p is prime;
2. $F[x]/(m(x)) \cong F[x]$ is a field $\iff$ $m(x)$ is irreducible over F.

We knew (1) already; (2) is illustrated below.

$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is reducible over $\mathbb{R}$, so $\mathbb{R}[x]/(x^2 - 2)$ is *not* a field, and moreover not even an integral domain (from Corollary 17) – it can easily be shown explicitly to have zerodivisors as follows:

$$\mathbb{R}[x]/(x^2 - 2) \cong \mathbb{R}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{R}\},$$

where $\alpha^2 - 2 = 0$. Then

$$(\sqrt{2} + \alpha)(\sqrt{2} - \alpha) = 2 - \alpha^2 = 0$$

and we have constructed two zerodivisors.

However, $x^2 - 2$ is irreducible over $\mathbb{Q}$, so $\mathbb{Q}[x]/(x^2 - 2)$ *is* a field, in which inverse elements can easily be constructed explicitly as follows:

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Q}\},$$

where $\alpha^2 - 2 = 0$. Then

$$\begin{aligned} \frac{1}{a + b\alpha} &= \frac{1}{a + b\alpha} \cdot \frac{a - b\alpha}{a - b\alpha} = \frac{a - b\alpha}{a^2 - 2b^2} \quad (\text{since } \alpha^2 = 2) \\ &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\,\alpha \ \in \mathbb{Q}[\alpha]. \end{aligned}$$

Unfortunately, this technique of “rationalizing the denominator” works only for square roots, and not for modulus polynomials of degree > 2; in general the “extended gcd formula” must be used.

2 Extension fields

This section is essentially the theory of *irrational* quantities, i.e. how to represent and manipulate irrational numbers and more general irrational expressions, by building on what we already know about rational quantities.

F will denote a ground field and E an extension field of F, $E \geq F$.

2.1 Root adjunction

As an element of $\mathbb{Q}[x]$ the polynomial $x^3 - 2$ has no linear factors because it has no roots in $\mathbb{Q}$, and so it is irreducible over $\mathbb{Q}$. However, if the coefficient field $\mathbb{Q}$ is extended to $\mathbb{R}$ the polynomial is reducible. This suggests the general *root adjunction problem*:

> Given a field F and an irreducible polynomial $m(x)$ over F, extend F to a field E in which $m(x)$ has a root.

The following constructive solution, due to Kronecker (1823–1891), uses quotient rings.

Theorem 20 *Let $m(x)$ be an irreducible polynomial over F. Then $E = F[x]/(m(x))$ is an extension of F in which $m(x)$ has a root.*

This construction relies on the definition of arithmetic in a quotient ring, and before proving the theorem we need the following preliminary theory.

Lemma 21 *Let $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. Then in $R[x]/I$, where I is some ideal $(m(x))$, $a(x + I) = a(x) + I$.*

Proof Identifying $a_i \in R$ with the coset $a_i + I \in R[x]/I$, and using the definition of an ideal, gives

$$\begin{aligned}
a(x+I) &= (a_n + I)(x+I)^n + \cdots \\
&= (a_n x^n + I) + \cdots \\
&= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) + I \\
&= a(x) + I.
\end{aligned}$$

□

Then if $\alpha = x + I$, where $I = (m(x))$,

$$\begin{aligned} m(\alpha) &= m(x+I) \\ &= m(x)+I && \text{by the above lemma} \\ &= 0+I && \text{since } m(x) \in I \\ &= 0 \in R && \text{by agreed identification.} \end{aligned}$$

Proof of the theorem. $m(x)$ irreducible over $F \Rightarrow F[x]/(m(x))$ is a field (by Corollary 19). Identifying the coset $a+(m(x)) \in F[x]/(m(x))$ with $a \in F$ makes $F[x]/(m(x))$ an extension field of F. Finally, $\alpha = x + (m(x))$ is a root of $m(x)$ in $F[x]/(m(x))$. □

Remark This solution is formal, but it is no more formal than a solution such as $\sqrt{2}$.

Corollary 22 *Let $m(x)$ be an irreducible polynomial over a field F. Then $E = F[x]/(m(x))$ is an extension over which $m(x)$ has a linear factor (and hence over which $m(x)$ is reducible).*

Proof Apply the Factor Theorem. □

This construction puts the "obvious" way to extend a field by a root of a polynomial on a firm basis – we saw some examples at the end of the last section.

Theorem 23 *Let $f(x)$ be any polynomial over F having degree ≥ 1, where $f(x)$ need not be irreducible. Then F can be extended to a field E in which $f(x)$ has a root (and hence a linear factor).*

Proof Extend by a root of an irreducible factor of $f(x)$. □

Theorem 24 *Let $f(x)$ be a polynomial of degree ≥ 1 over a field F. Then F can be extended to a field E in which $f(x)$ has n roots.*

Proof Use induction on the degree of the polynomial. □

Definition 6 *A* root field *over F of a polynomial $f(x) \in F[x]$ is a field $E \geq F$ such that*

1. All *roots of $f(x)$ lie in E;*

2. E is the smallest extension of F that satisfies (1) (in that no proper subfield of E is an extension of F that contains all roots of $f(x)$.

Theorem 25 *Any polynomial $f(x) \in F[x]$ has a root field over F.*

Corollary 26 *A polynomial factors or "splits" into* linear *factors over its root field (hence a root field is also called a "splitting field").*

2.2 Analysis of simple extension fields

The smallest extension field of F that contains $\alpha \in E$ is denoted $F(\alpha)$ and called "F adjoined by α". $F(\alpha)$ is called *simple* because only one element is adjoined to F – one can also adjoin several elements to form the *multiple*, or *iterated*, extension $F(\alpha_1, \alpha_2, \ldots, \alpha_r)$, which is the smallest extension field of F that contains $\alpha_1, \alpha_2, \ldots, \alpha_r$. Multiple extension fields are important in the theory of integration, for example, but for many other purposes, for reasons that will be exlained later, simple extension fields suffice.

The following categorization of elements of extension fields is extremely important.

Definition 7 *Let $\alpha \in E \geq F$. Then α is called* algebraic over F *if α satisfies a* polynomial *equation over F, so that $f(\alpha) = 0$ for some $f(x) \in F[x]$; otherwise α is called* transcendental over F. *$F(\alpha)$ is called a (simple)* algebraic *or* transcendental *extension of F according to whether α is algebraic or transcendental over F.*

Examples: The classic (and default) setting is $F = \mathbb{Q}$, $E = \mathbb{C}$, and referring to a (complex) number as being "algebraic" or "transcendental" without qualification implies over $\mathbb{Q}$, thus:

1. $\sqrt[3]{2}$ is algebraic, because it is a root of $x^3 - 2 \in \mathbb{Q}[x]$;

2. $i = \sqrt{-1}$ is algebraic, because it is a root of $x^2 + 1 \in \mathbb{Q}[x]$;

3. $\sqrt[3]{2 + \sqrt{5}}$ is algebraic, because if $x = \sqrt[3]{2 + \sqrt{5}}$ then $x^3 = 2 + \sqrt{5}$ or $(x^3 - 2)^2 = 5$, so $x^6 - 4x^3 - 1 = 0$ over $\mathbb{Q}[x]$;

4. e and π are both transcendental, which is much harder to prove.

Generally, the ground field F should be specified, because (e.g.) e and π are both trivially algebraic over $\mathbb{R}$.

These notions can be generalized to functions, and the elementary functions log, exp, sin, etc. are referred to as *transcendental* functions. A function $\mathbb{R} \to \mathbb{R}$ is said to be *transcendental* if it is transcendental over the ring $P_{\mathbb{R}}$ of all polynomial functions $\mathbb{R} \to \mathbb{R}$. Thus $y = f(x) \in \mathbb{R}^{\mathbb{R}}$ is transcendental if it satisfies no polynomial of the form $a(x, y) = \sum_i a_i(x)y^i$, $a_i(x) \in \mathbb{R}[x]$; otherwise $f(x)$ is called an *algebraic* function. For example, $y(x) = \sqrt[3]{x^2 + 1}$ is clearly algebraic because $y^3 - x^2 - 1 = 0$, and so is $y(x) = 1/x$ because $xy - 1 = 0$, whereas proving that a function is transcendental is not so easy.

We are mainly interested in algebraic extension fields, which have the following useful characterization. Let $\alpha \in E$ be algebraic over F. Then we define the *minimum polynomial of α over F*, denoted $m_\alpha(x)$, to be the *monic* polynomial of smallest degree in $F[x]$ having α as a root.

Proposition 27 (Properties of the minimum polynomial) *Let $\alpha \in E$ have minimum polynomial $m_\alpha(x)$ over F. Then*

1. *$m_\alpha(x)$ is unique;*
2. *$m_\alpha(x)$ is irreducible over F;*
3. *for any $f(x) \in F[x]$, $f(x) = 0 \iff m_\alpha(x) \,|\, f(x)$.*

Proposition 28 (Characterization of minimum polynomial) *If $\alpha \in E$ is a root of a monic irreducible polynomial $m(x)$ over F then $m(x)$ is the minimum polynomial of α over F.*

Hence an irreducible polynomial over a field F is the minimum polynomial over F of any of its roots.

We have now seen *two* ways to construct extension fields: as quotients by ideals and as fields generated by elements. The two are related by the following:

Theorem 29 *Let $\alpha \in E$ be algebraic over $F \leq E$ with minimum polynomial $m_\alpha(x)$ over F. Then*

$$F(\alpha) \cong F[x]/(m_\alpha(x)).$$

Proof Use the Ring Isomorphism Theorem. □

Corollary 30 (Representation of $F(\alpha)$) *Let $\alpha \in E$ have minimum polynomial of degree n over F. Then each $\beta \in F(\alpha)$ can be uniquely represented in the form*

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_i \in F).$$

We have already seen this in a ring context. Note that since $m_\alpha(\alpha) = 0$ in $F(\alpha)$, arithmetic in $F(\alpha)$ is essentially polynomial arithmetic modulo $m_\alpha(\alpha)$, regarding α as an indeterminate (which it is not!).

Example: The minimum polynomial of $\mathbb{Q}(\sqrt[3]{2})$ is $x^3 - 2$, and

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2).$$

Each element $\beta \in \mathbb{Q}(\sqrt[3]{2})$ has a unique representation in the form

$$\beta = a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q}).$$

In particular, each $\beta \neq 0$ has an *inverse* expressible in the same form.

As a final remark about general extension fields, note the following:

Theorem 31 *Let $\alpha \in E$ be transcendental over $F \leq E$. Then*

$$F(\alpha) \cong F(x).$$

Hence whereas a simple algebraic extension of a finite field is finite, a simple transcendental extension of a finite field is infinite.

3 Finite fields

3.1 Cyclic property

The multiplicative group of a finite field is cyclic, which has some important practical consequences for the structure of finite fields. To prove this requires a little group theory, as follows.

Lemma 32 *Let a, b be elements of an abelian (multiplicative) group, and let their orders be $o(a) = m$, $o(b) = n$, where $\gcd(m, n) = 1$. Then $o(ab) = mn$.*

Proof Let $r = o(ab)$. Now $(ab)^{mn} = (a^m)^n(b^n)^m = 1.1 = 1$, so $r \leq mn$. In the other direction,

$$1 = \gcd(m, n) = sm + tn, \quad s, t \in \mathbb{Z}.$$

Hence

$$\begin{aligned} a^r &= (a^{sm+tn})^r \\ &= (a^m)^{sr}(a^n)^{tr} \\ &= (a^n)^{tr} && \text{since } o(a) = m \\ &= (a^n b^n)^{tr} && \text{since } o(b) = n \\ &= ((ab)^r)^{nt} \\ &= 1, \end{aligned}$$

so that $m \,|\, r$. Similarly, $n \,|\, r$, so $\gcd(m, n) = 1 \;\Rightarrow\; mn \,|\, r \;\Rightarrow\; mn \leq r$. Hence $r = o(ab) = mn$. □

Theorem 33 *Let G be a finite abelian (multiplicative) group and let m be the order of a maximal order element of G. Then the order of any element of G divides m.*

Proof Let $a \in G$ have maximal order m, and let $b \in G$ have order n. Assume to the contrary that $n \nmid m$. Then there must be some prime p in the prime power factorizations of m and n that occurs with higher power in n than in m, and thus

$$m = p^e q, \quad n = p^f r, \quad \text{where } f > e > 0,\ p \nmid q,\ p \nmid r.$$

Now $o(a^{p^e}) = q$ and $o(b^r) = p^f$ since $o(a) = m$ and $o(b) = n$. Then $o(a^{p^e} b^r) = p^f q$ by the above lemma, since $\gcd(p^f, q) = 1$. But $p^f q > m$, in contradiction to m being the maximal order of elements in G. Hence $n \,|\, m$. □

A cyclic group G is one generated by a single element, so that $G = [a]$ for *some* $a \in G$, i.e. $[a] = \{a^i \mid i \in \mathbb{Z}\}$. More precisely, if $n = o(a)$ and $\mathbb{Z}_\infty = \mathbb{Z}$ then $[a] = \{a^i \mid i \in \mathbb{Z}_n\}$, where $a^i \neq a^j$ if $i \neq j$ $(i, j \in \mathbb{Z}_n)$. Hence $o(a) = |[a]|$, i.e. the order of an element is the order of the cyclic subgroup that it generates.

Now we can state and prove the main theorem.

Theorem 34 *Let E be a finite field. Then E^*, the multiplicative group of E, is cyclic.*

Proof Let $|E| = r$, the *order* of E or number of elements in E, and let $\alpha \in E^*$ have maximal order m. Then we have to prove that $m = r-1 = |E^*|$.

By Lagrange's Theorem, the order of any element of E^* divides the order of E^*. Hence $m \,|\, (r-1)$, giving $m \leq (r-1)$.

In the other direction, consider the roots of $x^m - 1$ in E^*. For any $b \in E^*$, $o(b) = n$, we have $n \,|\, m$ by Theorem 33, so $m = kn$. Then $b^m = (b^n)^k = 1$, which makes every one of the $r - 1$ elements $b \in E^*$ a root of $x^m - 1$. But $x^m - 1$ has at most m distinct roots, hence $r - 1 \leq m$. □

Theorem 35 *Let $a \in G$ be an element of order n. Then $o(a^i) = n \iff \gcd(i, n) = 1$.*

Definition 8 *The Euler phi-function (or totient function) $\phi(n)$ is defined to be the number of positive integers $\leq n$ that are relatively prime to n, i.e. integers $1 \leq i < n$ such that $\gcd(i, n) = 1$, which always includes 1 and never includes n.*

For example, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$. Hence a cyclic group of order n has $\phi(n)$ distinct generators.

Definition 9 *A generator of the cyclic group E^* is called a* primitive element *of E.*

Hence any element of maximal order (i.e. $|E| - 1$) is primitive.

From the above group theory follows:

Theorem 36 *Let $|E| = r$. Then E has $\phi(r - 1)$ primitive elements. If $\alpha \in E^*$ is primitive then a^i is primitive if and only if $\gcd(i, r - 1) = 1$.*

Thus from one primitive element one can easily compute all of them, but unfortunately it is not easy in a large field to find one!

3.2 Finite fields as algebraic extensions

The cyclic property plays a major rôle in the behaviour of finite fields, e.g.

Lemma 37 *Let E be a finite field, $|E| = r$. Then any $\beta \in E^*$ is a root of $x^{r-1} - 1$ (over E).*

Proof For any $\beta \in E^*$, Lagrange's Theorem asserts that $k = o(\beta)$ divides $|E^*| = r - 1$. Hence $r - 1 = km$ for some $m \in \mathbb{Z}^+$, so $\beta^{r-1} = (\beta^k)^m = 1$. □

Theorem 38 *Let F be a finite field and E a finite extension field of F. Then any $\beta \in E$ is algebraic over F.*

Proof Let $|E| = r$. By Lemma 37 any $\beta \in E^*$ is a root of $x^{r-1} - 1 \in F[x]$, and $0 \in E$ is a root of $x \in F[x]$. □

The next theorem explains the importance of *simple* algebraic extensions:

Theorem 39 *Let F be a finite field and E any* finite *extension field of F, then E is a* simple algebraic *extension of F.*

Proof Since E is a *finite* field it contains a primitive element α. Since α generates E^* we have $E = F(\alpha)$. Therefore E is a *simple* extension of F, and hence by Theorem 38 a simple algebraic extension of F. □

It now follows from previous results that:-

Theorem 40 *Let F be a finite field and E a finite extension field of F. Then*

$$E \cong F[x]/(m_\alpha(x))$$

where $m_\alpha(x)$ is the minimum polynomial over F of a primitive element $\alpha \in E$.

Moreover, each $\beta \in E$ can be uniquely represented in the form

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_i \in F)$$

where $n = \deg m_\alpha(x)$. From this follows:

Corollary 41 *Let F be a finite field, $|F| = q$, and let E be a finite extension of F. Then $|E| = q^n$ for some positive integer n (namely, the degree of the minimum polynomial over F of a primitive element (generator) of E).*

We now make a distinguished choice of ground field F. We saw earlier that a field E of characteristic p has a unique prime (i.e. smallest) subfield isomorphic to $\mathbb{Z}_p$, namely its unital subring

$$[1] = \{0 \cdot 1_E, 1 \cdot 1_E, 2 \cdot 1_E, \ldots, (p-1) \cdot 1_E\}.$$

Identifying $a \cdot 1_E \in E$ with $a \in \mathbb{Z}_p$ $(0 \leq a < p)$ allows us to regard $\mathbb{Z}_p$ *itself* as the unique prime subfield of *any* field E of characteristic p. Applying Corollary 41 then leads to:

Theorem 42 *Any finite field has p^n elements for some prime p (the characteristic of the field) and positive integer n (the degree of the minimum polynomial over $\mathbb{Z}_p$ of any primitive element of the field).*

3.3 Galois fields

The notation $GF(q)$ ("Galois field of order q") is used to denote any finite field with q elements, where q must be a *prime power* p^n. The name honours the discoverer of finite fields, the French mathematician Evariste Galois, and anticipates the result that any two finite fields with the same number of elements are isomorphic.

3.3.1 Uniqueness of $GF(p^n)$

To prove this we need a few properties of irreducible polynomials over finite fields.

Lemma 43 *Let $a_1(x), a_2(x), \ldots, a_L(x) \in F[x]$ be distinct irreducible factors of $f(x) \in F[x]$; then*

$$\prod_{i=1}^{L} a_i(x) \mid f(x).$$

This follows essentially from the definition of irreducible (i.e. prime) factors.

Now with $q = p^n$, let $GF(q)$ be a given ground field and $GF(q^n)$ an extension of it, and let us determine the irreducible factorization of $x^{q^n} - 1$ over $GF(q^n)$ and $GF(q)$. We denote $q^n - 1$ by Q.

Proposition 44 *Let $GF(q^n)$ have distinct elements $\alpha_0 = 0, \alpha_1, \ldots, \alpha_Q$. Then over $GF(q^n)$, $x^Q - 1$ has the irreducible factorization*

$$x^Q - 1 = \prod_{i=1}^{Q} (x - \alpha_i).$$

Proof Each α_i is a root of $x^Q - 1$ by Lemma 37, hence by the Factor Theorem $x^Q - 1$ has a linear factor $x - \alpha_i$ for each $\alpha_i \in GF(q^n)^*$. Then by Lemma 43

$$x^Q - 1 = c(x) \prod_{i=1}^{Q} (x - \alpha_i).$$

In order for the degrees and leading coefficients to match we must have $c(x) = 1$. □

Proposition 45 *Let $m_1(x), \ldots, m_L(x)$ be distinct minimum polynomials over $GF(q)$ of the elements of $GF(q^n)^*$. Then over $GF(q)$, $x^Q - 1$ has the irreducible factorization*

$$x^Q - 1 = \prod_{i=1}^{L} m_i(x).$$

Proof Each $m_i(x)$ is the minimum polynomial over $GF(q)$ of some $\alpha \in GF(q^n)^*$, and this α is also a root of $x^Q - 1$. Hence $m_i(x) \,|\, x^Q - 1$ by the properties of a minimum polynomial. Then since each $m_i(x)$ is irreducible, $\prod_{i=1}^{L} m_i(x) \,|\, x^Q - 1$ by Lemma 43, so that

$$x^Q - 1 = c(x) \prod_{i=1}^{L} m_i(x).$$

Hence $\deg[\prod_i m_i(x)] \leq Q$. But each of the Q elements of $GF(q^n)^*$ is a root of some $m_i(x)$ and hence of $\prod_i m_i(x)$. Therefore $\deg[\prod_i m_i(x)] \geq Q$, and hence $\deg[\prod_i m_i(x)] = Q$ making $c(x)$ a constant, which must be 1 by equating leading coefficients because the $m_i(x)$ are all monic. □

Comparing the factorization of $x^Q - 1$ over both $GF(q^n)$ and $GF(q)$ leads to

Corollary 46 *Let $\alpha \in GF(q^n)$ have minimum polynomial $m_\alpha(x)$ over $GF(q)$. Then $m_\alpha(x)$ has distinct roots, all of which lie in $GF(q^n)$.*

Theorem 47 (Uniqueness of $GF(p^n)$)
Any two fields with p^n elements are isomorphic.

Proof Every field F includes a smallest *prime subfield* P, of which every extension field must contain a power of $|P|$ elements; hence $|P|$ is the smallest factor of $|F|$. Moreover, char F = char P. Hence if F is a field with p^n elements then F has characteristic p and is an extension field of $\mathbb{Z}_p$. By Proposition 45, $x^{p^n} - 1$ has the irreducible factorization over $\mathbb{Z}_p$

$$x^{p^n} - 1 = \prod_{i=1}^{L} m_i(x)$$

where the $m_i(x)$ are the distinct minimum polynomials over $\mathbb{Z}_p$ of the elements of F^*.

Choosing α to be a primitive element of F, we have

$$F = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(m_\alpha(x)).$$

Now suppose that F' is also a field with p^n elements, then $x^{p^n} - 1$ also has the irreducible factorization over $\mathbb{Z}_p$

$$x^{p^n} - 1 = \prod_{i=1}^{L'} m_i'(x)$$

where the $m_i'(x)$ are the distinct minimum polynomials over $\mathbb{Z}_p$ of the elements of F'^*. But by the uniqueness of prime factorization in the Euclidean domain $\mathbb{Z}_p[x]$ the set of factors $\{m_i(x)\}$ must be the same as $\{m_i'(x)\}$, and in particular $m_\alpha(x) = m_\beta(x)$ for some $\beta \in F'$ so that

$$\mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/(m_\alpha(x)).$$

Since $\mathbb{Z}_p[x]/(m_\alpha(x)) \cong F$ has p^n elements, so does the subfield $\mathbb{Z}_p(\beta)$ of F', and hence $\mathbb{Z}_p(\beta) = F'$. Therefore,

$$F = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(m_\alpha(x)) \cong \mathbb{Z}_p(\beta) = F',$$

and hence $F \cong F'$. □

3.3.2 Existence of $GF(p^n)$

Lemma 48 *In an integral domain of characteristic $p \neq 0$ (and hence p prime),*

$$(a+b)^p = a^p + b^p.$$

Proof By the binomial theorem,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k.$$

But for $1 \leq k \leq p-1$,

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}$$

contains p as a factor, for the following reason. Clearly the denominator divides the numerator, because the result is an integer. But the denominator cannot divide p because p is prime, so it must divide the remaining factor, and hence $\binom{p}{k} = mp$ for some positive integer m.

But for any x in an integral domain D of characteristic p,

$$mp \cdot x = m \cdot ((p \cdot 1_D)x) = m \cdot (0_D x) = m \cdot 0_D = 0_D.$$

Thus, every term in the binomial expansion vanishes except the first and last. □

Corollary 49 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Proof Use the previous lemma and induction on n. □

Armed with this result we can state and prove the final theorem in this introduction to abstract algebra:

Theorem 50 (Existence of $GF(p^n)$)
For every prime p and positive integer n there exists a field with p^n elements.

Proof Consider the polynomial $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. This polynomial has a root field, which is an extension E of $\mathbb{Z}_p$ that contains all the roots of $f(x)$ and is such that no proper subfield of E also contains all the roots of $f(x)$. We now show that E is a field of p^n elements.

By definition of root field, $f(x) = x^{p^n} - x$ has p^n roots, not necessarily distinct, in its root field E. But the derivative

$$f'(x) = p^n x^{p^n - 1} - 1 = -1 \neq 0$$

because E has characteristic p, and hence the p^n roots of $f(x)$ in E are in fact distinct.

Moreover, the roots form a field because they are a closed set under field operations. For example, if r_1, r_2 are roots of $f(x) = x^{p^n} - x$ then:

$$\begin{array}{rcll} f(r_1 + r_2) & = & (r_1 + r_2)^{p^n} - (r_1 + r_2) & \\ & = & r_1^{p^n} + r_2^{p^n} - (r_1 + r_2) & \text{by Corollary 49} \\ & = & r_1 + r_2 - (r_1 + r_2) & r_1, r_2 \text{ are roots of } x^{p^n} - x \\ & = & 0, & \end{array}$$

so $r_1 + r_2$ is also a root and the roots are closed under addition.

Thus the p^n roots of $f(x)$ themselves form a field, which clearly must be the root field E. Hence the root field of $x^{p^n} - x$ over $\mathbb{Z}_p$ is a field of p^n elements. □

4 Exercises

The assessed questions in this set of exercises are the last three.

1. Show that any congruence relation on $\mathbb{Z}$ with respect to addition is also a congruence relation with respect to multiplication. What about the converse?

2. Verify the claim that $\{\sum_{i=1}^{n} a_i r_i \mid r_i \in R\}$ is the smallest ideal containing $a_1, \ldots, a_n \in R$, where R is a commutative ring.

3. In an integral domain, prove that $(a) = (b) \iff a \sim b$ (where $\sim$ is the "associate" relation of differing by a factor of a unit).

4. Show that the ideal $(x, 2)$ in $\mathbb{Z}[x]$ is not principal (and hence that $\mathbb{Z}[x]$ is not a PID).

5. (*Simplicity of the matrix ring $M_n(F)$.*) Show that the ring $M_n(F)$ of all $n \times n$ matrices over a field F has no proper ideals. [*Hint*: Let $I \neq \{0\}$ contain a nonzero matrix $A = (a_{ij})$ with $a_{rs} \neq 0$. Now consider the product $a_{rs}^{-1} E_{ir} A E_{si}$ $(1 \leq i \leq n)$, where E_{ij} is the matrix with 1 in the (i, j) position and 0 elsewhere.]

6. Show that the ideal (x) is

(a) prime but not maximal in $\mathbb{Z}[x]$;

(b) maximal in $\mathbb{Q}[x]$.

7. Show that the following numbers are algebraic over $\mathbb{Q}$: (a) $\sqrt{2}i$, (b) $\sqrt[5]{1+\sqrt{3}}$, (c) $\sqrt{2}+\sqrt{3}$, (d) $\sqrt{2}+\sqrt[3]{2}$.

8. Let E be an extension field of F, $\alpha \in E$. Show that $F[\alpha] = F(\alpha)$. [Note that $F[\alpha]$ is the smallest extension *ring* containing α, whereas $F(\alpha)$ is the smallest extension *field* containing α.]

9. Show that for every positive integer n, a root field for the polynomial $x^n - 1$ over $\mathbb{Q}$ can be obtained as a simple algebraic extension of $\mathbb{Q}$. [*Hint*: Use your knowledge of complex numbers.]

10. Is $F(x) = F(x^2, x^3)$? Is $F(x) = F(x^4, x^6)$?

11. Find (by direct computation) all primitive elements of $\mathbb{Z}_{11}$.

12. ($**$ **Assessed** $**$)
For a commutative ring R show that the set of all polynomials in $R[x, y]$ with zero constant term is an ideal and show how to write it in terms of its minimal set of generators.

13. ($**$ **Assessed** $**$)
For each of the quotient rings $R[x]/(x^2 - 3)$ where (a) $R = \mathbb{Q}$ and (b) $R = \mathbb{Z}_7$ verify that it is a field, and find the inverse of the coset or equivalence class $[2 + 5x]$.

14. ($**$ **Assessed** $**$)
Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.