Math146 - Lecture notes

George McNinch

2025-03-28 09:31:23 EDT (george@valhalla)

Contents

1 Commutative rings

See [Stewart, chapter 16] [1] for general results about commutative rings.

1.1 Definitions

Definition 1.1.1. A ring R is an additive abelian group together with an operation of multiplication $R \times R \to R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*
- multiplication *distributes* over addition: for every $a, b, c \in R$ we have [2]

$$a(b + c) = ab + ac$$

and

$$(b + c)a = ba + ca$$

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity, i.e. if there is an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for every $a \in R$. [3]

In the course, we will consider (almost?) exclusively rings which are commutative and have identity.

Here are some examples of commutative rings:

Example 1.1.2. (a) $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$

(b) if X is a set and if R is a commutative ring, the set X^R of all R-valued functions on X can be viewed as a commutative ring in a natural way.

1.2 Polynomial rings

If R is a commutative ring, the collection of all polynomials in the variable T having coefficients in R is denoted $R[T]$.

Notice that the set of *monomials* $S = \{T^i \mid i \in \mathbb{N}\}$ has the following properties:

(M1) every element of $R[T]$ is an R-linear combination of elements of S. This just amounts to the statement that every polynomial $f(T) \in R[T]$ has the form

$$f(T) = \sum_{i=0}^{N} a_i T^i$$

for a suitable $N \geq 0$ and suitable coefficients $a_i \in R$.

[1] As noted in the course syllabus, Tisch library has an entry for this item here; click to find online access to the text *Galois Theory*, Ian Stewart. (CRC Press, 4th edition 2022).

[2] We often just denote multiplication by juxtaposition: i.e. we may write ab instead of $a \cdot b$ for $a, b \in R$

[3] Usually we write 1 for 1_R. The idea is that 1_R is the multiplicative identity of R. For example, the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity 1_R of the matrix ring $R = \mathrm{Mat}_2(\mathbf{R})$.

(M2) the elements of S are linearly independent i.e. if

$$\sum_{i=0}^{N} a_i T^i = 0 \quad \text{for} \quad a_i \in R,$$

then $a_i = 0$ for every i.

Polynomials in $R[T]$ can be added in a natural way. (This is just like adding vectors in a vector space).

And there is a product operation on polynomials, as follows:

if $f(T) = \sum_{i=0}^{N} a_i T^i$ and $g(T) = \sum_{i=0}^{M} b_i T^i$ then

$$f(T) \cdot g(T) = \sum_{i=0}^{N+M} c_i T^i \quad \text{where} \quad c_i = \sum_{s+t=i} a_s b_t.$$

Proposition 1.2.1. *$R[T]$ is a commutative ring with identity.*

2 Properties of rings

2.1 Ring Homomorphisms

Definition 2.1.1. If R and S are rings, a function $\phi : R \to S$ is called a *ring homomorphism* provided that

(a) ϕ is a homomorphism of *additive groups*,

(b) ϕ preserves multiplication; i.e. for all $x, y \in R$ we have $\phi(xy) = \phi(x)\phi(y)$, and

(c) $\phi(1_R) = 1_S$.

Definition 2.1.2. The *kernel* of the ring homomorphism $\phi : R \to S$ is given by

$$\ker \phi = \phi^{-1}(0) = \{x \in R \mid \phi(x) = 0\};$$

thus $\ker \phi$ is just the kernel of ϕ viewed as a homomorphism of additive groups.

Here are some properties of the kernel:

(K1) $\ker \phi$ is an additive subgroup of R

(K2) for every $r \in R$ and every $x \in \ker \phi$ we have $rx \in \ker \phi$.

2.2 Ideals of a ring

For simplicity suppose that the ring R (and S) are *commutative* rings.

Definition 2.2.1. A subset I of R is an *ideal* provided that

(a) I is an additive subgroup of R, and

(b) for every $r \in R$ and every $x \in I$ we have $rx \in I$.

We sometimes describe condition (b) by saying that "I is closed under multiplication by every element of R".

The proof of the following is immediate from definitions:

Proposition 2.2.2. *If $\phi : R \to S$ is a ring homomorphism , then* $\ker \phi$ *is an ideal of R.*

2.3 Quotient rings

Let R be a commutative ring and let I be an ideal of R.

Since I is a subgroup of the (abelian) additive group R, we may consider the quotient group R/I. Its elements are (additive) cosets $a + I$ for $a \in R$.

It follows from the definition of cosets that the $a + I = b + I$ if and only if $b - a \in I$.

The additive group can be made into a commutative ring by defining the multiplication as follows:

For $a + I, b + I \in R/I$ (so that $a, b \in R$), the product is given by

$$(a + I)(b + I) = ab + I.$$

In order to make this definition, one must confirm that this rule is well-defined. Namely, if we have equalities $a + I = a' + I$ and $b + I = b' + I$, we need to know that

$$(a + I)(b + I) = (a' + I)(b' + I).$$

Applying the definition, we see that we must confirm that

$$ab = I = a'b' + I.$$

For this, we need to argue that $a'b' - ab \in I$.

Since $a + I = a' + I$, we know that $a' - a = x \in I$ and since $b + I = b' + I$ we know that $b' - b = y \in I$.

Thus $a' = a + x$ and $b' = b + y$. Now we see that

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy$$

Since I is an ideal, we see that $ay, xb, xy \in I$ henc $ay + xb + xy \in I$. Now conclude that $a'b' + I = ab + I$ as required.

It is now straightforward to confirm that the ring axioms hold for the set R/I with these operations.

Proposition 2.3.1. *If I is an ideal of the commutative ring R, then R/I is a commutative ring with the addition and multiplication just described.*

2.4 Principal ideals

Definition 2.4.1. If R is a commutative ring and $a \in R$, the *principal ideal generated by a* – written Ra or $\langle a \rangle$ – is defined by

$$Ra = \langle a \rangle = \{ra \mid r \in R\}.$$

Proposition 2.4.2. *For $a \in R$, Ra is an* ideal *of R.*

Example 2.4.3. Let $n \in \mathbf{Z}_{>0}$ and consider the principal ideal $n\mathbf{Z}$ of the ring $\mathbf{Z}$ generated by $n \in \mathbf{Z}$.

As an additive group, $n\mathbf{Z}$ is the infinite cyclic group generated by n.

The quotient ring $\mathbf{Z}/n\mathbf{Z}$ is the finite commutative ring with n elements; these elements are precisely the *congruence classes* of integers modulo n.

2.5 Isomorphism Theorem

Theorem 2.5.1. *Let R, S be commutative rings with identity and let $\phi : R \to S$ be a ring homomorphism. Assume that ϕ is* surjective *(i.e.* onto*). Then ϕ determines an isomorphism $\overline{\phi} : R/I \to S$ where $I = \ker \phi$, where $\overline{\phi}$ is determined by the rule*

$$\overline{\phi}(a + I) = \phi(a) \quad \textit{for } a \in R.$$

Proof. First, you must confirm that $\overline{\phi}$ is *well-defined*; i.e. that if $a + I = a' + I$ then $\overline{\phi}(a + I) = \overline{\phi}(a' + I)$.

Next, you must confirm that $\overline{\phi}$ is a ring homomorphism (this is immediate from the definition of ring operations on R/I).

Finally, you must confirm that $\ker \overline{\phi} = \{0\}$, where here 0 refers to the additive identity of the quotient ring R/I. This additive identity is of course the trivial coset $I = 0 + I \in R/I$. □

2.6 A Homorphism from the polynomial ring to the scalars

Let F is a field and let $a \in F$. consider the mapping

$$\Phi : F[T] \to F$$

given by $\Phi(f(T)) = f(a)$. Namely, applying Φ to a polynomial $f(T)$ results in the value $f(a)$ of $f(T)$ at a.

The definition of multiplication in $F[T]$ guarantees that Φ is a ring homomorphism.

3 Polynomials over a field and the division algorithm

3.1 Some general notions for commutative rings

Definition 3.1.1. If R is a commutative ring with 1 and if $u \in R$ we say that u is a *unit* - or that u is *invertible* - provided that there is $v \in R$ with $uv = 1$; then $v = u^{-1}$.

We write $R^\times$ for the units in R.

A commutative ring R is a *field* provided that every non-zero element is invertible. Thus R is a field if $R^\times = R \setminus \{0\}$.

Proposition 3.1.2. *If R is a commutative, then $R^\times$ is an abelian group (with operation the multiplication in R).*

For any commutative ring R and elements $a, b \in R$ we say that a **divides** b – written $a \mid b$ – if $\exists x \in R$ with $ax = b$.

Proposition 3.1.3. *For $a, b \in R$ we have $a \mid b$ if and only if $b \in \langle a \rangle$.*

Recall that we introduced the principal ideal $\langle a \rangle = aR$ for any commutative ring R and any $a \in R$. In fact, given $a_1, \cdots, a_n \in R$ we can consider the ideal

$$\langle a_1, \cdots, a_n \rangle = \sum_{i=1}^{n} a_i R$$

defined as

$$\langle a_1, \cdots, a_n \rangle = \left\{ \sum_{i=1}^{n} r_i a_i | r_i \in R \right\}.$$

It is straightforward to check that $\langle a_1, \cdots, a_n \rangle$ is indeed an ideal of R.

Definition 3.1.4. A non-zero element $a \in R$ is said to be a *0-divisor* provided that there is $0 \neq b \in R$ with $ab = 0$.

Example 3.1.5. Let n be a composite positive integer, so that $n = ij$ for integers $i, j > 0$. Consider the elements $[i] = i + n\mathbf{Z}$, $[j] = j + n\mathbf{Z}$ in the quotient ring $\mathbf{Z}/n\mathbf{Z}$.

Then $[i]$ and $[j]$ are both non-zero since $0 < i, j < n$ so that $n \nmid i$ and $n \nmid j$. But $[i] \cdot [j] = [n] = 0$ so that $[i]$ and $[j]$ are 0-divisors of the ring $\mathbf{Z}/n\mathbf{Z}$.

Definition 3.1.6. A commutative ring R is said to be an *integral domain* provided that it has no zero-divisors.

Example 3.1.7. (a) Any field is an integral domain.

(b) The ring $\mathbf{Z}$ of integers is an integral domain.

(c) Any subring of an integral domain is an integral domain.

For example, the ring $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ of gaussian integers is an integral domain.

(d) $\mathbf{Z}/n\mathbf{Z}$ is not an integral domain whenever n is composite.

(e) If R and S are commutative rings, the direct product $R \times S$ is *never* an integral domain. Indeed, the elements $(1, 0)$ and $(0, 1)$ are 0-divisors.

Lemma 3.1.8. ***(Cancellation)*** *Let R be an integral domain and let $a, b, c, \in R$ with $c \neq 0$. If $ac = bc$ then $a = b$.*

Proof. The equation $ac = bc$ implies that $ac - bc = 0$ so that $(a - b)c = 0$ by the distributive property. Since R has no zero divisors and since $c \neq 0$ by assumption, conclude that $a - b = 0$ i.e. that $a = b$. $\square$

Proposition 3.1.9. *Let R be an integral domain and let $d, d' \in R \setminus \{0\}$. If $\langle d \rangle = \langle d' \rangle$ then d and d' are associate.*

Proof. Since $d \in \langle d \rangle$ we may write $d = xd'$ and since $d' \in \langle d \rangle$ we may write $d' = yd$. Now we see that $d = xd' = xyd$. Since $d \neq 0$ cancellation (Lemma 3.1.8) implies that $xy = 1$. Thus $x, y \in R^\times$ and indeed d, d' are associate. $\square$

3.2 An important result on polynomial rings

Proposition 3.2.1. *Let R and S be rings, let $\phi : R \to S$ be a ring homomorphism, and let $\alpha \in S$ be an element. There is a unique ring homomorphism*

$$\Psi : R[T] \to S$$

such that $\Psi(T) = \alpha$ and such that $\Psi_{|R} = \phi$.

Proof. Let $f, g \in R[T]$, say

$$f = \sum_{i=0}^{n} a_i T^i \quad \text{and} \quad g = \sum_{i=0}^{m} b_i T^i$$

be elements of $R[T]$.

To see that Ψ is an additive homomorphism, note that $f + g = \sum_{i=0}^{\max(n,m)} (a_i + b_i) T^i$ so that

$$\Psi(f + g) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\alpha^i = \sum_{i=0}^{n} a_i \alpha^i + \sum_{i=0}^{m} b_i \alpha^i = \Psi(f) + \Psi(g)$$

Similarly, to see that Ψ is multiplicative, note that $fg = \sum_{i=0}^{n+m} c_i T^i$ where $c_i = \sum_{s+t=i} a_s b_t$. Now,

$$\Psi(fg) = \sum_{i=0}^{n+m} \phi(c_i)\alpha^i = \left(\sum_{i=0}^{n} \phi(a_i)\alpha^i \right) \left(\sum_{i=0}^{m} \phi(b_i)\alpha^i \right) = \Psi(f) \cdot \Psi(g)$$

$\square$

3.3 The degree of a polynomial

Let F be a field and consider the ring of polynomials $F[T]$.

Definition 3.3.1. The *degree* of a polynomial $f = f(T) \in F[T]$ is defined to be $\deg(f) = -\infty$ if $f = 0$, and otherwise $\deg(f) = n$ where

$$f = \sum_{i=0}^{n} a_i T^i \quad \text{with each } a_i \in F \text{ and } a_n \neq 0.$$

We have some easy and familiar properties of the degree function:

Proposition 3.3.2. *Let $f, g \in F[T]$.*

(a) $\deg(fg) = \deg(f) + \deg(g)$.

(b) $\deg(f + g) \le \max\{\deg(f), \deg(g)\}$ *and equality holds if* $\deg(f) \ne \deg(g)$.

(c) $f \in F[T]^\times$ *if and only if* $\deg(f) = 0$. *In particular,* $F[T]^\times = F^\times$.

Corollary 3.3.3. *For a field F, the polynomial ring $F[T]$ is an integral domain.*

Proof. Let $f, g \in F[T]$ and suppose that $fg = 0$. We must argue that either $f = 0$ or $g = 0$. $\square$

Proposition 3.3.4. *Let $f, g \in F[T]$. If $g \ne 0$ and $\deg g < \deg f$ then $[g] = g + \langle f \rangle$ is a non-zero element of $F[T]/\langle f \rangle$.*

3.4 The division algorithm

Theorem 3.4.1. *Let F be a field, and let $f, g \in F[T]$ with $0 \ne g$. Then there are polynomials $q, r \in F[T]$ for which*

$$f = qg + r$$

and $\deg r < \deg g$.

Proof. First note that we may suppose f to be non-zero. Indeed, if $f = 0$, we just take $q = r = 0$. Clearly $f = qg + r$, and $\deg(r) = -\infty < \deg(g)$ since g is non-zero.

We now proceed by induction on $\deg(f) \ge 0$.

For the base case in which $\deg(f) = 0$, we note that $f = c$ is a constant polynomial; here $c \in F^\times$.

If $\deg(g) = 0$ as well, then $g = d \in F^\times$ and then $c = (c/d)d + 0$ so we may take $q = c/d$ and $r = 0$. Now $\deg(r) = -\infty < \deg(g)$ as required.

If $\deg(g) > 0$, we simply take $q = 0$ and $r = f$: we then have $f = 0 \cdot g + f$ and $\deg(f) = 0 < \deg(g)$ as required.

We have now confirmed the Theorem holds when $\deg(f) = 0$.

Proceeding with the induction, we now suppose $n > 0$ and that the Theorem holds whenever f has degree $< n$. We must prove the Theorem holds when f has degree n.

Since f has degree n, we may write $f = a_n T^n + f_0$ where $a_n \in F^\times$ and $f_0 \in F[T]$ has $\deg(f_0) < n$.

Let us write $g = \deg(g)$; we may write $g = b_m T^m + g_0$ where $b_m \in F^\times$ and $g_0 \in F[T]$ has $\deg(g_0) < m$.

If $n < m$ we take $q = 0$ and $r = f$ to find that $f = qg + r$ and $\deg(r) < \deg(g)$.

Finally, if $m \le n$ we set

$$f_1 = f - (a_n/b_m)T^{n-m}g = a_n T^n + f_0 - \left(\frac{a_n}{b_m} b_m T^n + \frac{a_n}{b_m} T^{n-m} g_0\right) = f_0 - \frac{a_n}{b_m} T^{n-m} g_0.$$

We have $\deg(f_0) < n$ by assumption, and $\deg\left(\frac{a_n}{b_m} T^{n-m} g_0\right) < n$ by the Proposition together with the fact that $\deg(g_0) < m$.

Thus $\deg(f_1) < n$. Now we apply the induction hypothesis to write

$$f_1 = q_1 g + r_1 \quad \text{with } \deg(r_1) < \deg(g).$$

Finally, we have

$$f = f_1 + (a_n/b_m)T^{n-m}g = q_1 g + r_1 + (a_n/b_m)T^{n-m}g = \left(q_1 + (a_n/b_m)T^{n-m}\right) g + r_1$$

so we have indeed written $f = qg + r$ in the required form. $\square$

Corollary 3.4.2. *Let F be a field and let $f \in F[T]$. For $a \in F$, there is a polynomial $q \in F[T]$ for which*

$$f = q(T - a) + f(a).$$

Corollary 3.4.3. *For $f \in F[T]$ an element $a \in F$ is a* root *of the polynomial f if and only if $T - a \mid f$ in $F[T]$. In particular, if $d = \deg(f)$, f has no more than d distinct roots in F.*

Proof. The first statement is clear from Corollary 3.4.2. Now consider the distinct roots $\alpha_1, \cdots, \alpha_e \in F$ of f. Then $T - \alpha_1$ divides f so that $f = (T - \alpha_1)f_1$ for some $f_1 \in F[T]$. Since α_2 is a root of f we see that

$$0 = f(\alpha_2) = (\alpha_2 - \alpha_1)f_1(\alpha_2)$$

which shows that α_2 is a root of f_1 since $\alpha_1 \neq \alpha_2$. Thus we find that

$$f = (T - \alpha_1)(T - \alpha_2)f_2$$

for some $f_2 \in F[T]$. Continuing in this way we find that $\prod_{i=1}^{e}(T - \alpha_i)$ divides f, so that $e \leq \deg f$ by Proposition 3.3.2. $\square$

4 Ideals of the polynomial ring

4.1 Ideals of the polynomial ring $F[T]$

Corollary 4.1.1. *Let F be a field and let I be an ideal of the ring $F[T]$. Then I is a principal ideal; i.e. there is $g \in I$ for which*

$$I = \langle g \rangle = g \cdot F[T].$$

Proof. If $I = \{0\}$ [4] the results is immediate. Thus we may suppose $I \neq 0$.

Consider the set $\{\deg(g) | 0 \neq g \in I\}$. This is a non-empty set of natural numbers, hence it contains a minimal element by the **well-ordering principle**.

Choose $g \in I$ such that $\deg(g)$ is this minimal degree; we claim that $I = \langle g \rangle$.

Clearly $\langle g \rangle \subseteq I$. To complete the proof, it remains to establish the inclusion $I \subseteq \langle g \rangle$. Let $f \in I$ and use the **Division Algorithm** to write $f = qg + r$ for $q, r \in F[T]$ with $\deg r < \deg g$.

Observe that $f - qg \in I$ so that $r \in I$. Since $\deg r < \deg g$ conclude that $r = 0$. This shows that $f = qg \in \langle g \rangle$ as required, completing the proof. □

Let F be a field, $F[T]$ be the ring of polynomials with coefficients in F, let $f, g \in F[T]$ be polynomials which are not both 0.

Definition 4.1.2. The **greatest common divisor** $\gcd(f, g)$ of the pair f, g is a monic polynomial d such that

(a) $d \mid f$ and $d \mid g$,

(b) if $e \in F[T]$ satisfies $e \mid f$ and $e \mid g$, then $e \mid d$.

Remark 4.1.3. If d, d' are two gcds of f, g then $d \mid d'$ and $d' \mid d$. In particular, $\deg(d) = \deg(d')$ and $d' = \alpha d$ for some $\alpha \in F^{\times}$. It is then clear that there is no more than one monic polynomial satisfying i. and ii.

Proposition 4.1.4. *Let $f, g \in F[T]$ not both 0* [5].

(a) $\langle f, g \rangle$ is an ideal. According to the previous

corollary, there is a monic polynomial $d \in F[T]$ with

$$\langle d \rangle = \langle f, g \rangle.$$

Then $d = \gcd(f, g)$

(b) In particular, $d = \gcd(f, g)$ may be written in the form $d = uf + vg$ for $u, v \in F[T]$.

Proof. For a., write $I = \langle f, g \rangle = \langle d \rangle$. Since $f, g \in I$, the definition of $\langle d \rangle$ shows that $d \mid f$ and $d \mid g$.

Now suppose that $e \in F[T]$ and that $e \mid f$ and $e \mid g$. Then $f, g \in \langle e \rangle$ which shows that $\langle f, g \rangle \subseteq \langle e \rangle$.

But this implies that $\langle d \rangle \subset \langle e \rangle$ so that $e \mid d$ as required. Thus we see that d is indeed equal to $\gcd(f, g)$.

Since $d \in \langle d \rangle = \langle f, g \rangle$, assertion b. follows from the definition of $\langle f, g \rangle$. □

[4] We will write simply 0 for the ideal $\{0\}$.

[5] Note that f, g are not both 0 if and only if the ideal $\langle f, g \rangle$ is not 0.

4.2 Principal ideal domains (PIDs)

Definition 4.2.1. An integral domain R is said to be a **principal ideal domain** (abbreviated PID) provided that every ideal I of R has the form

$$I = \langle a \rangle \quad \text{for some } a \in R;$$

i.e. provided that every ideal of R is principal.

Example 4.2.2. (a) The ring $\mathbf{Z}$ of integers is a PID.

(b) For any field F, the ring $F[T]$ of polynomials is a PID - this follows from the Corollary to the divison algorithm, above.

(c) The rings $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{2}]$ are PIDs – to see this one can argue that these rings are Euclidean domains and then one proves that any Euclidean domain is a PID.

4.3 PIDs and greatest common divisors

Let R be a PID.

The results about gcd in the polynomial ring proved in Section 4.1 actually hold in the generality of the PID R. We quickly give the statements:

Definition 4.3.1. Let $a, b \in R$ such that $\langle a, b \rangle \neq 0$. A gcd of a and b is an element $d \in R$ such that

(i) $d \mid a$ and $d \mid b$ (in words: "d is a common divisor of a and b")

(ii) if $e \mid a$ and $e \mid b$ then $e \mid d$. (in words: "any common divisor of a and b divides d")

Lemma 4.3.2. *If R is a PID and if d and d' are* gcd*s of a and b then d and d' are associates.*

Proof. This follows from Proposition 3.1.9 □

Proof. Using the definition of gcd we see that $d \mid d'$ and $d' \mid d$. Thus $d' = dv$ and $d = d'u$ for $u, v \in R$.

This shows that $d' = dv = d'uv$. Using cancellation, find that $1 = uv$ so that $u, v \in R^\times$. □

Remark 4.3.3. This definition of course covers the cases when $R = \mathbf{Z}$ and when $R = F[T]$. The main thing to point out is that when $R = \mathbf{Z}$, there is a unique **positive** gcd for any pair $a, b \in \mathbf{Z}$ and when $R = F[T]$ there is a unique **monic** gcd for any pair $f, g \in F[T]$.

For a general PID there need not be a natural choice of gcd, so for $x, y \in R$ we can only speak of $\gcd(x, y)$ up to multiplication by a unit of R.

Proposition 4.3.4. *Let R be a PID and let $x, y \in R$ with $\langle x, y \rangle \neq 0$.*

(a) Since R is a PID, we may write find $d \in R$ with

$$\langle d \rangle = \langle x, y \rangle.$$

Then $d = \gcd(x, y)$.

(b) In particular, $d = \gcd(x, y)$ may be written in the form $d = ux + vv$ for $u, v \in R$.

To prove Proposition 4.3.4 proceed as in the proof of Proposition 4.1.4.

Proposition 4.3.5. *Let R be a PID and let $a, b \in R$ not both 0. Put $d = \gcd(a, b)$, so that $\frac{a}{d}, \frac{b}{d} \in R$. Then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. According to Proposition 4.3.4 (b), we may write $d = ax + by$ for suitable $x, y \in R$. Since $d \mid a$ we know that $\frac{a}{d} \in R$; similarly $\frac{b}{d} \in R$. We now see that

$$d = d\frac{a}{d}x + d\frac{b}{d}y = d\left(\frac{a}{d}x + \frac{b}{d}y\right);$$

now applying *cancellation* – i.e. Lemma 3.1.8 – we conclude that

$$1 = \frac{a}{d}x + \frac{b}{d}y.$$

This shows that $1 \in \left\langle \frac{a}{d}, \frac{b}{d} \right\rangle$, the ideal generated by $\frac{a}{d}$ and $\frac{b}{d}$. But this implies that $R \subset \left\langle \frac{a}{d}, \frac{b}{d} \right\rangle$ so that $\langle 1 \rangle = R = \left\langle \frac{a}{d}, \frac{b}{d} \right\rangle$. According to Proposition 4.3.4 this proves that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ as required. ☐

5 Prime elements and unique factorization

5.1 Irreducible elements

Let R be a principal ideal domain.

Definition 5.1.1. A non-zero element $p \in R$ is said to be *irreducible* provided that $p \notin R^\times$ and whenever $p = xy$ for $x, y \in R$ then either $x \in R^\times$ or $y \in R^\times$.

Remark 5.1.2. Assume that $p, a \in R$ with p irreducible. Then either $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

Proposition 5.1.3. *$p \in R$ is irreducible if and only if ($\clubsuit$): whenever $a, b \in R$ and $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Proof. ($\Rightarrow$): Assume that p is irreducible, suppose that $a, b \in R$ and that $p \mid ab$. We must show that $p \mid a$ or $p \mid b$.

For this, we may as well suppose that $p \nmid a$; we must then prove that $p \mid b$. Since $p \nmid a$, we see that $\gcd(a, p) = 1$ by the Remark above. Then $ua + vp = 1$ for elements $u, v \in R$.

Now we see that

$$b = 1 \cdot b = (ua + vp) \cdot b = uab + vpb.$$

Since $p \mid ab$ we see that $p \mid uab + vpb$ which proves that $p \mid b$, as required.

($\Leftarrow$): Assume that condition ($\clubsuit$) holds for p. We must show that p is irreducible. For this, assume $p = xy$ for $x, y \in R$; we must show that either $x \in R^\times$ or $y \in R^\times$.

Since $p = xy$, in particular $p \mid xy$ and we may apply ($\clubsuit$) to conclude without loss of generality that $p \mid x$.

Write $x = pa$. We now see that $p = xy = pay$; by cancellation, find that $1 = ay$ so that $y \in R^\times$. We conclude that p is irreducible, as required. $\square$

Remark 5.1.4. For any integral domain R, we can speak of *irreducible elements* defined as in Definition 5.1.1. And we can speak of *prime elements*, where an element $p \in R$ is *prime* if it satisfies condition ($\clubsuit$) of Proposition 5.1.3. In this language, Proposition 5.1.3 shows that in a PID, an element is prime iff it is irreducible.

Corollary 5.1.5. *Let R be a PID, let $p, a_1, \cdots, a_n \in R$ with p prime, and suppose that $p \mid a_1 a_2 \cdots a_n = \prod_{i=1}^n a_i$. Then $p \mid a_i$ for some $1 \le i \le n$.*

Example 5.1.6. Let F a field and let $f \in F[T]$ be a non-constant polynomial; i.e. $\deg(f) > 0$. If f is reducible there are polynomials $g, h \in F[T]$ for which $f = gh$ and $\deg(g), \deg(h) > 0$.

Example 5.1.7. If $f \in F[T]$ is reducible (i.e. not irreducible) then the quotient ring $F[T]/\langle f \rangle$ is not an integral domain.

Indeed, write $f = gh$ for $g, h \in F[T]$ non-units. Thus $\deg f > \deg g, \deg h > 0$ by Proposition 3.3.2. According to Proposition 3.3.4, the classes $[g], [h] \in F[T]$ are non-zero, but $[g] \cdot [h] = [f] = 0$ Thus $F[T]/\langle f \rangle$ has zero divisors and is not an integral domain.

5.2 Unique factorization in a PID

The Fundamental Theorem of Arithmetic says that any integer $n > 1$ may factored uniquely as a product of primes. This result holds for any PID, as follows:

Theorem 5.2.1. *Let R be a PID, let $0 \neq a \in R$, and suppose that a is not a unit.*

(a) There are irreducible elements $p_1, p_2, \cdots, p_n \in R$ such that $a = p_1 \cdot p_2 \cdots p_n$.

(b) if $q_1, \cdots, q_m \in R$ are irreducibles such that $a = q_1 \cdots q_m$ then $n = m$ and – after possibly reordering the q_i – there are units $u_i \in R^\times$ for which $q_i = u_i p_i$ for each i.

Proof. We first prove (a). For this, we first prove the following claim:

($*$): if the conclusion of (a) fails, there is a sequence of elements $a_1, a_2, \cdots \in R \setminus R^\times$ with the property that for each $i \geq 1$ we have: (i) $a_{i+1} \mid a_i$ and (ii) a_{i+1} and a_i are not associate.

To prove ($*$), let $x_1 = a$. Now suppose we have found elements $a_1, a_2, \cdots, a_n$ such that for each $1 \leq i \leq n$ conditions (i) and (ii) hold, and such that the conclusion of (a) fails for a_n. In particular, a_n is reducible, so we may write $a_n = xy$ with $x, y \in R$ and $x, y \notin R^\times$. Without loss of generality, we may suppose that the conclusion of (a) fails for x and we set $a_{n+1} = x$. By construction, $a_{n+1} \mid a_n$; moreover a_{n+1} and a_n are not associates. Thus we have proved by induction that ($*$) holds.

To prove (a), we will now show that ($*$) leads to a contradiction.

Let $\{a_i\}$ be a sequence of elements as in ($*$) and let I be given by

$$I = \bigcup_{i \geq 1} \langle a_i \rangle.$$

Since

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \cdots$$

it is straightforward to see that I is an ideal. Since R is a PID, we may write $I = \langle d \rangle$ for some $d \in R$. By the definition of I, we may find an index N for which $d \in \langle a_j \rangle$ for each $j \geq N$.

Fix $j \geq N$. We may write $d = x \cdot a_j$ for $x \in R$.

On the other hand, $\langle a_j \rangle \subseteq \langle d \rangle$, we we may write $a_j = y \cdot d$ for $y \in R$.

We now see that $d = x \cdot a_j = xyd$ so that $x, y \in R^\times$ by cancellation (Lemma 3.1.8). Thus d and a_j are *associates* so that $\langle d \rangle = \langle a_j \rangle$. In particular, we have proved that

$$\langle d \rangle = \langle a_N \rangle = \langle a_{N+1} \rangle = \langle a_{N+2} \rangle = \cdots$$

contradicting the assumption (ii) that a_{j+1} and a_j are not associates. This contradiction proves (a).

We now prove (b). We are given an equality

$$p_1 \cdots p_n = q_1 \cdots q_m$$

with p_i, q_j irreducible and $n, m \geq 1$.

We proceed by induction on the minimum $\min(n, m)$, and without loss of generality we suppose that $n \leq m$ so that $n = \min(n, m)$.

In case $n = 1$, our assumption is $p_1 = q_1 \cdots q_m$. Applying Corollary 5.1.5 we see that $p_i \mid q_j$ for some $1 \leq j \leq m$. Since p_i and q_j are irreducible, we see that $q_j = u \cdot p_1$ for some unit $u \in R^\times$ Thus

$$p_1 = u \cdot p_1 \cdot \prod_{i \neq j} q_i.$$

Applying cancellation (Lemma 3.1.8) we see $u \cdot \prod_{i \neq j} q_i = 1$ so that $q_i \in R^\times$ for $i \neq j$. Thus $m = 1$ and p_1 and q_1 are associates, as required. This confirms the base-case of the induction.

Now suppose that $n > 1$ and that the result is known when the element has an expression as a product of $< n$ irreducibles.

Thus we have

$$p_1 \cdots p_n = q_1 \cdots q_m$$

and $m \geq n$. Now $p_n \mid q_1 \cdots q_m$ and as before we see for some $1 \leq j \leq m$ that $q_j = up_n$ for a unit $u \in R^\times$. Without loss of generality we may suppose that $j = m$. We find

$$p_1 \cdots p_{n-1} \cdot p_n = u \cdot p_n \cdot q_1 \cdots q_{m-1}$$

Applying cancellation (Lemma 3.1.8) we find that

$$p_1 \cdots p_{n-1} = uq_1 \cdots q_{m-1}$$

Replacing q_1 by the irreducible uq_1, we can view the right-hand side as a product of $m-1$ irreducibles. Since $m-1 \geq n-1$ we may apply the induction hypothesis to find that $m-1 = n-1$ and that after re-ordering we have p_i associate to q_i for $1 \leq i \leq m-1$. Since p_n and q_m are associate as well, this proves (b). □

6 The Field of fractions of an Integral Domain

Recall Example 3.1.7 that any subring of a field is an integral domain. We now want to argue that the *converse* to this statement is true, as well. Namely, an integral domain R is a subring of a field. In fact, we are essentially going to give a *construction* of such a field from R.

Let's fix an integral domain R. To confirm the suggested converse to the above Corollary, we must construct a field F and an inclusion $i : R \subset F$.

Of course, if we have such a mapping i, then for any $0 \neq b \in R$, the element $i(b)$ is non-zero in F and hence $i(b)^{-1} = \dfrac{1}{i(b)}$ should be an element of F (even though $i(b)^{-1}$ is possibly not an element of R). For any $a \in R$ we should be able to multiply $i(a)$ and $\dfrac{1}{i(b)}$ in F to form the *fraction* $\dfrac{i(a)}{i(b)}$. If we choose to identify R with the image $i(R)$, we might simply write $\dfrac{a}{b} = \dfrac{i(a)}{i(b)}$ for this *fraction*.

So if the field F *exists*, it must contain all fractions $\dfrac{a}{b}$ for $a, b \in R$ with $0 \neq b$.

In fact, we are going to construct a field F by formally introducing such fractions.

Consider the set $W = \{(a, b) \mid a, b \in R, b \neq 0\}$ and define a relation $\sim$ on the set W by the condition

$$(a, b) \sim (s, t) \iff at = bs.$$

This relation is motivated by the observation that for *fractions* in a field F we have

$$\frac{a}{b} = \frac{s}{t} \iff at = bs.$$

One needs to check the following:

Proposition 6.0.1. $\sim$ *defines an* equivalence relation *on* W*.*

Proof. We must confirm properties of $\sim$:

(*reflexive*) if $(a, b) \in W$, then $ab = ba \implies (a, b) \sim (a, b)$.

(*symmetric*) if $(a, b), (s, t) \in W$ then

$$(a, b) \sim (s, t) \implies at = bs \implies sb = ta \implies (s, t) \sim (a, b).$$

(*transitive*) Let $(a, b), (s, t), (u, v) \in W$ and suppose that $(a, b) \sim (s, t)$ and $(s, t) \sim (u, v)$. The assumptions mean that $at = bs$ and $sv = tu$.

Multiplying the equation $at = bs$ by v on each side, we see that

$$atv = bsv \implies atv = btu \implies (av)t = (bu)t;$$

since $t \neq 0$ and since the cancellation law holds in an integral domain – see Lemma 3.1.8, conclude $av = bu$. Hence $(a, b) \sim (u, v)$ which confirms the transitive law.

$\square$

We are now going to show that the fractions - i.e. the equivalence classes in W – form a field. We define $Q = Q(R)$ to be the set of equivalence classes of W under the equivalence relation $\sim$.

We write $\dfrac{a}{b} = [(a,b)]$ for the equivalence class of $(a,b) \in W$. Thus Q is the set of (formal) fractions of elements of R, and

$$\frac{a}{b} = \frac{s}{t} \iff (a,b) \sim (s,t) \iff at = bs$$

It remains to argue that Q has the structure of a field. To do this, we must define binary operations $+$ and $\cdot$ on the set Q and check that they satisfy the correct axioms.

Define addition of fractions: for $a, b, s, t \in R$ with $b, t \neq 0$,

$$(\clubsuit) \quad \frac{a}{b} + \frac{s}{t} = \frac{at + bs}{bt}.$$

And define multiplication of fractions:

$$(\diamondsuit) \quad \frac{a}{b} \cdot \frac{s}{t} = \frac{as}{bt}.$$

Theorem 6.0.2. *For an integral domain R, the set $Q(R)$ of fractions of R forms a field with the indicated addition and multiplication.*

Sketch of proof. What must be checked??

- must first confirm that $(\clubsuit)$ is *well-defined*! i.e. if $a', b', s', t' \in R$ with $\dfrac{a}{b} = \dfrac{a'}{b'}$ and $\dfrac{s}{t} = \dfrac{s'}{t'}$, we must check that $\dfrac{a}{b} + \dfrac{s}{t} = \dfrac{a'}{b'} + \dfrac{s'}{t'}$; i.e. that

  $$\frac{at + bs}{bt} = \frac{a't' + b's'}{b't'}.$$

  This is straightforward if a bit tedious.

- One readily checks that $0 = \dfrac{0}{1}$ is an identity for the binary operation $+$ on Q.
- One readily checks that $+$ is commutative for Q.
- One readily checks that $\dfrac{-a}{b}$ is an additive inverse for $\dfrac{a}{b}$.
- With some more effort, one confirms that $+$ is *associative* on Q; i.e. for $\alpha, \beta, \gamma \in Q$

  $$(\alpha + \beta) + \gamma) = \alpha + (\beta + \gamma).$$

Thus $(Q, +)$ is an abelian group. Now consider the operation $\diamondsuit)$ of multiplication.

- must again confirm that $(\diamondsuit)$ is *well-defined*! i.e. if $a', b', s', t' \in R$ with $\dfrac{a}{b} = \dfrac{a'}{b'}$ and $\dfrac{s}{t} = \dfrac{s'}{t'}$, we must check that $\dfrac{a}{b} \cdot \dfrac{s}{t} = \dfrac{a'}{b'} \cdot \dfrac{s'}{t'}$; i.e. that

  $$\frac{as}{bt} = \frac{a's'}{b't'}.$$

- One readily checks that $1 = \frac{1}{1}$ is an identity for the binary operation $\cdot$ on Q.
- One readily checks that $\cdot$ is commutative for Q.
- With some more effort, one confirms that $\cdot$ is *associative* on Q; i.e. for $\alpha, \beta, \gamma \in Q$

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

- Next, one must confirm the *distributive law*: for $\alpha, \beta, \gamma \in Q$,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

Phew! $\square$

Remark 6.0.3. Despite the details of the preceding proof, all that is happening is confirming properties of operations of fractions that you have used since grade-school...

Now, we want to emphasize a crucial property of the field of fractions of an integral domain.

Let $Q(R)$ be the field constructed above, and note that there is a natural ring homomorphism $i : R \to Q(R)$ given by $r \mapsto i(r) = \frac{r}{1}$ for $r \in R$. This homomorphism is one-to-one: indeed, if $\frac{r}{1} = 0 = \frac{0}{1}$, then $r \cdot 1 = 0 \cdot 1 \implies r = 0$. Thus, we may identify R with a subring of $Q(R)$.

Proposition 6.0.4. *Let R be an integral domain, let $\phi : R \to S$ be any ring homomorphism, and suppose that for all $0 \neq d \in R$, $\phi(d) \in S^\times$ - i.e. $\phi(d)$ is a* unit *in S. Then there is a unique homomorphism $\widetilde{\phi} : Q(R) \to S$ with the property that $\widetilde{\phi}_{|R} = \phi$.*

Proof. Let $x \in Q(R)$ be any element. Thus $x = \frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b}$ for $a, b \in R$ with $b \neq 0$.

Let's first argue that uniqueness of $\widetilde{\phi}$. If $\widetilde{\phi}$ is a ring homomorphism, then

$$1 = \widetilde{\phi}(1) = \widetilde{\phi}(b \cdot \frac{1}{b}) = \phi(b)\widetilde{\phi}(\frac{1}{b}) \implies \widetilde{\phi}(\frac{1}{b}) = \phi(b)^{-1}$$

Since $\widetilde{\phi}$ is a ring homomorphism, we must have

$$(\clubsuit) \quad \widetilde{\phi}(x) = \widetilde{\phi}(\frac{a}{1})\widetilde{\phi}(\frac{1}{b}) = \phi(a) \cdot \phi(b)^{-1}$$

which confirms the uniqueness.

It now only remains to check that the rule ($\clubsuit$) determines a ring homomorphism, which is straightforward. $\square$

Example 6.0.5. The field of rational functions

Let F be a field, and consider $R = F[T]$ the ring of polynomials. This is in integral domain, and its field of fractions $Q(R)$ is usually written $F(T)$ and is known as the field of rational functions over F.

Note that

$$F(T) = \left\{ \frac{f}{g} \mid f, g \in F[T], g \neq 0 \right\};$$

thus elements of $F(T)$ are fractions $\frac{f}{g}$ whose numerator and denominator are *polynomials*; we usually call such expressions *rational functions*.

7 Irreducible polynomials over a field

7.1 Fields as quotient rings

Proposition 7.1.1. *Let R be a PID and let $p \in R$ be an irreducible element. Then the quotient ring $A = R/\langle p \rangle$ is a field.*

Proof. Let $\alpha \in A$ be non-zero. To prove that A is a field, we must show that α has a multiplicative inverse. Thus α has the form $h + \langle p \rangle$ and since $\alpha \neq 0$ we know that $p \nmid h$. Since p is irreducible, Remark 5.1.2 shows that $\gcd(p, h) = 1$.

Thus according to Proposition 4.3.4 there are elements $x, y \in R$ for which

$$1 = xp + yh$$

Let $\beta = y + \langle p \rangle \in A$. Then

$$\alpha\beta = yh + \langle p \rangle = 1 + \langle p$$

since $yh \equiv 1 \pmod{p}$. Thus β is the multiplicative inverse of α in A. □

Example 7.1.2.

- $\mathbf{Z}/p\mathbf{Z}$ is a field for a prime number p.

As a special case of Proposition 7.1.1, we have:

Corollary 7.1.3. *Let F be a field and let f be an irreducible polynomial in $F[T]$. Then $A = F[T]/\langle f \rangle$ is a field.*

For small degree polynomials, one can confirm irreducibility just by considering roots, as follows:

Proposition 7.1.4. *Let F be a field and let $f \in F[T]$ be a polynomial with $\deg(f) \leq 3$. If f has no root in F then f is irreducible.*

Proof. Suppose that f is reducible, say $f = gh$ with $\deg(g), \deg(h) > 0$. Since $\deg(f) \leq 3$ and since $\deg(g) + \deg(h) = \deg(f)$ by Proposition 3.3.2, we see that at least one of g or h must have degree 1; without loss of generality we suppose $\deg(g) = 1$.

Thus $g = aT + b$ for $a, b \in F$ with $a \neq 0$. Set $\alpha = \dfrac{-b}{a} \in F$ and observe that $f(\alpha) = g(\alpha)h(\alpha) = 0$; thus f has the root $\alpha \in F$. □

Example 7.1.5. Let p be a prime number. Then the polynomial $T^2 - p \in \mathbf{Q}[T]$ is *irreducible*. In particular,

$$\mathbf{Q}(\sqrt{p}) = \mathbf{Q}[T]/\langle T^2 - p \rangle$$

is a field.

7.2 The rational roots test

Theorem 7.2.1. *Let R be a PID with field of fractions F and let $f \in R[T]$, say*

$$f = a_0 + a_1 T + \cdots + a_n T^n$$

with $a_i \in R$ and $a_n \neq 0$.

If $\alpha = \dfrac{x}{y} \in F$ is a root of f for $x, y \in R$ and $y \neq 0$ and $\gcd(x, y) = 1$ then $x \mid a_0$ and $y \mid a_n$.

Proof. Since α is a root of f we have the equation

$$0 = f(\alpha) = a_0 + a_1\left(\frac{x}{y}\right) + \cdots + a_n\left(\frac{x}{y}\right)^n = \sum_{i=0}^{n} a_i\left(\frac{x}{y}\right)^i$$

in the field F. Multiplying by the non-zero element $y^n \in R$ we find the equation

$$0 = a_0y^n + a_1xy^{n-1} + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^iy^{n-i}$$

in R.

Thus we see that

$$a_0y^n = -(a_1xy^{n-1} + \cdots + a_nx^n) = -\sum_{i=1}^{n} a_ix^iy^{n-i} = -x\sum_{i=1}^{n} a_ix^{i-1}y^{n-i}$$

which shows that $x \mid a_0y^n$. Since $\gcd(x, y) = 1$ also $\gcd(x, y^n) = 1$. Now conclude that $x \mid a_0$.

Similarly, we see that

$$a_nx^n = -\sum_{i=0}^{n-1} a_ix^iy^{n-i} = -y\sum_{i=0}^{n-1} a_ix_iy^{n-i-1}$$

which shows that $y \mid a_nx^n$. Since $\gcd(x^n, y) = 1$ we conclude that $y \mid a_n$ as required. □

Remark 7.2.2. Let $f = \sum_{i=0}^{n} a_iT^i \in R[T]$ as in the statement of Theorem 7.2.1. According to theorem, to find a root of f in the field of fractions F of R, we must consider all fractions $\alpha = \frac{x}{y}$ where $\gcd(x, y) = 1$, where x is a divisor of a_0 and where y is a divisor of a_n.

Writing $a_0 = p1p_2 \cdots p_n$ and $a_n = q_1q_2 \cdots q_m$ for irreducibles p_i and q_j, we see that it is possible in principle to make a list of all possible α and then check for each candidate whether or note α is a root of f.

Example 7.2.3. Consider the polynomial $f = T^3 - 3T^2 + 2T - 6 \in \mathbf{Z}[T]$. For any root $\alpha = \frac{x}{y} \in \mathbf{Q}$ with $\gcd(x, y) = 1$ we must have that $x \mid 6$ and $y \mid 1$. Thus according to Theorem 7.2.1, the possible rational roots are $\alpha = \pm 1, \pm 2, \pm 3, \pm 6$.

Notice that if $x \in \mathbf{R}$ is negative, then $f(x) < 0$. Thus the possible rational roots are simple $\alpha = 1, 2, 3, 6$. We notice that $f(1) = -6$, $f(2) = -6$ and $f(3) = 0$. Using the division algorithm we see that

$$T^3 - 3T^2 + 2T - 6 = (T^2 + 2)(T - 3)$$

It is now clear that 6 is not a root and that $T^2 + 2$ is irreducible. We f has exactly one rational root, namely $\alpha = 3$.

7.3 The Gauss Lemma

Let R be a PID with field of fractions F. The polynomial ring $R[T]$ is the subring of $F[T]$ consisting of polynomials whose coefficients lie in R. In particular $R[T]$ is itself an integral domain.

Remark 7.3.1. Note that in the case where R is *already* a polynomial ring $F[X]$, we introduce a *new* variable T different from X.

Definition 7.3.2. The *content* content$(f)$of the element $f = \sum_{i=0}^{N} a_i T^i \in R[T]$ where $a_i \in R$ is defined to be

$$\text{content}(f) = \gcd(a_0, a_1, \cdots, a_N).$$

We say that the polynomial $f \in R[T]$ is *primitive* if content$(f) = 1$.

Lemma 7.3.3. *Let $f \in R[T]$ be a non-zero polynomial and let $c = \text{content}(f) \in R$. Then f may be written $f = cf_0$ where $f_0 \in R[T]$ is primitive.*

Proof. Write $f = \sum_{i=0}^{n} a_i T^i$ with $a_i \in R$. Then by definition we have $c = \gcd(a_0, \cdots, a_n)$. Note that $c \mid a_i$ for each i; we write $b_i = \dfrac{a_i}{c} \in R$.

We set $f_0 = \sum_{i=0}^{n} b_i T^i \in R[T]$ and notice that

$$c \cdot f_0 = \sum_{i=0}^{n} c \cdot b_i T^i = \sum_{i=0}^{n} a_i T^i = f$$

as required. Finally,

$$\text{content}(f_0) = \gcd(b_0, \cdots, b_n) = \gcd\left(\frac{a_0}{c}, \cdots, \frac{a_n}{c}\right) = 1$$

by Proposition 4.3.5. Thus f_0 is indeed primitive. $\square$

Lemma 7.3.4. *Let $p \in R$ be irreducible and consider the assignment*

$$h \mapsto \overline{h} : R[T] \to (R/\langle p \rangle)[T]$$

defined as follows: for $h = \sum_{i=0}^{N} c_i T^i \in R[T]$ with $c_i \in R$, the polynomial $\overline{h} \in (R/\langle p \rangle)[T]$ is given by

$$\overline{h} = \sum_{i=0}^{N} [c_i] T^i$$

where $[c_i] = c_i + pR$ is the class of c_i modulo pR.

(a) This assignment is a ring homomorphism.

(b) For $h \in R[T]$, $\overline{h} = 0$ if and only if $p \mid \text{content}(h)$.

Proof. (a) follows from Proposition 3.2.1. For (b), just observe that $\overline{h} = 0$ if and only if $p \mid c_i$ for every i. $\square$

Proposition 7.3.5. *("The Gauss Lemma") If $f, g \in R[T]$ are primitive, then the product fg is primitive.*

Proof. Suppose on the contrary that there are primitive polynomials $f, g \in R[T]$ for which fg is not primitive. Writing $d = \text{content}(fg)$ for the content of the product, we know that $\langle d \rangle \neq R$ so that d is divisible by some prime $p \in R$.

Consider the ring homomorphism $h \mapsto \overline{h}$ of Lemma 7.3.4.

Now, $p \mid \text{content}(fg) \implies 0 = \overline{fg} = \overline{f} \cdot \overline{g}$. Since R/pR is a field, the ring $(R/pR)[T]$ is an integral domain, so we may conclude that either $\overline{f} = 0$ or $\overline{g} = 0$.

But according to Lemma 7.3.4 (b), $\overline{f} = 0 \implies p \mid \text{content}(f)$ and $\overline{g} = 0 \implies p \mid \text{content}(g)$. This contradicts our assumption that $1 = \text{content}(f) = \text{content}(g)$. Thus indeed content$(fg) = 1$. $\square$

Theorem 7.3.6. *Suppose that $f \in R[T]$ is a primitive polynomial, and that $g, h \in K[T]$ are polynomials for which $f = gh$ in $K[T]$. Then there are polynomials $g_1, h_1 \in R[T]$ with $\deg g = \deg g_1$ and $\deg h = \deg h_1$ for which $f = g_1 h_1$ in $R[T]$.*

Proof. Using Lemma 7.3.3, we may write $g = \dfrac{x}{y} g_1$ and $h = \dfrac{z}{w} h_1$ where $g_1, h_1 \in R[T]$ are *primitive* and $x, y, z, w \in R$ with $y, w \neq 0$. We now see that

$$(\heartsuit) \quad yw \cdot f = xz \cdot g_1 h_1.$$

Since f is primitive, notice that $yw = \text{content}(ywf)$. Moreover,the Gauss Lemma – i.e. Proposition 7.3.5 – shows that $g_1 h_1$ is primitive; thus, we have $\text{content}(xzg_1h_1) = xz$.

It follows that

$$\langle yw \rangle = \langle xz \rangle$$

i.e. that ($\clubsuit$) $\quad u \cdot yw = xz$ for a unit $u \in R^\times$ – see Proposition 3.1.9.

But then ($\heartsuit$) and ($\clubsuit$) together show that $yw \cdot f = u \cdot yw \cdot g_1 h_1$ and now the cancellation law Lemma 3.1.8 in the integral domain $R[T]$ implies $f = (ug_1) \cdot h_1$ which proves the Theorem. □

7.4 Eisenstein's irreducibility criterion

Theorem 7.4.1. *Let $p \in R$ be irreducible, and let*

$$f = \sum_{i=0}^{n} a_i T^i \in R[T], \quad (\textit{where } a_i \in R,\ 0 \le i \le n)$$

be a polynomial with $a_n \neq 0$. Suppose that $p \nmid a_n$, that $p \mid a_i$ for $0 \le i \le n-1$ and that $p^2 \nmid a_0$. Then f is irreducible when viewed as an element of $F[T]$.

Proof. Let $c = \text{content}(f)$. Then $c \not\equiv 0 \pmod p$ since $p \nmid a_n$. Observe now that the polynomial $\widetilde{f} = \dfrac{1}{c} f \in R[T]$ still satisfies the assumptions of the Theorem. Since $\widetilde{f}$ is irreducible in $K[T]$ if and only if the same is true for f, it suffices to prove the Theorem when $f = \widetilde{f}$ is primitive.

Now, according to Theorem 7.3.6 the irreducibility of $f \in F[T]$ will follow once we show that if $f = gh$ for $g, h \in R[T]$ then either $\deg g = 0$ or $\deg h = 0$. So suppose $f = gh$ for $g, h \in R[T]$.

Consider the ring homomorphism $f \mapsto \overline{f} : R[T] \to (R/pR)[T]$ as in Lemma 7.3.4. Assumptions on the coefficients a_i show $\overline{f} = \overline{g}\overline{h}$ to be a non-zero multiple of T^n. Using unique factorization in the principal ideal domain $(R/pR)[T]$, it follows that $\overline{g}$ is a non-zero multiple of T^i and $\overline{h}$ is a non-zero multiple of T^j where $i + j = n$ and $0 \le i, j \le n$. Moreover $i = \deg g$ and $j = \deg h$.

Now the Theorem follows since if $i, j > 0$ then p divides the constant term of both g and h, and then $p^2 \mid a_0$ contradicting our assumption. □

Example 7.4.2. (a) Let p be a prime integer, let $n \ge 1$ and let $f = T^n - p$. Then Theorem 7.4.1 shows that $f \in \mathbf{Q}[T]$ is irreducible.

(b) Let K be a field and consider the ring $K[X]$ of polynomials over K. The field of fractions of $K[X]$ is the field $F = K(X)$ of rational functions.

Let $n \ge 1$ and consider the polynomial $f = T^n - X \in F[T] = K(X)[T]$. Then f is irreducible in $K(X)[T]$ by Theorem 7.4.1.

7.5 Irreducibility of certain cyclotomic polynomials

For a prime number p consider the polynomial

$$F(T) = F_p(T) = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \cdots + T + 1 \in \mathbf{Q}[T].$$

Applying the change of variables $U = T - 1$ we see that

$$\begin{aligned} F(U+1) &= \frac{(U+1)^p - 1}{(U+1) - 1} = \frac{\sum_{i=1}^{p} \binom{p}{i} U^i}{U} \\ &= \frac{U^p + \binom{p}{p-1} U^{p-1} + \cdots + \binom{p}{2} U^2 + \binom{p}{1} U}{U} \\ &= U^{p-1} + \binom{p}{p-1} U^{p-2} + \cdots + \binom{p}{2} U + p \end{aligned}$$

In particular, $g(U) = F(U+1) = \sum_{i=0}^{p-1} c_i U^i \in \mathbf{Q}[U]$ has degree $p - 1$ and the coefficients are given by the formulae

$$c_i = \binom{p}{i+1}, \quad 0 \le i \le p - 1.$$

Proposition 7.5.1. *For a prime number $p > 0$, the polynomial*

$$F(T) = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \cdots + T + 1 \in \mathbf{Q}[T]$$

of degree $p - 1$ is irreducible.

Proof. Clearly $F(T) \in \mathbf{Q}[T]$ is irreducible if and only if $g(U) \in \mathbf{Q}[U]$ is irreducible. Now, $g(U) \in \mathbf{Z}[U]$ since binomial coefficients $\binom{n}{m}$ are always integers. We are going to apply Eisenstein's criteria to show the irreducibility of $g(U)$. For this, we first note that $c_{p-1} = 1$ is not divisible by p and that $c_0 = p$ is divisible by p but not by p^2.

The irreducibility will now follow from Theorem 7.4.1 once we argue that ($\clubsuit$) : $p \mid \binom{p}{i}$ for each $1 \le i \le p - 1$.

To prove ($\clubsuit$) just note that

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Since $0 < i < p$, neither $i!$ nor $(p - i)!$ is divisible by p. On the other hand

$$p! = p \cdot (p-1) \cdot (p-2) \cdots 2 \cdot 1$$

is divisible by p.

Since one knows that $\binom{p}{i} \in \mathbf{Z}$, unique factorization Section 5.2 implies that $p \mid \binom{p}{i}$ as required. $\square$

Example 7.5.2. For example, $f(T) = T^4 + T^3 + T^2 + T + 1 \in \mathbf{Q}[T]$ is an irreducible since $f(T) = \frac{T^5 - 1}{T - 1}$ and since $p = 5$ is prime.

8 Some recollections of Linear Algebra

Let F be a field. Much of what you learned in a course on linear algebra remains valid for vector spaces over F and not just for vector spaces over $\mathbf{R}$or $\mathbf{C}$.

8.1 Vector Spaces

Definition 8.1.1. A *vector space* over F is an additive abelian group V together with a mapping

$$F \times V \to V$$

denoted by

$$(\alpha, v) \mapsto \alpha v$$

called *scalar multiplication* that is required to satisfy several axioms:

(VS1) the multiplicative identity $1 = 1_F \in F$ satisfies $1 \cdot v = v$ for all $v \in V$.

(VS2) scalar multiplication is associative: for all $\alpha, \beta \in F$ and all $v \in V$, we have $\alpha(\beta v) = (\alpha\beta)v$.

(VS3) scalar multiplication distributes over addition in V: for all $\alpha, \beta \in F$ and for all $v, w \in V$, we have

$$\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$$

and

$$(\alpha + \beta) \cdot v = \alpha v + \beta v.$$

You should compare these requirements with axioms you may have seen in a course in linear algebra. The present list is probably shorter – that is because one needs axioms governing the behavior of addition, which we have handled by requiring V to be an additive abelian group.

8.2 Linear Transformations, subspaces and quotient vector spaces

Definition 8.2.1. Let V be a vector space over F. A subset $W \subset V$ is called a **subspace** (or more precisely, an F-subspace) provided that

(a) W is an additive subgroup of V, and

(b) W is closed under scalar multiplication by F – i.e.

$$\alpha w \in W \quad \text{for all } \alpha \in F \text{ and all } w \in W.$$

Definition 8.2.2. If V and W are vector spaces over F, a function $T : V \to W$ is a *linear transformation* (or more precisely, an F-linear transformation) if

(a) T is a homomorphism of additive groups $V \to W$, and

(b) T commutes with scalar multiplication – i.e. $T(\alpha v) = \alpha T(v)$ for all $\alpha \in F$ and all $v \in V$.

Definition 8.2.3. If V, W are vector spaces, a linear transformation $T : V \to W$ is an *isomorphism* if there is a linear transformation $S : W \to V$ such that $T \circ S = 1_W$ and $S \circ T = 1_V$.

If T is an isomorphism, one says that V and W are isomorphic vector spaces.

Proposition 8.2.4. *Let V, W be F-vector spaces and let $T : V \to W$ be a linear transformation. Then T is an isomorphism if and only if T is bijective.*

Proof. Suppose that T is bijective. Then we know that T is an isomorphism of additive groups, and hence there is an inverse isomorphism $S : W \to V$. It only remains to show that S is a linear transformation (rather than simply a group homomorphism).

So let $\alpha \in F$ and $w \in W$. Since T is onto, we may write $w = T(v)$ for some $v \in V$. Now,

$$S(\alpha w) = S(\alpha T(v)) = S(T(\alpha v) = 1_W(\alpha v) = \alpha v = \alpha S(T(v)) = \alpha S(w).$$

On the other hand, if T is an isomorphism, then the inverseisomorphism S is an inverse function to T so in particular T is one-to-one and onto. $\square$

Proposition 8.2.5. *If $T : V \to W$ is a linear transformation, then*

(a) $\ker(T)$ *is a subspace of V, and*

(b) the image $T(V) = \{T(v) \mid v \in V\}$ is a subspace of W.

Proof. Exercise! $\square$

Proposition 8.2.6. *Let W be a subspace of the F-vector space V. The quotient group V/W has the structure of an F-vector space, and the natural quotient mapping $\pi : V \to V/W$ given by $\pi(v) = v + W$ is an F-linear transformation.*

Proof. We must define a scalar multiplication for the additive group V/W. Given $\alpha \in F$ and an element $v + W \in V/W$, define

$$\alpha \cdot (v + W) = (\alpha v) + W.$$

We must confirm that this rule is independent of the choice of coset representative v for $v + W$. Thus, we must suppose that

$$v + W = v' + W$$

and we must show that $\alpha \cdot (v + W) = \alpha \cdot (v' + W)$ i.e. that $\alpha v + W = \alpha v' + W$.

The assumption that $v + W = v' + W$ means that $v - v' \in W$. Since W is a F-subspace, we find that $\alpha(v - v') \in W$ and using the distributive law we conclude that $\alpha v - \alpha v' \in W$. This shows that $\alpha v + W = \alpha v' + W$ as required. This proves that we've given a well-defined operation of scalar multiplication.

It now remains to check that the associative and distributive laws hold for this operation. Since these properties hold for the scalar multiplication in V, the verification is straightforward; details are left to the reader. $\square$

Proposition 8.2.7. *If $T : V \to W$ is a linear transformation, there is an isomorphism $\widetilde{T} : V/\ker(T) \to T(V)$ given by $\widetilde{T}(v + \ker T) = T(v)$ for $v \in V$.*

Proof. The first isomorphism theorem for groups tells us that the rule $\widetilde{T}$ is an isomorphism of groups. In view of @prop:inv-iso, it remains to argue that $\widetilde{T}$ is a linear transformation.

Thus, let $\alpha \in F$ and $x \in V/\ker T$. We may write $x = v + \ker T$ for some $v \in V$. Now, by definition we have

$$\alpha x = \alpha(v + \ker T) = \alpha v + \ker T.$$

Thus, since T is a linear tranformation we find the following:

$$\widetilde{T}(\alpha x) = \widetilde{T}(\alpha v + \ker T) = T(\alpha v) = \alpha T(v) = \alpha \widetilde{T}(v + \ker T).$$

This confirms that $\widetilde{T}$ commutes with scalar multiplication and is thus a linear transformation. $\square$

8.3 Bases and dimension

You are probably familiar with the notions of *spanning set* and of *linear independence.* One issue to be aware of is how to handle possibly-infinite sets in this setting.

To quote from Michael Artin's algebra text (Artin 2011):

> In algebra it is customary to speak only of linear combinations of finitely many vectors. Therefore, the span of an infinite set S must be interpreted as the set of those vectors V which are linear combinations of finitely many elements of S...

Definition 8.3.1. If $S \subset V$ is a set of elements, the span of S is defined to be

$$\operatorname{span}(S) = \left\{ \sum_{i=1}^{r} a_i x_i \mid r \in \mathbf{Z}_{\geq 0}, a_i \in F, x_i \in V \; (1 \leq i \leq r) \right\}$$

It is clear that $\operatorname{span}(S)$ is a *subspace* of V.

Definition 8.3.2. A subset $S \subset V$ of the vector space V is said to be *linearly independent* if whenever $n \in \mathbf{Z}_{\geq 0}$, whenever $x_1, \cdots, x_n \in V$ are *distinct* elements of V, and whenever $\alpha_1, \cdots, \alpha_n \in F$ then

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \implies \alpha_j = 0 \quad \text{for each } 1 \leq j \leq n.$$

Remark 8.3.3. We say that the vector space is *finitely generated* if there is a *finite* set $S \subset V$ for which $V = \operatorname{span}(S)$. In fact, V is then *finite dimensional* (see Definition 8.3.6 below).

Definition 8.3.4. Let V be a vector space over the field F. A *basis* for V is a subset $S \subset V$

(a) S spans V; i.e. $V = \operatorname{span}(V)$, and

(b) S is linearly independent.

Proposition 8.3.5. *Let V be an F-vector space.*

(a) There is a basis $\mathscr{B}$ for V.

(b) If $W \subset V$ is a subspace of V, and if $\mathscr{C}$ is a basis for W, there is a basis $\mathscr{B}$ for V with $\mathscr{C} \subseteq \mathscr{B}$.

(c) If $V = \operatorname{span}(S)$ then there is a basis of V contained in S.

(d) If $S \subset V$ is a linearly independent subset, there is a basis of V containing S.

(e) Any two bases of V have the same cardinality.

Proof. When V is finitely generated,results (a)-(e) can be found in (Hoffman and Kunze 1971), §2.2 and 2.3, and in (Friedberg, Insel, and Spence 2002) §1.6.

For the general case of (a)-(d) see (Friedberg, Insel, and Spence 2002) §1.7.

A proof of (e) in case $\mathscr{B}_1$ and $\mathscr{B}_2$ are *infinite* bases for V requires the Schroeder-Bernstein Theorem; we won't need this result in the course. ☐

Definition 8.3.6. If V is a vector space with basis $\mathscr{B}$, the *dimension* of V

- written $\dim V$ or $\dim_F V$ - is equal to the cardinality of the set $\mathscr{B}$.

It follows from Proposition 8.3.5 (e) that the dimension of V doesn't depend on the choice of basis.

Proposition 8.3.7. *Let V, W be F-vector spaces, let $\mathscr{B}$ be a basis for V, and let $x_b \in W$ for each $b \in \mathscr{B}$. Then there is a unique linear transformation $T : V \to W$ such that $T(b) = x_b$ for each $b \in \mathscr{B}$.*

Example 8.3.8. Let $F[T]$ be the polynomial ring over the field F. THen $F[T]$ is in particular a vector space over F with countably infinite basis given by $\{T^i \mid i \geq 0\}$.

Th linear independence of this basis precisely means that if $f = \sum_{i=0}^{N} a_i T^i \in F[T]$ for $a_i \in F$, then $f = 0$ if and only if all $a_i = 0$.

Proposition 8.3.9. *Let $T : V \to W$ be a linear transformation of F-vector spaces with $\dim V < \infty$. Then*

$$\dim_F V = \dim_F T(V) + \dim_F \ker(V).$$

9 Field extensions

Definition 9.0.1. Let F and E be fields and suppose that $F \subset E$ is a *subring.* We say that F is a *subfield* of E and that E is a *field extension* of F.

Throughout this discussion, let $F \subseteq E$ be an extension of fields.

9.1 Algebraic extensions of fields

Definition 9.1.1. An element $\alpha \in E$ is said to be *algebraic* over F provided that there is some polynomial $0 \neq f \in F[T]$ for which α is a root – i.e. for which $f(\alpha) = 0$.

If α is not algebraic over F, we say that α is *transcendental* over F.

Example 9.1.2.

- it is a fact that $\pi, e \in \mathbf{R}$ are transcendental over $\mathbf{Q}$.
- Of course, π, e are algebraic over $\mathbf{R}$.
- Any element $\alpha = a + bi \in \mathbf{C}$ (for $a, b \in \mathbf{R}$) is algebraic over $\mathbf{R}$. Indeed, α is a root of the polynomial

$$\begin{aligned} f(T) &= (T - \alpha)(T - \overline{\alpha}) \\ &= T^2 - 2\,\mathrm{Re}(\alpha)T + |\alpha|^2 \\ &= T^2 - 2aT + (a^2 + b^2) \in \mathbf{R}[T] \end{aligned}$$

where $\mathrm{Re}(\alpha) = a$ denotes the *real part* of the complex number α.

9.2 The minimal polynomial

Proposition 9.2.1. *Let $\alpha \in E$ and suppose that α is algebraic over F. Then there is a unique monic irreducible polynomial $p \in F[T]$ for which α is a root.*

Moreover,

(a) p is the monic polynomial of smallest degree for which

α is a root.

(b) if $f \in F[T]$ is any polynomial with $f(\alpha) = 0$, then $p \mid f$.

Proof. Let $I = \{f \in F[T] \mid f(\alpha) = 0\}$. It is straightforward to check that it is an additive subgroup, and it is closed and under multiplication with any polynomial in $F[T]$); thus I is an ideal of $F[T]$.

Since α is algebraic, $I \neq \{0\}$. Thus I coincides with the principal ideal $I = \langle p \rangle$ for some monic $0 \neq p \in F[T]$, and p is the unique monic element of smallest degree in I.

It only remains to argue that p is irreducible. Suppose that $f, g \in F[T]$ and that $p \mid fg$. We need to argue that $p \mid f$ or $p \mid g$. Well, since $fg = pq$ for $q \in F[T]$, we see that

$$0 = (pq)(\alpha) = (fg)(\alpha) = f(\alpha) \cdot g(\alpha).$$

Since $f(\alpha), g(\alpha)$ are elements of the field E, the only way their product can be 0 is for at least one factor to be zero - i.e. either $f(\alpha) = 0$ or $g(\alpha) = 0$. But then either $f \in I$ or $g \in I$ and thus $p \mid f$ or $p \mid g$. $\square$

Corollary 9.2.2. *Let $\alpha \in E$. If $p \in F[T]$ is irreducible and monic, and if $p(\alpha) = 0$, then p is the minimal polynomial of α over F.*

Definition 9.2.3. Let $\alpha \in E$ be algebraic over F.

- The irreducible polyomial p of the proposition is known as the *minimal polynomial* of α over F.

- The *degree* of α over F is defined to be the degree of the minimal polynomial p.

Example 9.2.4. An element $\alpha \in F$ has degree 1 over F, since it is the root of the irreducible degree 1 polynomial $T - \alpha \in F[T]$.

Example 9.2.5. Consider the complex number $z = a + bi \in \mathbf{C}$ with $a, b \in \mathbf{R}$. Then z has degree ≤ 2 over $\mathbf{R}$, and that degree is 2 if and only if $b \neq 0$.

Indeed, if $b = 0$, then $z = a \in \mathbf{R}$ is a root of $T - a \in \mathbf{R}[T]$ so z has degree 1 over $\mathbf{R}$. Otherwise, z is a root of

$$p = (T - z)(T - \overline{z}) = T^2 - 2aT + (a^2 + b^2) \in \mathbf{R}[T].$$

Since p has roots $z, \overline{z}$, it has no real roots; since it has degree 2, p is irreducible over $\mathbf{R}$. Now the Corollary shows that p is the minimal polynomial of z.

Example 9.2.6. Let F be a field and let $F(X)$ be the field of fractions $Q(F[X])$ of the polynomial ring $F[X]$.

$F(X)$ is often called the field of rational functions over F; its elements have the form

$$\frac{f}{g} = \frac{f(X)}{g(X)} \quad \text{for } f, g \in F[X]$$

Then the element $X \in F(X)$ is *transcendental* over F.

Indeed, given any non-zero polynomial $f(T) \in F[T]$, we wonder: is $f(X) = 0$? and of course, the answer is "no" because $f(X)$ is just the polynomial $f(T)$ after the substitution $T \mapsto X$.

In particular, the degree of X over F is undefined (or we could define it to be ∞).

Example 9.2.7. Consider the field $F = \mathbf{Q}(\sqrt{2})$ defined by adjoining to $\mathbf{Q}$ a root of $T^2 - 2$. We identify F with a subfield of $\mathbf{R}$.

Consider the polynomial $p(T) = T^4 - 2$ and write $\alpha = 2^{1/4}$ for the positive real root of $p(T)$.

Since $p \in \mathbf{Q}[T]$ is irreducible, α has degree 4 over $\mathbf{Q}$.

On the other hand, α has degree 2 over F. Indeed, note that in $F[T]$,

$$p(T) = T^4 - 2 = (T^2 - \sqrt{2})(T^2 + \sqrt{2}).$$

Since α is a root of $T^2 - \sqrt{2} \in F[T]$, the degree of α over F is ≤ 2. To see that equality holds, we must argue that $T^2 - \sqrt{2}$ is irreducible over F.

To establish this irreducibility, we will argue that $T^2 - \sqrt{2}$ has no root in F.

A typical element of F has the form $x = a + b\sqrt{2}$ for $a, b \in \mathbf{Q}$.

Suppose that

$$(\diamondsuit) \quad \sqrt{2} = x^2 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

But then comparing coefficients we see that $a^2 + 2b^2 = 0$ and $2ab = 1$.

Now

$$a^2 + 2b^2 = 0 \implies a = b = 0 \implies 2ab \neq 1.$$

Thus the assumption ($\diamondsuit$) is impossible and so

$$T^2 - \sqrt{2} \in F[T] = \mathbf{Q}(\sqrt{2})[T]$$

is indeed irreducible.

We repeat for emphasis:

- the minimal polynomial of α over $\mathbf{Q}$ is $T^4 - 2$ and has degree 4,
- the minimal polynomial of α over $\mathbf{Q}(\sqrt{2})$ is $T^2 - \sqrt{2}$ and has degree 2.

9.3 Generation of extensions and primitive extensions

Definition 9.3.1. Let $S \subset E$ be a subset. The smallest subfield of E containing F and S is denoted by $F(S)$. If $S = \{u_1, u_2, \cdots, u_n\}$ is a finite set, we often write $F(S) = F(u_1, \cdots, u_n)$ for this field.

If $E = F(u_1, \ldots, u_n)$ we say that the elements u_i *generate* the extension E of F.

If $n = 1$, the extension $F(u) = F(u_1)$ of F is said to be a *primitive extension* (or sometimes: a *simple extension*).

Remark 9.3.2. **Remark:** Note that $F(S)$ is equal to the intersection

$$F(S) = \bigcap_{K \in \mathscr{E}} K$$

of the collection

$$\mathscr{E} = \{K \subset E \mid K \text{ a subfield of } E \text{ containing } F \text{ and } S\}.$$

Since the intersection of subfields is again a subfield (check!), the notation $F(S)$ is meaningful.

Remark 9.3.3. Note that by definition

$$F(u_1, u_2, \ldots, u_n) = F(u_1, u_2, \ldots, u_{n-1})(u_n).$$

So to "describe" the extension $F \subset F(u_1, \ldots, u_n)$ we can focus on describing primitive extensions. Given a description of primitive extensions, we can first describe the extension $F \subset F(u_1)$ of F, next we can describe the extension $F(u_1) \subset F(u_1)(u_2)$ of $F(u_1)$, and so on.

Proposition 9.3.4. *Let $\alpha \in E$.*

a. If α is algebraic over F with minimal polynomial $p \in F[T]$ over F, then

$$F(\alpha) \simeq F[T]/\langle p \rangle,$$

where α identifies with $T + \langle p \rangle$.

In particular, $F(\alpha)$ has as an F-basis the elements

$$1, \alpha, \cdots, \alpha^{n-1}$$

where $n = \deg p = \deg \alpha$.

b. If α is transcendental over F, then $F(\alpha) \simeq F(T)$ where $F(T)$ is the field of fractions of the polynomial ring $F[T]$.

Proof. Construct the homomorphism

$$\phi : F[T] \to E \quad \text{such that } \phi_{|F} \text{ is the identity, and } \phi(T) = \alpha.$$

We are going to argue in both case (a) and (b) that ϕ induces the desired isomorphism.

First consider case (a). Suppose that α is algebraic with minimal polynomial p. The previous Proposition now shows that $\ker \phi = \langle p \rangle$.

Since p is irreducible, the quotient $F[T]/\langle p \rangle$ is a *field*. According to the first isomorphism theorem, ϕ induces an isomorphism between $F[T]/\langle p \rangle$ and its image K. Thus $K \subset E$ is a subfield containing F and α, so by definition $F(\alpha) \subset K$.

On the other hand, α identifies with the class $T + \langle p \rangle$, and so we've seen that the elements $1, \alpha, \cdots, \alpha^{n-1}$ form an F-basis for K viewed as a vector space over F. Now, any subfield K_1 of E containing F and α must contain all F-linear combinations of the elements α^i; thus $K \subset K_1$ and this proves that

$$K \subset F(\alpha) = \bigcap_{K_1 \in \mathscr{E}} K_1.$$

We now conclude that $K = F(\alpha)$ as required.

Now consider case (b). The condition that α is transcendental is equivalent to the requirement that $\ker \phi = \{0\}$.

Thus for any non-zero polynomial $f \in F[T]$, $\phi(f) = f(\alpha)$ is a non-zero element of $F(\alpha)$. In particular, $f(\alpha)^{-1} \in E$.

Now the *defining property* of the field of fractions gives a unique ring homomorphism $\widetilde{\phi}$: $F(T) \to E$ for which $\widetilde{\phi}_{|F[T]} = \phi$.

Since $F(T)$ is a field, $\widetilde{\phi}$ is one-to-one, and its image is a subfield of E containing α. On the other hand, any subfield of E containing α must contain the image of $\widetilde{\phi}$ and statement (b) follows at once. □

Example 9.3.5. For any transcendental number $\gamma \in \mathbf{R}$, the subfield $\mathbf{Q}(\gamma)$ of $\mathbf{R}$ is isomorphic to the field $\mathbf{Q}(T)$ of rational functions.

In particular, Proposition 9.3.4 shows that there is an isomorphism $\mathbf{Q}(e) \simeq \mathbf{Q}(\pi)$.

Remark 9.3.6. Here is a question we'll answer in an upcoming lecture. As before, let $F \subset E$ be a field extension.

If $\alpha, \beta \in E$ are algebraic over F, is $\alpha + \beta$ algebraic over F? How about $\alpha \cdot \beta$?

Example 9.3.7. Let $E = \mathbf{Q}[T]/\langle T^3 - 2 \rangle$ and let $\gamma = T + \langle T^3 - 2 \rangle$. Of course, $E \simeq \mathbf{Q}(\sqrt[3]{2})$ and under this isomorphism, γ is mapped to $\sqrt[3]{2}$. Put another way, γ is a root of $T^3 - 2$ in F.

We recall that since $T^3 - 2$ has degree 3, E has dimension 3 as a $\mathbf{Q}$-vector space, and $\{1, \gamma, \gamma^2\}$ is a $\mathbf{Q}$-basis for E.

For an element $\alpha = a + b\gamma + c\gamma^2$ consider the $\mathbf{Q}$-linear mapping

$$\lambda_\alpha : E \to E$$

given by the left mutiplication with α; i.e. by the rule $\lambda_\alpha(\beta) = \alpha \cdot \beta$ for $\beta \in E$.

We are going to compute the *matrix* of λ_α in the above basis for E. For this, note that the choice of basis determines a linear isomorphism $\phi : E \to \mathbf{Q}^3$ given by $\phi(s + t\gamma + u\gamma^2) = \begin{bmatrix} s \\ t \\ u \end{bmatrix}$.

So we are looking for a 3×3 matrix $M = M_\alpha$ with the property that

$$\phi(\lambda_\alpha(\beta)) = M \cdot \phi(\beta).$$

- $\lambda_\alpha(1) = \alpha$ so that $\phi(\lambda_\alpha(1)) = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. This is the first column of M.

- $\lambda_\alpha(\gamma) = \alpha\gamma = a\gamma + b\gamma^2 + c\gamma^3 = a\gamma + b\gamma^2 + 2c = 2c + a\gamma + b\gamma^2$ so that $\phi(\lambda_\alpha(\gamma) = \begin{bmatrix} 2c \\ a \\ b \end{bmatrix}$.

  This is the second column of M.

- $\lambda_\alpha(\gamma^2) = \alpha\gamma^2 = a\gamma^2 + b\gamma^3 + c\gamma^4 = a\gamma^2 + 2b + 2c\gamma = 2b + 2c\gamma + a\gamma^2$ so that $\phi(\lambda_\alpha(\gamma^2) = \begin{bmatrix} 2b \\ 2c \\ a \end{bmatrix}$.

  This is the third column of M.

Thus

$$M = M_\alpha = M_{a+b\gamma+c\gamma^2} = \begin{bmatrix} a & c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}$$

We claim for $\alpha_1, \alpha_2 \in E$ that $M_{\alpha_1+\alpha_2} = M_{\alpha_1} + M_{\alpha_2}$ and $M_{\alpha_1 \cdot \alpha_2} = M_{\alpha_1} \cdot M_{\alpha_2}$. Since M_α is the matrix determined by the linear transformation λ_α, our claim will follow if we just observe that $\lambda_{\alpha_1} + \lambda_{\alpha_2} = \lambda_{\alpha_1+\alpha_2}$ and $\lambda_{\alpha_1} \circ \lambda_{\alpha_2} = \lambda_{\alpha_1 \cdot \alpha_2}$ (where $\circ$ denotes the *composition* of linear transformations). But for $\beta \in E$ notice that $\lambda_{\alpha_1} \circ \lambda_{\alpha_2}(\beta) = \lambda_{\alpha_1}(\alpha_2\beta) = \alpha_1\alpha_2\beta = \lambda_{\alpha_1\alpha_2}(\beta)$; the other verification is similarly straightforward.

This proves that $\alpha \mapsto M_\alpha$ determines a *ring homomorphism*

$$E \to \mathrm{Mat}_{3\times 3}(\mathbf{Q})$$

Consider the element $1 + \gamma \in E$ and notice that $M_{1+\gamma} = \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

Now, we can compute the inverse matrix ${M_{1+\gamma}}^{-1} = \dfrac{1}{3}\begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$ which we recognize as the matrix $M_{(1-\gamma+\gamma^2)/3}$.

Thus we see that

$$\frac{1}{1+\gamma} = \frac{1}{3}\left(1 - \gamma + \gamma^2\right)$$

\

9.4 The degree of a field extension

Definition 9.4.1. We write $[E : F] = \dim_F E$ and say that $[E : F]$ is the *degree* of the extension $F \subset E$.

If E is *not* a finite dimensional vector space over F, then $[E : F] = \dim_F E = \infty$.

Proposition 9.4.2. *Let $\alpha \in E$. Then α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.*

Remark 9.4.3. If α is transcendental, the cardinality of an F-basis for $F(\alpha)$ fails to be countable if F is uncountable. Indeed, you can show that the elements

$$\left\{ \frac{1}{T-a} \in F(T) \mid a \in F \right\}$$

are linearly independent.

Proposition 9.4.4. *Let E be an extension of the field F and let $\alpha \in E$. The following are equivalent:*

a. α is algebraic over F.

b. the primitive extension $F(\alpha)$ is a finite extension of F.

c. $\alpha \in E_1$ for some subfield $E_1 \subset E$ with $F \subset E_1$ which is a finite extension of F.

Proof. a. $\implies$ b: If α is algebraic, let $d = \deg \alpha$ be the degree of α over F. We have seen that $1, \alpha, \dots, \alpha^{d-1}$ form an F-basis for $F(\alpha)$, so $[F(\alpha) : F] = d$ and thus $F(\alpha)$ is indeed a finite extension of F.

b. $\implies$ c: This is immediate; just take $E_1 = F(\alpha)$.

c. $\implies$ a.: Assume $\dim_F E_1 = d$. Since $\alpha \in E_1$ and E_1 is a field, also $\alpha^i \in E_1$ for all $i \in \mathbf{Z}_{\geq 0}$. Since E_1 has dimension d over F, it *follows from linear algebra* that the $d+1$ elements

$$1, \alpha, \cdots, \alpha^{d-1}, \alpha^d$$

are linearly dependent. over F. Let $c_0, c_1, \dots, c_d \in F$ not all zero be such that

$$\sum_{i=0}^{d} c_i \alpha^i = 0$$

and consider the *polynomial*

$$f(T) = \sum_{i=0}^{d} c_i T^i \in F[T].$$

Since not all of the coefficients c_i are 0, $f(T) \neq 0$. Since $f(\alpha) = 0$, we have proved that α is algebraic over F as required. ☐

Proposition 9.4.5. *Let $F \subset E \subset K$ be fields where K is a finite extension of E and E is a finite extension of F. Then K is a finite extension of F and moreover:*

$$[K : F] = [K : E] \cdot [E : F].$$

Proof. Let

$$a_1, \dots, a_N \in E \quad \text{be an } F\text{-basis for } E$$

and let

$$b_1, \dots, b_M \in K \quad \text{be an } E\text{-basis for } K$$

Multiplying in the field K, we consider the elements $a_s b_t$, and we assert:

$$\mathscr{B} = \{a_s b_t \mid 1 \leq s \leq N, 1 \leq t \leq M\} \quad \text{is an } F\text{-basis for } K$$

- $\mathscr{B}$ spans K over F: indeed, let $x \in K$. We must express x as a linear combination of the vectors $\mathscr{B}$.

  Since the $\{b_t\}$ span K over E, we may write

  $$x = u_1 b_1 + \cdots u_M b_M \quad \text{for } u_t \in E.$$

  Since the $\{a_s\}$ span E over F, for each $1 \leq t \leq M$ we may write

  $$u_t = v_{1,t} a_1 + \cdots v_{N,t} a_N \quad \text{for } v_{s,t} \in F$$

  Now

  $$x = \sum_{t=1}^{M} u_t b_t = \sum_{t=1}^{M} \left(\sum_{s=1}^{N} v_{s,t} a_s \right) b_t = \sum_{1 \leq s \leq N, 1 \leq t \leq M} v_{s,t} \cdot a_s b_t$$

- $\mathscr{B}$ is linearly independent over F.

  Suppose that

  $$0 = \sum_{1 \leq s \leq N, 1 \leq t \leq M} v_{s,t} \cdot a_s b_t = \sum_{t=1}^{M} \left(\sum_{s=1}^{N} v_{s,t} a_s \right) b_t$$

  for coefficients $v_{s,t} \in F$.

  Now use the fact that $\{b_t\}$ are linearly independent over E to conclude for each $1 \leq t \leq M$ that

  $$0 = \sum_{s=1}^{N} v_{s,t} a_s$$

  For any $1 \leq t \leq M$, use the fact that $\{a_s\}$ are linearly independent over F to conclude for each $1 \leq s \leq N$ that $v_{s,t} = 0$.

$\square$

Corollary 9.4.6. *Let E be a finite extension of F. If $\alpha \in E$ then the degree of α over F is a divisor of $[E : F]$:*

$$deg_F(\alpha) \mid [E : F].$$

Proof. Apply Proposition 9.4.5 to the tower of field extensions

$$F \subset F(\alpha) \subset E$$

to deduce that

$$[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F]$$

and the result follows since $[F(\alpha) : F] = \deg_F \alpha$. $\square$

9.5 Examples of finite extensions

Example 9.5.1. $[\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}] = 4$.

The polynomials $T^2-, T^2-3 \in \mathbf{Q}$ are known to be irreducible over $\mathbf{Q}$ (can you give a quick argument?)

We claim that T^2-3 remains irreducible over $\mathbf{Q}(\sqrt{2})$ –i.e. that $T^2-3 \in \mathbf{Q}(\sqrt{2})[T]$ is irreducible.

If we verify the claim, it follows that

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}(\sqrt{2})] = 2$$

and thus

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}(\sqrt{2})] \cdot [\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2 \cdot 2 = 4$$

as required.

Let's now prove the claim. Since T^2-3 has degree 2, the irreducibility will follow provided we argue that T^2-3 has no root in $\mathbf{Q}(\sqrt{2})$.

So: suppose that $3 = (a+b\sqrt{2})^2$ for $a, b \in \mathbf{Q}$. Thus

$$3 + 0 \cdot \sqrt{2} = 3 = a^2 + 2b^2 + 2ab\sqrt{2}$$

and comparing coefficients we find that

$$3 = a^2 + 2b^2 \quad \text{and} \quad 0 = 2ab.$$

Now $2ab = 0 \implies a = 0$ or $b = 0$ and the equation $3 = a^2 + 2b^2$ is then impossible (since neither 3 nor $3/2$ is a square in $\mathbf{Q}$). This completes the proof that T^2-3 is irreducible over $\mathbf{Q}(\sqrt{2})$.

Example 9.5.2. $[\mathbf{Q}(\sqrt{2}+\sqrt{3}) : \mathbf{Q}] = 4$.

To prove the claim, we argue that

$$\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3});$$

the assertion then follows from the previous example.

Write $K = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. To confirm this equality, first note that trivially we have

$$K \subset \mathbf{Q}(\sqrt{2},\sqrt{3})$$

so it is enough to argue

$$\sqrt{2}, \sqrt{3} \in K.$$

(**Why?**)

In fact, it is easy to see that $\sqrt{2} \in K \iff \sqrt{3} \in K$ (since $\sqrt{2}+\sqrt{3} \in K$ by construction!).

So it only remains to argue e.g. that $\sqrt{3} \in K$.

Let's observe that

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \frac{1}{\sqrt{2}+\sqrt{3}} \cdot \frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}-\sqrt{2}} = \frac{\sqrt{3}-\sqrt{2}}{1} \in K$$

and since K is a field,

$$\frac{1}{\sqrt{2}+\sqrt{3}} + \sqrt{2} + \sqrt{3} = (\sqrt{3}-\sqrt{2}) + (\sqrt{2}+\sqrt{3}) = 2\sqrt{3} \in K$$

so indeed $\sqrt{3} \in K$.

The preceding calculation confirms (for example) that $\sqrt{2}$ may be written in the form

$$\begin{aligned}\sqrt{2} &= a + b\alpha + c\alpha^2 + d\alpha^3 \\ &= a + b(\sqrt{2}+\sqrt{3}) + c(\sqrt{2}+\sqrt{3})^2 + d(\sqrt{2}+\sqrt{3})^3\end{aligned}$$

for some coefficients $a, b, c, d \in \mathbf{Q}$, though we'd need to do some work to find a, b, c, d.

9.6 Algebraic extensions

Let $F \subset E$ be any extension of fields. We are going to argue that

$$E_{\mathrm{alg}} = \{u \in E \mid u \text{ is algebraic over } F\}$$

is a subfield of E.

For example, this requires us to know that if $x, y \in E_{\mathrm{alg}}$ then $x - y \in E_{\mathrm{alg}}$. It is not completely clear how to find an algebraic equation satisfies by $x - y$, so we use a more indirect argument.

Our main tool is the following:

Lemma 9.6.1. *Let $\alpha, \beta \in E$ be algebraic. Then $[F(\alpha,\beta)] : F]$ is a finite extension. In particular, $\alpha \pm \beta$ and $\alpha \cdot \beta$ are algebraic over F; if $0 \neq \alpha$, then also $\alpha^{-1} = \dfrac{1}{\alpha}$ is algebraic over F.*

Proof. Indeed, β is algebraic over F hence algebraic over $F(\alpha)$ so

$$[F(\alpha, \beta) : F(\alpha)] < \infty$$

since $F(\alpha, \beta) = F(\alpha)(\beta)$.

Since α is algebraic over F, $[F(\alpha) : F] < \infty$ and thus

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta)] : F(\alpha)] \cdot [F(\alpha) : F]$$

is finite. The result now follows from Proposition 9.4.4. □

Corollary 9.6.2. *Let E be an extension field of F. The set of all elements of E which are algebraic over F forms a subfield E_{alg} of E.*

Proof. We first observe that E_{alg} is an additive subgroup of E. For this, note that $0 \in E_{\mathrm{alg}}$ so it just remains to show that if $x, y \in E_{\mathrm{alg}}$ then $x - y \in E_{\mathrm{alg}}$. But this statement follows from the Lemma 9.6.1.

It now remains to argue that E_{alg} is closed under multiplication and contains the inverse of its non-zero elements. These statements again follow from Lemma 9.6.1. □

Definition 9.6.3. An extension field E of F is *algebraic* over F if each element of E is algebraic over F.

Proposition 9.6.4. *Every finite extension of fields is algebraic.*

Proof. Let $F \subset E$ be a finite extension and let $\alpha \in E$ be an arbitrary element of E. Since $[F(\alpha) : F]$ is a divisor of $[E : F]$, $[F(\alpha) : F]$ is finite and hence α is algebraic by Proposition 9.4.4. This shows that E is algebraic over F as required. □

Lemma 9.6.5. *Let $F \subset E$ be an algebraic extension, and let $\alpha_1, \dots, \alpha_n \in E$. Then*

$$[F(\alpha_1, \dots, \alpha_n) : F] < \infty.$$

Proof. Proceed by induction on $n \geq 1$.

First consider the case $n = 1$. Since E is algebraic over F, $\alpha = \alpha_1$ is algebraic over F and $[F(\alpha) : F]$ is finite by previous results.

Now suppose $n > 1$ and write $E_i = F(\alpha_1, \dots, \alpha_i)$ for $1 \leq i \leq n$. The induction hypothesis is then: $[E_i : F] < \infty$ for $i < n$. Note that $E_n = E_{n-1}(\alpha_n)$, and – since α_n is algebraic over F – α_n is algebraic over E_{n-1}. Thus

$$[E_n : E_{n-1}] = [E_{n-1}(\alpha_n) : E_{n-1}] < \infty$$

by Proposition 9.4.4 and it follows by induction that

$$[E_n : F] = [E_n : E_{n-1}] \cdot [E_{n-1} : F] < \infty$$

as required. □

Proposition 9.6.6. *Let E be an algebraic extension of F and let K be an algebraic extension of E. Then K is an algebraic extension of F.*

Proof. Let $\alpha \in K$. We must argue that α is algebraic over F. Since α is algebraic over E, it is the root of some polynomial

$$f(T) = a_0 + a_1 T + a_2 T^2 + \cdots + a_N T^N \quad a_i \in E.$$

Now, form the extension $E_1 = F(a_0, a_1, \dots, a_N)$. Since E is algebraic over F, all a_i are algebraic over F. It follows from Lemma 9.6.5 that $[E_1 : F] < \infty$. Since α is algebraic over E_1 we know that $[E_1(\alpha) : E_1] < \infty$ by Proposition 9.4.4. It now follows that

$$[E_1(\alpha) : F] = [E_1(\alpha) : E_1][E_1 : F] < \infty$$

so that α is algebraic over F by Proposition 9.6.4. □

9.7 Another example

Consider the field $K = \mathbf{Q}(T)$ where T is transcendental over $\mathbf{Q}$. It follows from Theorem 7.4.1 that

$$X^n - T - a \in K[X] = \mathbf{Q}(T)[X]$$

is irreducible for $n = 2, 3$ for any $a \in \mathbf{Q}$.

These irreducibility statements mean that

$$[K(\sqrt{T-a}) : K] = 2 \quad \text{and} \quad [K(\sqrt[3]{T-a}) : K] = 3$$

(or writing everything out in full detail, that

$$[\mathbf{Q}(T, \sqrt{T-a}) : \mathbf{Q}(T)] = 2 \quad \text{and} \quad [\mathbf{Q}(T, \sqrt[3]{T-a}) : \mathbf{Q}(T)] = 3.)$$

Lemma 9.7.1. *$K(\sqrt{T-a}, \sqrt[3]{T-a}) = \mathbf{Q}(T, \sqrt{T-a}, \sqrt[3]{T-a})$ has degree 6 over $K = \mathbf{Q}(T)$.*

Proof. Let $L = K(\sqrt{T-a}, \sqrt[3]{T-a})$. The claim will follow if we show that

$$(\clubsuit) \quad [L : K(\sqrt{T-a})] = 3$$

since then

$$[L : K] = [L : K(\sqrt{T-a})] \cdot [K(\sqrt{T-a}) : K] = 3 \cdot 2 = 6.$$

Now, $(\clubsuit)$ follows if we argue that $f(X) = X^3 - T - a \in K(\sqrt{T-a})[X]$ is irreducible; since f has degree 3, it suffices to argue that f has no root in $K(\sqrt{T-a})$.

But were $\alpha \in K(\sqrt{T-a})$ a root of f, we know that α has degree 3 over K. But this is impossible since

$$\alpha \in K(\sqrt{T-a}) \implies \deg_K \alpha \mid [K(\sqrt{T-a}) : K] = 2.$$

This completes the proof that f is irreducible over $K(\sqrt{T-a})$ and thus the Lemma is verified. $\square$

10 Constructible real numbers

As an example of the utility of field theory, we are going to describe a field-theory-based answer to a "geometric-constructions/geometric" question about numbers. Loosely put, we are going to answer the question: "can one trisect an angle using ruler and compass?"

10.1 Ruler and compass constructions

As a starting point, we are given two points at *unit distance* in the Euclidean plane.

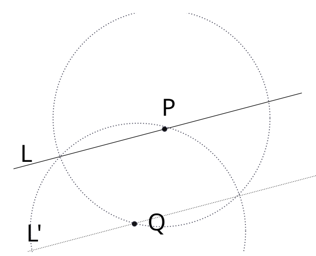
Given any two distinct known points P and Q, one can construct:

- the *line* through P and Q (this uses a *straightedge*)
- the circle with center P which passes through Q (this uses a *compass*)

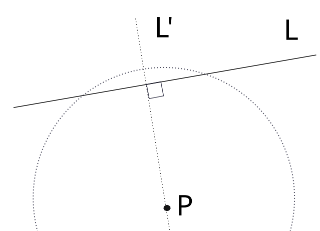
One views the points of intersection of lines and circles that have been constructed as *constructible* (i.e. known) points.

Here are some useful constructions that we are going to use without further argumentation:

Lemma 10.1.1. (♣) *Given a point P on a line L, and a second point Q not on L, we can construct a line L' parallel to L passing through Q.*

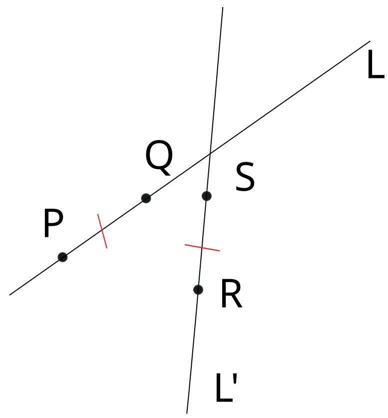


Lemma 10.1.2. (♡) *Given a line L and a point P not lying on L, one can construct a line L' containing P and perpendicular to L.*



Lemma 10.1.3. (♠) *Given two points $P \neq Q$ on a line L, a second line L', and a point R on L', we can construct a point S on L' such that*

$$|\overline{PQ}| = |\overline{RS}|.$$



10.2 Constructions

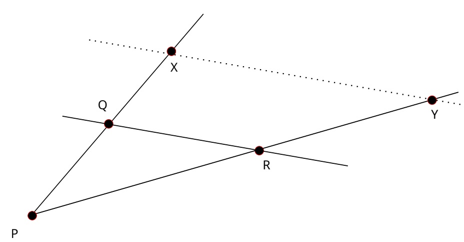
Definition 10.2.1. A real number r is *constructible* if one can construct a line segment of length $|r|$ using straightedge and compass.

Proposition 10.2.2. *The set of constructible real numbers forms a subfield $C \subset \mathbf{R}$.*

Sketch of proof. First, use Lemma 10.1.3 to show that C forms an additive subgroup of $\mathbf{R}$.

To argue that C is closed under multiplication, proceed as follows:

- Given positive constructible numbers y, z, w construct a diagram with points P, Q, R, Y as follows with $|PQ| = z$, $|PR| = w$ and $|PY| = y$.



- Now use (♣) to construct the line through Y parallel to the line through Q and R.
- Writing X for the (constructible) point of intersection of the indicated lines, write $x = |PX|$ and notice that $x/y = z/w$.
- Now let $a, b > 0$ be constructible and let $y = a$, $z = b$ and $w = 1$; the above argument shows that $x = yz = ab$ is constructible.

Similar arguments give the constructibility of a/b where $a, b > 0$ are constructible. $\square$

Let's observe that according to the Proposition, every rational number is constructible.

We may and will suppose that the points $(1, 0)$ and $(0, 1)$ in the plane are constructible. In particular, the coordinates r, s of any constructible point $P = (r, s)$ are constructible real numbers.

10.3 Lines and Circles over a field

Of course, any line may be described as the set of solutions to an equation

$$aX + bY + c = 0$$

for $a, b, c \in \mathbf{R}$, and any circle may be described as the solutions to an equation

$$X^2 + Y^2 + aX + bY + c = 0$$

for $a, b, c \in \mathbf{R}$.

If F is a subfield of $\mathbf{R}$, *a line over F* means a line with equation $aX + bY + c = 0$ where $a, b, c \in F$.

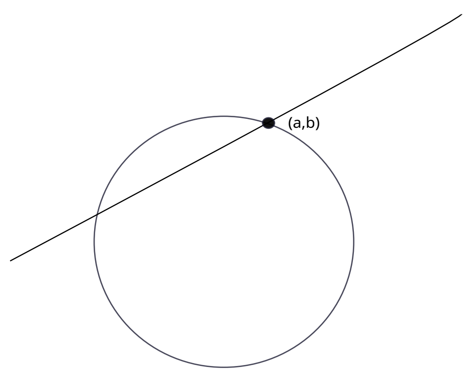
Similarly, *a circle over F* means a circle with equation

$$X^2 + Y^2 + aX + bY + c = 0 \quad \text{where } a, b, c \in F.$$

Lemma 10.3.1.
- *If the points $P \neq Q$ both have coordinates in F, the line through P and Q is a line over F.*
- *If C is circle for which both the radius and the coordinates of its center are all in F, then C is a circle over F.*

Constructing points via ruler and compass amounts to finding the intersections of lines and circles. We record the following fact about such intersections:

Proposition 10.3.2. *Let $F \subset \mathbf{R}$ be a subfield. The coordinates of the points of intersection of lines over F and circles over F belong to the field $F(\sqrt{u})$ for some $u \in F$.*



If in this diagram the line and the circle are "over F", the conclusion is that $a, b \in F(\sqrt{u})$ for a suitable $u \in F$.

10.4 Characterizing constructible numbers

Using Proposition 10.3.2, we can give an important characterization of constructible real numbers:

Theorem 10.4.1. $u \in \mathbf{R}$ *is constructible* $\iff$ *there are* $u_1, \ldots, u_n \in \mathbf{R}$ *such that:*

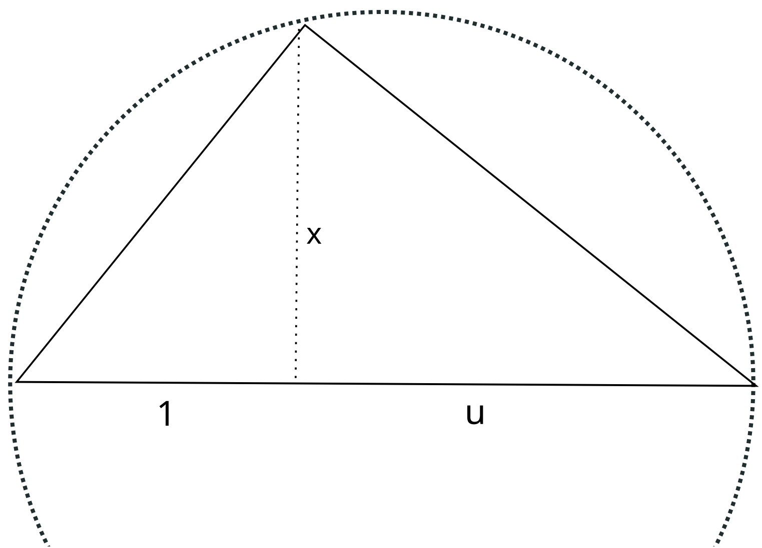
a. $u_1^2 \in \mathbf{Q}$,

b. $u_i^2 \in \mathbf{Q}(u_1, \ldots, u_{i-1})$ *for* $2 \leq i \leq n$, *and*

c. $u \in \mathbf{Q}(u_1, \ldots, u_n)$.

Proof. $\Rightarrow$: This follows from the Proposition.

$\Leftarrow$: Use the following: if F is any subfield of the field of constructible numbers, then $\sqrt{u}$ is constructible for each positive $u \in F$. For this, construct a circle of diameter $1 + u$, and a line perpindicular to the diameter, intersecting the diameter 1 unit from the west pole:



Then $x = \sqrt{u}$. $\square$

Corollary 10.4.2. *If u is a constructible real number, then u is algebraic over* $\mathbf{Q}$ *and* $\deg(u)$ *is a power of* 2.

10.5 Angle trisection

Lemma 10.5.1. *a. For any angle θ, we have the following identities:*

$$4\cos^3(\theta) - 3\cos(\theta) - \cos(3\theta) = 0.$$

b. Let $\alpha = \cos\left(\frac{\pi}{9}\right)$. *$\alpha$ is a root of the irreducible polynomial*

$$f(T) = 8T^3 - 6T - 1 \in \mathbf{Q}[T].$$

In particular, the degree of α over $\mathbf{Q}$ *is 3.*

c. α is not a constructible number.

Proof. Recall the trigonometric identities:

$$\sin(\alpha + \beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \tag{10.1}$$

and

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta). \tag{10.2}$$

Taking $\alpha = \beta$ we get

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$$

and

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha).$$

For a real number θ, we find that "double angle formula"

$$\begin{aligned}\cos(2\theta) &= \cos^2(\theta) - \sin^2(\theta)\\ &= \cos^2(\theta) - (1-\cos^2(\theta))\\ &= 2\cos^2(\theta) - 1\end{aligned}$$

This shows that

$$2\cos^2(\theta) - \cos(2\theta) - 1 = 0 \tag{10.3}$$

To prove (a), let $\alpha = 2\theta$ and $\beta = \theta$ in (10.2); we get

$$\begin{aligned}\cos(3\theta) &= \cos(2\theta + \theta)\\ &= \cos(2\theta)\cos(\theta) - \sin(2\theta)\sin(\theta)\\ &= (2\cos^2(\theta) - 1)\cos(\theta) - (2\sin(\theta)\cos(\theta))\sin(\theta)\\ &= 2\cos^3(\theta) - \cos(\theta) - 2\cos(\theta)\sin^2(\theta)\\ &= 2\cos^3(\theta) - \cos(\theta) - 2\cos(\theta)(1-\cos^2(\theta))\\ &= 4\cos^3(\theta) - 3\cos(\theta).\end{aligned}$$

This shows that $4\cos^3(\theta) - 3\cos(\theta) - \cos(3\theta) = 0$ as required.

We now prove (b). If $\theta = \dfrac{\pi}{9}$, then of course $\cos(3\theta) = \dfrac{1}{2}$, so (a) shows θ to be a root of the equation $4T^3 - 3T - \dfrac{1}{2} \in \mathbf{Q}[T]$. Multiplying this polynomial by 2 gives $8T^3 - 6T - 1$ and we can use the *rational roots test* Theorem 7.2.1 to confirm the that this polynomial has no root in $\mathbf{Q}$ and is thus irreducible in $\mathbf{Q}[T]$.

Now (c) follows from Corollary 10.4.2, since $3 \nmid 2^m$ for any $m \geq 1$. $\square$

Theorem 10.5.2. *It is impossible to find a general construction for trisecting an angle.*

Proof. Since $\cos\left(\dfrac{\pi}{3}\right) = \dfrac{1}{2}$ and $\sin\left(\dfrac{\pi}{3}\right) = \dfrac{\sqrt{3}}{2}$, one can construct points $Q = \dfrac{1}{2}(1, \sqrt{3}), P = (0,0), R = (1,0)$ and then $\angle QPR$ is $\dfrac{\pi}{3}$.

We claim that one can't construct further points S, T such that the $\angle QPS$, $\angle SPT$ and $\angle TPR$ are all equal.

Indeed, if it were so, the coordinates of T would be $(\cos\left(\dfrac{\pi}{9}\right), \sin\left(\dfrac{\pi}{9}\right))$, and then $\cos\left(\dfrac{\pi}{9}\right)$ would be a constructible number, contrary to Lemma 10.5.1 . $\square$

11 Splitting fields

11.1 The notion of a splitting field

Let F be a field and consider a polynomial

$$f = a_0 + a_1 T + \cdots + a_n T^n \in F[T]$$

of degree $n \geq 1$.

Definition 11.1.1. If E is an extension field of F, we say that f *splits over* E provided that there are elements $r_1, \ldots, r_n \in E$ such that

$$f = (T - r_1)(T - r_2) \cdots (T - r_n) = \prod_{i=1}^{n} (T - r_i) \in E[T].$$

Definition 11.1.2. If f splits over the field extension E of F, and if $r_1, \ldots, r_n \in E$ are the roots of f, we say thtat E is a *splitting field* for f over F if moreover $E = F(r_1, \ldots, r_n)$.

Thus a splitting field E is somehow a minimal field extension over which f splits.

Example 11.1.3. $E = \mathbf{Q}(i)$ is a splitting field over $\mathbf{Q}$ for the polynomial $f = T^2 - 2T + 2$ since

$$f = (T - 1 - i)(T - 1 + i) \in \mathbf{Q}(i)[T]$$

and since $\mathbf{Q}(i) = \mathbf{Q}(1 + i, 1 - i)$.

Theorem 11.1.4. *Let $f \in F[T]$ has degree $n \geq 1$. Then there exists a splitting field E for f over F with $[E : F] \leq n!$.*

Proof. Proceed by induction on $n \geq 1$. The result holds when $n = 1$, since then f splits over $E = F$.

Now suppose that the result is known for all fields F and all polynomials of degree $\leq n - 1$.

Now, choose an irreducible factor p of f in $F[T]$, say of degree $d \leq n$. Choose a root of p in some field extension of F, and consider the field $K = F(\alpha)$. We know that $[K : F] = [F(\alpha) : F] = d = \deg p$.

Since α is a root of p, it is also a root of f; thus by the *remainder theorem* – see Corollary 3.4.2 –, we may write

$$f = (T - \alpha) \cdot g \quad \text{for } g \in K[T] \text{ with } \deg g = n - 1.$$

Now use the *induction hypothesis* to construct a splitting field E for g over K with $[E : K] \leq (n - 1)!$.

Thus $E = K(r_2, \ldots, r_n)$ and

$$g = \prod_{i=2}^{n} (T - r_i) \in E[T].$$

We now have

$$f = (T - \alpha) \cdot g = (T - \alpha) \cdot \prod_{i=2}^{n} (T - r_i) \in E[T];$$

thus, f splits over E. Moreover, $E = K(r_2, \ldots, r_n) = F(\alpha, r_2, \ldots, r_n)$ which confirms that E is a splitting field of f over F.

Finally, note that

$$[E : F] = [E : K][K : F] \leq (n - 1)! \cdot d \leq n!$$

since $d \leq n$. □ □

11.2 More examples of splitting fields

11.2.1 Fourth root of 2

The field $E = \mathbf{Q}(i, \sqrt[4]{2})$ is a splitting field for $f = T^4 - 2$ over $\mathbf{Q}$, and $[E : \mathbf{Q}] = 8$.

First, if we write $\alpha = \sqrt[4]{2}$ for the *real* fourth root of 2, the roots of f are precisely $\pm\alpha, \pm i\alpha$. Indeed,

$$(T - \alpha)(T + \alpha)(T - i\alpha)(T + i\alpha) = (T^2 - \sqrt{2})(T^2 + \sqrt{2}) = f.$$

Now, $E = \mathbf{Q}(i, \sqrt[4]{2}) = \mathbf{Q}(\pm\alpha, \pm i\alpha)$.

Finally, to see that $[E : \mathbf{Q}] = 8$, first note that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$ since $T^4 - 2$ is irreducible over $\mathbf{Q}$.

Now $\alpha \in \mathbf{R} \implies \mathbf{Q}(\alpha) \subset \mathbf{R}$, so $\mathbf{Q}(\alpha)$ does not contain a root of $T^2 + 1$. Thus $T^2 + 1$ is irreducible over $\mathbf{Q}(\alpha)$

This shows that

$$[E : \mathbf{Q}] = [E : \mathbf{Q}(\alpha)] \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}] = 2 \cdot 4 = 8.$$

11.2.2 Transcendental extension

$E = \mathbf{C}(X, \sqrt[4]{X+1})$ is a splitting field over $\mathbf{C}(X)$ for $T^4 - (X + 1)$, and $[E : \mathbf{C}(T)] = 4$.

11.2.3 Finite field example

Let $F = \mathbf{F}_7$ be the field with 7 elements.

Let's describe the splitting field for $f = T^3 - 3 \in F[T]$ over F.

First, note that the cubes mod 7 are as follows:

```
return [ (n,n**3 % 7) for n in range(7) ]
```

```
[(0, 0), (1, 1), (2, 1), (3, 6), (4, 1), (5, 6), (6, 6)]
```

In particular, $f = T^3 - 3$ has no root in $F = \mathbf{F}_7$. So if α denotes a root of f in some extension field, then $F(\alpha)$ is a degree 3 extension of F.

Now let's notice that the multiplicative order of (the class of) 2 in ${\mathbf{F}_7}^\times$ is 3: indeed $2^3 = 8 \equiv 1 \pmod 7$ but $2, 2^2 \not\equiv 1 \pmod 7$. So we can observe that also 2α and 4α are also roots of $T^3 - 3$. Thus

$$f = (T - \alpha)(T - 2\alpha)(T - 4\alpha) \in F(\alpha)[T] = \mathbf{F}_7(\alpha)[T].$$

This shows that $F(\alpha) = \mathbf{F}_7(\alpha)$ is a splitting field over F of $f = T^3 - 3$.

Observe that $|F(\alpha)| = 7^3 = 343$; elements of $F(\alpha)$ all have the form

$$a + b\alpha + c\alpha^2 \quad a, b, c \in \mathbf{F}_7.$$

11.3 Uniqueness of splitting fields

We are going to argue that a splitting field for a polynomial f over F is *essentially unique.*

Let us first make an observation: if $\theta : F \to F_1$ is an isomorphism of fields, then θ may be extended to an isomorphism

$$\theta : F[T] \to F_1[T]$$

with the property that $\theta(T) = T$. Note that polynomials satisfy

$$p \in F[T] \quad \text{is irreducible} \iff \quad \theta(p) \in F_1[T] \quad \text{is irreducible.}$$

Lemma 11.3.1. *Let $\theta : F \to F_1$ be an isomorphism of fields, let $E = F(u)$ where u is algebraic over F with minimal polynomial $p \in F[T]$, and let $p_1 = \theta(p)$. If v is a root of p_1 in an extension field of F_1, there is a unique way of extending θ to an isomorphism $\phi : F(u) \to F_1(v)$ subject to the conditions (i) $\phi(u) = v$, and (ii) $\phi_{|F} = \theta$, i.e. the restriction of ϕ to F is given by θ.*

This diagram might be useful for visualizing the situation:

$$\begin{array}{ccc} F(u) & \stackrel{\phi}{\to} & F_1(v) \\ \uparrow & \circ & \uparrow \\ F & \stackrel{\theta}{\to} & F_1 \end{array}$$

Proof. We first observe that ϕ is uniquely determined by the indicated conditions. Indeed, $F(u)$ is spanned as F-vector space by elements of the form u^i, and since ϕ is a ring homomorphism it must satisfy $\phi(u^i) = v^i$.

We now prove the existence of ϕ. We first note that –according to Proposition 9.3.4 – there are isomorphisms $\gamma : F[T]/\langle p\rangle \xrightarrow{\sim} F(u)$ and $\psi : F_1[T]/\langle p_1\rangle \xrightarrow{\sim} F_1(v)$ with

$$\gamma(T + \langle p\rangle) = u \quad \text{and} \quad \psi(T + \langle p_1\rangle) = v$$

such that $\gamma_{|F} = \mathrm{id}$ and $\psi_{|F_1} = \mathrm{id}$.

Now, consider the ring homomorphism $F[T] \stackrel{\theta}{\to} F_1[T] \xrightarrow{\pi_1} F_1[T]/\langle p_1\rangle$ where π_1 is the quotient mapping. This mapping $\pi_1 \circ \theta$ is onto and has kernel $\langle p\rangle$; according to the First Isomorphism Theorem – see Theorem 2.5.1 – it induces an isomorphism

$$\Phi : F[T]/\langle p\rangle \xrightarrow{\sim} F_1[T]/\langle p_1\rangle$$

such that $\Phi_{|F} = \theta$ and such that $\Phi(T + \langle p\rangle) = T + \langle p_1\rangle$.

Now $\psi \circ \Phi \circ \gamma^{-1} : F(u) \xrightarrow{\sim} F_1(v)$ has the required properties. □

Remark 11.3.2. Using the notations of the preceding proof, the isomorphism $F(u) \to F_1(v)$is given by

$$F(u) \xrightarrow{\gamma^{-1}} F[T]/\langle p\rangle \stackrel{\Phi}{\to} F_1[T]/\langle p_1\rangle \stackrel{\psi}{\to} F_1(v).$$

Example 11.3.3. Consider the field $F = \mathbf{Q}(i)$. Write $\sigma : \mathbf{Q}(i) \to \mathbf{Q}(i)$ for *complex conjugation*; thus $\sigma(a + bi) = \overline{a + bi} = a - bi$ for $a, b \in \mathbf{Q}$. The mapping σ is an *automorphism* of the field $F = \mathbf{Q}(i)$.

We claim that the polynomials $f_1 = T^2 - (1+i)$ and $f_2 = T^2 - (1-i)$ in $F[T]$ are irreducible. Note that $f_2 = \sigma(f_1)$ so it is sufficient to argue that f_1 is irreducible.

According to Proposition 7.1.4 it is enough to argue that the degree 2 polynomial f_1 has no roots in $F = \mathbf{Q}(i)$.

If $\alpha \in \mathbf{Q}(i)$ is a root of f_1 then $\alpha^2 = 1 + i$ so that

$$\alpha^2 \cdot \sigma(\alpha^2) = (1 + i) \cdot \sigma(1 + i) = (1 + i)(1 - i) = 2$$

But then $(\alpha\sigma(\alpha))^2 = 2$, and it is easy to see that $\alpha \cdot \sigma(\alpha) = \alpha\overline{\alpha} \in \mathbf{Q}$. Since $\sqrt{2} \notin \mathbf{Q}$ this contradiction proves that there is no root $\alpha \in F$ of f_1. Thus indeed f_1 and f_2 are irreducible.

In particular $F(\sqrt{1+i}) = \mathbf{Q}(i, \sqrt{1+i})$ and $F(\sqrt{1-i}) = \mathbf{Q}(i, \sqrt{1-i})$ are degree 2 extensions of the field $F = \mathbf{Q}(i)$.

Now Lemma 11.3.1 shows that there is an isomorphism $\phi : \mathbf{Q}(i, \sqrt{1+i}) \to \mathbf{Q}(i, \sqrt{1-i})$ such that $\phi(\sqrt{1+i}) = \sqrt{1-i}$ and such that $\phi_{|\mathbf{Q}(i)} = \sigma$; in particular, $\phi(i) = -i$.

Proposition 11.3.4. *Let E be a splitting field over F for $f \in F[T]$, let $\theta : F \to F_1$ be a field isomorphism, and let $g = \theta(f) \in F_1[T]$. Let E_1 be a splitting field for g over F_1. Then there is an isomorphism $\phi : E \to E_1$ such that $\phi_{|F} = \theta$.*

Proof. We use induction on $n = \deg f$. If $n = 1$, then $E = F$, $E_1 = F_1$ and we can simply take $\phi = \theta$.

Now suppose that $n > 1$ and that the result holds for all field F and all polynomials of degree $< n$.

Let $p \in F[T]$ be an irreducible factor of f, so that $q = \theta(p)$ is an irreducible factor of g.

Since f splits over E, also p splits over E. Choose a root $u \in E$ of p. Thus $F \subset F(u) \subset E$.

Choose also a root $v \in E_1$ of q, so that $F_1 \subset F_1(v) \subset E$.

According to the preceding Lemma, there is an isomorphism $\widehat{\theta} : F(u) \to F_1(v)$ such that $\widehat{\theta}_{|F} = \theta$ and such that $\widehat{\theta}(u) = v$.

Write

$$f = (T-u)s \in F(u)[T] \quad \text{for } s \in F(u)[T]$$

and

$$g = (T-v)s_1 \in F_1(v)[T] \quad \text{for } s_1 \in F_1(v)[T]$$

Now, E is a splitting field for s over $F(u)$ and E_1 is a splitting field for s_1 over $F_1(v)$. And since $\theta(f) = g$ and $\widehat{\theta}(u) = v$ it is easy to see that $\widehat{\theta}(s) = s_1$.

Thus the induction hypothesis gives an isomorphism $\phi : E \to E_1$ such that $\phi_{|F(u)} = \widehat{\theta}$. This isomorphism ϕ has the required properties. □

We find the following theorem as an immediate consequence:

Theorem 11.3.5. *Let $f \in F[T]$ be a polynomial with $\deg f > 0$. If E and E_1 are splitting fields for f over F, there is an isomorphism $\phi : E \to E_1$ such that $\phi(a) = a$ for each $a \in F$ – i.e. such that $\phi_{|F}$ is the identity mapping.*

Proof. In the Proposition, just take θ to be the identity map! □

Remark 11.3.6. Observe that the proof of Proposition 11.3.4 requires us to prove the statement involving θ, even though in Theorem 11.3.5 we are interested in only in the case $\theta = \mathrm{id}$.

11.3.1 Example: automorphisms of a splitting field

The ideas behind the results Proposition 11.3.4 and Theorem 11.3.5 will be really important as we start talking about Galois theory. So, it seems useful to first do a non-trivial example.

Let's give an example of automorphisms of a splitting field.

Let's fix a prime number p, consider the polynmomial $f = T^3 - p \in \mathbf{Q}[T]$, and let E be a splitting field for this polynomial over $\mathbf{Q}$.

The Theorem 11.3.5 tells us that any splitting field of f over $\mathbf{Q}$ is isomorphic to E. Let's try to understand what this statement could mean about automorphisms of E.

First, let's make some observations. Notice that if β and β' are roots of f, then $\left(\dfrac{\beta}{\beta'}\right)^3 = 1$ i.e. $\dfrac{\beta}{\beta'}$ is a root of $T^3 - 1$. Moreover, $\dfrac{\beta}{\beta'} = 1$ if and only if $\beta = \beta'$.

Let's exclude the "trivial" cube root of unity; observe that

$$\frac{T^3-1}{T-1} = T^2+T+1 \in \mathbf{Q}[T]$$

has roots $\omega, \omega^2 \in \mathbf{C}$ where

$$\omega = \exp\left(\frac{2\pi i}{3}\right) = \cos\left(\frac{2\pi i}{3}\right) + i \sin\left(\frac{2\pi i}{3}\right) \in \mathbf{C};$$

Notice that $\omega \neq 1$ and $\omega^3 = 1$ so viewed as an element of the *group* $\mathbf{C}^\times$, ω has order 3.

Neither ω nor ω^2 is rational, so T^2+T+1 is *irreducible* over $\mathbf{Q}$.

We can now construct a splitting field E of f over $\mathbf{Q}$ *abstractly.* Take $E = \mathbf{Q}(\alpha, \omega)$ where α is a root of $T^3 - p$ and ω is a root of T^2+T+1.

First notice that

$$E = \mathbf{Q}(\alpha, \omega) = \mathbf{Q}(\alpha, \omega\alpha, \omega^2\alpha)$$

so that E is a splitting field. Now notice that $\deg_{\mathbf{Q}} \alpha = 3$ and $\deg_{\mathbf{Q}} \omega = 2$ so T^2+T+1 remains irreducible over $\mathbf{Q}(\alpha)$. Thus we may conclude that

$$[E : \mathbf{Q}] = [\mathbf{Q}(\alpha, \omega) : \mathbf{Q}(\alpha)] \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}] = 6.$$

Now observe that this argument actually shows that if we fix *any* root β of f in E, and *any* root ζ of T^2+T+1 in E then

$$f = (T-\beta)(T-\zeta\beta)(T-\zeta^2\beta).$$

E.g. if we choose $\zeta = \omega^2$ and $\beta = \omega\alpha$, then

$$f = (T-\beta)(T-\zeta\beta)(T-\zeta^2\beta) = (T-\omega\alpha)(T-\omega^2(\omega\alpha))(T-\omega^4(\omega\alpha))$$

since

$$\{\omega\alpha, \omega^2(\omega\alpha), \omega^4(\omega\alpha)\} = \{\omega\alpha, \omega^3\alpha, \omega^5\alpha\} = \{\omega\alpha, \alpha, \omega^2\alpha\}.$$

The thing to take home from all this is that there are some choices to be made in describing the roots of f. In this case, you could pin things down more precisely e.g. by taking for α the "real" cube root of P and for ω the complex root of T^2+T+1 which is in "quadrant 2". But a more systematic way of keeping track of choices is through study of automorphisms of the splitting field E.

Notice that α and $\beta = \omega\alpha$ are roots of the irreducible polynomial $T^3 - p \in \mathbf{Q}[T]$. Thus, there is an isomorphism of fields

$$\theta : \mathbf{Q}(\alpha) \to \mathbf{Q}(\beta)$$

such that θ is the identity on $\mathbf{Q}$ and $\theta(\alpha) = \beta = \omega\alpha$.

Notice that $\theta(T^2+T+1) = T^2+T+1$ is irreducible over $\mathbf{Q}(\alpha)$ and over $\mathbf{Q}(\beta)$.

Now, Lemma 11.3.1 tells us that there is an isomorphism

$$\Theta : \mathbf{Q}(\alpha, \omega) \to \mathbf{Q}(\beta, \zeta)$$

such that $\Theta_{|\mathbf{Q}(\alpha)} = \theta$ – i.e. for which $\Theta(\alpha) = \beta$ – and for which $\Theta(\omega) = \zeta$.

This Θ is an isomorphism between splitting fields of f. Since we took $\beta = \omega\alpha$ and $\zeta = \omega^2$, we have

$$E = \mathbf{Q}(\alpha, \omega) = \mathbf{Q}(\beta, \zeta)$$

so in fact $\Theta : E \to E$ is an *automorphism* of E.

Note that Θ is not the identity mapping on the roots of f:

$$(\Theta(\alpha), \Theta(\omega\alpha), \Theta(\omega^2\alpha)) = (\omega\alpha, \zeta\omega\alpha, \zeta^2\omega\alpha) = (\omega\alpha, \alpha, \omega^2\alpha).$$

Also note that upon restriction to $\mathbf{Q}(\omega)$, $\Theta_{|\mathbf{Q}(\omega)}$ is *complex conjugation*, since

$$\Theta(\omega) = \omega^2 = \overline{\omega}.$$

12 Finite fields

12.1 The prime subfield of a field

First let's recall for any field F that there is always a ring homomorphism $\mathbf{Z} \to F$ for which $n \mapsto n.1_F$.

Proposition 12.1.1. *Let F be a field.*

a. *If the homomorphism $\mathbf{Z} \to F$ is one-to-one, then F contains a copy of the field $\mathbf{Q}$ of rational numbers.*

b. *If the homomorphism $\mathbf{Z} \to F$ is not one-to-one, then F contains a copy of the field $\mathbf{Z}/p\mathbf{Z}$ for some prime number p.*

Remark 12.1.2. In case a., we say that F has *characteristic* 0. Note in that case that the *additive order* of any non-zero element of F is ∞.

In case b., we say that F has *characteristic* p. In that case, the additive order of any non-zero element of F is p.

Definition 12.1.3. The *prime subfield* of F is the smallest subfield containing the image of the homomorphism $\mathbf{Z} \to F$; thus when F has characteristic 0, the prime subfield identifies with $\mathbf{Q}$, and when F has characteristic $p > 0$, the prime subfield identifies with $\mathbf{Z}/p\mathbf{Z}$.

Proof of the Proposition. If the homomorphism $\phi : \mathbf{Z} \to F$ is injective, it maps non-zero elements of $\mathbf{Z}$ to *invertible* elements of F. Thus by the *defining property* of the field of fractions $\mathbf{Q} = Q(\mathbf{Z})$, the homomorphism ϕ extends to a homomorphism $\widetilde{\phi} : \mathbf{Q} \to F$; see Proposition 6.0.4. Thus F indeed contains a copy of $\mathbf{Q}$.

Suppose on the other hand that the homomorphism ϕ is not one-to-one; thus $\ker \phi = n\mathbf{Z}$ for some $n \neq 0$. The *First Isomorphism Theorem* Theorem 2.5.1 now implies that the image of ϕ is a subring of F isomorphic to the finite ring $\mathbf{Z}/n\mathbf{Z}$. Since F is a field, this subring must be an integral domain – see Example 3.1.7 (c); thus by Example 3.1.7 (d) we see that $n = p$ must be a prime number. $\square$

12.2 Some properties of finite fields

We've met some finite fields already, namely $\mathbf{Z}/p\mathbf{Z}$ for a prime number p.

We've can construct finite extensions of $\mathbf{Z}/p\mathbf{Z}$ to get fields F for which $|F|$ is not prime. Let's first make an observation about $|F|$, as follows:

Proposition 12.2.1. *Let F be a finite field. Then F has characteristic $p > 0$ for some prime number p. The number of elements of F is p^m for some whole number $m \geq 1$.*

Proof. Since $\mathbf{Q}$ is not finite, the previous proposition shows that F must have characteristic $p > 0$ for a prime number p.

Write $F_0 \subset F$ where F_0 is the prime subfield; thus $F_0 \simeq \mathbf{Z}/p\mathbf{Z}$.

Now, F may be viewed as an F_0-vector space. A basic theorem in linear algebra says that F must have a *basis* $\mathscr{B}$ as an F_0-vector space; see Proposition 8.3.5. Since F is finite, this basis must be finite; say $|\mathscr{B}| = m$.

Write $\mathscr{B} = \{b_1, b_2, \ldots, b_m\}$. Then an element x of F may be written uniquely in the form

$$x = t_1 b_1 + t_2 b_2 + \cdots + t_m b_m$$

for $t_i \in F_0$; see e.g. Section 8.3. Since $F_0 \simeq \mathbf{Z}/p\mathbf{Z}$, there are p choices for each t_i; this shows that the number of elements of F is

$$|F| = p \cdot p \cdot \cdots \cdot p = p^m$$

as required. $\square$

12.3 Finite fields as splitting fields over the prime field

Proposition 12.3.1. *Let F be a finite field with p^m elements for some prime number p. Then F is the splitting field over the prime subfield $F_0 \simeq \mathbf{Z}/p\mathbf{Z}$ of the polynomial*

$$T^{p^m} - T \in F_0[T].$$

Proof. Since F has p^m elements, the multiplicative group $F^\times$ has $p^m - 1$ elements. This means that every element $x \in F^\times$ satisfies the condition

$$x^{p^m - 1} = 1.$$

It is then immediate that every element $x \in F$ satifies

$$x^{p^m} = x.$$

Put another way, every element of F is a root of the polynomial

$$f = T^{p^m} - T \in F_0[T].$$

Since f can have no more than p^m roots in an extension field, it follows that F contains all roots of f. Since F is generated by these roots, F is a splitting field for f over F_0. $\square$

Remark 12.3.2. The proof shows that the identity

$$f = T^{p^m} - T = \prod_{\alpha \in F} (T - \alpha)$$

holds in $F[T]$.

Corollary 12.3.3. *Two finite fields F and E are isomorphic if and only if $|F| = |E|$.*

Proof. If F and E are isomorphic, there is a one-to-one onto function $\phi : F \to E$ and thus $|F| = |E|$.

On the other hand, if $|F| = |E|$, we know that $|F| = p^m$ and $|E| = q^n$ for some primes p, q and some $m, n \geq 1$. By unique factorization of integers, $p = q$ and $m = n$. Now the Proposition shows that E, F are splitting fields of $T^{p^m} - T$ over $\mathbf{Z}/p\mathbf{Z}$.

Now the existence of an isomorphism $F \simeq E$ is a consequence of the uniqueness of splitting fields. $\square$

12.4 Existence of a finite field of any prime-power order

Let p be a prime number. One might see the following Lemma in a class in elementary number theory:

Lemma 12.4.1. *For $x, y \in \mathbf{Z}$, we have:*

a. $x^p \equiv x \pmod{p}$

b. $(x+y)^p \equiv x^p + y^p \equiv x + y \pmod{p}$.

We are going to prove a slightly more general version of this result that is valid for elements of *any* field of characteristic $p > 0$, as follows:

Lemma 12.4.2. *Let F be a field of char. $p > 0$, let $x, y \in F$, and let $n \in \mathbf{Z}_{>0}$. Then:*

a. $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.

b. $\{x \in F \mid x^{p^n} = x\}$ *is a subfield of F.*

Proof. For $0 < i < p$, the binomial coefficients $\dbinom{p}{i} = \dfrac{p!}{i! \cdot (p-i)!}$ satisfy the congruence

$$\binom{p}{i} \equiv 0 \pmod{p}.$$

Indeed, p dvides the numerator $p!$ but p does not divide the denominator $i! \cdot (p-i)!$ and the result follows since the quotient is integral.

Since $\dbinom{p}{0} = \dbinom{p}{p} = 1$, it follows that

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p \tag{12.1}$$

for elements $x, y \in F$. To prove a., proceed by induction on $n \geq 1$. The case $n = 1$ is just (12.1). Assuming the result is valid for $n-1$, we see that

$$(x+y)^{p^n} = \left((x+y)^{p^{n-1}}\right)^p = \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p = x^{p^n} + y^{p^n};$$

we used the induction hypothesis for the second equality, and we used (12.1) applied to $x^{p^{n-1}}$ and $y^{p^{n-1}}$\) for the final equality. This proves a.

For b., write

$$F_1 = \{x \in F \mid x^{p^n} = x\}.$$

To see that F_1 is an additive subgroup of F, first note that $0 \in F_1$. Now, the result from a. shows that if $x, y \in F_1$ then $x - y \in F_1$.

Next we argue that F_1 is closed under multiplication. This follows since if $x, y \in F_1$ then

$$(xy)^{p^n} = x^{p^n} y^{p^n} = xy.$$

Finally, if $x \in F_1$ is non-zero, then

$$1 = 1^{p^n} = (x \cdot x^{-1})^{p^n} = x^{p^n} x^{-p^n} = x x^{-p^n}$$

which shows that $(x^{-1})^{p^n} = x^{-p^n} = x^{-1}$ hence $x^{-1} \in F_1$. ∎

Lemma 12.4.3. *Let F be a field of characteristic $p > 0$ and let $\mathscr{F} : F \to F$ be the mapping $\mathscr{F}(x) = x^p$. Then $\mathscr{F}$ is a ring homomorphism.*

Proof. Part a. of Lemma 12.4.2 shows that $\mathscr{F}$ is a homomorphism of additive group. If $x, y \in F$ then $\mathscr{F}(xy) = (xy)^p = x^p y^p = \mathscr{F}(x)\mathscr{F}(y)$ which completes the proof. □

Lemma 12.4.4. *Let m, n be positive integers for which $n = qm$.*

a. $T^m - 1 \mid T^n - 1$ in the polynomial ring $\mathbf{Z}[T]$.

b. For any commutative ring R (with identity) and any $y \in R$ we have $y^m - 1 \mid y^n - 1$.

Proof. For a., first note that for a polynomial variable u, we have the identity

$$\frac{u^q - 1}{u - 1} = u^{q-1} + u^{q-2} + \cdots + u + 1 \tag{12.2}$$

in the field of fractions of $\mathbf{Z}[u]$. Substituting $u = T^m$ in (12.2) gives

$$\begin{aligned} f(T) = \frac{T^n - 1}{T^m - 1} &= \frac{(T^m)^q - 1}{T^m - 1} \\ &= (T^m)^{q-1} + (T^m)^{q-2} + \cdots + T^m + 1 \\ &= T^{m(q-1)} + T^{m(q-2)} + \cdots + T^m + 1 \in \mathbf{Z}[T] \end{aligned}$$

Now b. follows from a. Indeed, if $T^n - 1 = g(T) \cdot (T^m - 1)$ for $g(T) \in \mathbf{Z}[T]$, then for $y \in R$ we see that $y^n - 1 = g(y) \cdot (y^m - 1)$ since evaluation at y determines a ring homomorphism $\mathbf{Z}[T] \to R$. □

Proposition 12.4.5. *Let F be a field with p^n elements. Each subfield of F has p^m elements for some divisor m of n. Conversely, for each divisor $m \mid n$, there exists a unique subfield of F having p^m elements.*

Proof. Let F_0 be the prime subfield of F. Any subfield E of F must contain F_0 and must have p^m elements, where $m = [E : F_0]$. Since

$$n = [F : F_0] = [F : E][E : F_0] = [F : E] \cdot m$$

we conclude that m must be a divisor of n.

Conversely, let m be a divisor of n. Then $p^m - 1$ is a divisor of $p^n - 1$ by Lemma 12.4.4. Applying Lemma 12.4.4 a second time, we see that the polynomial $g(T) = T^{(p^m-1)} - 1$ is a divisor of $h(T) = T^{(p^n-1)} - 1$ in the polynomial ring $F_0[T]$.

Since F is the splitting field of $T \cdot h(T)$ over F_0, it must contain all p^m distinct roots of $T \cdot g(T)$.

Now, part b. of Lemma 12.4.2 implies that the roots of $T \cdot g(T) = T^{p^m} - T$ form a subfield E of F. Any other subfield having order p^m must be a splitting field of $T \cdot g(T)$ and so it must coincide with E. This completes the proof. □

Lemma 12.4.6. *Let F be a field of char. $p > 0$. If $n \in \mathbf{Z}_{>0}$ and $n \not\equiv 0 \pmod{p}$ then $T^n - 1$ has no repeated roots in any extension field of F. Put another way, if E denotes a splitting field of $T^n - 1$ over F, then*

$$T^n - 1 = \prod_{i=1}^{n} (T - \alpha_i)$$

for n distinct elements $\alpha_i \in E$.

Proof. Let c be a root of $T^n - 1$ in a splitting field E. The remainder theorem – Corollary 3.4.2 – shows that $T^n - 1 = (T-c)g(T)$ for some polynomial

$$g(T) = \sum_{i=0}^{n-1} a_i T^i$$

with $a_0, a_1, \cdots, a_{n-1} \in F(c)$. Now, we have

$$\begin{aligned} T^n - 1 = (T-c)g(T) = (T-c)\left(\sum_{i=0}^{n-1} a_i T^i\right) &= \left(\sum_{i=0}^{n-1} a_i T^{i+1}\right) - \left(\sum_{i=0}^{n-1} c a_i T^i\right) \\ &= \left(\sum_{i=1}^{n} a_{i-1} T^i\right) - \left(\sum_{i=0}^{n-1} c a_i T^i\right) \\ &= a_{n-1}T^n + \left(\sum_{i=1}^{n-1} a_{i-1} T^i - \sum_{i=1}^{n-1} c a_i T^i\right) - c a_0 \end{aligned}$$

Comparing coefficients, we find that $a_{n-1} = 1$ and that $a_{i-1} = c a_i$ for $1 \le i \le n-1$. Thus we find that $a_i = c^{n-1-i}$ for $1 \le i \le n-1$ and that $a_0 = c^{n-1}$ since then $c a_0 = c^n = 1$. Thus

$$g(T) = T^{n-1} + cT^{n-2} + c^2 T^{n-3} + \cdots + c^{n-2} T + c^{n-1}$$

.

To prove the Lemma, we must show that $g = g(T)$ is not divisible by $T - c$. By the remainder theorem, it is sufficient to prove that $g(c) \neq 0$. But we have:

$$g(c) = c^{n-1} + c c^{n-2} + c^2 c^{n-3} + \cdots + c^{n-2} c + c^{n-1} = n \cdot c^{n-1}$$

and the result follows since $n 1_F \neq 0$ and $c \neq 0$. □

Theorem 12.4.7. *For every prime p and every positive integer n, there is a field $\mathbf{F}_q$ with $q = p^n$ elements, and any field of order q is isomorphic to $\mathbf{F}_q$.*

Proof. The uniqueness has already been proved; it remains to argue the *existence* of $\mathbf{F}_q$ for $q = p^n$.

Let F be the splitting field of the polynomial $T^{p^n} - T$ over $\mathbf{Z}/p\mathbf{Z}$. The previous Lemma shows that $T^{p^n} - T$ has p^n distinct roots. By an earlier Lemma, these roots form a *subfield* of F, so we conclude that F consists exactly in these roots. Thus $|F| = p^n$ as required. □

Remark 12.4.8. For a prime power q, some texts write $\mathrm{GF}(q)$ for the field we have denoted $\mathbf{F}_q$. The symbol GF stands for "Galois Field".

12.5 Some examples of finite fields

We have seen in Theorem 12.4.7 that for each prime power $q = p^n$, there is a field of that order. The computer algebra system `sagemath` knows how to to do some computations with finite fields. We are next going to demonstrate this facility with some calculations.

12.5.1 Extensions of $\mathbf{F}_{19}$

For example, we can ask to to represent the field of $19^2 = 361$ elements.

```
H.<a>=FiniteField(19^2)
a.minpoly()
```

```
x^2 + 18*x + 2
```

The output here tells us that

$$H = \mathbf{F}_{19}[T]/\langle T^2 + 18T + 2\rangle.$$

We can construct larger finite fields and ask about `subfields`:

```
G.<z>=FiniteField(19^6)
z.minpoly()
```

```
x^6 + 17*x^3 + 17*x^2 + 6*x + 2
```

```
G.subfields()
```

```
[(Finite Field of size 19,
  Ring morphism:
    From: Finite Field of size 19
    To:   Finite Field in z of size 19^6
    Defn: 1 |--> 1),
 (Finite Field in z2 of size 19^2,
  Ring morphism:
    From: Finite Field in z2 of size 19^2
    To:   Finite Field in z of size 19^6
    Defn: z2 |--> 18*z^5 + 9*z^4 + 5*z^3 + 2*z^2 + 12*z + 7),
 (Finite Field in z3 of size 19^3,
  Ring morphism:
    From: Finite Field in z3 of size 19^3
    To:   Finite Field in z of size 19^6
    Defn: z3 |--> 13*z^5 + 10*z^4 + 2*z^3 + 15*z^2 + 7*z + 18),
 (Finite Field in z of size 19^6,
  Identity endomorphism of Finite Field in z of size 19^6)]
```

Th output here tells us that the field G of order $19^6 = 47045881$ – roughly forty seven million elements – has exactly 4 subfields: $G = \mathbf{F}_{19}(z)$, a subfield $\mathbf{F}_{19}(z3)$ of order 19^3, a subfield $\mathbf{F}_{19}(z2)$ of order 19^2 and a subfield of order 19.

Here `sage` has found an element z for which

$$G = \mathbf{F}_{19}(z) \simeq \mathbf{F}_{19}[T]/\langle T^6 + 17 \cdot T^3 + 17 \cdot T^2 + 6 \cdot T + 2\rangle,$$

The subfield

$$\mathbf{F}_{19}(z3) = \mathbf{F}_{19}(13 \cdot z^5 + 10 \cdot z^4 + 2 \cdot z^3 + 15 \cdot z^2 + 7 \cdot z + 18)$$

has order $19^3 = 6859$.

The subfield

$$\mathbf{F}_{19}(z2) = \mathbf{F}_{19}(18 \cdot z^5 + 9 \cdot z^4 + 5 \cdot z^3 + 2 \cdot z^2 + 12 \cdot z + 7)$$

has order $19^2 = 361$.

Let's pause and ask `sagemath` to compute the non-squares in $\mathbf{F}_{19}$:

```
F.<a>=FiniteField(19)
squares = [ x^2 for x in F]
nonSquares = [x for x in F if not(x in squares)]
len(nonSquares)
```

```
9
```

This output tells us that there are 9 elements $a \in \mathbf{F}_{19}$ for which $T^2 - a$ is **irreducible**. Those elements are:

```
nonSquares
```

```
[2, 3, 8, 10, 12, 13, 14, 15, 18]
```

According to Corollary 12.3.3, up to isomorphism there is a unique field of order 19^2. It follows that

$$\mathbf{F}_{19}(\sqrt{2})$$

must contain a square root of each of these `nonSquares`. We can ask `sagemath` to describe these roots in terms of $a = \sqrt{2}$ as follows:

We first describe solutions to $T^2 - 2$:

```
F= FiniteField(19)
R.<T>=PolynomialRing(F)
E.<a> = F.extension(T^2 - 2)
[x for x in E if x^2==2]
```

```
[a, 18*a]
```

And here are solutions to $T^2 - 13$:

```
[x for x in E if x^2==13]
```

```
[4*a, 15*a]
```

Similarly we can find solutions to $T^2 - 8$:

```
[x for x in E if x^2==8]
```

```
[2*a, 17*a]
```

This makes clear for example that

$$\mathbf{F}_{19}(\sqrt{13}) = \mathbf{F}_{19}(4\sqrt{2}) = \mathbf{F}_{19}(\sqrt{2}).$$

In fact, we can get a full list of irreducible polynomials:

```
irred = [T^2 + a*T + b for a in F for b in F if (T^2+a*T+b).is_irreducible()]
len(irred)
```

```
171
```

The output tells us that there are 171 monic irreducible quadratic polynomials in $\mathbf{F}_{19}[T]$. Let's look at a few:

```
irred[0:11]
```

```
[T^2 + 1,
 T^2 + 4,
 T^2 + 5,
 T^2 + 6,
 T^2 + 7,
 T^2 + 9,
 T^2 + 11,
 T^2 + 16,
 T^2 + 17,
 T^2 + T + 2,
 T^2 + T + 3]
```

We can use the `sage` command `polroots` to find roots of a polynomial:

```
def polroots(p):
    return [x for x in E if p(x)==0]
[irred[10],
 polroots(irred[10])]
```

```
[T^2 + T + 3, [a + 9, 18*a + 9]]
```

The output shows that the two roots of $T^2 + T + 3$ in $\mathbf{F}_{19}(\sqrt{2})$ are

$$9 + \sqrt{2} \quad \text{and} \quad 9 + 18\sqrt{2} = 9 - \sqrt{2}.$$

(Of course, we have obtained those roots using the quadratic formula!)

This makes clear that $\mathbf{F}_{19}(\sqrt{2})$ is a splitting field for $T^2 + T + 3$.

In fact, we know that $\mathbf{F}_{19}(\sqrt{2})$ is a splitting field for all 171 polynomials p in the list `irred`.

12.5.2 Fields of order 4 and 8

There are 4 monic polynomials of degree 2 over the field $\mathbf{F}_2$ of two elements. Of these, only one is irreducible, namely

$$T^2 + T + 1.$$

Thus

$$\mathbf{F}_4 \simeq \mathbf{F}_2(\alpha)$$

where $\deg \alpha = 2$ and $\alpha^2 = \alpha + 1$. Notice that

$$T^2 + T + 1 = (T + \alpha)(T + \alpha + 1).$$

There are 8 monic polynomials of degree 3 over $\mathbf{F}_2$. Of these, only two are irreducible:

```
H = FiniteField(2)
R.<T>=PolynomialRing(H)
[T^3 + a*T^2 + b*T + c
 for a in H
 for b in H
 for c in H
 if (T^3+a*T^2+b*T + c).is_irreducible()]
```

```
[T^3 + T + 1, T^3 + T^2 + 1]
```

Thus $\mathbf{F}_8 = \mathbf{F}_2(\beta)$ where $\deg \beta = 3$ and $\beta^3 = \beta + 1$. And indeed we may confirm that $\mathbf{F}_2(\beta)$ is a splitting field for *both* the irreducible polynomials of degree 3:

```
HH.<b>=FiniteField(8)
RR.<T>=PolynomialRing(HH)
[RR(T^3+T+1).factor(),
 RR(T^3+T^2+1).factor()]
```

```
[(T + b) * (T + b^2) * (T + b^2 + b),
 (T + b + 1) * (T + b^2 + 1) * (T + b^2 + b + 1)]
```

12.6 The multiplicative group of a finite field

Let $F = \mathbf{F}_q$ be a finite field, where $q = p^n$. Then of course the multiplicative group $F^\times = F \setminus \{0\}$ is a finite abelian group having $q - 1$ elements.

In this section we are going to argue that the group $F^\times$ is *cyclic*, so that

$$F^\times \simeq \mathbf{Z}/(q-1)\mathbf{Z}.$$

We begin with a Lemma from group theory:

Lemma 12.6.1. *Let G be a finite abelian group (written multiplicatively). If $a \in G$ is an element of maximal order in G, then the order of every element of G is a divisor of the order $o(a)$ of a.*

Proof. Let $x \in G$ be any element different from 1. If $o(x) \nmid o(a)$ then in the prime factorizations of $o(x)$ and $o(a)$ we can find a prime p that occurs to a higher power in $o(x)$ than in $o(a)$.

Write $o(a) = p^\alpha n$ and $o(x) = p^\beta m$ where $\alpha < \beta$ and $p \nmid n$, $p \nmid m$.

Now $o(a^{p^\alpha}) = n$ and $o(x^m) = p^\beta$, so the orders of a^{p^α} and x^m are relatively prime. It follows that the order of the product $a^{p^\alpha} \cdot x^m$ is equal to the product of the orders of the elements, i.e. to np^β. But this exceeds $o(a)$ contrary to the hypothesis. □

Theorem 12.6.2. *Let F be any field. Any finite subgroup of the multiplicative group $F^\times$ is cyclic.*

Proof. Let H be a finite subgroup of $F^\times$ and let $a \in H$ be an element with maximal order. Write $N = o(a)$. Now Lemma 12.6.1 shows that $o(x) \mid N$ for all $x \in H$. Thus, every element of H is a root of the polynomial $T^N - 1$. Now, this polynomial has no more than N roots – see Corollary 3.4.3. It follows that $|H| \leq N$. Since the cyclic group $\langle a \rangle$ has order N, conclude that $H = \langle a \rangle$. □

Corollary 12.6.3. $\mathbf{F}_q{}^\times$ *is a cyclic group of order $q - 1$ for any prime power $q = p^n$.*

Corollary 12.6.4. *For any prime power $q = p^n$, there is $\alpha \in \mathbf{F}_q$ for which $\mathbf{F}_q = \mathbf{F}_p(\alpha)$. In words: each finite field is a* primitive *extension of its prime subfield.*

Proof. Let β be a generator for the cyclic group $\mathbf{F}_q{}^\times$. Then

$$\langle \beta \rangle \subseteq \mathbf{F}_p(\beta) \subseteq \mathbf{F}_q \implies q - 1 \leq |\mathbf{F}_p(\beta)| \leq q.$$

Since $|\mathbf{F}_p(\beta)|$ must be a power of p – see Proposition 12.2.1 – it follows that $\mathbf{F}_p(\beta) = \mathbf{F}_q$. □

13 Perfect fields and separable polynomials

Let F be a field.

13.1 Common roots and root multiplicity

If $f \in F[T]$ is a non-zero polynomials, recall that according to Theorem 5.2.1 we may write

$$f = u \prod_{i=1}^{r} p_i^{e_i}$$

where $u \in F^\times$, where the $p_i \in F[T]$ are pairwise non-associate *irreducible* polynomials, and where $e_i \geq 0$. observe that a splitting field for f over F is the same as a splitting field for

$$g = \prod_{i=1}^{r} p_i.$$

Lemma 13.1.1. *Suppose that $f, g \in F[T]$.*

a. If $\gcd(f, g) = 1$ then f and g have no common root in any extension of F.

b. If f, g are irreducible and not associate, they have no common root in any extension of F.

Proof. Assertion b. is of course an immediate consequence of assertion a.

As to a., note that $\gcd(f, g) = 1 \implies$ that $1 = uf + vg$ for polynomials $u, v \in F[T]$ Proposition 4.3.4.

Let E be an extension field of F and suppose that $\alpha \in E$ is a root of both f and g. Then $0 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = 1$ which is impossible. Thus there can be no such common root α. □

Let $f \in F[T]$ be monic and let E be a splitting field for f over F. Write

$$f = (T - \alpha_1)^{e_1} \cdots (T - \alpha_r)^{e_r}.$$

for **distinct** elements $\alpha_i \in E$ and exponents $e_i \in \mathbf{Z}_{\geq 1}$. Since the linear polynomials $T - \alpha_i$ are irreducible and pairwise relatively prime in $E[T]$, it follows from Theorem 5.2.1 that this representation is unique (up to re-ordering, of course).

Definition 13.1.2. We say that the root α_i of f has *multiplicity* e_i. If $e_i = 1$, we say that α_i is a *simple root* of f. If $e_i > 1$, we say that α_i is a **multiple root* of f.

Proposition 13.1.3. *The polynomial $f \in F[T]$ has no multiple roots if and only if $\gcd(f, f') = 1$ where f' is the formal derivative of f.*

Proof. We are actually going to prove the (equivalent) assertion: f has a multiple root if and only if $\gcd(f, f') \neq 1$.

$\Rightarrow$: We show that if f has a multiple root, then $\gcd(f, f') \neq 1$. Suppose that f has a multiple root α in some extension field E.

In $E[T]$ we may write

$$f = (T - \alpha)^2 \cdot g \quad \text{for some } g \in E[T].$$

One must check that the product rule holds for formal differentiation; using that rule, one then notes that

$$f' = (T-\alpha)^2 g' + 2(T-\alpha)g.$$

It is evident that α is a root of both f and f' and thus Lemma 13.1.1 implies that $\gcd(f, f') \neq 1$.

$\Leftarrow$: We suppose that $\gcd(f, f') \neq 1$ and we must prove that f has a multiple root.

Our assumption implies that there is a polynomial $g \in F[T]$ of positive degree which divides both f and f'. Let α be a root of g in some extension field of F. Thus α is a root of both f and f'. We now claim that α is a multiple root of f.

Since α is a root of f, we may write

$$f = (T-\alpha) \cdot h \quad \text{for some } h \in F[T].$$

In order to show that α is a multiple root of f, we must argue that α is a root of h.

Well, we find using the product rule that

$$f' = h + \cdot (T-\alpha) \cdot h'.$$

Since α is a root of f' we find that

$$0 = f'(\alpha) = h(\alpha) + (\alpha - \alpha)h'(\alpha) = h(\alpha).$$

We have now argued that $h(\alpha) = 0$; as already observed, this proves that α is a multiple root of f. □

13.2 Multiple roots and the characteristic of F

Lemma 13.2.1. *Suppose that the field F has characteristic 0, and let $g \in F[T]$ be a polynomial with $\deg g \geq 1$. Then the formal derivative $g' \in F[T]$ is non-zero.*

Proof. Let $d = \deg g \geq 1$ and write

$$g = \sum_{i=0}^{d} a_i T^i \in F[T]$$

with $a_d \neq 0$. Then

$$g' = \sum_{i=0}^{d} i \cdot a_i T^{i-1}$$

so that the coefficient of T^{d-1} in g' is equal to $d \cdot a_d$. Since F has characteristic 0, $d1_F \neq 0$. Since $a_d \neq 0$ by assumption, we conclude that the coefficient of T^{d-1} in g' is non-zero, hence g' itself is indeed non-zero. □

Proposition 13.2.2. *Let $f \in F[T]$ be an irreducible polynomial.*

a. If F has characteristic 0, then f has no multiple roots.

b. If F has characteristic $p > 0$ then f has no multiple roots unless f has the form

$$f(T) = g(T^p)$$

for some polynomial $g \in F[T]$.

Proof. Suppose that f has a multiple root. It follows from Proposition 13.1.3 that $\gcd(f, f') \neq 1$. But $\deg(f') < \deg(f)$. Thus if $f' \neq 0$, the irreducibility of f guarantees that f and f' have no common factor. Hence, the assumption that f has a multiple root implies that $(\clubsuit) \quad f' = 0$.

Now a. follows since if F has characteristic 0, Lemma 13.2.1 shows that the polynomial f' is non-zero, contradicting $(\clubsuit)$.

Now suppose that the characteristic of F is $p > 0$ and write

$$f = \sum_{i=0}^{N} a_i T^i \quad \text{for } a_i \in F.$$

Suppose that $f' = 0$. Then

$$f' = \sum_{i=1}^{n} a_i \cdot i \cdot T^{i-1}.$$

So $f' = 0 \implies a_i \cdot i$ for all i. This equation show that $a_i = 0$ whenever $i \not\equiv 0 \pmod p$.

Thus the polynomial f has the form

$$f = \sum_{j=0}^{M} a_{jp} T^{jp} = g(T^p)$$

where

$$g = \sum_{j=0}^{M} a_{jp} T^j.$$

$\square$

13.3 Perfect fields and separable polynomials

Definition 13.3.1. A polynomial $f \in F[T]$ is said to be *separable* if each irreducible factor of f has only simple roots.

Definition 13.3.2. A field F is said to be *perfect* if each irreducible polynomial is separable.

Remark 13.3.3. a. Proposition 13.2.2 implies that any field of characteristic 0 is perfect.

b. Let $F = \mathbb{F}_p(X)$ be the field of rational functions over $\mathbb{F}_p$ in the variable X. Then F is not perfect.

Indeed, the polynomial $T^p - X \in F[T]$ is irreducible by Eisenstein's criterion Theorem 7.4.1. But this polynomial has only one root α (with multiplicity p) in a splitting field since $T^p - X = (T - \alpha)^p$ by (12.1).

On the other hand, some fields of characteristic p *are* perfect. Here is a useful characterization:

Proposition 13.3.4. *Let F be a field of characteristic $p > 0$. Then F is perfect if and only if*

$$F = F^p = \{x^p \mid x \in F\}.$$

Proof. $\Leftarrow$: Suppose that $F = F^p$ and let $f \in F[T]$ be an irreducible polynomial. We must argue that f is separable.

If f has a multiple root, we argued above that $f = g(T^p)$ for some polynomial

$$g = \sum_{i=0}^{r} a_i T^i.$$

For each i, choose $b_i \in F$ with $b_i^p = a_i$. Then

$$f = g(T^p) = \sum_{i=0}^{r} a_i T^{pi} = \sum_{i=0}^{r} b_i^p T^{pi} = \left(\sum_{i=0}^{r} b_i T^i \right)^p.$$

But this expression contradicts the assumption that f is irreducible in $F[T]$.

$\Rightarrow$: Suppose that F is perfect and let $x \in F$. Consider the polynomial

$$f = T^p - x$$

and let g denote a monic irreducible factor of f in $F[T]$. Find a root α of g in some extension field.

Then α is also a root of f, so that $\alpha^p = x$. In $F(\alpha)[T]$ we have

$$f = T^p - x = T^p - \alpha^p = (T - \alpha)^p.$$

By unique factorization in $E[T]$, we find that $g = (T - \alpha)^m$ for some $1 \le m \le p$. But g is irreducible and F is perfect, so g has no multiple roots in the extension field E. Thus $m = 1$ so that $g = (T - \alpha)$. This implies that $\alpha \in F$ so indeed x has a p-th root in F. $\square$

We can now prove the following important fact:

Proposition 13.3.5. *A finite field is perfect.*

Proof. Let F be a finite field, and recall that the Frobenius mapping $\mathscr{F}(x) = x^p$ is a ring homomorphism $F \to F$ – see Lemma 12.4.3. Moreover, $\ker \mathscr{F} = \{0\}$ since $x^p = 0 \implies x = 0$; this shows that $\mathscr{F}$ is *injective.*

Since F is finite and $\mathscr{F}$ is injective, one knows that $\mathscr{F}$ is also *surjective.* This proves that $F = F^p$; thus the field F is perfect by Proposition 13.3.4. $\square$

Remark 13.3.6. Observe that the proof shows that $\mathscr{F}$ is always injective for a field of characteristic p. Moreover, the image $\mathscr{F}(F)$ coincides with F^p, which is therefore a *subfield* of F.

We see that the following are equivalent:

i) F is perfect

ii) the Frobenius mapping $\mathscr{F}$ is *onto*

iii) the Frobenius mapping $\mathscr{F}$ is bijective, i.e. an *automorphism* of F.

14 Automorphisms of algebraic objects

Consider an algebraic object $\mathscr{X}$ – e.g. a *group*, or a *ring*, or a *field*, or a *field extension*, or a *vector space over a field*.

Within the family of algebraic objects of the same type, there is a notion if *isomorphism*.

For the above list, probably the only case that raises eyebrows is the question: "what is an isomorphism of a field extension?"

Though a related question is: what is the right notion for isomorphism of "vector spaces over fields"? We'll have more to say on this in the examples, below.

Once one has agreed on a notion of isomorphism, then for a fixed object $\mathscr{X}$ one can consider the collection of all isomorphisms

$$\mathscr{X} \to \mathscr{X}$$

This collection is a group

$$\mathrm{Aut}(\mathscr{X}),$$

the group of *automorphisms* of $\mathscr{X}$.

14.1 Automorphism examples

- Vector spaces

  For a field F and an n-dimensional vector space V over F, the automorphism group

  $$\mathrm{Aut}(V) = \mathrm{GL}(V) \simeq \mathrm{GL}_n(F)$$

  identifies with the group of invertible $n \times n$ matrices with coefficients in F.

- Automorphisms of some finite abelian groups

  Let $m \geq 1$ and consider the group

  $$A = \mathbb{Z}_m \times \mathbb{Z}_m,$$

  a group with $|A| = m^2$.

  Let's represent elements x of A as column vectors:

  $$x = \begin{bmatrix} a \\ b \end{bmatrix} \quad \text{for} \quad a, b \in \mathbb{Z}_m.$$

  Any matrix

  $$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad \text{for } \alpha, \beta, \delta, \gamma \in \mathbb{Z}_m$$

  determines a *group homomorphism*

  $\phi_M : A \to A$ given by the rule

  $$\phi_M(x) = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = a \begin{bmatrix} \alpha \\ \gamma \end{bmatrix} + b \begin{bmatrix} \beta \\ \delta \end{bmatrix}$$

  and ϕ_M is an *automorphism* if and only if the determinant of M is a unit in $\mathbb{Z}_m$ – i.e. $\det M \in (\mathbb{Z}_m)^\times$.

  Thus

  $$\mathrm{Aut}(A) \simeq \mathrm{GL}_2(\mathbb{Z}_m).$$

So, for example the matrix

$$M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

has determinant $-2 \equiv m - 2 \pmod{m}$, and so it defines an automorphism of A whenever

$$\gcd(m, m-2) = 1$$

i.e. whenever m is *odd*.

14.2 Automorphisms of field extensions

Our real interest in this course is in automorphisms of a field extension $F \subset E$. Here, an automorphism of the field extension is an automorphism $\phi : E \to E$ such that $\phi(a) = a$ for all $a \in F$.

To remind ourself of the "bottom field" of the field extension $F \subset E$ (F is sometimes called the "ground field" or "base field") we write

$$\mathrm{Aut}_F(E) \quad \text{or} \quad \mathrm{Aut}(E/F)$$

for the automorphism group of this field extension.

- Example: quadratic extensions when the characteristic is not 2

  Suppose that $[E : F] = 2$ and that the charateristic of F is not 2.

  Then $E = F(\beta)$ for some element $\beta \in E$, $\beta \notin F$, $\beta^2 \in F$.

  Indeed, we may choose a basis of E as an F vector space of the form $1, \gamma$. Then linear independence implies that $\gamma \notin F$. Let

  $$f(T) = T^2 + aT + b \in F[T]$$

  be the monic minimal polynomial of γ over F.

  For any $s \in F$, we claim that the minimal polynomial of the element $\gamma - s \in E$ has the form

  $$\begin{aligned} f(T+s) &= (T+s)^2 + a(T+s) + b \\ &= T^2 + (a+2s)T + s^2 + as + b \end{aligned}$$

  Taking $s = \dfrac{-a}{2}$, we find that $g(T) = f(T+s)$ has the form

  $$g(T) = T^2 - c$$

  for some $c \in F$, so that $\beta = \gamma - s$ satisfies $\beta^2 = c$. Now it just remains to observe that

  $$F(\gamma) = F(\gamma + s) = F(\beta).$$

  Now, notice that every element of E has the form

  $$a + b\beta \quad \text{for} \quad a, b \in F.$$

Now, the roots of $T^2 - c$ in E are $\pm\beta$. Since $T^2 - c$ is irreducible over F, it follows that there is an isomorphism

$$\phi : E = F(\beta) \to E = F(\beta)$$

for which $\phi(\beta) = -\beta$ and $\phi(s) = s$ for all $s \in F$.

Thus

$$\phi(a + b\beta) = a - b\beta \quad \text{for } a, b \in F.$$

Proposition 14.2.1. *Suppose that the characteristic of F not equal 2. For $E = F(\gamma) = F(\beta)$ a quadratic extension as above, $\operatorname{Aut}_F(E) = \langle\phi\rangle$ and in particular $|\operatorname{Aut}_F(E)| = 2$.*

- Example: quadratic extensions in characteristic 2.

Suppose that the characteristic of F is 2, and consider a polynomial of the form $T^2 - c \in F[T]$. If β is a root of this polynomial then

$$T^2 - c = T^2 - \beta^2 = (T - \beta)^2$$

since the characteristic is 2.

Just for emphasis, let's double check this:

$$(T - \beta)^2 = T^2 - 2\beta T + (-\beta)^2 = T^2 + c = T^2 - c.$$

Thus the polynomial $T^2 - c$ has a single root β which is repeated twice. It is irreducible over F if and only if $\beta \notin F$.

However, in general at least, there are irreducible quadratic polynomials with distinct roots in characteristic 2.

Consider a polynomial of the form

$$f = T^2 + T + a \quad \text{for } a \in F$$

and suppose that β is a root of f; thus

$$\beta^2 + \beta + a = 0.$$

We claim that also $\beta + 1$ is a root of f. Indeed,

$$\begin{aligned} f(\beta + 1) &= (\beta + 1)^2 + (\beta + 1) + a \\ &= \beta^2 + 1 + \beta + 1 + a \\ &= \beta^2 + \beta + a + 2 \\ &= \beta^2 + \beta + a \\ &= f(\beta) = 0. \end{aligned}$$

It follows that

$$f = T^2 + T + a = (T + \beta)(T + \beta + 1)$$

i.e. β and $\beta + 1$ are the distinct roots of f. Recall that $\mathbb{F}_4 = \mathbb{F}_2(\beta)$ where $\beta^2 + \beta = 1$.

Note that the for any F of char. 2, the polynomial $f = T^2 + T + a$ is irreducible if and only if $\beta \notin F$.

Suppose f is irreducible and let $E = F(\beta)$. Recall that an element of E has the form

$$a = b\beta \quad \text{for } a, b \in F.$$

Since β and $\beta + 1$ are the roots of f, there is a automorphism

$$\phi : E = F(\beta) \to E = F(\beta + 1) = F(\beta)$$

for which $\phi(\beta) = \beta + 1$ and $\phi(s) = s$ for $s \in F$.

Thus

$$\phi(a + b\beta) = a + b + b\beta.$$

Remark 14.2.2. When $F = \mathbb{F}_2$ and $\beta^2 + \beta = 1$, notice that

$$(a + b\beta)^2 = \phi(a + b\beta) = a + b + b\beta.$$

15 The Fundamental Theorem of Galois Theory

Let F be a field and let E be the splitting field over F of some *separable* polynomial $g \in F[T]$. Loosely speaking, the fundamental theorem of Galois Theory relates two things:

- *intermediate fields* L, where $F \subset L \subset E$, and
- *subgroups* H, where $H \subset \mathrm{Gal}(E/F)$.

15.1 Subfields from subgroups

Proposition 15.1.1. *Let K be any field and let H be any subgroup of the group* $\mathrm{Aut}(K)$ *of automorphisms of K. Then*

$$K^H = \{x \in K \mid h \cdot x = x \quad \forall h \in H\}$$

is a subfield of K.

Proof. If $x, y \in K^H$ with $x \neq 0$, we must argue that $x - y \in K^H$, that $x \cdot y \in K^H$ and that $\dfrac{1}{x} \in K^H$. But for each $h \in H$ we have:

$$h(x-y) = h(x) - h(y) = x - y \implies x - y \in K^H$$

$$h(x \cdot y) = h(x) \cdot h(y) = x \cdot y \implies x \cdot y \in K^H$$

and

$$h\left(\frac{1}{x}\right) = \frac{1}{h(x)} = \frac{1}{x} \implies \frac{1}{x} \in K^H.$$

□

15.2 Splitting fields and Galois groups

The following result follows the proof of Lemma 11.3.1

Proposition 15.2.1. *Let $g \in F[T]$ be a separable polynomial and let E be a splitting for g over F. Suppose that $\phi : F \to F_1$ is a field isomorphism*

Proposition 15.2.2. *Suppose that E is the splitting field over F of a separable polynomial $g \in F[T]$. Let $\Gamma = \mathrm{Gal}(E/F)$. Then $F = E^\Gamma$.*

Proof. Let $L = E^\Gamma$, so that L is an intermediate field:

$$F \subset L = E^\Gamma \subset E.$$

Viewing g as a polynomial in $L[T]$, it is clear that E is a splitting field of g over L.

Now, applying the main result about the plitting field of a separable polynomial from the lecture of *Week 10**, we see that

$$[E : L] = |\,\mathrm{Gal}(E/L)|$$

and that

$$[E : F] = |\operatorname{Gal}(E/F)|.$$

Since $F \subset L$, we have $\operatorname{Gal}(E/L) \subset \Gamma = \operatorname{Gal}(E/F)$. The assumption $L = E^\Gamma$ shows that any automorphism of E which is the identity on F is the identity on L; this shows that

$$\Gamma = \operatorname{Gal}(E/F) = \operatorname{Gal}(E/L).$$

It now follows that $[E : L] = [E : F]$ and hence that $L = F$. □

15.3 Fixed fields and some linear algebra

The correspondence between subgroups $H \subset \operatorname{Gal}(E/F)$ and intermediate fields $F \subset L \subset E$ will be given by the assignment

$$H \mapsto E^H$$

(we'll formulate the statement more precisely later on).

We are ultimately going to argue that this assignment determines a one-to-one correspondence between the subgroups and the intermediate fields. For this, we require some numerical estimates relating the degrees $[E : E^H]$ and the orders $|H|$. These estimates are obtained using a result of E. Artin:

Proposition (Artin).

Proposition 15.3.1. *Let G be a finite group of automorphisms of a field K and let $L = K^G$. Then $[K : L] \le |G|$.*

Proof. If $|G| = n$, let us write

$$G = \{\theta_1, \theta_2, \ldots, \theta_n\}$$

where $\theta_1 = 1_G$.

We must argue that $[K : L] \le n$. Suppose the contrary, and choose $n + 1$ elements $u_1, u_2, \ldots, u_{n+1} \in K$ which are linearly independent over L.

Now form the following $n \times (n + 1)$ matrix with entries in K:

$$M = \begin{pmatrix} \theta_1(u_1) & \theta_1(u_2) & \cdots & \theta_1(u_{n+1}) \\ \theta_2(u_1) & \theta_2(u_2) & \cdots & \theta_2(u_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \theta_n(u_1) & \theta_n(u_2) & \cdots & \theta_n(u_{n+1}) \end{pmatrix} \in \operatorname{Mat}_{n\times(n+1)}(K).$$

Since M has n rows, we know that the *rank* of M satisfies

$$\operatorname{rk}(M) \le n.$$

On the other hand, linear algebra tells us that

$$\dim_K \operatorname{Null}(M) + \operatorname{rk}(M) = n + 1 = \#\text{ of columns of } M.$$

Thus

$$\dim_K \operatorname{Null}(M) = n + 1 - \operatorname{rk}(M) \ge n + 1 - n = 1$$

and we conclude that there is a non-zero solution $\mathbf{x} = \mathbf{a} \in K^{n+1}$ to the matrix equation

$$(\clubsuit) \quad M \cdot \mathbf{x} = \mathbf{0}.$$

Among all possible non-zero solutions

$$\mathbf{0} \neq \mathbf{a} = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n+1} \end{pmatrix}^T$$

to (♣), choose one with the smallest number of non-zero coefficients $a_i \in K$.

After renumbering the indices on the u_i and the x_j, we may suppose that $a_1 \neq 0$. Since the vector $\left(\frac{1}{a_1}\right) \cdot \mathbf{a}$, remains a solution to (♣), we may and will suppose that $a_1 = 1$.

Recall that $\theta_1 = 1_G = \mathrm{id}_K$. The first coefficient in the vector equation

$$\mathbf{0} = M \cdot \mathbf{a}$$

gives

$$0 = \sum_{i=1}^{n+1} a_i \theta_1(u_i) = \sum_{i=1}^{n+1} a_i u_i.$$

Since the u_i are linearly independent over L by assumption, some a_j must be in K and not in $L = K^G$.

Renumbering again, we may and will suppose that $a_2 \in K$, $a_2 \notin L = K^G$.

Of course, $a_2 \notin K^G \implies ga_2 \neq a_2$ for some $g \in G$, and in turn we recall that $g = \theta_i$ for some $i > 1$ hence we have

$$\theta_i(a_2) \neq a_2.$$

Consider the matrix $\theta_i(M) \in \mathrm{Mat}_{n \times (n+1)}(K)$ given b y

$$\theta_i(M) = \begin{pmatrix} \theta_i \cdot \theta_1(u_1) & \theta_i \cdot \theta_1(u_2) & \cdots & \theta_i \cdot \theta_1(u_{n+1}) \\ \theta_i \cdot \theta_2(u_1) & \theta_i \cdot \theta_2(u_2) & \cdots & \theta_i \cdot \theta_2(u_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \theta_i \cdot \theta_n(u_1) & \theta_i \cdot \theta_n(u_2) & \cdots & \theta_i \cdot \theta_n(u_{n+1}) \end{pmatrix}.$$

Since G is group, the rows of $\theta_i(M)$ are the same as those of M, but in a different *order*. In particular,

$$\mathrm{Null}(M) = \mathrm{Null}(\theta_i(M)).$$

On the other hand, it is clear that

$$\mathbf{0} = \theta_i(\mathbf{0}) = \theta_i(M \cdot \mathbf{a}) = \theta_i(M) \cdot \theta_i(\mathbf{a}).$$

This proves that both $\mathbf{a}$ and $\theta_i(\mathbf{a})$ are solutions to (♣), hence $\mathbf{v} = \mathbf{a} - \theta_i(\mathbf{a})$ is a solution to (♣), as well.

Now

$$\mathbf{a} = \begin{pmatrix} 1 & a_2 & \cdots & a_{n+1} \end{pmatrix}^T$$

and

$$\theta_i(\mathbf{a}) = \begin{pmatrix} 1 & \theta_i(a_2) & \cdots & \theta_i(a_{n+1}) \end{pmatrix}^T.$$

Since $a_2 \neq \theta_i(a_2)$, $\mathbf{v} = \mathbf{a} - \theta_i(\mathbf{a})$ is non-zero. On the other hand, the first coefficient of $\mathbf{v} = \mathbf{a} - \theta_i(\mathbf{a})$ is 0, hence $\mathbf{v}$ has more non-zero terms than does $\mathbf{a}$. This contradicts the choice of $\mathbf{a}$, and completes the proof. □

15.4 Normal extensions

Let E be an algebraic extension of the field F. We will say that E is a *normal extension* of F if every polynomial that contains a root in E actually *splits* over E.

In order to check that E is a normal extension of F, it is enough to verify that each *irreducible* polynomial with a root in E actually splits over E.

Proposition 15.4.1. *Let E be an extension field of F, and let $\Gamma = \mathrm{Gal}(E/F)$.*

a. If $F = E^\Gamma$, then E is a normal, separable extension of F.

b. ::Let E be the splitting field over F of some separable polynomial $g \in F[T]$. Then E is a normal (and separable) extension of F

Proof. According to the [Proposition on splitting fields and fixed fields](#splitting-fields-and-fixed-fields), the field extension $E \supset F$ in b. satisfies the condition in a. So b. is an immediate consequence of a.

To prove a., let $h \in F[T]$ be an *irreducible* polynomial, and suppose that $\alpha \in E$ is a root of h. We must argue that h is separable and actually *splits* over E

Consider the *orbit* $\mathcal{O}$ of the root α under the action of Γ:

$$\mathcal{O} = \{g\alpha \mid g \in G/H\}$$

where $H = \mathrm{Stab}_\Gamma(\alpha)$.

If $g_1, \dots, g_m$ is a system of coset representatives for H in Γ, there are $m = [\Gamma : H]$ distinct elements of $\mathcal{O}$:

$$\mathcal{O} = \{g_1\alpha, g_2\alpha, \cdots, g_m\alpha\}.$$

Form the polynomial

$$h_1 = \prod_{\beta \in \mathcal{O}} (T - \beta) = \prod_{g \in \Gamma/H} (T - g\alpha) \in E[T].$$

Note that by construction h_1 has m distinct roots in E. We first claim that in fact $h_1 \in F[T]$.

Of course, for any polynomial $\ell \in E[T]$, we know that

$$\ell \in F[T] = E^\Gamma[T] \quad \iff \quad x\ell = \ell \quad \text{for all } x \in \Gamma.$$

Thus, we must argue for each $x \in \Gamma$ that $xh_1 = h_1$.

Well, for $x \in \Gamma$, we have

$$xh_1 = x.\left(\prod_{g \in \Gamma/H} (T - g\alpha)\right) = \prod_{g \in \Gamma/H} (T - xg\alpha) = \quad (\diamondsuit).$$

Now using the substitution $h = xg$, note that

$$(\diamondsuit) = \prod_{h \in \Gamma/H} (T - h\alpha) = h_1.$$

This proves that $h_1 \in F[T]$.

Since h is the *minimal polynomial* of α over F, since $h_1 \in F[T]$, and since h_1 has α as a root by construction, we conclude that $h \mid h_1$. Since h_1 splits over E, unique factorization in $E[T]$ shows that h splits over E. Since h_1 is separable, also h is separable. This completes the proof that E is a normal, separable extension of F. □

Proposition 15.4.2. *Let E be a finite, normal, separable extension of F. Then E is the splitting field over F of a separable polynomial $g \in F[T]$.*

Proof. Let $\alpha_1, \dots, \alpha_n \in E$ be elements such that $E = F(\alpha_1, \dots, \alpha_n)$. For $1 \le i \le n$, write $f_i \in F[T]$ for the minimal polynomial over F of the element α_i.

Since f_i has the root α_i in E and since E is normal over F, the polynomial f_i splits over E. Since E is generated over F by the roots of the f_i, it follows that E is a splitting field of the separable polynomial

$$f = \prod_{i=1}^{n} f_i \in F[T].$$

□

Remark 15.4.3. It is actually true that any finite separable extension $F \subset E$ is *primitive*; namely, there is an element $\alpha \in E$ such that $E = F(\alpha)$ – this result is known as the *Primitive Element Theorem*. We don't require this fact, and so I haven't given a proof. The proof of the previous Proposition would be slightly more streamlined using the Primitive Element Theorem.

15.5 The Fundamental Theorem

Before stating the main theorem of Galois theory, observe that results so far enable us to recognize Galois groups in some useful situations:

Proposition 15.5.1. *Suppose that $F \subset E$ is an extension field, that $G \subset \mathrm{Aut}(E)$ is a finite group of automorphisms, and that $F = E^G$. Then*

$$G = \mathrm{Gal}(E/F).$$

Proof. According to the [Proposition](#normal-as-fixed-field}) above, E is a separable and normal extension of F, and $[E : F] = |\,\mathrm{Gal}(E/F)|$.

Since $F = E^G$, note that $G \subset \mathrm{Gal}(E/F)$. Artin's Proposition implies that $[E : F] \le |G|$, and we see that

$$[E : F] \le |G| \le |\,\mathrm{Gal}(E/F) = [E : F].$$

Thus equality holds everywhere, and we conclude that $G = \mathrm{Gal}(E/F)$ as required. □

Theorem 15.5.2. *Let E be a splitting field over F of a separable polynomial $g \in F[T]$, and let $\Gamma = \mathrm{Gal}(E/F)$.*

a. There is a one-to-one correspondence between subgroups of Γ and intermediate fields of the extension $F \subset E$ given by $H \mapsto E^H$.

i. If H is a subgroup of Γ, we have

$$H = \mathrm{Gal}(E/E^H).$$

ii. If $F \subset K \subset E$ is an intermediate field, the corresponding subgroup is $\mathrm{Gal}(E/K) \subset \Gamma$, and we have

$$K = E^{\mathrm{Gal}(E/K)}.$$

b. *For any subgroup $H \subset \Gamma$,*

$$[E : E^H] = |H| \quad \textit{and} \quad [E^H : F] = [\Gamma : H].$$

c. *::Under the correspondence of a., the subgroup H is normal in Γ if and only if the subfield $K = E^H$ is a normal extension of F. If this is the case, then*

$$\mathrm{Gal}(E^H/F) = \Gamma/H \simeq \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K).$$

Proof. For (a), write $\mathscr{G}$ for the set of subgroups of Γ and write $\mathscr{I}$ for the set of intermediate fields K (so $F \subset K \subset E$).

We consider the mapping

$$\mathscr{G} \to \mathscr{I} \quad \text{given by } H \mapsto E^H$$

and the mapping

$$\mathscr{I} \to \mathscr{G} \quad \text{given by } K \mapsto \mathrm{Gal}(E/K).$$

Let us pause to observe that if $H_1, H_2 \subset G$ are subgroups with $H_1 \subset H_2$, then $E^{H_2} \subset E^{H_1}$ – so the assignment $H \mapsto E^H$ is *inclusion reversing.*

Similarly, if $K_1 \subset K_2$ are intermediate fields, then $\mathrm{Gal}(E/K_2) \subset \mathrm{Gal}(E/K_1)$, so the assignment $K \mapsto \mathrm{Gal}(E/K)$ is inclusion reversing.

We observe that the statements of i. and ii. precisely confirm that these mappings are inverse to one another. So to prove a., we need to confirm that

$$\text{i.} \quad \mathrm{Gal}(E/E^H) = H,$$

and that

$$\text{ii.} \quad K = E^{\mathrm{Gal}(E/K)}$$

.

Now, i. is an immediate consequence of [Proposition (Recognition of Galois Groups)](#recognition-of-galois-groups).

On the other hand, suppose that K is an intermediate field: $F \subset K \subset E$. Since E is the splitting field of a separable polynomial over F, then also E is the splitting field over K. Thus the [Proposition on splitting fields and fixed fields](#splitting-fields-and-fixed-fields) implies that $E^{\mathrm{Gal}(E/K)} = K$ as required.

This completes the proof of a. As to b., let H be a subgroup of Γ. Since E is a splitting field over E^H of a separable polynomial, and since we've already seen that $H = \mathrm{Gal}(E/E^H)$, [an earlier Theorem](10a–galois-first-steps.html##automorphisms-and-splitting-fields) shows that

$$[E : E^H] = |H|.$$

Now, the same reasoning shows that $F = E^\Gamma$ and

$$[E : F] = [E : E^\Gamma] = |\Gamma|.$$

The remaining statement of b. now follows from a calculation:

$$[E^H : F] = \frac{[E : F]}{[E : E^H]} = \frac{|\Gamma|}{|H|} = [\Gamma : H].$$

This completes the proof b.

Finally, consider c. Let $F \subset K \subset E$ be an intermediate extension, and let $H = \mathrm{Gal}(E/K) \subset \Gamma$. We must argue that K is a normal extension of F if and only if H is a normal subgroup of Γ, and in case H is normal, we will argue that Γ/H is isomorphic to $\mathrm{Gal}(K/F)$.

$\Rightarrow$: Suppose that K is a normal extension of F. To show that H is a normal subgroup of Γ, let ϕ be an arbitrary element of Γ, and let $\theta \in H = \mathrm{Gal}(E/K)$.

We must argue that $\phi^{-1} \circ \theta \circ \phi \in H$. For this, we must argue that $\phi^{-1} \circ \theta \circ \phi$ is the identity on K.

Let $u \in K$ and let $p \in F[T]$ be the minimal polynomial of u over F. Since $\phi \in \Gamma = \mathrm{Gal}(E/F)$, the element $\phi(u)$ is again a root of p. Since K is a normal extension, it follows that $\phi(u) \in K$. Now, $\theta_{|K}$ is the identity on K, so that

$$\theta(\phi(u)) = \phi(u) \implies \phi^{-1} \circ \theta \circ \phi(u) = u.$$

This proves that indeed H is normal in K.

$\Leftarrow$: Suppose that H is a normal subgroup of Γ. We must argue that K is a normal extension of F.

We are first going to argue that $\Gamma/H \simeq \mathrm{Gal}(K/F)$. To carry out this argument, we first contend that for any automorphism ϕ in Γ, the restriction of ϕ to K takes values in K. Let $u \in K$.

To argue that $\phi(u) \in K = E^H$, let $\theta \in H$. Since H is normal in Γ, $\theta_1 = \phi^{-1} \circ \theta \circ \phi \in H$. Thus

$$\theta \circ \phi = \phi \circ \theta_1.$$

Now notice that

$$\theta(\phi(u)) = \phi(\theta_1(u)) = \phi(u)$$

since θ_1 is the identity on K. This shows that indeed $\phi(u) \in E^H = K$.

It now follows that the restriction of ϕ to K takes values in K. Since $\ker \phi = \{0\}$, ϕ is a one-to-one mapping. Since ϕ is an F-linear mapping and K is a finite dimensional vector space over F, conclude that $\phi_{|K}$ is onto and thus determines an automorphism of K.

We have thus defined a *group homomorphism*

$$(\diamondsuit) \quad \phi \mapsto \phi_{|K} : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F).$$

The kernel of the group homomorphism $(\diamondsuit)$ consists in the automorphisms ϕ whose restriction to K is the identity – i.e. the kernel is $\mathrm{Gal}(E/K) = H$.

On the other hand, we claim that the homomorphism $(\diamondsuit)$ is *onto*. Indeed, since E is a splitting field over K of a (separable) polynomial, an earlier [Proposition on uniqueness of splitting fields](04c–Splitting-fields.html#uniqueness-of-splitting-fields) shows that for any automorphism $\theta : K \to K$, we may find an automorphism $\widehat{\theta} : E \to E$ with $\widehat{\theta}_{|K} = \theta$.

It now follows that $\Gamma/H \simeq \mathrm{Gal}(K/F)$.

To complete the proof that K is normal, note first that $[\Gamma : H] = [K : F]$ by b. This proves that $|\mathrm{Gal}(K/F)| = [K : F]$. Since $\mathrm{Gal}(K/F)$ is a finite group, the [Proposition on normal extensions as fixed fields](#normal-as-fixed-field) implies that K is a normal separable extension of $K^{\mathrm{Gal}(K/F)}$.

But then

$$[K : K^{\mathrm{Gal}(K/F)}] = |\mathrm{Gal}(K/F)| = [K : F]$$

which implies that $F = K^{\mathrm{Gal}(K/F)}$ and we conclude that K is a normal separable extension of F. This completes the proof of c, and of the Theorem. $\square$

Bibliography

Artin, Michael. 2011. *Algebra*. 2nd ed. Pearson Education.

Friedberg, Stephen H., Arnold J. Insel, and Lawrence E. Spence. 2002. *Linear Algebra*. 4th edition. Upper Saddle River, NJ: Pearson.

Hoffman, Kenneth, and Ray Alden Kunze. 1971. *Linear Algebra*. 2nd ed. Prentice-Hall.