# Math146 - Lecture notes

George McNinch

2025-02-14 09:50:37 EST (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) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

(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 $R = \mathrm{Mat}_2(\mathbb{R})$.

(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) $\phi$ is a homomorphism of *additive groups*,

(b) $\phi$ 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 $\phi$ 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 $n \in \mathbb{Z}_{>0}$ and consider the principal ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ generated by $n \in \mathbb{Z}$.

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

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ 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 $\phi$ is* surjective *(i.e.* onto*). Then $\phi$ 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 $I = 0+I \in R/I$. $\square$

## 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 $\Phi$ 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 $\Phi$ 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 $a = b$. □

**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. □

## 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 $\Psi$ 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 $\Psi$ 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,

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

□

## 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)* $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ *and equality holds if* $\deg(f) \neq \deg(g)$.

*(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 $g = 0$. □

**Proposition 3.3.4.** *Let $f, g \in F[T]$. If $g \neq 0$ 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 $0 \neq g$. 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 $\deg(f) \geq 0$.

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 $m \leq n$ 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. □

**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 $\alpha_2$ is a root of $f$ we see that

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

which shows that $\alpha_2$ 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. □

# 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 (♣): 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 (♣) 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 (♣) 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. □

*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 (♣) 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 $1 \leq i \leq n$.*

*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). $\square$

# 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.

□

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 $\frac{a}{b} = [(a,b)]$ 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 $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{s}{t} = \frac{s'}{t'}$, we must check that $\frac{a}{b} + \frac{s}{t} = \frac{a'}{b'} + \frac{s'}{t'}$; 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 $0 = \frac{0}{1}$ is an identity for the binary operation $+$ on $Q$.

- One readily checks that $+$ is commutative for $Q$.

- One readily checks that $\frac{-a}{b}$ is an additive inverse for $\frac{a}{b}$.

- 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 $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{s}{t} = \frac{s'}{t'}$, we must check that $\frac{a}{b} \cdot \frac{s}{t} = \frac{a'}{b'} \cdot \frac{s'}{t'}$; i.e. that

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

- One readily checks that $1 = \dfrac{1}{1}$ 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!* □

*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 $r \mapsto i(r) = \dfrac{r}{1}$ for $r \in R$. This homomorphism is one-to-one: indeed, if $\dfrac{r}{1} = 0 = \dfrac{0}{1}$, 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 $x = \dfrac{a}{b} = \dfrac{a}{1} \cdot \dfrac{1}{b}$ 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. □

*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 $\dfrac{f}{g}$ 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 $\alpha$ has a multiplicative inverse. Thus $\alpha$ 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 $\beta$ is the multiplicative inverse of $\alpha$ 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 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* 7.2.1. Note that in the case where $R$ is *already* a polynomial ring $F[X]$, we introduce a *new* variable $T$ different from $X$.

*Definition* 7.2.2. 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 7.2.3.** *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. □

**Lemma 7.2.4.** *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 $i$. □

**Proposition 7.2.5.** *("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 7.2.4.

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 7.2.4 (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 $\text{content}(fg) = 1$. □

**Theorem 7.2.6.** *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 7.2.3, we may write $g = \frac{x}{y} g_1$ and $h = \frac{z}{w} h_1$ 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 7.2.5 – 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. □

## 7.3 Eisenstein's irreducibility criterion

**Theorem 7.3.1.** *Let $p \in R$ be irreducible, and let*

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

*be a polynomial with $a_n \neq 0$. Suppose that $p \nmid a_n$, that $p \mid a_i$ for $0 \leq i \leq n-1$ 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 $\widetilde{f} = \frac{1}{c} f \in R[T]$ 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 7.2.6 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 7.2.4. 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 $0 \leq i, j \leq n$. 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* 7.3.2. (a) Let $p$ be a prime integer, let $n \geq 1$ and let $f = T^n - p$. Then Theorem 7.3.1 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 $n \geq 1$ and consider the polynomial $f = T^n - X \in F[T] = K(X)[T]$. Then $f$ is irreducible in $K(X)[T]$ by Theorem 7.3.1.

## 7.4 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

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

**Proposition 7.4.1.** *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 irreduciblity will now follow from Theorem 7.3.1 once we argue that (♣) : $p \mid \binom{p}{i}$ for each $1 \leq i \leq p-1$.

To prove (♣) 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. □

*Example* 7.4.2. For example, $f(T) = T^4 + T^3 + T^2 + T + 1 \in \mathbf{Q}[T]$ is an irreducible since $f(T) = \dfrac{T^5 - 1}{T - 1}$ 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. □

**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! □

**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. □

**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. □

## 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 $V = \mathrm{span}(S)$ 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 $\alpha$ is a root – i.e. for which $f(\alpha) = 0$.

If $\alpha$ is not algebraic over $F$, we say that $\alpha$ is *transcendental* over $F$.

*Example* 9.1.2.

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

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

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

## 9.2 The minimal polynomial

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

*Moreover,*

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

*$\alpha$ 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 $\alpha$ 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 $p \mid g$. □

**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 $\alpha$ 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 $\alpha$ over $F$.
- The *degree* of $\alpha$ 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 $z = a+bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$. Then $z$ has degree $\leq 2$ over $\mathbb{R}$, and that degree is 2 if and only if $b \neq 0$.

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

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

Since $p$ has roots $z, \overline{z}$, it has no real roots; since it has degree 2, $p$ is irreducible over $\mathbb{R}$. 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 $\infty$).

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

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

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

On the other hand, $\alpha$ 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 $\alpha$ is a root of $T^2 - \sqrt{2} \in F[T]$, the degree of $\alpha$ over $F$ is $\leq 2$. 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 $a, b \in \mathbb{Q}$.

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

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

is indeed irreducible.

We repeat for emphasis:

- the minimal polynomial of $\alpha$ over $\mathbb{Q}$ is $T^4 - 2$ and has degree 4,
- the minimal polynomial of $\alpha$ over $\mathbb{Q}(\sqrt{2})$ 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 $\alpha$ is algebraic over $F$ with minimal polynomial $p \in F[T]$ over $F$, then*

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

*where $\alpha$ 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 $\alpha$ 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 $\phi$ induces the desired isomorphism.

First consider case (a). Suppose that $\alpha$ 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, $\phi$ induces an isomorphism between $F[T]/\langle p \rangle$ and its image $K$. Thus $K \subset E$ is a subfield containing $F$ and $\alpha$, so by definition $F(\alpha) \subset K$.

On the other hand, $\alpha$ 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 $\alpha$ must contain all $F$-linear combinations of the elements $\alpha^i$; 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 $\alpha$ 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 $\alpha$. On the other hand, any subfield of $E$ containing $\alpha$ must contain the image of $\widetilde{\phi}$ and statement (b) follows at once. □

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

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

*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, $\gamma$ is mapped to $\sqrt[3]{2}$. Put another way, $\gamma$ 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 $\alpha$; i.e. by the rule $\lambda_\alpha(\beta) = \alpha \cdot \beta$ for $\beta \in E$.

We are going to compute the *matrix* of $\lambda_\alpha$ 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 $3 \times 3$ 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 $M_\alpha$ is the matrix determined by the linear transformation $\lambda_\alpha$, 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 ${M_{1+\gamma}}^{-1} = \frac{1}{3}\begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$ 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 $\alpha$ is algebraic over $F$ if and only if $[F(\alpha) : F] < \infty$.*

*Remark* 9.4.3. If $\alpha$ 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. $\alpha$ 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 $\alpha$ is algebraic, let $d = \deg \alpha$ be the degree of $\alpha$ over $F$. We have seen that $1, \alpha, \ldots, \alpha^{d-1}$ 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 $i \in \mathbb{Z}_{\geq 0}$. 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 $c_0, c_1, \ldots, c_d \in F$ 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 $\alpha$ 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

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

and let

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

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 $v_{s,t} = 0$.

□

**Corollary 9.4.6.** *Let $E$ be a finite extension of $F$. If $\alpha \in E$ then the degree of $\alpha$ 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 $[F(\alpha) : F] = \deg_F \alpha$. □

## 9.5 Examples of finite extensions

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

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

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

If we verify the claim, it follows that

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

and thus

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

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 $\mathbb{Q}(\sqrt{2})$.

So: suppose that $3 = (a+b\sqrt{2})^2$ for $a, b \in \mathbb{Q}$. 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 $\mathbb{Q}$). This completes the proof that $T^2-3$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

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

To prove the claim, we argue that

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

the assertion then follows from the previous example.

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

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

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 $a, b, c, d \in \mathbb{Q}$, 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

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

is a subfield of $E$.

For example, this requires us to know that if $x, y \in E_{\text{alg}}$ then $x - y \in E_{\text{alg}}$. 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, $\beta$ is algebraic over $F$ hence algebraic over $F(\alpha)$ so

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

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

Since $\alpha$ 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 $E_{\text{alg}}$ of $E$.*

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

It now remains to argue that $E_{\text{alg}}$ 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 $\alpha$ 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 $\alpha_1, \ldots, \alpha_n \in E$. Then*

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

*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 $E_i = F(\alpha_1, \ldots, \alpha_i)$ 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 $\alpha_n$ is algebraic over $F$ – $\alpha_n$ 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 $\alpha$ is algebraic over $F$. Since $\alpha$ 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 $E_1 = F(a_0, a_1, \ldots, a_N)$. 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 $\alpha$ 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 $\alpha$ is algebraic over $F$ by Proposition 9.6.4. □

## 9.7 Another example

Consider the field $K = \mathbb{Q}(T)$ where $T$ is transcendental over $\mathbb{Q}$. It follows from Theorem 7.3.1 that

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

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

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

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

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

*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 $\alpha$ 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. □

## 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.