CHAPTER 2

Rings and Modules

2.1. Rings, Basic Definitions

Definition 2.1. A *ring* is a nonempty set R equipped with two operations $+$ and $\cdot$ such that

(i) $(R,+)$ is an abelian group;
(ii) $(ab)c = a(bc)\ \forall a,b,c \in R$;
(iii) $a(b+c) = ab+ac$, $(a+b)c = ac+bc\ \forall a,b,c \in R$.

If $ab = ba$ for all $a,b \in R$, R is called *commutative*. If $\exists 1_R \in R$ such that $1_R a = a 1_R = a\ \forall a \in R$, 1_R is called the identity of R.

Subring. Let $(R,+,\cdot)$ be a ring. $S \subset R$ is called a *subring* of R if $(S,+,\cdot)$ is a ring.

Homomorphism. Let R and S be rings. A map $f : R \to S$ is called a *homomorphism* if $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ for all $a,b \in R$. An *isomorphism* is a bijective homomorphism.

Note. In general, a ring may not have an identity, e.g. $2\mathbb{Z}$. If S is a subring of R, any of the following could happen: (i) R has identity, S does not ($R = \mathbb{Z}$, $S = 2\mathbb{Z}$); (ii) S has identity, R does not ($R = \mathbb{Z}\times 2\mathbb{Z}$, $S = \mathbb{Z}\times\{0\}$); (iii) R and S both have identity but $1_R \neq 1_S$ ($R = \mathbb{Z}\times\mathbb{Z}$, $S = \mathbb{Z}\times\{0\}$). If R and S are two rings with identity, a homomorphism $f : R \to S$ does not necessarily map 1_R to 1_S. However, we make the following declaration.

Declaration. In these notes, unless specified otherwise, it is assumed that a ring has identity; if S is a subring of R, $1_S = 1_R$; a homomorphism maps identity to identity.

Basic properties of rings.

(i) $0_R \cdot a = a \cdot 0_R = 0_R$, $a \in R$.
(ii) $(na)b = a(nb) = n(ab)$, $m(na) = (mn)a,\ a,b \in R,\ m,n \in \mathbb{Z}$.
(iii)
$$\Big(\sum_{i=1}^n a_i\Big)\Big(\sum_{j=1}^m b_j\Big) = \sum_{i=1}^n\sum_{j=1}^m a_ib_j.$$
(iv) Assume $a_1,\dots,a_s \in R$ are pairwise commutative. Then
$$(a_1+\cdots+a_s)^n = \sum_{i_1+\cdots+i_s=n} \frac{n!}{i_1!\cdots i_s!} a_1^{i_1}\cdots a_s^{i_s}.$$

The multiplicative group. $a \in R$ is call a *unit* (or invertible) if $\exists b \in R$ such that $ab = ba = 1_R$. $R^\times :=$ the set of all units of R. $(R^\times,\cdot)$ is the *multiplicative group* of R.

Types of rings.

Integral domain. R: commutative, $1_R \neq 0$, no zero divisors (i.e., $ab = 0 \Rightarrow a = 0$ or $b = 0$).

Division ring (skew field). R: $1_R \neq 0$, $R^\times = R \setminus \{0\}$.

Field. Commutative division ring.

Examples.

Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (p prime).

Integral domains (not fields): $\mathbb{Z}$, $D[x]$ (the polynomial ring over an integral domain D).

Noncommutative rings: $M_{n\times n}(R)$ = the ring of $n \times n$ matrices over a ring R.

Endomorphism ring. Let A be an abelian group, $\text{End}(A) = \text{Hom}(A, A)$. $(\text{End}(A), +, \circ)$ is the *endomorphism ring* of A.

Fact. Every ring R is a subring of $\text{End}\big((R, +)\big)$.

Proof. We have

$$\begin{array}{rccc} f: & R & \hookrightarrow & \text{End}\big((R,+)\big) \\ & r & \longmapsto & f(r) \end{array}$$

where

$$\begin{array}{rccc} f(r): & (R,+) & \longrightarrow & (R,+) \\ & x & \longmapsto & rx. \end{array}$$

□

Example (*Real quaternions*, a division ring which is not a field).

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k : a_1, \dots, a_4 \in \mathbb{R}\}.$$

Addition: coordinate wise; multiplication: defined by the distributive laws and the rules $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ik = -j$, $kj = -i$, $ji = -k$. If $z = a_1 + a_2 i + a_3 j + a_4 k$, define $\bar{z} = a_1 - a_2 i - a_3 j - a_4 k$. $z\bar{z} = a_1^2 + a_2^2 + a_3^2 + a_4^2$. If $z \neq 0$, $z^{-1} = \frac{1}{z\bar{z}} z$.

Group rings. Let G be a group (written multiplicatively) and R a ring. The *group ring* $R[G]$:= the set of all *formal* sums $\sum_{g\in G} r_g g$, where $r_g \in R$ and $r_g = 0$ except for finitely many $g \in G$.

$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g := \sum_{g\in G} (r_g + s_g) g,$$

$$\Big(\sum_{h\in G} r_h h\Big)\Big(\sum_{k\in G} s_k k\Big) = \sum_{g\in G}\Big(\sum_{\substack{h,k\in G\\ hk=g}} r_h s_k\Big) g.$$

If $X \subset G$ is closed under multiplication and $e \in X$, then $R[X] = \{\sum_{g\in X} r_g g \in R[G]\}$ is a subring of $R[G]$.

Characteristic. The *characteristic* of a ring R ($\text{char}\, R$) is the smallest $n \in \mathbb{Z}^+$ such that $na = 0$ for all $a \in R$. If no such n exists, $\text{char}\, R = 0$. ($\text{char}\, \mathbb{Z}_n = n$, $\text{char}\, \mathbb{Q} = 0$.)

Fact. If D is an integral domain, $\text{char}\, D = 0$ or a prime.

Ideals. Let R be a ring. $I \subset R$ is called a *left* (*right*) *ideal* of R if I is a subgroup of $(R, +)$ and $ax \in R$ for all $a \in R$, $x \in I$. An *ideal* is a two-sided ideal.

If $X \subset R$, the ideal of R generated by X (the smallest ideal containing X) is

$$\langle X \rangle \text{ (or } (X)) = \Big\{ \sum_{i=1}^{n} a_i x_i b_i : n \geq 0,\ a_i, b_i \in R,\ x_i \in X \Big\}.$$

An ideal generated by one element is called a *principal ideal*.

Sum and product of ideals. Let I, J be left (right) ideals of R. Define

$$I + J = \{a + b : a \in I,\ b \in J\}.$$

$I + J$ is the smallest left (right) ideal of R containing $I \cup J$.

If I and J are ideals of R, define

$$IJ = \Big\{ \sum_{i=1}^{n} a_i b_i : n \geq 0,\ a_i \in I,\ b_i \in J \Big\}.$$

IJ is an ideal of R and $IJ \subset I \cap J$.

The quotient ring. Let I be an ideal of R. Then R/I is an abelian group. For $a + I, b + I \in R/I$, define $(a + I)(b + I) = ab + I$. The multiplication is well defined and $(R/I, +, \cdot)$ is a ring, called the *quotient ring* of R by I.

$$\begin{array}{rccc} \pi : & R & \longrightarrow & R/I \\ & r & \longmapsto & r + I \end{array}$$

is an onto homomorphism (canonical homomorphism).

Fact. I is an ideal of $R \Leftrightarrow I = \ker f$ for some homomorphism $f : R \to S$.

Proposition 2.2 (Universal mapping property). *Let $f : R \to S$ be a homomorphism of rings and let I be an ideal of R such that $I \subset \ker f$. Then there exists a unique homomorphism $\bar{f} : R/I \to S$ such that the following diagram commutes.*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Isomorphism theorems.

(i) Let $f : R \to S$ be a homomorphism of rings. Then $R/\ker f \cong f(R)$.

(ii) Let $I \subset J$ be ideals of R. Then $(R/I)/(J/I) \cong R/J$.

The correspondence theorem. Let I be an ideal of R. Let $\mathcal{A}$ = the set of all ideals of R containing I, $\mathcal{B}$ = the set of all ideals of R/I. Then $\mathcal{A} \to \mathcal{B}$: $J \mapsto J/I$, is a bijection.

$\mathfrak{m}$-adic topology. Let R be a ring and $\mathfrak{m}$ an ideal of R. For each $x \in R$, $\{x + \mathfrak{m}^n : n \in \mathbb{N}\}$ form a neighborhood base of x. The topology on R defined by this neighborhood base is called the $\mathfrak{m}$-*adic topology*. The following mappings are continuous in the $\mathfrak{m}$-adic topology.

(i) $R \times R \to R$, $(x, y) \mapsto x + y$;

(ii) $R \to R$, $x \mapsto -x$;

(iii) $R \times R \to R$, $(x, y) \mapsto xy$.

(A ring R endowed with a topology such that mappings (i) – (iii) are continuous is called a *topological ring*. Thus R with the $\mathfrak{m}$-adic topology is a topological ring.)

Proof. (i) $(x+\mathfrak{m}^n)+(y+\mathfrak{m}^n)\subset x+y+\mathfrak{m}^n$.
(ii) $-(x+\mathfrak{m}^n)\subset -x+\mathfrak{m}^n$.
(iii) $(x+\mathfrak{m}^n)(y+\mathfrak{m}^n)\subset x+y+\mathfrak{m}^n$. □

The ideal $\mathfrak{m}^n$ is both open and closed. (For every $x\in\mathfrak{m}^n$, $x+\mathfrak{m}^n\subset\mathfrak{m}^n$; hence $\mathfrak{m}^n$ is open. $R\smallsetminus\mathfrak{m}^n=\bigcup_{x\in R\smallsetminus\mathfrak{m}^n}(x+\mathfrak{m}^n)$ is open. So $\mathfrak{m}^n$ is closed.) The $\mathfrak{m}$-adic topology is Hausdorff $\Leftrightarrow\bigcap_{n=0}^{\infty}\mathfrak{m}^n=\{0\}$. The $\mathfrak{m}$-adic topology is discrete $\Leftrightarrow\mathfrak{m}$ is nilpotent (i.e., $\mathfrak{m}^n=0$ for some $n>0$).

2.2. Prime Ideals and Maximal Ideals

Definition 2.3. An ideal P of R is called a *prime* ideal if (i) $P\neq R$ and (ii) if A,B are ideals of R such that $AB\subset P$, then $A\subset P$ or $B\subset P$.

An ideal M of R is called *maximal* if $M\neq R$ and there is no ideal strictly between M and R. Maximal left (right) ideals are defined in the same way.

Proposition 2.4. *Let P be an ideal of R such that $P\neq R$.*

(i) *If for all $a,b\in P$, $ab\in P$ implies $a\in P$ or $b\in P$, then P is prime.*
(ii) *If R is commutative, the converse of* (i) *is true.*

Proof. (i) Suppose $AB\subset P$ and $A\not\subset P$. Choose $a\in A\smallsetminus P$. For all $b\in B$, $ab\in AB\subset P$. So $b\in P$; hence $B\subset P$.
(ii) Assume $ab\in P$. Then $(a)(b)=(ab)\subset P\Rightarrow(a)\subset P$ or $(b)\subset P$. □

Note. If R is not commutative, the converse of (i) is false. Example: $R=M_{2\times2}(F)$ where F is any field. The only ideals of R are 0 and R. So 0 is a primes ideal of R. But $[\,{}^{1}\;{}_{0}\,][\,{}^{0}\;{}_{1}\,]=0$.

Proposition 2.5. *Let R be a ring and $I\neq R$ a (left) ideal of R. Then I is contained in a maximal (left) ideal of R.*

Proof. Look at all (left) ideals J such that $I\subset J\not\ni 1$. Use Zorn's lemma. □

Theorem 2.6. *Let R be a commutative ring and I an ideal of R.*

(i) *I is prime $\Leftrightarrow R/I$ is an integral domain.*
(ii) *I is maximal $\Leftrightarrow R/I$ is a field.*
(iii) *I is a maximal $\Rightarrow I$ is prime.*

Fact. If I is an ideal of a ring R such that R/I is a division ring, then I is a maximal ideal. The converse is false: 0 is a maximal ideal of $M_{2\times2}(F)$.

Proposition 2.7. *Let $I_1,\dots,I_n$ be ideals of R such that $I_1+\cdots+I_n=R$ and $I_iI_j=\{0\}$ for all $i\neq j$. Write $1=e_1+\cdots+e_n$, where $e_i\in I_i$. Then we have the following conclusions.*

(i)
$$e_ie_j=\begin{cases}e_i & \textit{if } i=j,\\ 0 & \textit{if } i\neq j.\end{cases}$$
($e_1,\dots,e_n$ are called orthogonal idempotents.*)*

(ii) *I_i is a ring with identity e_i. (It follows that $e_1,\dots,e_n$ are unique.) Moreover, $e_1,\dots,e_n$ are in the center of R and $I_i=Re_i$.*

(iii) $R \cong I_1 \times \cdots \times I_n$.

PROOF. (i) If $i \neq j$, then $e_i e_j \in I_i I_j = \{0\}$; hence $e_i e_j = 0$. Thus $e_i = e_i(e_1 + \cdots + e_n) = e_i^2$.

(ii) Let $x \in I_i$. Then for each $j \neq i$, $xe_j \in I_i I_j = \{0\}$; hence $xe_j = 0$. So, $x = x(e_1 + \cdots + e_n) = xe_i$. In the same way, $e_i x = x$.

Since e_i is the identity of I_i and $e_i x = 0 = xe_i$ for all $x \in I_j$, $j \neq i$, we see that e_i is in the center if R. Since $Re_i \subset I_i \subset I_i e_i \subset Re_i$, we have $I_i = Re_i$.

(iii) $f : R \to I_1 \times \cdots \times I_n$, $a \mapsto (ae_1, \dots, ae_n)$ is an isomorphism. (In fact, $g : I_1 \times \cdots \times I_n \to R$, $(x_1, \dots, x_n) \mapsto x_1 + \cdots + x_n$, is the inverse of f.) □

THEOREM 2.8 (The Chinese remainder theorem). *Let $I_1, \dots, I_n$ be ideals of a ring R such that $I_i + I_j = R$ $(i \neq j)$. Then*

$$\begin{array}{rccc} f: & R & \longrightarrow & (R/I_1) \times \cdots \times (R/I_n) \\ & a & \longmapsto & (a + I_1, \dots, a + I_n) \end{array}$$

is an onto homomorphism with $\ker f = I_1 \cap \cdots \cap I_n$. *(I.e., $\forall a_i \in I_i$, $1 \leq i \leq n$, $\exists a \in R$ (unique mod $I_1 \cap \cdots \cap I_n$) such that $a \equiv a_i \pmod{I_i}$ for all $1 \leq i \leq n$.)*

PROOF. Only have to show that f is onto. It suffices to show that $\exists a \in R$ such that

$$a \equiv \begin{cases} 1 \pmod{I_1}, \\ 0 \pmod{I_i}, \ 2 \leq i \leq n. \end{cases}$$

Since $I_1 + I_i = R$ $(i \geq 2)$, there exists $a_i \in I_1$ such that $a_i \equiv 1 \pmod{I_i}$. Then $a = (1 - a_2) \cdots (1 - a_n)$ works. □

COROLLARY 2.9. *Let $m_1, \dots, m_n \in \mathbb{Z}^+$ such that $(m_i, m_j) = 1$, $i \neq j$. Let $a_i, \dots, a_n \in \mathbb{Z}$ be arbitrary. Then there exists $x \in \mathbb{Z}$ (unique mod $\operatorname{lcm}(m_1, \dots, m_n)$) such that $x \equiv a_i \pmod{m_i}$ for all $1 \leq i \leq n$.*

EXAMPLE. Let X be a compact topological space and $C(X, \mathbb{R})$ the ring of all continuous functions from X to $\mathbb{R}$. For each $a \in X$, let $M_a = \{f \in C(X, \mathbb{R}) : f(a) = 0\}$. Then M_a, $a \in X$, are all the maximal ideals of $C(X, \mathbb{R})$.

PROOF. $C(X, \mathbb{R})/M_a \cong \mathbb{R}$ is a field. So M_a is maximal.

Let M be a maximal ideal of $C(X, \mathbb{R})$. Assume to the contrary that $M \neq M_a$ for all $a \in X$. Then $\forall a \in X$, $\exists f_a \in C(X, \mathbb{R})$ such that $f_a(a) \neq 0$. So, $f_a(x)^2 > 0$ for all x in an open neighborhood U_a of a. Let $U_{a_1}, \dots, U_{a_n}$ be a finite cover of X. Then $f_{a_1}^2 + \cdots + f_{a_n}^2 \in M$ is invertible. So $M = C(X, \mathbb{R})$, which is a contradiction. □

2.3. Factorization in Commutative Rings; UFD, PID and ED

Let R be a commutative ring and $a, b \in R$. $a \mid b$ (a divides b) means that $b = ax$ for some $x \in R$. If $a \mid b$ and $b \mid a$, then a, b are called *associates*, denoted as $a \sim b$. (If R is an integral domain, $a \sim b \Leftrightarrow a = bu$ for some $u \in R^\times$.) An element $a \in R \smallsetminus (R^\times \cup \{0\})$ is called *irreducible* if $a = bc$ $(b, c \in R) \Rightarrow b$ or c is a unit. $a \in R \smallsetminus (R^\times \cup \{0\})$ is called *prime* if $a \mid bc$ $(b, c \in R) \Rightarrow a \mid b$ or $a \mid c$.

DEFINITION 2.10 (PID). An integral domain P is called a *principal ideal domain* (PID) if every ideal of P is principal.

DEFINITION 2.11 (UFD). An integral domain R is called a *unique factorization domain* (UFD) if

(i) $\forall a \in R \smallsetminus (R^\times \cup \{0\})$, $a = c_1 \cdots c_n$ for some irreducible $c_1, \dots, c_n \in R$;

(ii) if $c_1 \cdots c_n = d_1 \cdots d_m$, where $c_i, d_j \in R$ are irreducible, then $n = m$ and after a suitable reordering, $c_i \sim d_i$, $1 \le i \le n$.

Definition 2.12 (ED). An integral domain R is called a *Euclidean domain* (ED) if $\exists \partial : R \smallsetminus \{0\} \to \mathbb{N}$ such that

(i) $\forall a, b \in R \smallsetminus \{0\}$, $\partial(a) \le \partial(ab)$;

(ii) $\forall a \in R$, $0 \ne b \in R$, $\exists\, q, r \in R$ such that $a = qb + r$, where $r = 0$ or $\partial(r) < \partial(b)$.

Note.

(i) If ∂ satisfies (i) and (ii) of Definition 2.12, so does $\partial - \min\{\partial(x) : x \in R \smallsetminus \{0\}\}$. Thus, we may assume 0 is in the range of ∂.

(ii) Let R be an ED and $0 \ne x \in R$. Then $x \in R^\times \Leftrightarrow \partial(x) = \min\big\{\partial(y) : y \in R \smallsetminus \{0\}\big\}$.

Proposition 2.13. *Let R be an integral domain.*

(i) *$p \in R$ is prime $\Leftrightarrow$ (p) is a nonzero prime ideal.*

(ii) *$a \in R$ is irreducible $\Leftrightarrow$ (a) is maximal in $\{(b) : 0 \ne b \in R,\ (b) \ne R\}$.*

(iii) *p is prime $\Rightarrow$ p is irreducible.*

(iv) *If R is a UFD, p is a prime $\Leftrightarrow$ p is irreducible.*

Proof. (iii) Suppose $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ (say). So, $a = pu$ ($u \in R$), $p = pub \Rightarrow ub = 1 \Rightarrow b$ is a unit.

(iv) ($\Leftarrow$) Assume $p \mid ab$ ($a, b \in R$). Then $pq = ab$ for some $q \in R$. By the uniqueness of factorization, p appears in the factorization of a or b, i.e., $p \mid a$ or $p \mid b$. □

Note. If R is not a UFD, p irreducible $\not\Rightarrow$ p prime. Example: $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. $2 \in R$ is irreducible. (If $2 = xy$ for some $x, y \in \mathbb{Z}[\sqrt{-5}]$. Then $4 = |2|^2 = |x|^2|y|^2$. It follows that of $|x|^2$ and $|y|^2$, say $|x|^2$, is 1; hence x is invertible.) $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $2 \nmid (1 + \sqrt{-5})$, $2 \nmid (1 - \sqrt{-5})$.

Fact. ED $\Rightarrow$ PID $\Rightarrow$ UFD.

Proof. ED $\Rightarrow$ PID. Let R be an ED and $I \ne \{0\}$ an ideal of R. Let $a \in I$ such that $\partial(a)$ is the smallest. Then $I = (a)$.

PID $\Rightarrow$ UFD.

Existence of factorization. Let $a \in R \smallsetminus (R^\times \cup \{0\})$. Assume to the contrary that a is not a product of finitely many irreducibles. Since a is not irreducible, $a = a_1 a_1'$, where $a_1, a_1' \in R \smallsetminus (R^\times \cup \{0\})$ and w.l.o.g., a_1 is not a product of finitely many irreducibles. Write $a_1 = a_2 a_2'$, ... $\Rightarrow (a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$. $\bigcup_{i=1}^\infty (a_i)$ is an ideal of R. So, $\bigcup_{i=1}^\infty (a_i) = (b)$ for some $b \in R \Rightarrow b \in (a_i)$ for some $i \Rightarrow (a_{i+1}) \subset (b) \subset (a_i)$, which is a contradiction.

Uniqueness of factorization. First show that every irreducible element a of R is a prime. (By Proposition 2.13 (ii), (a) is a maximal ideal; hence (a) is a prime ideal and a is a prime.) Then use induction on the number of irreducible factors in the factorization. □

Examples of ED. $\mathbb{Z}$, $F[x]$ (F a field), and (cf. [**17**, §5.4])

$$\begin{aligned} &\mathbb{Z}[\sqrt{d}], && d = -2,\ -1,\ 2,\ 3,\ 6,\ 7,\ 11,\ 19, \\ &\mathbb{Z}[\tfrac{1+\sqrt{d}}{2}], && d = -11,\ -7,\ -3,\ 5,\ 13,\ 17,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73. \end{aligned}$$

Example (UFD $\not\Rightarrow$ PID). $\mathbb{Z}[x]$. $(2, x)$ is not a principal ideal.

Example 2.14 (PID $\not\Rightarrow$ ED). $\mathbb{Z}[\alpha]$, $\alpha = \frac{1}{2}(1 + \sqrt{-19})$.

Proof. 1° $\mathbb{Z}[\alpha]$ is not a ED.

The units of $\mathbb{Z}[\alpha]$ are ± 1. ($u \in \mathbb{Z}[\alpha]$ is a unit $\Leftrightarrow |u|^2 = 1$.) Assume to the contrary that $\mathbb{Z}[\alpha]$ is an ED with degree function ∂. We may assume that $0 \in \operatorname{im} \partial$. Let $\epsilon \in \mathbb{Z}[\alpha]$ such that $\partial(\epsilon)$ is the smallest in $\mathbb{Z}^+$. We have

$$2 = q\epsilon + r, \quad r = 0, \pm 1.$$

So, $q\epsilon = 1, 2, 3$. Thus $|\epsilon|^2 \bigm| 1^2, 2^2, 3^2 \Rightarrow |\epsilon|^2 = 1, 2, 4, 3, 9$. Also,

$$\alpha = q_1\epsilon + r_1, \quad r_1 = 0, \pm 1.$$

So, $q_1\epsilon \in \frac{1}{2}\sqrt{-19} + \frac{1}{2}\{\pm 1, 3\} \Rightarrow |\epsilon|^2 \bigm| \frac{1}{4}(19 + 1^2)$ or $\frac{1}{4}(19 + 3^2)$, i.e. $|\epsilon|^2 \bigm| 5$ or 7. So, $|\epsilon|^2 = 1$, which is a contradiction.

2° $\forall z \in \mathbb{C}$, $\exists q \in \mathbb{Z}[\alpha]$ such that either $|z - q| < 1$ or $|z - \frac{q}{2}| < \frac{1}{2}$.

Let $z = x + yi$. $\exists p \in \mathbb{Z}[\alpha]$ such that $z + p$ belongs to the (closed) parallelogram $0, 1, \alpha + 1, \alpha$, see Figure 2.1. We want to show that z has distance < 1 from one of the dots or has distance $< \frac{1}{2}$ from one of the circles. For this purpose, we may assume $z \in \triangle(0, \frac{1}{2}, \alpha)$. Assume $|z - \frac{\alpha}{2}| \geq \frac{1}{2} \Rightarrow (x - \frac{1}{4})^2 + (y - \frac{\sqrt{19}}{4})^2 \geq \frac{1}{4}$. Since $|x - \frac{1}{4}| \leq \frac{1}{4}$, we have $|y - \frac{\sqrt{19}}{4}| \geq \frac{\sqrt{3}}{4} \Rightarrow y \leq \frac{\sqrt{19} - \sqrt{3}}{4}$ or $y \geq \frac{\sqrt{19} + \sqrt{3}}{4}$. In the first case, $|z - 0| < 1$; in the second case, $|z - \alpha| < 1$.

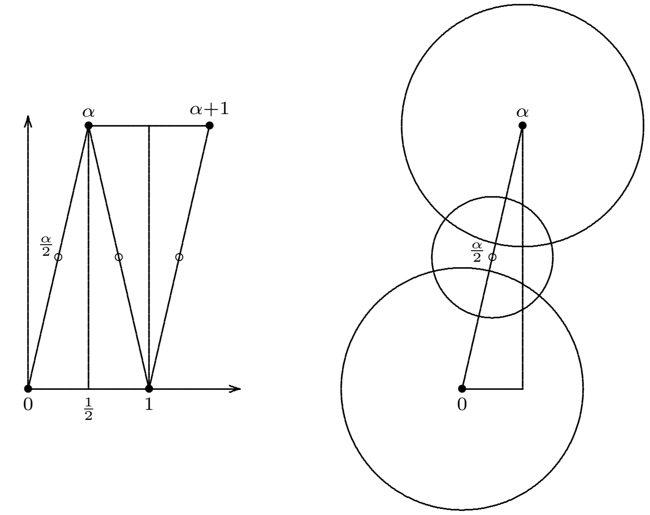


Figure 2.1. Example 2.14

3° $\mathbb{Z}[\alpha]$ is a PID.

Let $I \neq \{0\}$ be an ideal of $\mathbb{Z}[\alpha]$. Let $0 \neq \beta \in I$ such that $|\beta|^2$ is the smallest. We claim that $I = (\beta)$.

$\forall \sigma \in I$, by 2°, $\exists q \in \mathbb{Z}[\alpha]$ such that $|\frac{\sigma}{\beta} - q| < 1$ or $|\frac{\sigma}{\beta} - \frac{q}{2}| < \frac{1}{2}$. If $|\frac{\sigma}{\beta} - q| < 1$, then $|\sigma - q\beta| < |\beta| \Rightarrow \sigma - q\beta = 0 \Rightarrow \sigma \in (\beta)$. So, assume $|\frac{\sigma}{\beta} - \frac{q}{2}| < \frac{1}{2}$. Then $|2\sigma - q\beta| < |\beta| \Rightarrow \sigma = \frac{q}{2}\beta$. It suffices to show that $\frac{q}{2} \in \mathbb{Z}[\alpha]$. Assume the contrary. Then $q = a + b\alpha$, where at least one of a, b is odd.

(i) a is odd, b is even. Then $\frac{q+1}{2} \in \mathbb{Z}[\alpha] \Rightarrow \frac{1}{2}\beta = \frac{q+1}{2}\beta - \sigma \in I$ with $0 < |\frac{1}{2}\beta| < |\beta|$, contradiction.

(ii) a is even, b is odd. We have

$$q\bar{\alpha} = a\bar{\alpha} + 5b = (a+5b) - a\alpha = a' + b'\alpha =: q',$$

where $\frac{q'}{2}\beta \in I$, a' odd, b' even. This is (i).

(iii) a, b both odd. We have

$$q\bar{\alpha} = (a+5b) - a\alpha = a' + b'\alpha =: q',$$

where $\frac{q'}{2}\beta \in I$, a' even, b' odd. This is (ii). □

Gauss integers. $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ is an ED with $\partial(\alpha) = |\alpha|^2$.

Proof. Let $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. $\exists\, q \in \mathbb{Z}[i]$ such that $|\frac{\alpha}{\beta} - q| < 1$. So, $|\alpha - \beta q| < |\beta|$. □

Primes in $\mathbb{Z}[i]$. Let $\alpha \in \mathbb{Z}[i]$ be neither 0 nor a unit. Then α is a prime (i.e. irreducible) $\Leftrightarrow$

(i) $\alpha \sim p$ for some prime $p \in \mathbb{Z}$ with $p \equiv -1 \pmod 4$ or
(ii) $|\alpha|^2$ is prime in $\mathbb{Z}$.

Proof. ($\Leftarrow$) Assume (i). Assume to the contrary that p is not a prime. $\Rightarrow p = \beta\gamma$, where $\beta, \gamma \in \mathbb{Z}[i]$, $|\beta|^2 > 1$, $|\gamma|^2 > 1$. Since $p^2 = |\beta|^2|\gamma|^2$ (in $\mathbb{Z}$) $\Rightarrow p = |\beta|^2 \Rightarrow p \not\equiv -1 \pmod 4$, $\rightarrow\leftarrow$.

Assume (ii). If $\alpha = \beta\gamma$, where $\beta, \gamma \in \mathbb{Z}[i]$, $\Rightarrow |\alpha|^2 = |\beta|^2|\gamma|^2$ (in $\mathbb{Z}$) $\Rightarrow |\beta|^2 = 1$ or $|\gamma|^2 = 1$.

($\Rightarrow$) We have $|\alpha|^2 = p_1 \cdots p_n$, where $p_1, \dots, p_m$ are primes in $\mathbb{Z}$. Since $\alpha \mid \alpha\bar{\alpha} = p_1 \cdots p_n$ and α is prime, $\alpha \mid p_i =: p$ for some i. So, $|\alpha|^2 \;\big|\; p^2$ in $\mathbb{Z}$, $\Rightarrow |\alpha|^2 = p$ or p^2. If $|\alpha|^2 = p$, we have (ii). So, assume $|\alpha|^2 = p^2$. Since $\alpha \mid p$, $p = u\alpha$ for some $u \in \mathbb{Z}[i]$. So, $|u|^2 = 1$, i.e., u is a unit. It remains to show that $p \equiv -1 \pmod 4$. If $p = 2$ or $p \equiv 1 \pmod 4$, by Lemma 2.15, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, $\Rightarrow \alpha = u^{-1}p = u^{-1}(a+bi)(a-bi)$ is not irreducible, which is a contradiction. □

Lemma 2.15. *Let p be an odd prime integer. Then the following are equivalent.*

(i) $p \equiv 1 \pmod 4$.
(ii) -1 *is a square in* $\mathbb{Z}_p$.
(iii) $p = a^2 + b^2$ *for some* $a, b \in \mathbb{Z}$.

Proof. (i) $\Rightarrow$ (ii). $4 \mid p - 1 = |\mathbb{Z}_p^\times| \Rightarrow \exists x \in \mathbb{Z}_p^\times$ with $o(x) = 4 \Rightarrow -1 = x^2$.

(ii) $\Rightarrow$ (iii). We claim that p is not irreducible in $\mathbb{Z}[i]$. (Otherwise, by (ii), $\exists x \in \mathbb{Z}$ such that $p \mid x^2 + 1 = (x+i)(x-i) \Rightarrow p \mid x + i$ or $p \mid x - i \Rightarrow x \pm i = p(a+bi) \Rightarrow \pm 1 = pb$, contradiction.) So, $p = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$ are nonunits, $\Rightarrow p^2 = |\alpha|^2|\beta|^2$ (in $\mathbb{Z}$) $\Rightarrow p = |\alpha|^2$ ($= |\beta|^2$). □

Theorem 2.16 (Sum of two squares). *Let $x \in \mathbb{Z}^+$ have factorization $x = p_1^{e_1} \cdots p_m^{e_m} q_1^{f_1} \cdots q_n^{f_n}$, where $p_1, \dots, p_m, q_1, \dots, q_n$ are distinct primes with $p_i \equiv -1 \pmod 4$ and $q_j = 2$ or $q_j \equiv 1 \pmod 4$. Then $x = a^2 + b^2$ for some $a, b \in \mathbb{Z} \Leftrightarrow e_1, \dots, e_m$ are all even.*

PROOF. ($\Leftarrow$) $q_j = |\alpha_j|^2$ for some $\alpha_j \in \mathbb{Z}[i]$, $\Rightarrow x = |p_1^{e_1/2} \cdots p_m^{e_m/2} \alpha_1^{f_1} \cdots \alpha_n^{f_n}|^2$.

($\Rightarrow$) We have $x = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$. Assume to the contrary that e_i is odd for some i. Write $e_i = 2k+1$. Since p_i is a prime of $\mathbb{Z}[i]$ and $p_i^{2k+1} \mid \alpha\bar{\alpha}$, we have $p_i^{k+1} \mid \alpha$ or $\bar{\alpha}$, say $p_i^{k+1} \mid \alpha$. Then $p_i^{-e_i-1} n = \left|\frac{\alpha}{p_i^{k+1}}\right|^2 \in \mathbb{Z}$, $\rightarrow\leftarrow$. □

GCD AND LCM. Let R be a commutative ring and $X \subset R$. An element $d \in R$ is called a *greatest common divisor* of X, denoted by $\gcd(X)$, if

(i) $d \mid x \ \forall x \in X$ and
(ii) if $c \mid x \ \forall x \in X$, then $c \mid d$.

An element $m \in R$ is called a *least common multiple* of X, denoted by $\operatorname{lcm}(X)$, if

(i′) $x \mid m \ \forall x \in X$ and
(ii′) if $x \mid c \ \forall x \in X$, then $m \mid c$.

gcd's (lcm's) of X may not exist. If they do, all gcd's (lcm's) of X are associates.

If R is a PID, then $\langle \gcd(X) \rangle = \langle X \rangle$ and $\langle \operatorname{lcm}(X) \rangle = \bigcap_{x \in X} \langle x \rangle$.

Assume R is a UFD. Two primes in R which are associates will be treated as being the same. Let $\mathcal{P}$ be the set of all distinct primes in R. Then for each $x \in R \setminus \{0\}$,

$$x \sim \prod_{p \in \mathcal{P}} p^{\nu_p(x)},$$

where $\nu_p(x) \in \mathbb{N}$ and $\nu_p(x) = 0$ for almost all $p \in \mathcal{P}$. Also define $\nu_p(0) = \infty$ for all $p \in \mathcal{P}$. Moreover, define $\prod_{p \in \mathcal{P}} p^{e_p} = 0$ if $e_p = \infty$ for some $p \in \mathcal{P}$ or $e_p > 0$ for infinitely many $p \in \mathcal{P}$. Then

$$\gcd(X) \sim \prod_{p \in \mathcal{P}} p^{\inf\{\nu_p(x) : x \in X\}},$$
$$\operatorname{lcm}(X) \sim \prod_{p \in \mathcal{P}} p^{\sup\{\nu_p(x) : x \in X\}}.$$

2.4. Fractions and Localization

THE RING OF FRACTIONS. Let R be a commutative ring and let $\emptyset \neq S \subset R \setminus \{0\}$ be a *multiplicative set* (i.e., S is closed under multiplication). For $(r, s), (r', s') \in R \times S$, define $(r, s) \sim (r', s')$ if $\exists s_1 \in S$ such that $s_1(rs' - r's) = 0$. "$\sim$" is an equivalence relation on $R \times S$. The equivalence class of (r, s) in $R \times S$ is denoted by $\frac{r}{s}$. Let $S^{-1}R = R \times S/\!\sim\, = \{\frac{r}{s} : r \in R, s \in S\}$. For $\frac{r}{s}, \frac{r'}{s'} \in R$, define

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}, \qquad \frac{r}{s} + \frac{r'}{s'} = \frac{rs' + sr'}{ss'}.$$

Then $(S^{-1}R, +, \cdot)$ is a commutative ring, called the *ring of fractions* of R by S. If R is an integral domain, so is $S^{-1}R$. If R is a integral domain and $S = R \setminus \{0\}$, $S^{-1}R$ is a field, called the *fractional field* of R.

EXAMPLES. $\mathbb{Q}$ = the fractional field of $\mathbb{Z}$. The fractional field of $F[x]$ (F a field) is $F(x)$, the field of rational functions over F.

PROPOSITION 2.17. *Let R be a commutative ring and S ($\neq \emptyset$, $\not\ni 0$) a multiplicative set of R.*

(i) *The map*

$$\begin{array}{rccl} \phi_S : & R & \longrightarrow & S^{-1}R \\ & r & \longmapsto & \frac{rs}{s} \qquad (s \in S \textit{ arbitary}) \end{array}$$

is a homomorphism. For every $s \in S$, $\phi_S(s)$ *is a unit of* $S^{-1}R$.

(ii) ϕ_S *is 1-1* $\Leftrightarrow$ S *contains no zero divisors.*

Proposition 2.18 (Universal mapping property). *Let* R *be a commutative ring and* S $(\neq \emptyset, \not\ni 0)$ *a multiplicative set of* R. *Let* T *be another commutative ring and* $f : R \to T$ *a homomorphism such that* $f(S) \subset T^\times$. *Then there is a unique homomorphism* $\bar{f} : S^{-1}R \to T$ *such that the following diagram commutes.*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\phi_S"'] & T \\ S^{-1}R \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Proof. *Existence.* Define $\bar{f} : S^{-1}R \to T$, $\frac{r}{s} \mapsto f(r)f(s)^{-1}$.

Uniqueness. Assume $g : S^{-1}R \to T$ is another homomorphism such that $g \circ \phi_S = f$. Then for each $r \in R$ and $s \in S$, $g(\frac{r}{s})f(s) = g(\frac{r}{s})g(\frac{s^2}{s}) = g(\frac{rs^2}{s^2}) = f(r)$; hence $g(\frac{r}{s}) = f(r)f(s)^{-1}$. □

Local rings. A *local ring* is a commutative ring R with a unique maximal ideal M. R/M is called the residue field of R. Example: Let p be a prime and $n > 0$. $\mathbb{Z}_{p^n}$ is a local ring with maximal ideal $p\mathbb{Z}_{p^n}$ and residue field $\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n} \cong \mathbb{Z}_p$.

Proposition 2.19. *Let* R *be a commutative ring.*

(i) *If* R *is local, the unique maximal ideal of* R *is* $R \setminus R^\times$.

(ii) R *is local* $\Leftrightarrow$ $R \setminus R^\times$ *is closed under* $+$.

Proof. (i) Let M be the unique maximal ideal of R. $\forall x \in R \setminus R^\times$, by Zorn's lemma, x is contained in a maximal ideal of R, so $x \in M$. So $R \setminus R^\times \subset M$. Clearly, $M \subset R \setminus R^\times$. So $M = R \setminus R^\times$.

(ii) $(\Leftarrow)$ $R \setminus R^\times$ is an ideal of R. Let M be any maximal ideal of R. Then $M \subset R \setminus R^\times$. Hence $M = R \setminus R^\times$ is unique. So, R is local. □

Localization. Let R be a commutative ring and P a prime ideal of R. Then $S = R \setminus P$ is multiplicative subset of R and $0 \notin S \neq \emptyset$. $S^{-1}R$ is a local ring with maximal ideal $S^{-1}P$. (If $\frac{r}{s} \in (S^{-1}R) \setminus (S^{-1}P)$, where $r \in R$ and $s \in S$, then $r \in R \setminus P = S$. So $\frac{r}{s}$ is invertible in $S^{-1}R$.) $S^{-1}R$ is called the *localization* of R at P and denoted by R_P. Example: Let $p \in \mathbb{Z}$ be a prime. Then $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ p \nmid b\}$.

2.5. Polynomial Rings

Polynomial ring in one indeterminate. Let R be a ring. A *polynomial* in x (the indeterminate) with coefficients in R is a *formal* sum

$$f = a_0 + a_1x + \cdots + a_nx^n, \qquad n \in \mathbb{N},\ a_i \in R.$$

$\deg f := \max\{i : a_i \neq 0\}$. ($\deg 0 = -\infty$.) $R[x] :=$ the set of all polynomials in x with coefficients in R. $+$ and $\cdot$ in $R[x]$ are defined as follows:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i;$$

$$\Big(\sum_{i=0}^{n} a_i x^i\Big)\Big(\sum_{j=0}^{m} b_j x^j\Big) = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j\Big) x^k.$$

$(R[x], +, \cdot)$ is a ring, called the *polynomial ring* over R in x.

Polynomial ring in a set of indeterminates. Let R be a ring. Let X be a set of symbols (indeterminates). Let A be the set of all functions $\alpha : X \to \mathbb{N}$ such that $\alpha(x) = 0$ for almost all (all but finitely many) $x \in X$. A polynomial in X with coefficients in R is a *formal* sum

$$f = \sum_{\alpha \in A} a_\alpha X^\alpha,$$

where $a_\alpha = 0$ for almost all $\alpha \in A$. We may write $X^\alpha = \prod_{x \in X} x^{\alpha(x)}$. For each $\alpha \in A$, $\operatorname{supp} \alpha = \{x \in X : \alpha(x) > 0\}$ is finite. If $\operatorname{supp} \alpha = \{x_1, \dots, x_n\}$, we write $X^\alpha = x_1^{\alpha(x_1)} \cdots x_n^{\alpha(x_n)}$. $R[X] :=$ the set of all polynomials in X with coefficients in R. $+$ and $\cdot$ in $R[X]$ are defined as follows:

$$\sum_{\alpha \in A} a_\alpha X^\alpha + \sum_{\alpha \in A} b_\alpha X^\alpha = \sum_{\alpha \in A} (a_\alpha + b_\alpha) X^\alpha;$$

$$\Big(\sum_{\alpha \in A} a_\alpha X^\alpha\Big)\Big(\sum_{\beta \in A} b_\beta X^\beta\Big) = \sum_{\gamma \in A} \Big(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\Big) X^\gamma.$$

$(R[X], +, \cdot)$ is the *polynomial ring* over R in X.

Note. Let F be the free abelian group on X (written multiplicatively) and

$$\mathcal{X} = \{x_1^{d_1} \cdots x_n^{d_n} : n \geq 0,\ x_i \in X,\ d_i \in \mathbb{Z}^+\}.$$

Then $\mathcal{X}$ is a multiplicative set of F containing 1. The subring $R[\mathcal{X}]$ of the group ring $R[F]$ is precisely the polynomial ring $R[X]$.

Note. $\forall f \in R[X]$, $\exists x_1, \dots, x_n \in X$ such that $f \in R[x_1, \dots, x_n]$.

Proposition 2.20 (Universal mapping property). *Let $R[X]$ be the polynomial ring over R in X. Let S be another ring and $f : R \to S$ a homomorphism. Let $\phi : X \to S$ be a function such that every element in $\phi(X)$ commutes with every element in $\phi(X) \cup f(R)$. Then there exists a unique homomorphism $\bar{f} : R[X] \to S$ such that the following diagram commutes.*

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, hook] & S \\
R[X] \arrow[ur, "\bar{f}"] & X \arrow[l, hook'] \arrow[u, "\phi"']
\end{tikzcd}$$

Proof. Define $\bar{f} : R[X] \to S$ by

$$\sum_{d_1,\dots,d_n} a_{d_1,\dots,d_n} x_1^{d_1} \cdots x_n^{d_n} \mapsto \sum_{d_1,\dots,d_n} f(a_{d_1,\dots,d_n}) \phi(x_1)^{d_1} \cdots \phi(x_n)^{d_n}.$$

□

Fact 2.21. If X and Y are disjoint sets of indeterminates, then $(R[X])[Y] \cong R[X \cup Y]$.

Proof. By Proposition 2.20, $\exists$ homomorphisms $g : (R[X])[Y] \to R[X \cup Y]$ and $h : R[X \cup Y] \to (R[X])[Y]$ such that the following diagram commutes.

$$\begin{tikzcd}
R[X] \arrow[r, "\subset"] \arrow[d, "\cap"'] & R[X \cup Y] \\
(R[X])[Y] \arrow[ur, "g"] & Y \arrow[l, "\supset"] \arrow[u, "\cup"']
\end{tikzcd}
\qquad
\begin{tikzcd}
R \arrow[r, "\subset"] \arrow[d, "\cap"'] & (R[X])[Y] \\
R[X \cup Y] \arrow[ur, "h"] & X \cup Y \arrow[l, "\supset"] \arrow[u, "\cup"']
\end{tikzcd}$$

Use the uniqueness of Proposition 2.20 to show $h \circ g = \mathrm{id}$ and $g \circ h = \mathrm{id}$ (Exercise 2.3). □

Proposition 2.22 (The division algorithm). *Let R be a ring and $f, g \in R[x]$ such that the leading coefficient of g is a unit. Then $\exists! q, r, q', r' \in R[x]$ such that*

$$f = qg + r \qquad \textit{and} \qquad f = gq' + r',$$

where $\deg r < \deg g$, $\deg r' < \deg g$.

Fact. If F is a field, $F[x]$ is a ED with $\partial(f) = \deg f$.

Let R be a commutative ring, $f = \sum_{d_1,\dots,d_n} a_{d_1,\dots,d_n} x_1^{d_1} \cdots x_n^{d_n} \in R[x_1, \dots, x_n]$ and $(c_1, \dots, c_n) \in R^n$. We write $f(c_1, \dots, c_n) = \sum_{d_1,\dots,d_n} a_{d_1,\dots,d_n} c_1^{d_1} \cdots c_n^{d_n}$. If $f(c_1, \dots, c_n) = 0$, $(c_1, \dots, c_n)$ is called a *root* of f.

Facts.

(i) Let R be a commutative ring, $f \in R[x]$ and $c \in R$. Then $f(c) = 0 \Leftrightarrow x - c \mid f$.

(ii) If D is an integral domain and $0 \neq f \in D[x]$ with $\deg f = n$, then f has at most n distinct roots in D.

Derivative. Let R be a commutative ring and $f = a_0 + \cdots + a_n x^n \in R[x]$. $f' := a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. The differentiation rules hold.

The Multiplicity of a root. Let R be a commutative ring, $0 \neq f \in F[x]$ and $c \in R$. Then f can be uniquely written as $f = (x - c)^m g$, where $m \in \mathbb{N}$ and $g \in R[x]$, $g(c) \neq 0$. (To see the uniqueness of m and g, note that $(x - c)h = 0$ $(h \in R[x]) \Rightarrow h = 0$.) m is called the *multiplicity* of root c of f. c is a *multiple root* of f (i.e., with multiplicity $m > 1$) $\Leftrightarrow f(c) = f'(c) = 0$.

The Hasse derivative. Let R be a commutative ring. For $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ and $k \geq 0$, define

$$\partial_k f = \binom{k}{k} a_k + \binom{k+1}{k} a_{k+1} x + \cdots + \binom{n}{k} a_n x^{n-k}.$$

$\partial_k f$ is called the kth order *Hasse derivative* of f. We have $f^{(k)} = k!\, \partial_k f$.

Properties of the Hasse derivative. Let $f, g \in R[x]$ and $a, b \in R$.

(i) $\partial_k(af + bg) = a\partial_k f + b\partial_k g$.

(ii) $\partial_k(fg) = \sum_{i+j=k} (\partial_i f)(\partial_j g)$.

(iii) $\partial_k\big(f(x+a)\big) = (\partial_k f)(x+a)$.

(iv) For each $c \in R$, $f = \sum_{k \geq 0} (\partial_k f)(c)(x-c)^k$. In particular, c is a root of f of multiplicity $\geq m \Leftrightarrow (\partial_0 f)(c) = \cdots = (\partial_{m-1} f)(c) = 0$.

Definition 2.23 (Content). Let D be a UFD and $0 \neq f = a_0 + \cdots + a_n x^n \in D[x]$. The *content* of f is $C(f) = \gcd(a_0, \dots, a_n)$. If $C(f) \sim 1$, f is called *primitive.*

Lemma 2.24 (Gauss). *Let D be a UFD and $f, g \in D[x]$ primitive. The fg is primitive.*

Proof. Assume to the contrary that $\exists$ irreducible $p \in D$ such that $p \mid C(fg)$. Let $\phi : D[x] \to (D/(p))[x]$ be the homomorphism induced by the natural homomorphism $D \to D/(p)$. Then $0 = \phi(fg) = \phi(f)\phi(g)$, where $\phi(f) \neq 0$, $\phi(g) \neq 0$. Since $D/(p)$ is an integral domain, so is $(D/(p))[x]$. We have a contradiction. □

Corollary 2.25. *Let D be a UFD and $f, g \in D[x]$ nonzero. Then $C(fg) \sim C(f)C(g)$.*

Proposition 2.26. *Let D be a UFD and F its fractional field. Let $f \in D[x]$.*

(i) *f is irreducible in $D[x]$ $\Rightarrow$ f is irreducible in $F[x]$.*

(ii) *Assume f is primitve. Then f is irreducible in $F[x]$ $\Rightarrow$ f is irreducible $D[x]$.*

Proof. (i) Assume to the contrary that $f = gh$, $g, h \in F[x]$, $\deg g > 0$, $\deg h > 0$. Choose $a, b \in D \setminus \{0\}$ such that $ag, bh \in D[x]$. Then $abf = (ag)(bh) \in D[x]$; hence, $ab = C(abf) = C(ag)C(bh)$. So, $f = \frac{1}{ab}(ag)(bh) = \frac{ag}{C(ag)} \cdot \frac{bh}{C(bh)}$, where $\frac{ag}{C(ag)}, \frac{bh}{C(bh)} \in D[x]$ have degree > 0. Contradiction.

(ii) Assume to the contrary that $f = gh$, where $g, h \in D[x]$ are nonzero and non units. Since f is irreducible in $F[x]$, one of g and h has degree 0. Thus f is not primitive, $\rightarrow\leftarrow$. □

Theorem 2.27. *Let D be a UFD. Then $D[x]$ is also a UFD. The irreducible elements of $D[x]$ are precisely irreducible elements of D and primitive polynomials in $D[x]$ which are irreducible in $F[x]$, where F is the fractional field of D.*

Proof. The second claim follows from Proposition 2.26. It remains to show that $D[x]$ is a UFD.

1° Existence of factorization.

Let $f \in D[x]$ be nonzero and nonunit. Since $F[x]$ is a UFD, $f = f_1 \cdots f_n$, where $f_i \in F[x]$ is irreducible. Choose $0 \neq a_i \in D$ such that $a_i f_i \in D[x]$. Write $a_i f_i = c_i g_i$, where $c_i \in D$ and $g_i \in D[x]$ is primitive and irreducible. Then

$$a_1 \cdots a_n f = (a_1 f_1) \cdots (a_n f_n) = c_1 \cdots c_n g_1 \cdots g_n.$$

Compare the contents of both sides. We have $\frac{c_1,\cdots c_n}{a_1\cdots a_n} \in D$. Thus,

$$f = \frac{c_1, \cdots c_n}{a_1 \cdots a_n} g_1 \cdots g_n,$$

where $\frac{c_1,\cdots c_n}{a_1\cdots a_n}$ is a product of irreducibles in D.

2° Uniqueness of factorization.

Suppose

$$a_1 \cdots a_m f_1 \cdots f_n = b_1 \cdots b_s g_1 \cdots g_t, \tag{2.1}$$

where $a_1, \dots, a_m, b_1, \dots, b_s \in D$ are irreducible and $f_1, \dots, f_n, g_1, \dots, g_t \in D[x]$ are irreducible of degree > 0. Compare the contents of the two sides of (2.1). We have $a_1 \cdots a_m \sim b_1 \cdots b_s$. So, $m = s$ and after reordering, $a_i \sim b_i$.

In $F[x]$,

$$f_1 \cdots f_n \sim g_1 \cdots g_t.$$

Thus, $n = t$ and after reordering, $f_j \sim g_j$ in $F[x]$. So, $f_j = \frac{u}{v} g_j$ for some $u, v \in D \setminus \{0\}$, i.e., $vf_j = ug_j$. Then $v = C(uf_j) \sim C(ug_j) = u$ in D. Thus, $f_j \sim g_j$ in $D[x]$. □

Corollary 2.28. *If D is a UFD and X is a set of indeterminates, then $D[X]$ is a UFD.*

Eisenstein's criterion. *Let D be a UFD with fractional field F and let $f = a_0 + \cdots + a_n x^n \in D[x]$, $n > 0$. If there is an irreducible element $p \in D$ such that $p \nmid a_n$, $p \mid a_i$ for $0 \le i \le n-1$ and $p^2 \nmid a_0$, then f is irreducible in $F[x]$.*

Proof. Assume to the contrary that $f = gh$, $g, h \in F[x]$, $\deg g > 0$, $\deg h > 0$. Then $\exists g_1, h_1 \in D[x]$ such that $f = g_1 h_1$ and $g_1 \sim g$ and $h_1 \sim h$ in $F[x]$; see the proof of Proposition 2.26 (i). Let $\phi : D[x] \to (D/(p))[x]$ be the homomorphism induced by the natural homomorphism $D \to D/(p)$. Then $\phi(a_n)x^n = \phi(g_1)\phi(h_1)$. Since $D/(p)$ is an integral domain, we have $\phi(g_1) = \alpha x^k$, $\phi(h_1) = \beta x^l$, $\alpha, \beta \in D/(p)$. Since $k \le \deg g_1$, $l \le \deg h_1$, but $k + l = n = \deg g_1 + \deg h_1$, we have $k = \deg g_1$ and $l = \deg h_1$; hence $k, l > 0$. Then $p \mid g_1(0)$, $p \mid h_1(0)$, $\Rightarrow p^2 \mid g_1(0)h_1(0) = a_0$, which is a contradiction. □

Example. Let p be a prime. Then $\Phi_p(x) = 1 + x + \cdots + x^{p-1} \in \mathbb{Q}[x]$ is irreducible. (Apply Eisenstein's criterion to $\Phi_p(x+1) = \frac{1}{x}\big[(x+1)^p - 1\big] = \sum_{i=1}^p \binom{p}{i} x^{i-1}$.)

2.6. Modules, Definitions and Basic Facts

Definition 2.29. Let R be a ring (not required to have identity). A *left R-module* is an abelian group $(A, +)$ equipped with a scalar multiplication $R \times A \to A$, $(r, a) \mapsto ra$ such that for $r, s \in R$ and $a, b \in A$,

(i) $r(a + b) = ra + rb$;
(ii) $(r + s)a = ra + sa$;
(iii) $r(sa) = (as)a$.

A right R-module is an abelian group $(A, +)$ equipped with a scalar multiplication $A \times R \to A$. $(a, r) \mapsto ar$ such that the analogies of (i) – (iii) hold. A left (right) R-module is sometimes denoted by ${}_RA$ (A_R). If R has identity and

(iv) $1_R a = a$ for all $a \in A$,

A is called a *unitary* left R-module.

Declaration. Unless specified otherwise, all modules are assumed to be unitary. A module is assumed to be left if the side is not specified.

Examples of modules. Abelian groups are $\mathbb{Z}$-modules. A vector space over a field F is an F-module. A ring R is an R-module; submodules of ${}_RR$ are left ideals.

Let V be a vector space over a field F and $\alpha \in \operatorname{Hom}_F(V,V)$. For each $f \in F[x]$ and $v \in V$, define $fv = f(\alpha)v$. Then V is an $F[x]$-module.

Let A be an abelian group. For each $a \in A$ and $f \in \operatorname{End}(A)$, define $fa = f(a)$. Then A is an $\operatorname{End}(A)$-module.

Homomorphism. Let A, B be R-modules. A function $f : A \to B$ is called a *homomorphism*, or an *R-map*, if $f(a+b) = f(a) + f(b)$ and $f(ra) = rf(a)$ for all $a, b \in A$ and $r \in R$.

Submodule. Let A be an R-module and $B \subset A$. B is called a *submodule* of A if B (with the inherited operations) is an R-module.

If $X \subset A$, the smallest submodules of A containing X, called the submodule generated by X, is

$$\langle X\rangle = \Big\{\sum_{i=1}^{n} r_i x_i : n \in \mathbb{N},\ r_i \in R,\ x_i \in X\Big\}.$$

Quotient module. Let A be an R-module and B a submodule of A. Let A/B be the quotient abelian group. For $a+B \in A/B$ and $r \in R$, define $r(a+B) = ra+B$. Then A/B is an R-module, called the *quotient module* of A by B.

Isomorphism Theorems.

First isomorphism theorem. *Let $f : A \to B$ be a homomorphism of R-modules. The*

$$\begin{array}{rrcl} \tilde{f}: & A/\ker f & \longrightarrow & \operatorname{im} f \\ & a+\ker f & \longmapsto & f(a) \end{array}$$

is an isomorphism.

Second isomorphism theorem. *Let A, B be submodules of an R-module. Then $(A+B)/B \cong A/A\cap B$.*

Third isomorphism theorem. *Let $C \subset B \subset A$ be R-modules. Then $(A/C)/(B/C) \cong A/B$.*

Direct product and external direct sum. Let $\{A_i : i \in I\}$ be a family of R-modules. The *direct product* of $\{A_i : i \in I\}$, denoted by $\prod_{i\in I} A_i$, is the cartesian product of A_i, $i \in I$. Elements in $\prod_{i\in I} A_i$ are of the form $(a_i)_{i\in I}$, where $a_i \in A_i$. $\prod_{i\in I} A_i$ is an R-module with addition and scalar multiplication defined component wise.

The *external direct sum* of $\{A_i : i \in I\}$ is

$$\bigoplus_{i\in I}^{(\mathrm{ex})} A_i = \Big\{(a_i)_{i\in I} \in \prod_{i\in I} A_i : \text{only finitely many } a_i \neq 0\Big\},$$

which is a submodule of $\prod_{i\in I} A_i$. If $|I| < \infty$, $\bigoplus_{i\in I}^{(\mathrm{ex})} A_i = \prod_{i\in I} A_i$.

Internal direct sum. If $\{A_i : i \in I\}$ is a family of submodules of an R-modules A, the submodule

$$\langle \bigcup_{i\in I} A_i \rangle = \Big\{ \sum_{i\in I} a_i : a_i \in A_i,\ a_i = 0 \text{ for almost all } i \Big\}$$

is called the *sum* of $\{A_i : i \in I\}$ and is denoted by $\sum_{i\in I} A_i$. If $A_i \cap \sum_{j\in I\smallsetminus\{i\}} A_j = \{0\}$ for all $i \in I$, then $\sum_{i\in I} A_i$ is called an *internal direct sum* and is denoted by $\bigoplus_{i\in I}^{(\text{in})} A_i$. Moreover,

$$\begin{array}{ccc} \bigoplus_{i\in I}^{(\text{ex})} A_i & \longrightarrow & \bigoplus_{i\in I}^{(\text{in})} A_i \\ (a_i)_{i\in I} & \longmapsto & \sum_{i\in I} a_i \end{array}$$

is an isomorphism. Most of the time, we write both $\bigoplus^{(\text{ex})}$ and $\bigoplus^{(\text{in})}$ as $\bigoplus$.

Hom. Let ${}_RA$, ${}_RB$ be R-modules. $\text{Hom}_R({}_RA,\ {}_RB)$ = the abelian group of all R-maps from A to B. Let S be anther ring.

(i) If ${}_RA_S$ is a bimodule, $\text{Hom}_R({}_RA_S,\ {}_RB)$ is a left S-module. (For $f \in \text{Hom}_R({}_RA_S,\ {}_RB)$, $s \in S$ and $a \in A$, define $(sf)(a) = f(as)$.)

(ii) If ${}_RB_S$ is a bimodule, $\text{Hom}_R({}_RA,\ {}_RB_S)$ is a right S-module. (For $f \in \text{Hom}_R({}_RA,\ {}_RB_S)$, $s \in S$ and $a \in A$, define $(fs)(a) = (f(a))s$.)

Free modules. Let A be an R-module. A subset $X \in A$ is called *linearly independent* if $r_1x_1 + \cdots + r_nx_n = 0$ ($r_i \in R$, $x_1, \dots, x_n \in X$ distinct) $\Rightarrow r_1 = \cdots = r_n = 0$. X is called a *basis* of A if X is independent and $\langle X \rangle = A$. If A has a basis X, A is called a *free* module (on X); in this case,

$$A = \bigoplus_{x\in X}^{(\text{in})} Rx \cong \bigoplus_{x\in X}^{(\text{ex})} R.$$

If all bases of A have the same cardinality, this common cardinality is denoted by $\operatorname{rank} A$. If A is free with a basis X and B is another R-module, then every function $f : X \to B$ can be uniquely extended to an R-map $\bar{f} : A \to B$. Every R-module is a quotient of a free R-module.

Example (A direct product that is not free). $\prod_{i=1}^{\infty} \mathbb{Z}$ is not a free Z-modules. Let

$$A = \big\{ (a_1, a_2, \dots) \in \prod_{i=1}^{\infty} \mathbb{Z} : \text{for every } k > 0,\ 2^k \mid a_i \text{ for almost all } i \big\}.$$

We claim that A is not free. (By Theorem 2.36, $\prod_{i=1}^{\infty} \mathbb{Z}$ is not free.) Clearly, $|A| \geq 2^{\aleph_0} > \aleph_0$. Assume to the contrary that A is free. Then $\operatorname{rank} A > \aleph_0$. Every coset of $2A$ in A contains an element in $\bigoplus_{i=1}^{\infty} \mathbb{Z}$. Hence $A/2A$ is countable. So, $\dim_{\mathbb{Z}_2}(A/2A) \leq \aleph_0$. However, $\operatorname{rank} A = \dim_{\mathbb{Z}_2}(A/2A)$. We have a contradiction.

Theorem 2.30. *Let D be a division ring. Then every D-module V is free. Any two bases of V have the same cardinality. V is called a* vector space *over D; $\dim_D V := |X|$, where X is any basis of V.*

Proof. A maximal linearly independent subset of V, which exists by Zorn's lemma, is a basis.

Let X and Y be two bases of V. If $|X| = \infty$ or $|Y| = \infty$, we have $|X| = |Y|$ by the next lemma. So assume $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$. Assume to the contrary that $n > m$. We have

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = A \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}, \qquad \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = B \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

for some matrices $A \in M_{n\times m}(D)$ and $B \in M_{m\times n}(D)$. It follows that $AB = I_n$. There exists an invertible $C \in M_n(D)$ such that $CA = \left[\begin{smallmatrix} & * & \\ 0 & \cdots & 0 \end{smallmatrix}\right]$. Thus, $(0, \dots, 0, 1)C = (0, \dots, 0, 1)CAB = 0$, $\rightarrow\leftarrow$. □

Lemma 2.31. *Let R be a ring and F a free R-module with an infinite basis X. Then every basis of F has the same cardinality as X.*

Proof. Let Y be another basis of F. We claim that $|Y| = \infty$. (Otherwise, since each $y \in Y$ is a linear combination of finitely many $x \in X$, F is generated by a finite subset X_1 of X. But any $x \in X \setminus X_1$ is not a linear combination of elements in X_1, $\rightarrow\leftarrow$.)

For each $x \in X$, $\exists$ a finite subset $\{y_1, \dots, y_n\} \subset Y$ such that $x = r_1y_1 + \cdots + r_ny_n$, $r_i \in R$. Define $f(x) = \{y_1, \dots, y_n\}$. We claim that $\bigcup_{x\in X} f(x) = Y$. (Otherwise, X is spanned by $Y_1 := \bigcup_{x\in X} f(x) \subsetneq Y$; hence Y is spanned by Y_1, $\rightarrow\leftarrow$.) Now,

$$|Y| = \Big|\bigcup_{x\in X} f(x)\Big| \le |X|\aleph_0 = |X|.$$

By symmetry, $|X| \le |Y|$. Hence, $|X| = |Y|$. □

Facts. Let D be a division ring.

(i) If $W \subset V$ are vector spaces over D, then $\dim V = \dim W + \dim(V/W)$.

(ii) (The dimension formula) If V and W are subspaces of some vector space over D, then

$$\dim V + \dim W = \dim(V + W) + \dim(V \cap W).$$

Proof. (i) Let X be a basis of W. Extend X to a basis $X \dot\cup Y$ of V. Then $y + W$ $(y \in Y)$ are all distinct and form a basis of V/W. So, $\dim V/W = |Y|$.

(ii) Define a D-map

$$\begin{array}{rccc} f: & V \times W & \longrightarrow & V + W \\ & (v, w) & \longmapsto & v + w. \end{array}$$

Then f is onto and $\ker f = \{(v, -v) : v \in V \cap W\} \cong V \cap W$. Hence

$$\dim V + \dim W = \dim(V \times W) = \dim(\operatorname{im} f) + \dim(\ker f) = \dim(V + W) + \dim V \cap W.$$

□

The invariant dimension property. A ring R is said to have the *invariant dimension property* (IDP) if for every free R-module F, any two bases of F have the same cardinality.

Division rings (Theorem 2.30) and commutative rings (the next theorem) have IDP. If $A = \bigoplus_{j=0}^{\infty} \mathbb{Z}$ and $R = \operatorname{End}(A)$, then R does not have IDP. For any positive integer n, partition $\mathbb{N}$ as $N_1 \cup \cdots \cup N_n$ such that $|N_i| = \aleph_0$. Let $\tau_i : N_i \to \mathbb{N}$ be a bijection. Define $f_i \in \operatorname{End}(A)$ by setting

$$f_i(e_j) = \begin{cases} e_{\tau_i(j)} & \text{if } j \in N_i, \\ 0 & \text{if } j \notin N_i, \end{cases}$$

where $e_j = (0, \dots, 0, \overset{j}{1}, 0, \dots)$. Then $f_1, \dots, f_n$ is a basis of ${}_R R$. (Proof. $\forall h \in \operatorname{End}(A)$, let $g_i \in \operatorname{End}(A)$ such that $g_i(e_{\tau_i(j)}) = h(e_j)$. Then $\bigl(\sum_{i=1}^n g_i f_i\bigr)(e_j) = h(e_j)$ $\forall j \in \mathbb{N}$. So, $h = \sum_{i=1}^n g_i f_i$; hence $f_1, \dots, f_n$ generate ${}_R R$. If $\sum_{i=1} g_i f_i = 0$, where $g_i \in \operatorname{End}(A)$, then $g_k(A) = \bigl(\sum_{i=1}^n g_i f_i\bigr)(\langle e_j : j \in N_k \rangle) = \{0\}$. So, $g_k = 0$ for all $1 \le k \le n$; hence $f_1, \dots, f_n$ are linearly independent.)

Proposition 2.32. *A commutative ring R has IDP.*

Proof. Let F be a free R-module and let X be a basis of F. Let I be a maximal ideal of R. Then F/IF is a vector space over R/I.

1° We claim that $x + IF$, $x \in X$, form a basis of ${}_{R/I}(F/IF)$. Assume $\sum_{i=1}^n (a_i + I)(x_i + IF) = 0$, where $a_i \in F$, $x_i \in X$ (x_i distinct). Then $\sum_{i=1}^n a_i x_i \in IF$. Hence $\sum_{i=1}^n a_i x_i = \sum_{j=1}^m b_j y_j$, $b_j \in I$, $y_j \in X$. It follows that $a_i \in I$, $1 \le i \le n$.

2° By 1°, $|X| = |\{x + IF : x \in X\}| = \dim_{R/I}(F/IF)$, where $\dim_{R/I}(F/IF)$ is independent of X. □

2.7. Projective and Injective Modules

Exact sequences. A sequence of R-modules and R-maps

$$\cdots \longrightarrow A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is called *exact* if $\operatorname{im} f_{i-1} = \ker f_i$ for all i. An exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is called a *short exact sequence.* Two short exact sequences $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ and $0 \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to 0$ are called isomorphic if $\exists$ isomorphisms α, β, γ such that

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$

commutes.

Proposition 2.33. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of R-modules. Then the following statements are equivalent.*

(i) *$\exists$ an R-map $h : C \to B$ such that $g \circ h = \mathrm{id}_C$.*
(ii) *$\exists$ an R-map $k : B \to A$ such that $k \circ f = \mathrm{id}_A$.*
(iii) *$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is isomorphic to $0 \to A \xrightarrow{\iota_1} A \oplus C \xrightarrow{\pi_2} C \to 0$.*

If (i) – (iii) *are satisfied, the short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is called* split.

Proof. (i) ⇒ (iii).

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, shift left, "g"] & C \arrow[l, dashed, shift left, "h"] \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[u, "\mathrm{id}_A"] & A \oplus C \arrow[r, "\pi_2"] \arrow[u, "\phi"] & C \arrow[r] \arrow[u, "\mathrm{id}_C"'] & 0
\end{tikzcd}$$

commutes, where

$$\begin{array}{rccc}
\phi: & A \oplus C & \longrightarrow & B \\
 & (a,c) & \longmapsto & f(a)+h(c)
\end{array}$$

is an isomorphism by the five lemma (next).

(ii) ⇒ (iii).

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, shift left, "f"] \arrow[d, "\mathrm{id}_A"'] & B \arrow[l, dashed, shift left, "k"] \arrow[r, "g"] \arrow[d, "\psi"'] & C \arrow[r] \arrow[d, "\mathrm{id}_C"] & 0 \\
0 \arrow[r] & A \arrow[r, "\iota_1"] & A \oplus C \arrow[r, "\pi_2"] & C \arrow[r] & 0
\end{tikzcd}$$

commutes, where

$$\begin{array}{rccc}
\psi: & B & \longrightarrow & A \oplus C \\
 & b & \longmapsto & \big(k(b), g(b)\big)
\end{array}$$

is an isomorphism by the five lemma.

(iii) ⇒ (i) and (ii).

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, shift left, "\iota_1"] \arrow[d, "\alpha"'] & A \oplus C \arrow[l, dashed, shift left, "\pi_1"] \arrow[r, shift left, "\pi_2"] \arrow[d, "\beta"'] & C \arrow[l, dashed, shift left, "\iota_2"] \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & A \arrow[r, shift left, "f"] & B \arrow[l, dashed, shift left, "k"] \arrow[r, shift left, "g"] & C \arrow[l, dashed, shift left, "h"] \arrow[r] & 0
\end{tikzcd}$$

Let $k = \alpha \circ \pi_1 \circ \beta^{-1}$, $h = \beta \circ \iota_2 \circ \gamma^{-1}$. □

Lemma 2.34 (The five lemma). *Let*

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"'] & A_2 \arrow[r, "f_2"] \arrow[d, "\alpha_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "\alpha_3"'] & A_4 \arrow[r, "f_4"] \arrow[d, "\alpha_4"'] & A_5 \arrow[d, "\alpha_5"'] \\
B_1 \arrow[r, "g_1"] & B_2 \arrow[r, "g_2"] & B_3 \arrow[r, "g_3"] & B_4 \arrow[r, "g_4"] & B_5
\end{tikzcd}$$

be a commutative diagram of R-modules with exact rows.

(i) *If α_1 is surjective and α_2, α_4 are injective, then α_3 is injective.*

(ii) *If α_5 is injective and α_2, α_4 are surjective, then α_3 is surjective.*

Proof. (i) Let $a_3 \in \ker \alpha_3$. Then $\alpha_4 f_3(a_3) = g_3\alpha_3(a_3) = 0$. Since α_4 is injective, $f_3(a_3) = 0$. So, $a_3 = f_2(a_2)$ for some $a_2 \in A_2$. Let $b_2 = \alpha_2(a_2)$. Then $g_2(b_2) = \alpha_3(a_3) = 0$. So, $b_2 = g_1(b_1)$ for some $b_1 \in B_1$. Let $a_1 \in A_1$ such that $\alpha_1(a_1) = b_1$. Then $\alpha_2(a_2 - f_1(a_1)) = \alpha_2(a_2) - \alpha_2 f_1(a_1) = b_2 - g_1\alpha_1(a_1) = b_2 - b_2 = 0$. So, $a_2 = f_1(a_1)$. Hence, $a_3 = f_2(a_2) = 0$.

(ii) Let $b_3 \in B_3$. Then $g_3(b_3) = \alpha_4(a_4)$ for some $a_4 \in A_4$. Since $\alpha_5 f_4(a_4) = g_4\alpha_4(a_4) = g_4 g_3(b_3) = 0$, we have $f_4(a_4) = 0$. So, $a_4 = f_3(a_3)$ for some $a_3 \in A_3$. Since $g_3(b_3 - \alpha_3(a_3)) = \alpha_4(a_4) - g_3\alpha_3(a_3) = \alpha_4(a_4) - \alpha_4 f_3(a_3) = \alpha_4(a_4) - \alpha_4(a_4) = 0$, $b_3 - \alpha_3(a_3) = g_2(b_2)$ for some $b_2 \in B_2$. Let $a_2 \in B_2$ such that $b_2 = \alpha_2(a_2)$. Then $\alpha_3(a_3 + f_2(a_2)) = \alpha_3(a_3) + \alpha_3 f_2(a_2) = \alpha_3(a_3) + g_2\alpha_2(a_2) = \alpha_3(a_3) + g_2(b_2) = b_3$. □

Projective modules. An R-module P is called projective if for every surjection $p : A \to B$ and homomorphism $f : P \to B$, there exists a homomorphism $g : P \to A$ such that

$$\begin{tikzcd}
& P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
A \arrow[r, "p"] & B \arrow[r] & 0
\end{tikzcd}$$

commutes.

Free modules are projective.

Theorem 2.35 (Characterizations of projective modules). *Let P be an R-module. The following statements are equivalent.*

(i) *P is projective.*

(ii) *Every short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{p} P \to 0$ is split.*

(iii) *There exists an R-module K such that $K \oplus P$ is free.*

Proof. (i) ⇒ (ii).

$$\begin{tikzcd}
& & & P \arrow[dl, dashed, "g"'] \arrow[d, "\mathrm{id}"] & \\
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "p"] & P \arrow[r] & 0
\end{tikzcd}$$

(ii) ⇒ (iii). There exists a free R-module F and surjection $p : F \to P$. Since $0 \to \ker p \hookrightarrow F \xrightarrow{p} P \to 0$ is exact, hence split, $F \cong \ker p \oplus P$.

(iii) ⇒ (i).

$$\begin{tikzcd}
& F = K \oplus P \arrow[d, shift right, "\pi"'] \arrow[ddl, dashed, "g_1"'] & \\
& P \arrow[u, shift right, "\iota"'] \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
A \arrow[r, "p"] & B \arrow[r] & 0
\end{tikzcd}$$

Since F is projective, there exists $g_1 : F \to A$ such that $pg_1 = f\pi$. Let $g = g_1\iota$. Then $pg = pg_1\iota = f\pi\iota = f$. □

Pull back. Let

$$\begin{tikzcd}
& A \arrow[d, "f"] \\
B \arrow[r, "g"'] & C
\end{tikzcd} \tag{2.2}$$

be a diagram of R-modules. Define $D = \{(a,b) \in A \times B : f(a) = g(b)\}$ and $\alpha : D \to A$, $(a,b) \mapsto a$; $\beta : D \to B$, $(a,b) \mapsto b$. Then

$$\begin{tikzcd} D \arrow[r, "\alpha"] \arrow[d, "\beta"'] & A \arrow[d, "f"] \\ B \arrow[r, "g"'] & C \end{tikzcd}$$

is a commutative diagram of R-modules. (D,α,β) is called the *pull back* of (2.2). g is onto $\Rightarrow$ α is onto. (Proof. $\forall\, a \in A$, $\exists\, b \in B$ such that $f(a) = g(b)$. Then $(a,b) \in D$ and $a = \alpha(a,b)$.)

In Theorem 2.35, (ii) $\Rightarrow$ (i) can also be proved using a pull back:

$$\begin{tikzcd} 0 \arrow[r] & \ker\alpha \arrow[r, hook] & D \arrow[r, shift left, "\alpha"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[l, shift left, dashed] \arrow[d, "f"] \arrow[dl, dashed] & 0 \\ & & A \arrow[r, "p"] & B \arrow[r] & 0 \end{tikzcd}$$

Note that p is onto $\Rightarrow$ α is onto.

Example. Let $R = \mathbb{Z}_6$. ${}_R\mathbb{Z}_3$ is projective ($\mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong R$) but not free.

Theorem 2.36. *Let F be a free module over a PID R and A a submodule of F. Then A is free with* $\operatorname{rank} A \le \operatorname{rank} F$.

Proof. Let X be a basis of F. Let

$$\mathcal{Y} = \{(Y,Z,f) : Z \subset Y \subset X,\ f : Z \to A \cap \langle Y \rangle \text{ 1-1, } f(Z) \text{ is a basis of } A \cap \langle Y \rangle\}.$$

For (Y_1,Z_1,f_1), $(Y_2,Z_2,f_2) \in \mathcal{Y}$, define $(Y_1,Z_1,f_1) \prec (Y_2,Z_2,f_2)$ if $Y_1 \subset Y_2$, $Z_1 \subset Z_2$ and $f_2|_{Z_1} = f_1$. Then $(\mathcal{Y},\prec)$ is a nonempty poset in which every chain has an upper bound. By Zorn's lemma, $(\mathcal{Y},\prec)$ has a maximal element (Y_0,Z_0,f_0). It suffices to show $Y_0 = X$.

Suppose to the contrary that $Y_0 \ne X$. Let $x_0 \in X \smallsetminus Y_0$. Put

$$I = \{r \in R : rx_0 + y \in A \text{ for some } y \in \langle Y_0 \rangle\}.$$

I is an ideal of R; hence $I = \langle s \rangle$ for some $s \in R$. If $s = 0$, $A \cap \langle Y_0 \cup \{x_0\}\rangle = A \cap \langle Y_0 \rangle$. Then $(Y_0 \cup \{x_0\}, Z_0, f_0) \gneqq (Y_0,Z_0,f_0)$, $\to\leftarrow$. So, $s \ne 0$. Let $u \in A$ such that $u = sx_0 + y$ for some $y \in \langle Y_0 \rangle$. We claim that

$$A \cap \langle Y_0 \cup \{x_0\}\rangle = A \cap \langle Y_0 \rangle \oplus \langle u \rangle. \tag{2.3}$$

First we show that $A \cap \langle Y_0 \cup \{x_0\}\rangle = A \cap \langle Y_0 \rangle + \langle u \rangle$. If $w \in A \cap \langle Y_0 \cup \{x_0\}\rangle$, then $w = tx_0 + z$ for some $z \in \langle Y_0 \rangle$ and $t \in R$ with $s \mid t$. So, $w - \frac{t}{s}u \in A \cap \langle Y_0 \rangle \Rightarrow w \in A \cap \langle Y_0 \rangle + \langle u \rangle$. Next note that $\langle Y_0 \rangle \cap \langle u \rangle = \{0\}$. (If $au = y'$ for some $a \in R$ and $y' \in \langle Y_0 \rangle$, then $a(sx_0 + y) = y'$, so $a = 0$.) Thus, $A \cap \langle Y_0 \rangle + \langle u \rangle = A \cap \langle Y_0 \rangle \oplus \langle u \rangle$, and claim (2.3) is proved. Now $f_0(Z_0) \cup \{u\}$ is a basis of $A \cap \langle Y_0 \cup \{x_0\}\rangle$. Extend $f_0 : Z_0 \to A \cap \langle Y_0 \rangle$ to $g : Z_0 \cup \{x_0\} \to A \cap \langle Y_0 \cup \{x_0\}\rangle$ by setting $g(x_0) = u$. Then $(Y_0 \cup \{x_0\}, Z_0 \cup \{x_0\}, g) \gneqq (Y_0,Z_0,f_0)$. $\to\leftarrow$. □

Note. If $\operatorname{rank} F < \infty$, Theorem 2.36 can be proved by an induction on $\operatorname{rank} F$; the argument is similar to the above proof but Zorn's lemma is not needed.

Theorem 2.37. *Every projective module over a PID is free.*

Proof. Let P be a projective module over a PID R. By Theorem 2.35 (iii), P is a submodule of a free R-module. By Theorem 2.36, P is free. □

Theorem 2.38 ([**1, 16, 21**]). *Let k be a field. Then every projective module over $k[x_1,\dots,x_n]$ is free.*

In Theorem 2.38, the case when the projective module is non-finitely generated was proved by Bass [**1**]; the case when the projective module is finitely generated is known as *Serre's conjecture* and *Quillen-Suslin's theorem.* See [**14**, Ch. III] for some elementary proofs of Serre's conjecture.

Projective modules over a local ring.

Theorem 2.39 (Kaplansky [**13**]). *Every projective module over a local ring (not necessarily commutative) is free.*

Lemma 2.40. *If A is a direct sum of countably generated R-modules and B is a direct summand of A, then B is a direct sum of countably generated R-modules.*

Proof. Let $A=\bigoplus_{i\in I}A_i$, where A_i is countably generated. Let $A=B\oplus C$. For each $J\subset I$, put $A_J=\sum_{i\in J}A_i$. Let

$$\begin{aligned}\mathcal{X}=\big\{(J,\mathcal{L}):J\subset I,\ A_J=A_J\cap B+A_J\cap C,\ &\mathcal{L}\text{ is a family of countably}\\ &\text{generated submodules of } B \text{ such that } A_J\cap B=\textstyle\bigoplus_{L\in\mathcal{L}}L\big\}.\end{aligned}$$

$(\mathcal{X},\subset)$ is a poset in which every chain has an upper bound. (If $(J_j,\mathcal{L}_j)$ is a chain in $(\mathcal{X},\subset)$, then $(\bigcup_j J_j,\,\bigcup_j\mathcal{L}_j)\in\mathcal{X}$.) By Zorn's lemma, $(\mathcal{X},\subset)$ has a maximal element $(J_0,\mathcal{L}_0)$.

We claim that $J_0=I$. (The conclusion of the lemma follows from the claim.) Assume to the contrary that $\exists i_1\in I\smallsetminus J_0$. Let $J_1=\{i_1\}$ and $A_{J_1}=\langle x_{11},x_{12},\dots\rangle$. Write $x_{1j}=x'_{1j}+x''_{1j}$, where $x'_{1j}\in B$, $x''_{2j}\in C$. Each x'_{1j} (x''_{1j}) is contained in A_J for some finite $J\subset I$. So, $\bigcup_{j=1}^{\infty}\{x'_{1j},x''_{1j}\}\subset A_{J_2}$ for some countable $J_2\subset I$. Write $A_{J_2}=\langle x_{21},x_{22},\dots\rangle$, $x_{2j}=x'_{2j}+x''_{2j}$, $x'_{2j}\in B$, $x''_{2j}\in C$. Then $\bigcup_{j=1}^{\infty}\{x'_{2j},x''_{2j}\}\subset A_{J_3}$ for some countable $J_3\subset I$. In general,

$$A_{J_i}\subset A_{J_{i+1}}\cap B+A_{J_{i+1}}\cap C.$$

Let $J^*=\bigcup_{i=0}^{\infty}J_i$. Then

$$A_{J^*}\subset A_{J^*}\cap B+A_{J^*}\cap C.$$

Since $A_{J_0}\cap B$ is a direct summand of A_{J_0} and A_{J_0} is a direct summand of A, $A_{J_0}\cap B$ is a direct summand of A. Hence $A_{J_0}\cap B$ is a direct summand of $A_{J^*}\cap B$. (Cf. Exercise 2.7.) Since $A_{J^*}=A_{J^*}\cap B\oplus A_{J^*}\cap C$ and $A_{J_0}=A_{J_0}\cap B\oplus A_{J_0}\cap C$, we have

$$\frac{A_{J^*}}{A_{J_0}}=\frac{A_{J^*}\cap B}{A_{J_0}\cap B}\oplus\frac{A_{J^*}\cap C}{A_{J_0}\cap C}.$$

Thus, $(A_{J^*}\cap B)/(A_{J_0}\cap B)$ is a homomorphic image of A_{J^*}/A_{J_0}. Since A_{J^*} is countably generated, so is $(A_{J^*}\cap B)/(A_{J_0}\cap B)$. We have

$$A_{J^*}\cap B=(A_{J_0}\cap B)\oplus L,$$

where $L\cong(A_{J^*}\cap B)/(A_{J_0}\cap B)$ is countably generated. Thus $(J^*,\mathcal{L}_0\cup\{L\})\in\mathcal{X}$, which contradicts the maximality of $(J_0,\mathcal{L}_0)$. □

Proof of Theorem 2.39. Let R be a local ring with maximal ideal $\mathfrak{m}$. Let P be a projective module over R.

1° Every $x \in P$ is contained in a free direct summand of P.

There exists an R-module Q such that $F := P \oplus Q$ is free. Let $\mathcal{U}$ be a basis of F. Write $x = a_1u_1 + \cdots a_nu_n$, $a_i \in R$, $u_1, \dots, u_n \in \mathcal{U}$ distinct. Assume $\mathcal{U}$ is chosen such that n is as small as possible. Then for each $1 \le i \le n$,

$$a_i \notin a_1R + \cdots + a_{i-1}R + a_{i+1}R + \cdots + a_nR. \tag{2.4}$$

(If $a_n = a_1b_1 + \cdots a_{n-1}b_{n-1}$, then $x = a_1(u_1 + b_1u_n) + \cdots + a_{n-1}(u_{n-1} + b_{n-1}u_n)$. Note that $\{u_1 + b_1u_n, \dots, u_{n-1} + b_{n-1}u_n, u_n\} \cup \mathcal{U}'$ is a basis of F, where $\mathcal{U}' = \mathcal{U} \setminus \{u_1, \dots, u_n\}$. This contradicts the minimality of n.) Write $u_i = y_i + z_i$, $y_i \in P$, $z_i \in Q$. Then

$$a_1u_1 + \cdots + a_nu_n = a_1y_1 + \cdots + a_ny_n. \tag{2.5}$$

Write

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \equiv C \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \pmod{\langle \mathcal{U}' \rangle}. \tag{2.6}$$

By (2.5) and (2.6), we have

$$[a_1, \dots, a_n] = [a_1, \dots, a_n]C,$$

i.e., $[a_1, \dots, a_n](I - C) = 0$. By (2.4), all entries of $I - C$ are in $\mathfrak{m}$. Since R is local, C is invertible in $M_{n \times n}(R)$. So, by (2.6), $\{y_1, \dots, y_n\} \cup \mathcal{U}'$ is a basis of F. Let $Y = \langle y_1, \dots, y_n \rangle$. Then $x \in Y$ and Y is free and is a direct summand of F hence a direct summand of P.

2° P is a direct summand of a free R-module. By Lemma 2.40, P is a direct sum of countably generated R-modules. Thus we may assume that P is countably generated.

Let $P = \langle x_1, x_2, \dots \rangle$. By 1°, $P = F_1 \oplus P_1$, where F_1 is free and $x_1 \in F_1$. Write $x_2 = x_2' + x_2''$, $x_2' \in F_1$, $x_2'' \in P_1$. By 1° again, $P_1 = F_2 \oplus P_2$, where F_2 is free and $x_2'' \in F_2$. Write $x_3 = x_3' + x_3''$, $x_3' \in F_1 \oplus F_2$, $x_3'' \in P_2$, ... Then $P = F_1 \oplus F_2 \oplus \cdots$. □

Injective modules. An R-module E is called *injective* if for every injection $i : A \to B$ and homomorphism $f : A \to E$, there exists a homomorphism $g : B \to E$ such that

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"'] & B \arrow[dl, dashed, "g"] \\
 & E &
\end{tikzcd}$$

commutes.

Fact. Let $\{E_i : i \in I\}$ be a family of R-modules. Then $\prod_{i \in I} E_i$ is injective $\Leftrightarrow$ E_i is injective for all $i \in I$.

Proof. (⇒)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "j"] \arrow[d, "f"'] & B \arrow[dl, dashed] \arrow[ddl] \\
& E_i \arrow[d, shift right, "\iota_i"'] & \\
& \prod_{i\in I} E_i \arrow[u, shift right, "\pi_i"'] &
\end{tikzcd}$$

(⇐)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "j"] \arrow[d, "f"'] & B \arrow[dl, dashed, "h"'] \arrow[ddl, "h_i"] \\
& \prod_{i\in I} E_i \arrow[d, "\pi_i"'] & \\
& E_i &
\end{tikzcd} \qquad h(b) = (h_i(b))_{i\in I}.$$

□

Push out. Let

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \\
C &
\end{tikzcd} \tag{2.7}$$

be a diagram of R-modules. Let $S = \big\{(f(a), -g(a)) : a \in A\big\} \subset B \oplus C$, $D = (B \oplus C)/S$, $\alpha : B \to D$, $b \mapsto (b, 0) + S$, $\beta : C \to D$, $c \mapsto (0, c) + S$. Then

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "\alpha"] \\
C \arrow[r, "\beta"'] & D
\end{tikzcd}$$

is a commutative diagram of R-modules. (D, α, β) is called the *push out* of (2.7).

Proposition 2.41 (Characterizations of injective modules). *Let E be an R-module. The following statements are equivalent.*

(i) *E is injective.*

(ii) *Every short exact sequence $0 \to E \xrightarrow{i} A \xrightarrow{p} B \to 0$ is split.*

(iii) *If E is a submodule of A, then $A = E \oplus B$ for some submodule B of A.*

Proof. (i) ⇒ (ii).

$$\begin{tikzcd}
0 \arrow[r] & E \arrow[r, "i"] \arrow[d, "\mathrm{id}"'] & A \arrow[r, "p"] \arrow[dl, dashed, "g"] & B \arrow[r] & 0 \\
& E & & &
\end{tikzcd}$$

(ii) ⇒ (i). Use a push out

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"'] & B \arrow[d, "\alpha"] \arrow[dl, dashed] & & \\
0 \arrow[r] & E \arrow[r, shift right, "\beta"'] & D \arrow[l, shift right, dashed] \arrow[r] & \operatorname{coker}\beta \arrow[r] & 0
\end{tikzcd}$$

Note that i is 1-1 ⇒ β is 1-1. (If $x \in \ker\beta$, $(0,x) \in S$, i.e., $(0,x) = (i(a), -f(a))$ for some $a \in A$. So, $i(a) = 0 \Rightarrow a = 0 \Rightarrow x = f(a) = 0$.)

(ii) ⇒ (iii). $0 \to E \hookrightarrow A \to A/E \to 0$ is split.

(iii) ⇒ (ii). Obvious. □

Note. Theorem 2.45 also provides a quick proof of (iii) ⇒ (i).

Theorem 2.42 (Baer's criterion). *An R-module E is injective ⇔ given any left ideal L of R and R-map $\alpha : L \to E$, α can be extended to an R-map $\beta : R \to E$.*

Proof. (⇐) Given

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"'] & B \\
& E &
\end{tikzcd}$$

May assume that $A \subset B$ and i is the inclusion. Let

$$\mathcal{S} = \{(C,h) : A \subset {}_R C \subset B,\ h : C \to E \text{ is an } R\text{-map},\ h|_A = f\}.$$

For (C_1,h_1), $(C_2,h_2) \in \mathcal{S}$, define $(C_1,h_1) \prec (C_2,h_2)$ if $C_1 \subset C_2$ and $h_2|_{C_1} = h_1$. $(\mathcal{S},\prec)$ is a nonempty poset in which every chain has an upper bound. By Zorn's lemma, $(\mathcal{S},\prec)$ has a maximal element of (C_0,h_0). It remains to show that $C_0 = B$.

Assume to the contrary that $\exists b \in B \setminus C_0$. Let $L = \{r \in R : rb \in C_0\}$. L is a left ideal of R. $\alpha : L \to E$, $r \mapsto h_0(rb)$ is an R-map. So, α extends to an R-map $\beta : R \to E$. Define

$$\begin{array}{rccc} h_1 : & C_0 + Rb & \longrightarrow & E \\ & c + rb & \longmapsto & h_0(c) + r\beta(1) \end{array}$$

h_1 is a well-defined R-map. (If $c + rb = c' + r'b$, then $(r - r')b = c' - c \in C_0$. So, $h_0(c' - c) = h_0((r - r')b) = \alpha(r - r') = \beta(r - r') = (r - r')\beta(1)$.) Also $h_1|_{C_0} = h_0$. So, $(C_0 + Rb, h_1) \gneqq (C_0, h_0)$, →←. □

Divisible modules. Let R be an integral domain and D and R-module. D is called *divisible* if $\forall y \in D$, and $0 \neq r \in R$, $\exists x \in D$ such that $rx = y$. D is divisible ⇔ $rD = D$ $\forall 0 \neq r \in R$.

Facts.

(i) D_i, $i \in I$ divisible ⇔ $\bigoplus_{i \in I} D_i$ divisible.

(ii) D divisible and $E \subset D \Rightarrow D/E$ divisible.

(iii) D injective ⇒ D divisible.

Proof. (iii) Let $y \in D$ and $0 \neq r \in R$. Consider

$$\begin{tikzcd}
0 \arrow[r] & rR \arrow[r, hook] \arrow[d, "f"'] & R \arrow[dl, dashed, "g"] \\
& D &
\end{tikzcd}$$

where $f(r) = y$. Then $rg(1) = f(r) = y$. □

Proposition 2.43. *Let D be a modules over a PID R. Then D is injective $\Leftrightarrow$ D is divisible.*

Proof. ($\Leftarrow$) Let $I \neq 0$ be an ideal of R and $f : I \to D$ an R-map. We have $I = \langle a \rangle$ for some $0 \neq a \in R$. Since D is divisible, $\exists x \in D$ such that $ax = f(a)$. Define $g : R \to D$, $r \mapsto rx$. Then g is an R-map and $g|_I = f$. By Baer's criterion, D is injective. □

Proposition 2.44. *Every abelian group A can be embedded in a divisible abelian group.*

Proof. $A \cong (\bigoplus_{i \in I} \mathbb{Z})/K \hookrightarrow (\bigoplus_{i \in I} \mathbb{Q})/K$, where $(\bigoplus_{i \in I} \mathbb{Q})/K$ is divisible. □

Theorem 2.45. *Every R-module A can be embedded in an injective R-module.*

Proof. By Proposition 2.44, $\exists\, \mathbb{Z}$-module embedding $f : A \to B$, where B is a divisible abelian group. Then we have R-module embeddings

$$A \xrightarrow{\phi} \mathrm{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}A) \xrightarrow{\bar{f}} \mathrm{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}B)$$

where

$$\begin{array}{rccc} \phi(a): & R & \longrightarrow & A \\ & r & \longmapsto & ra \end{array} \qquad \begin{array}{rccc} \bar{f}(\alpha): & R & \longrightarrow & B \\ & r & \longmapsto & f(\alpha(r)) \end{array}$$

By the next lemma, $\mathrm{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}B)$ is an injective R-modules. □

Lemma 2.46. *Let R be a ring and B a divisible abelian group. Then* $\mathrm{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}B)$ *is an injective R-module.*

Proof. Let L be a left ideal of R and $f : L \to \mathrm{Hom}_{\mathbb{Z}}(R, B)$ an R-map. Let

$$\begin{array}{rccc} g: & L & \longrightarrow & B \\ & x & \longmapsto & [f(x)](1_R). \end{array}$$

g is a $\mathbb{Z}$-map. So, g extends to a $\mathbb{Z}$-map $\bar{g} : R \to B$. For each $r \in R$, define

$$\begin{array}{rccc} h(r): & R & \longrightarrow & B \\ & y & \longmapsto & \bar{g}(yr). \end{array}$$

Then $h(r) \in \mathrm{Hom}_{\mathbb{Z}}(R, B)$, $h : R \to \mathrm{Hom}_{\mathbb{Z}}(R, B)$ is an R-map and $h|_L = f$. By Baer's criterion, $\mathrm{Hom}_{\mathbb{Z}}(R, B)$ is injective. □

2.8. Chain Conditions

Let ${}_RA$ be an R-module. Two finite descending (or ascending) sequences of submodules

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{0\}$$
$$A = A'_0 \supset A'_1 \supset \cdots \supset A'_m = \{0\}$$

are called *equivalent* if there is a bijection between $\{A_{i-1}/A_i : 1 \le i \le n,\ A_{i-1} \supsetneq A_i\}$ and $\{A'_{j-1}/A'_j : 1 \le j \le m,\ A'_{j-1} \supsetneq A'_j\}$ such that the corresponding factors are isomorphic. A descending sequence $A = A_0 \supset A_1 \supset \cdots \supset A_n = \{0\}$ is called a *composition series* of A if A_{i-1}/A_i is simple for all $1 \le i \le n$.

Theorem 2.47 (Scherier). *Any two finite desceding (or ascending) sequences of submodules of a module ${}_RA$ have equivalent refinements.*

Theorem 2.48 (Jordan-Hölder). *Any two composition series of a module ${}_RA$ are equivalent.*

Proofs of Theorems 2.47 and 2.48 are the same as the proofs in the group case; see Theorem 1.37 and 1.39.

ACC and DCC. An R-module A is said to have the *ascending chain condition* (ACC) if for every ascending chain of submodules $A_1 \subset A_2 \subset \cdots$, there exists n such that $A_n = A_{n+1} = \cdots$. A is said to have the *descending chain condition* (DCC) if for every descending chain of submodules $A_1 \supset A_2 \supset \cdots$, there exists n such that $A_n = A_{n+1} = \cdots$.

Example. $\mathbb{Z}$ as a $\mathbb{Z}$-module has ACC but no DCC. Let p be a prime and let $\mathbb{Z}(p^\infty)$ be the subgroup of $\mathbb{Q}/\mathbb{Z}$ defined by

$$\mathbb{Z}(p^\infty) = \Big\{\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z} : a, b \in \mathbb{Z},\ b = p^i \text{ for some } i \ge 0\Big\}.$$

The every proper subgroup is generated by $\frac{1}{p^i} + \mathbb{Z}$ for some $i \ge 0$. Since

$$0 = \Big\langle \frac{1}{p^0} + \mathbb{Z} \Big\rangle \subsetneq \Big\langle \frac{1}{p^1} + \mathbb{Z} \Big\rangle \subsetneq \cdots,$$

$\mathbb{Z}(p^\infty)$ as a $\mathbb{Z}$-module has DCC but not ACC.

Proposition 2.49. *Let A be an R-module.*

(i) *A has ACC $\Leftrightarrow$ every nonempty family of submodules of A contains a maximal element $\Leftrightarrow$ every submodule of A is finitely generated.*
(ii) *A has DCC $\Leftrightarrow$ every nonempty family of submodules of A contains a minimal element.*

Proof. (i) *Every submodule of A is finitely generated $\Rightarrow$ A has ACC.*
Let $A_0 \subset A_1 \subset \cdots$ be an ascending sequence of submodules of A. Then $\bigcup_{i=0}^\infty A_i = (a_1, \dots, a_k)$ for some $a_1, \dots, a_k \in \bigcup_{i=0}^\infty A_i$. Choose n such that $a_0, \dots, a_k \in A_n$. Then $A_n = \bigcup_{i=0}^\infty A_i$. □

Proposition 2.50. *A module ${}_RA$ has a composition series $\Leftrightarrow$ A has both ACC and DCC.*

Proof. ($\Rightarrow$) Assume that A has a composition series with $n+1$ terms. Assume to the contrary that A does not have ACC or DCC. Then there is a squence of submodules of A:

$$A = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_{n+1} = \{0\}.$$

Any refinement of this sequence has at least $n+1$ nonzero factors hence cannot be equivalent to the composition series of A. This is a contradiction to Theorem 2.47.

($\Leftarrow$) We construct a composition series $A = A_0 \supset A_1 \supset \cdots$ as follows. Let $A_0 = A$. If $A_0 \neq 0$, since A has ACC, among all proper submodules of A_0, there is a maximal one, say, A_1. Clearly, A_0/A_1 is simple. By induction, there are submodules $A_0 \supset A_1 \supset A_2 \supset \cdots$ such that A_i/A_{i+1} is simple for all i and A_{i+1} is defined whenever $A_i \neq 0$. Since A has DCC, the above descending series must stop at A_n. So, $A_n = 0$. Now, $A = A_0 \supset A_1 \supset \cdots \supset A_n = 0$ is a composition series of A. □

Definition 2.51. A ring R is called left (right) *noetherian* if the module ${}_RR$ (R_R) has ACC. R is called left (right) *artinian* if the module ${}_RR$ (R_R) has DCC. R is called noetherian (artinian) if it is both left and right noetherian (artinian).

The Hopkins-Levitzki theorem (Theorem 4.25). A left (right) artinian ring is left (right) noetherian.

Proof. Not easy, will be given in §4.3. □

Theorem 2.52 (Hilbert basis theorem). *If R is a left (right) noetherian ring, then so is $R[x_1, \dots, x_n]$.*

Proof. We only have to show that $R[x]$ is left noetherian. Assume to the contrary that there exists a left ideal I of $R[x]$ which is not finitely generated. Let $f_0 \in I$ be a polynomial of the smallest degree. Then $I \neq (f_0)$. Let $f_1 \in I \setminus (f_0)$ be of the smallest degree. In general, let $f_{n+1} \in I \setminus (f_0, \dots, f_n)$ be of the smallest degree. Let $d_n = \deg f_n$. Then $d_0 \leq d_1 \leq \cdots$. Let a_n be the leading coefficient of f_n. Then $(a_0) \subset (a_0, a_1) \subset \cdots$ is an ascending chain of ${}_RR$. Since R is left noetherian, $\exists m$ such that $(a_0, \dots, a_m) = (a_0, \dots, a_m, a_{m+1})$. So,

$$a_{m+1} = r_0 a_0 + \cdots + r_m a_m, \quad r_i \in R.$$

Put

$$f = f_{m+1} - \sum_{i=0}^{m} r_i f_i(x) x^{d_{m+1} - d_i}.$$

Then $f \in I \setminus (f_0, \dots, f_m)$ and $\deg f < d_{m+1}$, which is a contradiction. □

Proposition 2.53. *Let $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ be an exact sequence of R-modules. Then B has ACC (DCC) $\Leftrightarrow$ both A and C have ACC (DCC).*

Proof. *B has ACC $\Rightarrow$ A and C have ACC.*

Let $A_1 \subset A_2 \subset \cdots$ be an ascending sequence of submodules of A. Then $i(A_1) \subset i(A_2) \subset \cdots$ is an ascending sequence of submodules of B. Thus $i(A_1) \subset i(A_2) \subset \cdots$ stabilizes and so does $A_1 \subset A_2 \subset \cdots$.

Let $C_1 \subset C_2 \subset \cdots$ be an ascending sequence of submodules of C. Then $p^{-1}(C_1) \subset p^{-1}(C_2) \subset \cdots$ is an ascending sequence of submodules of B, so it stabilizes. Since $C_i = p(p^{-1}(C_i))$, $C_1 \subset C_2 \subset \cdots$ also stabilizes.

A and C have ACC $\Rightarrow$ B has ACC.

Let $B_1 \subset B_2 \subset \cdots$ be an ascending sequence of submodules of B. Then $\exists n > 0$ such that for all $k > 0$, $p(B_n) = p(B_{n+k})$ and $i^{-1}(B_n) = i^{-1}(B_{n+k})$. We have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & i^{-1}(B_n) \arrow[r, "i"] \arrow[d, "\text{id}"] & B_n \arrow[r, "p"] \arrow[d, hook] & p(B_n) \arrow[r] \arrow[d, "\text{id}"] & 0 \\
0 \arrow[r] & i^{-1}(B_{n+k}) \arrow[r, "i"] & B_{n+k} \arrow[r, "p"] & p(B_{n+k}) \arrow[r] & 0
\end{tikzcd}$$

By the five lemma, $B_k = B_{n+k}$. □

Proposition 2.54. *Let R be a left noetherian (artinian) ring. Then every finitely generated R-module A has ACC (DCC).*

Proof. $A \cong R^n/K$. Since R has ACC, by Proposition 2.53, R^n and R^n/K has ACC. □

Proposition 2.55. *Let $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ be an exact sequence of R-modules.*

(i) *Assume that $A = \langle X \rangle$ and $C = \langle Y \rangle$. Choose $Z \subset B$ such that $p(Z) = Y$. Then $B = \langle X \cup Z \rangle$. In particular, A and C are finitely generated $\Rightarrow$ B is finitely generated.*

(ii) *If R is left noetherian, then B is finitely generated $\Leftrightarrow$ both A and C are finitely generated.*

Proof. (ii) ($\Rightarrow$) By Proposition 2.56 (i), A is finitely generated. □

Proposition 2.56. *Let R be a left noetherian ring and M a finitely generated R-module.*

(i) *Every submodule of M is finitely generated.*

(ii) *If R is a PID and M is generated by n elements, then every submodules of M can be generated by $\le n$ elements.*

Proof. (i) Let $M = \langle x_1, \dots, x_n \rangle$ and let S be a submodule of M. Use induction on n.

If $n = 1$, $M = \langle x_1 \rangle \cong R/I$ for some left ideal I of R. Then $S \cong J/I$ for some left ideal J of R with $J \supset I$. Since R is left noetherian, J is fnitely generated and so is J/I.

Assume $n > 1$. Let $M_1 = \langle x_1, \dots, x_{n-1} \rangle$. Then

$$0 \to S \cap M_1 \to S \to S/(S \cap M_1) \to 0$$

is exact. Since $S \cap M_1 \subset M_1$, by the induction hypothesis, $S \cap M_1$ is finitely generated. Since $S/(S \cap M_1) \cong (S + M_1)/M_1 \subset M/M_1 = \langle x_n + M_1 \rangle$, $S/(S \cap M_1)$ is also finitely generated. Thus S is finitely generated.

(ii) In the proof of (i), $S/(S \cap M_1)$ is cyclic. □

2.9. Finitely Generated Modules over a PID

Theorem 2.57 (Structure of finitely generated modules over a PID). *Let A be a finitely generated module over a PID R. Then*

$$A = Rz_1 \oplus \cdots \oplus Rz_s, \tag{2.8}$$

where

$$R \neq \operatorname{ann}(z_1) \supset \cdots \supset \operatorname{ann}(z_s). \tag{2.9}$$

Moreover, $\operatorname{ann}(z_1), \cdots, \operatorname{ann}(z_s)$ *are uniquely determined by* (2.8) *and* (2.9). *(Note.* $Rz_i \cong R/\operatorname{ann}(z_i)$*.)*

PROOF. *Existence of decomposition* (2.8).

Since A is finitely generated, we may assume $A = R^n/K$, where K is a submodule of R^n. Since R is a PID, by Proposition 2.56, K is finitely generated. (In fact, by Theorem 2.36, K is free of rank $m \le n$.) Let $K = (f_1, \dots, f_m)$ and write

$$\begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = C \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix},$$

where $e_1, \dots, e_n$ is the standard basis of R^n and $C \in M_{m\times n}(R)$. There exist $P \in \mathrm{GL}(m, R)$ and $Q \in \mathrm{GL}(n, R)$ such that

$$PCQ = \begin{bmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ & 0 & & 0 \end{bmatrix},$$

where $d_i \neq 0$, $d_1 \mid d_2 \mid \cdots \mid d_r$. (This is the *Smith normal form* of A; see [**12**, §3.7].) We assume $d_1 = \cdots = d_a = 1$ and $d_{a+1} \notin R^\times$. Let

$$P \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} = \begin{bmatrix} f'_1 \\ \vdots \\ f'_m \end{bmatrix} \quad \text{and} \quad Q^{-1} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} e'_1 \\ \vdots \\ e'_n \end{bmatrix}.$$

Then

$$\begin{bmatrix} f'_1 \\ \vdots \\ f'_m \end{bmatrix} = \begin{bmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ & 0 & & 0 \end{bmatrix} \begin{bmatrix} e'_1 \\ \vdots \\ e'_n \end{bmatrix}.$$

So, $K = (f'_1, \dots, f'_m) = (d_1 e'_1, \dots, d_r e'_r)$. Since

$$\begin{aligned} R^n &= Re'_1 \oplus \cdots \oplus Re'_n, \\ K &= Rd_1e'_1 \oplus \cdots \oplus Rd_ne'_n \quad (d_i = 0 \text{ for } i > r), \end{aligned}$$

we have

$$\begin{aligned} A = R^n/K &\cong Re'_1/Rd_1e'_1 \oplus \cdots \oplus Re'_n/Rd_ne'_n \\ &\cong R/(d_1) \oplus \cdots \oplus R/(d_n) \\ &\cong R/(d_{a+1}) \oplus \cdots \oplus R/(d_n). \end{aligned}$$

Let $w_i = 1 + (d_i) \in R/(d_i)$, $a+1 \le i \le n$. Then $R/(d_i) = Rw_i$, $\operatorname{ann}(w_i) = (d_i)$ and

$$A \cong Rw_{a+1} \oplus \cdots \oplus Rw_n.$$

Uniqueness of $\operatorname{ann}(z_1), \dots, \operatorname{ann}(z_s)$.

Assume that

$$A = Rz_1 \oplus \cdots \oplus Rz_s = Rw_1 \oplus \cdots \oplus Rw_t,$$

where $R \neq \operatorname{ann}(z_1) \supset \cdots \supset \operatorname{ann}(z_s)$ and $R \neq \operatorname{ann}(w_1) \supset \cdots \supset \operatorname{ann}(w_t)$. We will show that $s = t$ and $\operatorname{ann}(z_i) = \operatorname{ann}(w_i)$.

Without loss of generality, assume $s \geq t$. Let $(w_1', \dots, w_s') = (0, \dots, w_1, \dots, w_t)$. Then

$$A = Rz_1 \oplus \cdots \oplus Rz_s = Rw_1' \oplus \cdots \oplus Rw_s', \tag{2.10}$$

where $\operatorname{ann}(z_1) \supset \cdots \supset \operatorname{ann}(z_s)$ and $\operatorname{ann}(w_1') \supset \cdots \supset \operatorname{ann}(w_s')$. It suffices to show that $\operatorname{ann}(z_i) = \operatorname{ann}(w_i')$ for all $1 \leq i \leq s$.

First, $\operatorname{ann}(z_s) = \operatorname{ann} A = \operatorname{ann}(w_s')$. Let $1 \leq i < s$ and let $\operatorname{ann}(z_i) = (d_i)$. By (2.10),

$$Rd_iz_{i+1} \oplus \cdots \oplus Rd_iz_s \supset Rd_iw_i' \oplus \cdots \oplus Rd_iw_s'.$$

So,

$$d_i \begin{bmatrix} w_i' \\ \vdots \\ w_s' \end{bmatrix} = d_iC \begin{bmatrix} z_{i+1} \\ \vdots \\ z_s \end{bmatrix}, \qquad C \in M_{(s-i+1)\times(s-i)}(R).$$

There exists $P \in \mathrm{GL}(s-i+1, R)$ such that $PA = \left[\begin{smallmatrix} & * & \\ 0 & \cdots & 0 \end{smallmatrix}\right]$. Hence,

$$d_iP \begin{bmatrix} w_i' \\ \vdots \\ w_s' \end{bmatrix} = d_iPC \begin{bmatrix} z_{i+1} \\ \vdots \\ z_s \end{bmatrix} = \begin{bmatrix} * \\ \vdots \\ * \\ 0 \end{bmatrix}.$$

Write $P = \left[\begin{smallmatrix} & * & \\ p_i & \cdots & p_s \end{smallmatrix}\right]$. Then

$$d_i[p_i, \dots, p_s] \begin{bmatrix} w_i' \\ \vdots \\ w_s' \end{bmatrix} = 0.$$

So, $d_ip_jw_j' = 0$, $i \leq j \leq s$, since $Rw_i' \oplus \cdots \oplus Rw_s'$ is a direct sum. So, $d_ip_j \in \operatorname{ann}(w_j') \subset \operatorname{ann}(w_i')$, $i \leq j \leq s$. Since P is invertible, $\gcd(p_i, \dots, p_s) = 1$. Thus, $d_i \in \operatorname{ann}(w_i')$. So, $\operatorname{ann}(z_i) = (d_i) \subset \operatorname{ann}(w_i')$. By symmetry, $\operatorname{ann}(w_i') \subset \operatorname{ann}(z_i)$. □

Note. In the above theorem, assume $\operatorname{ann}(z_i) = (d_i)$, $1 \leq i \leq s$, $d_t \neq 0$, $d_{t+1} = \cdots = d_s = 0$. Write

$$d_i = p_1^{e_{i1}} \cdots p_k^{e_{ik}}, \quad 1 \leq i \leq t,$$

where $p_1, \dots, p_k \in R$ are distinct irreducibles and $e_{ij} \in \mathbb{N}$. Then

$$A \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R^{s-t} \cong \Big[\bigoplus_{\substack{1 \leq i \leq t \\ 1 \leq j \leq k}} R/(p_j^{e_{ij}}) \Big] \oplus R^{s-t}.$$

The integer $s - t$ is called the *rank* of A; $d_1, \dots, d_t$ are called the *invariant factors* of A; $p_j^{e_{ij}}$ with $e_{ij} > 0$ are called the *elementary divisors* of A.

Two finitely generated modules over a PID are isomorphic iff they have the same rank and the same invariant factors (elementary divisors).

Example. Let

$$A = \begin{bmatrix} -18 & 7 & 91 & -14 & 87 \\ 14 & -5 & 3 & 10 & 7 \\ 8 & -3 & 3 & 6 & 5 \\ 126 & -47 & -275 & 94 & -243 \end{bmatrix}$$

and $A = \mathbb{Z}^5/\{xA : x \in \mathbb{Z}^4\}$. The Smith normal form of A is

$$\begin{bmatrix} 1 & & & & \\ & 2 & & & \\ & & 20 & & \\ & & & 0 & 0 \end{bmatrix}.$$

So, $A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}^2$. The elementary divisors of A are $2, 2^2, 5$; $\operatorname{rank} A = 2$.

The structure theorem of finitely generated modules over a PID can also be derived by the following method. The advantage of the above method is that it allows one to compute the invariant factors.

Another proof of Theorem 2.57. Let A be a finitely generated module over a PID R.

Existence of the decomposition of A.

1° Let $A_{\text{tor}} = \{a \in A : ra = 0 \text{ for some } 0 \neq r \in R\}$. Then A/A_{tor} is torsion free. By the next lemma, A/A_{tor} is a free R-module. Thus the exact sequence $0 \to A_{\text{tor}} \hookrightarrow A \to A/A_{\text{tor}} \to 0$ is split. So,

$$A \cong A_{\text{tor}} \oplus (A/A_{\text{tor}}).$$

2° For each irreducible $p \in R$, let

$$A(p) = \{a \in A : p^n a = 0 \text{ for some } n > 0\}.$$

Then

$$A_{\text{tor}} = \bigoplus_p A(p),$$

where the sum is over finitely many irreducibles $p \in R$.

3° Assume $p^n A(p) = 0$ but $p^{n-1}A(p) \neq 0$. Let $a \in A(p)$ such that $p^{n-1}a \neq 0$. Then $Ra \cong R/(p^n)$ (as R-modules and as $R/(p^n)$-modules). Using Baer's criterion, it is easy to see that $R/(p^n)$ is an injective $R/(p^n)$-module. Since Ra is an injective submodule of $A(p)$ (as $R/(p^n)$-modules), we have $A(p) = Ra \oplus B$ for some $R/(p^n)$- and R-submodule B of $A(p)$. Apply the same argument to B. ... Since $A(p)$ is finitely generated, it has ACC (Proposition 2.54). So eventually,

$$A(p) \cong R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_k}).$$

Uniqueness of the decomposition of A. Let

$$A = R^r \oplus \Big[\bigoplus_p \Big(R/(p^{n(p,1)}) \oplus \cdots \oplus R/(p^{n(p,i_p)})\Big)\Big].$$

Then $r = \operatorname{rank}(A/A_{\text{tor}})$ and

$$\dim_{A/(p)}\big(p^{n-1}A/p^nA\big) = \big|\{1 \leq i \leq i_p : n(p,i) \geq n\}\big|.$$

□

LEMMA 2.58. *Let R be a PID. If A is a finitely generated torsion free R-module, then A is free.*

PROOF. Assume $A = \langle x_1, \dots, x_n\rangle$. Let $\{y_1, \dots, y_m\}$ be a maximal linearly independent subset of $\{x_1, \dots, x_n\}$. Then for every $1 \le i \le n$, $\exists\, 0 \ne a_i \in R$ such that $a_i x_i \in \langle y_1, \dots, y_m\rangle$. Let $a = a_1 \cdots a_n$. Then $aA \subset \langle y_1, \dots, y_m\rangle \cong R^m$. So, aA is free. Since A is torsion free, $aA \cong A$. □

THE RATIONAL CANONICAL FORM OF A LINEAR TRANSFORMATION. Let V be an n-dimensional vector space over a field F with a basis $\epsilon_1, \dots, \epsilon_n$. Let $T \in \text{End}_F(V)$ such that

$$T \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix} = A \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix}, \qquad A \in M_n(F).$$

For each $f \in F[x]$ and $v \in V$, define $fv = f(T)v$. Then V is an $F[x]$-module. Define

$$\begin{array}{rccc} \phi: & F[x]^n & \longrightarrow & V \\ & (f_1, \dots, f_n) & \longmapsto & (f_1, \dots, f_n) \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix}. \end{array}$$

Then ϕ is an $F[x]$-map with

$$\ker \phi = \big\{ y(xI - A) : y \in F[x]^n \big\}. \tag{2.11}$$

Proof of (2.11): $\forall (f_1, \dots, f_n) \in F[x]^n$, by the division algorithm, $(f_1, \dots, f_n) = y(xI - A) + (a_1, \dots, a_n)$ for some $y \in F[x]^n$ and $(a_1, \dots, a_n) \in F^n$. Then

$$(f_1, \dots, f_n) \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix} = \big(y(xI - A) + (a_1, \dots, a_n)\big) \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix} = (a_1, \dots, a_n) \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix}.$$

Hence $(f_1, \dots, f_n) \in \ker \phi \Leftrightarrow (a_1, \dots, a_n) = 0$.

Therefore, we have an $F[x]$-module isomorphism

$$V \cong F[x]^n / \{ y(xI - A) : y \in F[x]^n \} = F[x]^n / (\alpha_1, \dots, \alpha_n),$$

where

$$xI - A = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

and $(\alpha_1, \dots, \alpha_n)$ is the $F[x]$-module generated by $\alpha_1, \dots, \alpha_n$. Let the Smith normal form of $xI - A$ be

$$\begin{bmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& d_1 && \\ &&&& \ddots & \\ &&&&& d_r \end{bmatrix}.$$

Then by the proof of Theorem 2.57,

$$V \cong F[x]/(d_1) \oplus \cdots \oplus F[x]/(d_r),$$

i.e., $V = V_1 \oplus \cdots \oplus V_r$, where $V_i \cong F[x]/(d_i)$. Let $d_i = x^{e_i} + a_{i,e_i-1}x^{e_i-1} + \cdots + a_{i,0}$. Then $1, x, \dots, x^{e_i-1}$ is an F-basis of $F[x]/(d_i)$ and

$$x \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{e_i-1} \end{bmatrix} = M(d_i) \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{e_i-1} \end{bmatrix},$$

where

$$M(d_i) = \begin{bmatrix} 0 & 1 &&&& \\ & 0 & 1 &&& \\ && \cdot & \cdot && \\ &&& \cdot & \cdot & \\ &&&& 0 & 1 \\ -a_{i,0} & \cdot & \cdot & \cdot & \cdot & -a_{i,e_i-1} \end{bmatrix}$$

is the companion matrix of d_i. $1, x, \dots, x^{e_i-1}$ correspond to an F-basis $\epsilon_{i,1}, \dots, \epsilon_{i,e_i}$ of V_i. We have

$$T \begin{bmatrix} \epsilon_{i,1} \\ \vdots \\ \epsilon_{i,e_i} \end{bmatrix} = M(d_i) \begin{bmatrix} \epsilon_{i,1} \\ \vdots \\ \epsilon_{i,e_i} \end{bmatrix}.$$

Now $\bigcup_{i=1}^r \{\epsilon_{i,1}, \dots, \epsilon_{i,e_i}\}$ is an F-basis of V and

$$T \begin{bmatrix} \epsilon_{1,1} \\ \vdots \\ \epsilon_{1,e_1} \\ \vdots \\ \epsilon_{r,1} \\ \vdots \\ \epsilon_{r,e_r} \end{bmatrix} = \begin{bmatrix} M(d_1) && \\ & \ddots & \\ && M(d_r) \end{bmatrix} \begin{bmatrix} \epsilon_{1,1} \\ \vdots \\ \epsilon_{1,e_1} \\ \vdots \\ \epsilon_{r,1} \\ \vdots \\ \epsilon_{r,e_r} \end{bmatrix}.$$

Exercises

2.1. (Boolean ring) Let R be a ring such that $a^2 = a$ for all $a \in R$. Prove that R is commutative.

2.2. Let R be a ring. Let $a, b \in R$ such that $1 - ab$ is left invertible. Prove that $1 - ba$ is also left invertible. (Note. "left invertible" can be replaced with "right invertible" or "invertible".)

2.3. In the proof of Fact 2.21, show that $h \circ g = \mathrm{id}$ and $g \circ h = \mathrm{id}$.

2.4. Let p be a prime and $n \in \mathbb{N}$. Then $f(x) = \sum_{i=0}^{p-1} x^{ip^n} \in \mathbb{Q}[x]$ is irreducible.

2.5. (i) Let R be a commutative ring and $f \in R[x]$. Suppose that $\exists\, 0 \neq g \in R[x]$ such that $gf = 0$. prove that $\exists c \in R \setminus \{0\}$ such that $cf = 0$.
(ii) If R is not commutative, the conclusion in (i) is false.

2.6. Let D be a UFD and let F be the fractional field of D. Prove that $F^\times/D^\times$ is a free abelian group.

2.7. Let V be an infinite dimensional vector space over a field F and let $R = \mathrm{End}_F(V \oplus V)$. Clearly, $1_{V\oplus V}$ is a basis of ${}_RR$. Let $\epsilon : V \to V \oplus V$ be an isomorphism. Prove that $\epsilon\pi_1$, $\epsilon\pi_2$ is also a basis of ${}_RR$. ($\pi_i : V \oplus V \to V$ is the projection onto the ith component.) Hence R does not have IDP.

2.8. Let $A \subset B \subset C$ be R modules. If $C = A \oplus A'$ for some submodule A' of C, then $B = A \oplus (A' \cap B)$.

2.9. (Fitting) Let ${}_RA$ be an R-module which is both noetherian and artinian. Let $f \in \mathrm{End}_R(A)$ and define $\mathrm{im}\, f^\infty = \bigcap_{k=0}^\infty f^k(A)$, $\ker f^\infty = \bigcup_{k=0}^\infty \ker f^k$. Prove that

$$A = \mathrm{im}\, f^\infty \oplus \ker f^\infty.$$

Also show that $f|_{\mathrm{im}\, f^\infty} : \mathrm{im}\, f^\infty \to \mathrm{im}\, f^\infty$ is an automorphism and that $f|_{\ker f^\infty} : \ker f^\infty \to \ker f^\infty$ is nilpotent, i.e., $(f|_{\ker f^\infty})^n = 0$ for some $n > 0$.

2.10. (i) Let

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, dashed, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C'
\end{tikzcd}$$

be a commutative diagram of R-modules with exact rows. Prove that $\exists!$ R-map $\alpha : A \to A'$ such that the resulting diagram commutes.

(ii) Let

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, dashed, "\gamma"] & 0 \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

be a commutative diagram of R-modules with exact rows. Prove that $\exists!$ R-map $\gamma : C \to C'$ such that the resulting diagram commutes.

(iii) Let

$$\begin{tikzcd}
 & 0 \arrow[rr] & & A_3 \arrow[rr, "f_3"] \arrow[dd, dashed, "\alpha^3_4"] & & B_3 \arrow[rr, "g_3"] \arrow[dd, "\beta^3_4"] & & C_3 \arrow[dd, "\gamma^3_4"] \\
0 \arrow[rr] & & A_1 \arrow[rr, "f_1"] \arrow[ur, dashed, "\alpha^1_3"] \arrow[dd, dashed, "\alpha^1_2"'] & & B_1 \arrow[rr, "g_1"] \arrow[ur, "\beta^1_3"] \arrow[dd, "\beta^1_2"'] & & C_1 \arrow[ur, "\gamma^1_3"] \arrow[dd, "\gamma^1_2"'] & \\
 & 0 \arrow[rr] & & A_4 \arrow[rr, "f_4"] & & B_4 \arrow[rr, "g_4"] & & C_4 \\
0 \arrow[rr] & & A_2 \arrow[rr, "f_2"'] \arrow[ur, dashed, "\alpha^2_4"'] & & B_2 \arrow[rr, "g_2"'] \arrow[ur, "\beta^2_4"'] & & C_2 \arrow[ur, "\gamma^2_4"'] &
\end{tikzcd}$$

be a commutative diagram with exact rows. Then $\exists!$ R-maps $\alpha^1_2, \alpha^1_3, \alpha^2_4, \alpha^3_4$ such that the resulting diagram commutes. (Of course, there is a 3-D version of (ii).)

CHAPTER 3

Fields

3.1. Field Extensions

Degree of extension. Let $F \subset K$ be fields. $[K : F] := \dim_F K$ is called the *degree* of K over F. If $[K : F] < \infty$, K is called a *finite extension* over F.

Examples. $[\mathbb{C} : \mathbb{R}] = 2$; $[\mathbb{R} : \mathbb{Q}] = \aleph$. In general, if $F \subset K$ are fields such that $|K| = \infty$ and $|K| > |F|$, then $[K : F] = |K|$. Let X be a basis of K/F. Then $K \cong \bigoplus_{x\in X} F$. Clearly, $|X| = \infty$ and $|X| \le |K|$. Let $\mathcal{P}_0(X)$ be the set of all finite subsets of X. Then

$$\begin{aligned} |K| &= \Big|\bigoplus_{x\in X} F\Big| \le \sum_{Y\in\mathcal{P}_0(X)} |F|^{|Y|} \le |\mathcal{P}_0(X)| \max\{|F|, \aleph_0\} \\ &= |X| \max\{|F|, \aleph_0\} = \max\{|F|, |X|\}. \end{aligned}$$

Since $|K| > |F|$, we must have $|K| \le |X|$.

Fact. Let F be a field and let $f \in F[x]$ be irreducible with $\deg f = n$. Then $K = F[x]/(f)$ is an extension field of F with $[K : F] = n$. $x^0 + (f), \dots, x^{n-1} + (f)$ is a basis of K over F. $x + (f) \in K$ is a root of f.

Fact. Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$.

Proof. Let $\mathcal{A}$ be a basis of K/F and $\mathcal{B}$ a basis of L/K. Then the elements ab $(a \in \mathcal{A},\ b \in \mathcal{B})$ are all distinct and form a basis of L/F. □

Notation. Let $F \subset K$ be fields and $X \subset K$.

$F[X] :=$ the smallest subring $R \subset K$ such that $R \supset F$ and $R \supset X$,

$F(X) :=$ the smallest subfiled $E \subset K$ such that $E \supset F$ and $E \supset X$.

We have

$$\begin{aligned} &F[X] = \{f(u_1, \dots, u_n) : n \in \mathbb{N},\ f \in F[x_1, \dots, x_n],\ u_1, \dots, u_n \in X\}, \\ &F(X) = \Big\{\frac{u}{v} : u, v \in F[X],\ v \ne 0\Big\}. \end{aligned}$$

If E and F are both subfields of K, the *compositum* of E and F, denoted by EF, is the smallest subfield of K containing $E \cup F$.

Definition 3.1. Let $F \subset K$ be fields and $u \in K$. If $\exists 0 \ne f \in F[x]$ such that $f(u) = 0$, u is called *algebraic* over F. The monic polynomial $m \in F[x]$ of the smallest degree such that $m(x) = 0$ is called the *minimal polynomial* of u over F. If u is not algebraic over F, it is called *transcendental* over F. K is called an *algebraic extension* of F if every element of K is algebraic over F; otherwise, K is called *transcendental* over F.

Example. $\sqrt{2}+\sqrt[3]{3}\in\mathbb{R}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $(x^3+6x-3)^2-2(3x^2+2)^2$.

Proof. Let $\alpha=\sqrt{2}+\sqrt[3]{3}$. Then $3=(\alpha-\sqrt{2})^3=\alpha^3-3\sqrt{2}\alpha^2+6\alpha-2\sqrt{2}$. So, $\alpha^3+6\alpha-3=\sqrt{2}(3\alpha^2+2)$, $(\alpha^3+6\alpha-3)^2=2(3\alpha^2+2)^2$. On the other hand, it is obvious that $\sqrt{2},\sqrt[3]{3}\in\mathbb{Q}(\alpha)$ ($\sqrt{2}=\frac{\alpha^3+6\alpha-3}{3\alpha^2+2}$). So $6\mid[\mathbb{Q}(\alpha):\mathbb{Q}]$. □

Let $A=\{u\in\mathbb{C}: u \text{ is algebraic over } \mathbb{Q}\}$. Then $|A|=\aleph_0$ (since $|\mathbb{Q}[x]|=\aleph_0$). So, $|\mathbb{C}\setminus A|=\aleph$. Examples of transcendental numbers over $\mathbb{Q}$: e, π (difficult), $\sum_{n=1}^{\infty}\frac{1}{10^{n!}}$ (Liouville's number, Theorem 3.8).

Let F be a field. Then $x\in F(x)$ is transcendental over F. $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{-19})/\mathbb{Q}$ are algebraic extensions. $\mathbb{R}/\mathbb{Q}$, $F(x)/F$ are transcendental extensions. If $u\in F(x)\setminus F$, $F(x)/F(u)$ is algebraic. (Assume $u=f(x)/g(x)$, where $f,g\in F[x]$. Let $h(y)=g(y)-uf(y)\in(F(u))[y]$. Then $h\neq 0$ and $h(x)=0$.)

Basic facts. Let $F\subset K$ be fields.

(i) If $u\in K$ is transcendental over F, then $F(u)\cong F(x)$.

(ii) Let $u\in K$ be algebraic over F and $f\in F[x]$ monic. Then f is the minimal polynomial of u $\Leftrightarrow$ f is irreducible and $f(u)=0$. In this case, $F(u)=F[u]\cong F[x]/(f)$ and $[F(u):F]=\deg f$; $1,u,\dots,u^{\deg f-1}$ is a basis of $F(u)/F$.

(iii) $u\in K$ is algebraic over F $\Leftrightarrow$ $[F(u):F]<\infty$.

(iv) If $[K:F]<\infty$, K/F is algebraic. (The converse is false; cf. Example 3.3.)

Proposition 3.2 (Relative algebraic closure). *Let $F\subset K$ be fields and let*

$$A=\{u\in K: u \textit{ is algebraic over } F\}.$$

Then A is a subfield of K and is called the algebraic closure *of F in K.*

Example 3.3. Let A be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then $A/\mathbb{Q}$ is algebraic but $[A:\mathbb{Q}]=\infty$. Proof: Let p be a prime and n any positive integer. By Eisenstein's criterion, $x^n-p\in\mathbb{Q}[x]$ is irreducible. Thus $[A:\mathbb{Q}]\geq[\mathbb{Q}(p^{1/n}):\mathbb{Q}]=n$.

Proposition 3.4. *Let $F\subset K\subset L$ be fields such that K/F and L/K are both algebraic. Then L/K is algebraic.*

Proof. $\forall u\in L$, since u is algebraic over K, we have $u^n+b_{n-1}u^{n-1}+\cdots+b_0=0$ for some $b_0,\dots,b_{n-1}\in K$. Then

$$\begin{aligned}[F(u):F]&\leq[F(b_0,\dots,b_{n-1})(u):F]\\&=[F(b_0,\dots,b_{n-1})(u):F(b_0,\dots,b_{n-1})][F(b_0,\dots,b_{n-1}):F]<\infty.\end{aligned}$$

Hence u is algebraic over F. □

Ruler and compass constructions. On the complex $\mathbb{C}$ with 0 and 1 given, a point (complex number) is called *constructible* if it can be obtained through a sequence of steps; in each step, one uses a ruler and a compass to determine the intersection point(s) of two curves on $\mathbb{C}$ each of which is either a line through two points already constructed or a circle whose center and radius are already constructed.

Theorem 3.5.

(i) *$z\in\mathbb{C}$ is constructible $\Leftrightarrow$ $\exists$ fields $\mathbb{Q}=K_0\subset K_1\subset\cdots\subset K_n\subset\mathbb{C}$ such that $[K_j:K_{j-1}]=2$ and $z\in K_n$.*

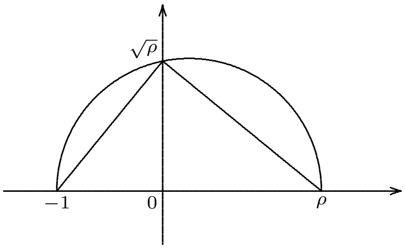


FIGURE 3.1. Construction of $\sqrt{\rho}$, $\rho \geq 0$

(ii) *The set of all constructible numbers in $\mathbb{C}$ is a field.*

PROOF. (i) ($\Rightarrow$) Consider a step in a ruler and compass construction. Let $K \subset \mathbb{C}$ be a subfield containing all numbers already constructed. The current step produces $a + bi$ where (a, b) is a common root of two polynomials in $K[x, y]$, each of which is of the form $cx + dy + e$ ($(c, d) \neq (0, 0)$) or the form $x^2 + y^2 + fx + gy + h$. It's easy to see that $[K(a) : K] = 1$ or 2 and $[K(b) : K] = 1$ or 2. So, $K \subset K(a) \subset K(a, b) \subset K(a, b, i) \ni a + bi$, where each extension is of degree 1 or 2. Therefore, each constructible number is contained in the last field of a tower of extensions $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$ with $[K_j : K_{j-1}] = 2$, $1 \leq j \leq n$.

($\Leftarrow$) Using induction on n, we only have to show that every element in K_j is constructible from K_{j-1}. Note that $K_j = K_{j-1}(\sqrt{d})$ for some $d \in K_{j-1}$. Let $d = \rho e^{i\theta}$ where $\rho \geq 0$. Then $\sqrt{d} = \sqrt{\rho} e^{i\theta/2}$. The angle $\theta/2$ is constrctible from θ. Also, $\sqrt{\rho}$ is constructible form ρ, see Figure 3.1. So $\sqrt{d}$ is constructible form d. Each element in $K_{j-1}(\sqrt{d})$ is of the form $a + b\sqrt{d}$ with $a, b \in K_{j-1}$. Clearly, $a + b\sqrt{d}$ is constructible from K_{j-1}.

(ii) Let $z, w \in \mathbb{C}$ ($w \neq 0$) be constructible. Try to show that $z - w$ and z/w are both constructible. The geometric proof of this is obvious. The algebraic proof is also easy. Let $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \ni z$ and $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_m \ni w$, where $[K_i : K_{i-1}] = 2$ and $[L_j : L_{j-1}] = 2$. Then

$$\mathbb{Q} \subset K_1 \subset \cdots \subset K_n \subset K_n L_1 \subset \cdots \subset K_n L_m \ni z,\ w,$$

where each extension is of degree 1 or 2. □

COROLLARY 3.6. *If $z \in \mathbb{C}$ is constructible, then $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of* 2.

THREE ANCIENT RULER-COMPASS PROBLEMS.

(i) *Squaring the circle* (constructing a square having the same area of a unit circle). Impossible since π is transcendental hence not constructible.

(ii) *Doubling the cube* (constructing a cube with volume 2). Impossible since $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$.

(iii) *Trisection of an arbitrary angle.* An angle of 60° cannot be trisected by rule and compass. Since $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, $\cos 20^\circ$ is a root of $8x^3 - 6x - 1$, which is irreducible in $\mathbb{Q}[x]$. So, $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$ and $\cos 20^\circ$ is not constructible.

THE PRIME FIELD. Let F be a field. The intersection of all subfields of F is called the *prime field* of F.

$$(\text{The prime field of } F) \cong \begin{cases} \mathbb{Q} & \text{if } \operatorname{char} F = 0, \\ \mathbb{Z}_p & \text{if } \operatorname{char} F = p. \end{cases}$$

Proof. Let P be the prime field of F. When $\operatorname{char} F = 0$, the isomorphism is $\mathbb{Q} \to P$, $\frac{m}{n} \mapsto \frac{m\cdot 1_F}{n\cdot 1_F}$; when $\operatorname{char} F = p$, the isomorphism is $\mathbb{Z}_p \to P$, $a + p\mathbb{Z} \mapsto a \cdot 1_F$. □

Transcendence of Liouville's number.

Theorem 3.7 (Liouville's inequality). *Let $\alpha \in \mathbb{C}$ be a root of a polynomial of degree d in $\mathbb{Z}[x]$. Then for each $\epsilon > 0$, there are only finitely many rational numbers $\frac{a}{b}$ $(a, b \in \mathbb{Z},\ b > 0)$ such that*

$$\left|\frac{a}{b} - \alpha\right| < \frac{1}{b^{d+\epsilon}}.$$

Proof. Assume that α is a root of $c_d x^d + \cdots + c_0 \in \mathbb{Z}[x]$. Let $\frac{a}{b} \in \mathbb{Q}$ such that $|\frac{a}{b} - \alpha| < \frac{1}{b^{d+\epsilon}}$ but $f(\frac{a}{b}) \neq 0$. Then

$$\left|f\Big(\frac{a}{b}\Big)\right| = \left|c_d\Big(\frac{a}{b}\Big)^d + \cdots + c_0\right| = \left|\frac{c_d a^d + c_{d-1}a^{d-1}b + \cdots + c_0 b^d}{b^d}\right| \geq \frac{1}{b^d}.$$

Write $f(x) = (x - \alpha)g(x)$, where $g(x) = e_{d-1}x^{d-1} + \cdots e_0$. Note that

$$\left|g\Big(\frac{a}{b}\Big)\right| \leq |e_{d-1}|\left|\frac{a}{b}\right|^{d-1} + \cdots + |e_0| \leq |e_{d-1}|(|\alpha| + 1)^{d-1} + \cdots + |e_0| =: C,$$

where C does not depend on $\frac{a}{b}$. Therefore,

$$\frac{1}{b^d} \leq \left|f\Big(\frac{a}{b}\Big)\right| = \left|\frac{a}{b} - \alpha\right|\left|g\Big(\frac{a}{b}\Big)\right| \leq \frac{C}{b^{d+\epsilon}},$$

i.e., $b^\epsilon \leq C$. There are only finitely many such b. For each such b, there are only finitely many $a \in \mathbb{Z}$ such that $|\frac{a}{b} - \alpha| < 1$. □

Theorem 3.8. *Liouville's number $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.*

Proof. For each $N \geq 1$, let $r_N = \sum_{n=1}^{N} \frac{1}{10^{n!}} = \frac{a_N}{10^{N!}} \in \mathbb{Q}$. Then for each $D > 0$,

$$|r_N - \alpha| = \sum_{n=N+1}^{\infty} \frac{1}{10^{n!}} \leq \frac{2}{10^{(N+1)!}} < \frac{1}{(10^{N!})^D},$$

where N is large enough. By Loiuville's inequality, α is transcendental. □

Remark. Let $u_n \in \{0, \ldots, 9\}$, $n \geq 1$, be a sequence with infinitely many nonzero terms. Then $\sum_{n=1}^{\infty} \frac{u_n}{10^{n!}}$ is transcendental; this is clear from the proof of the above theorem. So we have exhibited $\aleph$ transcendental numbers.

3.2. Galois Theory

The Galois group. Let $F \subset K$ be fields. $\operatorname{Aut}(K/F) := \{\sigma \in \operatorname{Aut}(K) : \sigma|_F = \mathrm{id}\}$ is called the *Galois group* of K over F.

Examples. $\operatorname{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \overline{(\ )}\}$.

$\operatorname{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$. Proof: Let $\sigma \in \operatorname{Aut}(\mathbb{R}/\mathbb{Q})$. If $a, b \in \mathbb{R}$ such that $a > b$, then $\sigma(a - b) = \sigma(\sqrt{a-b}^{\,2}) = \sigma(\sqrt{a-b})^2 > 0$; hence $\sigma(a) > \sigma(b)$. For each $x \in \mathbb{R}$, choose sequences $a_n, b_n \in \mathbb{Q}$ such that $a_n \nearrow x$ and $b_n \searrow x$, Then $a_n = \sigma(a_n) < \sigma(x) < \sigma(b_n) = b_n$ for all n. Hence $\sigma(x) = x$.

$|\operatorname{Aut}(\mathbb{C}/\mathbb{Q})| = \aleph!$. (Cf. Exercise **??**.)

Fact. Let $F \subset K$ be fields, $f \in F[x]$ and $\sigma \in \operatorname{Aut}(K/F)$. Then σ permutes the roots of f in K. It follows that if $[K : F] < \infty$, then $|\operatorname{Aut}(K/F)| < \infty$.

Subfields and subgroups. Let $F \subset K$ be fields and let

$$\mathcal{F}(K/F) = \text{the set of all fields between } F \text{ and } K,$$
$$\mathcal{G}(K/F) = \text{the set of all subgroups of } \mathrm{Aut}(K/F).$$

For $L \in \mathcal{F}(K/F)$ and $H \in \mathcal{G}(K/F)$, define

$$L' = \mathrm{Aut}(K/L) \in \mathcal{G}(K/F),$$
$$H' = \{x \in K : \sigma(x) = x \ \forall \sigma \in H\} \in \mathcal{F}(K/F).$$

Proposition 3.9.

(i) $K' = \{\mathrm{id}\}$, $F' = \mathrm{Aut}(K/F)$, $\{\mathrm{id}\}' = K$.

(ii) $L, M \in \mathcal{F}(K/F)$, $L \subset M \Rightarrow L' \supset M'$; $H, J \in \mathcal{G}(K/F)$, $H \subset J \Rightarrow H' \supset J'$.

(iii) *For* $L \in \mathcal{F}(K/F)$ *and* $H \in \mathcal{G}(K/F)$, $L \subset L''$, $H \subset H''$, $L''' = L'$, $H''' = H'$.

(iv) $H \in \mathcal{G}(K/F)$, $|H| < \infty \Rightarrow H'' = H$.

(v) *For* $L, M \in \mathcal{F}(K/F)$, $(LM)' = L' \cap M'$; *for* $H, J \in \mathcal{G}(K/F)$, $\langle H \cup J \rangle' = H' \cap J'$.

Proof. (iii) To show that $L''' = L'$, note that $L \subset L'' \Rightarrow L' \supset L'''$ and that $L' \subset (L')'' = L'''$.

(iv) See the second paragraph of the proof of the fundamental theorem of Galois theory.

(v) Obviously, $(LM)' \subset L' \cap M'$. Also, $(L' \cap M')' \supset L''M'' \supset LM$. So, $L' \cap M' \subset (L' \cap M')'' \subset (LM)'$. Hence $(LM)' = L' \cap M'$. □

Note. In (i), we do not always have $\mathrm{Aut}(K/F)' = F$. If this happens, K/F is called a Galois extension.

$$\begin{tikzcd}
K \arrow[rr, leftrightarrow, "(\ )'"] \arrow[d, dash] & & \{\mathrm{id}\} \arrow[d, dash] \\
\mathrm{Aut}(K/F)' \arrow[d, dash] & & \mathrm{Aut}(K/F) \arrow[ll, "(\ )'"'] \\
F \arrow[urr, "(\ )'"']
\end{tikzcd}$$

Definition 3.10 (Galois extension). Let $F \subset K$ be fields. K is called a *Galois extension* over F if $\{x \in K : \sigma(x) = x \ \forall \sigma \in \mathrm{Aut}(K/F)\} = F$. Equivalently, K/F is Galois iff $\forall x \in K \setminus F$, $\exists \sigma \in \mathrm{Aut}(K/F)$ such that $\sigma(x) \neq x$.

Example. $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois since $\mathrm{Aut}(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = \{\mathrm{id}\}$. $\mathbb{Q}(2^{1/3}, e^{2\pi i/3})/\mathbb{Q}$ is Galois. Let $\xi = e^{2\pi i/3}$. Then $\overline{(\ )} \in \mathrm{Aut}\big(\mathbb{Q}(2^{1/3}, \xi)/\mathbb{Q}(2^{1/3})\big)$. Also, $\exists \sigma \in \mathrm{Aut}\big(\mathbb{Q}(2^{1/3}, \xi)/\mathbb{Q}(\xi)\big)$ such that $\sigma(2^{1/3}) = 2^{1/3}\xi$. Every $x \in \mathbb{Q}(2^{1/3}, \xi)$ fixed by $\overline{(\ )}$ and σ must be in $\mathbb{Q}$.

The fundamental theorem of Galois theory. *Let* K/F *be a finite Galois extension. Then* $(\ )' : \mathcal{F}(K/F) \to \mathcal{G}(K/F)$ *and* $(\ )' : \mathcal{G}(K/F) \to \mathcal{F}(K/F)$ *are bijections and are inverses of each other. Moreover,*

(i) *if $L, M \in \mathcal{F}(K/F)$ and $L \subset M$, then $[M : L] = [L' : M']$; if $H, J \in \mathcal{G}(K/F)$ and $H \subset J$, then $[J : H] = [H' : J']$;*

(ii) *for $L, M \in \mathcal{F}(K/F)$, $(L \cap M)' = \langle L' \cup M' \rangle$; for $H, J \in \mathcal{G}(K/F)$, $(H \cap J)' = H'J'$;*

(iii) *for every $L \in \mathcal{F}(K/F)$, K/L is Galois; L/F is Galois $\Leftrightarrow L' \lhd F'$; when $L' \lhd F'$, $\mathrm{Aut}(L/F) \cong F'/L' = \mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$.*

$$\begin{tikzcd}
K \arrow[r, leftrightarrow, "(\ )'"] \arrow[d, dash] & \{\mathrm{id}\} \arrow[d, dash] \\
(\ ) \arrow[r, leftrightarrow] \arrow[d, dash] & (\ ) \arrow[d, dash] \\
(\ ) \arrow[r, leftrightarrow] \arrow[u, phantom, "\text{dgree} \quad = \quad \text{index}" near start, shift left=8ex] \arrow[d, dash] & (\ ) \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & \mathrm{Aut}(K/F)
\end{tikzcd}$$

$$\begin{tikzcd}
K \arrow[r, leftrightarrow, "(\ )'"] \arrow[d, dash, "\text{always Galois}"'] & \{\mathrm{id}\} \arrow[d, dash] \\
(\ ) \arrow[r, leftrightarrow] \arrow[d, dash, "\text{Galois} \quad \Leftrightarrow \quad \triangle"'] & (\ ) \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & \mathrm{Aut}(K/F)
\end{tikzcd}$$

Proof. The proof relies on two key lemmas (Lemmas 3.12 and 3.13) which will be proved afterwards.

Since K/F is Galois, $F'' = F$. For each $L \in \mathcal{F}(K/F)$, we have $L \subset L''$ and, by Lemmas 3.12 and 3.13, $[L'' : F] = [L'' : F''] \le [F' : L'] \le [L : F]$, So, $L'' = L$. For each $H \in \mathcal{G}(K/F)$, we have $H \subset H''$ and $[H'' : \{\mathrm{id}\}] = [H'' : \{\mathrm{id}\}''] \le [\{\mathrm{id}\}' : H'] \le [H : \{\mathrm{id}\}]$. So, $H'' = H$. (Note. In the proof of $H'' = H$, we only used the fact that $|H| < \infty$; the extension K/F could be arbitrary.)

(i) Since $[L' : M'] \le [M : L] = [M'' : L''] \le [L' : M']$, we have $[M : L] = [L' : M']$.

(ii) Obviously, $(L \cap M)' \supset L' \cup M'$. So, $(L \cap M)' \supset \langle L' \cup M' \rangle$. Also, $\langle L' \cup M' \rangle' \subset L'' \cap M'' = L \cap M$. So, $\langle L' \cup M' \rangle \supset (L \cap M)'$. Hence $(L \cap M)' = \langle L' \cup M' \rangle$.

(iii) K/L is Galois since $L'' = L$.

Now we prove that L/F is Galois $\Leftrightarrow L' \lhd F'$.

($\Rightarrow$) Let $\sigma \in L'$ and $\tau \in F'$. We want to show that $\tau^{-1}\sigma\tau \in L'$. It suffices to show that $\tau(L) \subset L$. Let $u \in L$ and let $f \in F[x]$ be the minimal polynomial of u over F. Let $u_1 (= u), u_2, \dots, u_r$ be all the distinct roots of f in L. Then $\forall \alpha \in \mathrm{Aut}(L/F)$, α permutes $u_1, \dots, u_r$; hence $\alpha((x - u_1) \cdots (x - u_r)) = (x - u_1) \cdots (x - u_r)$. Since L/F is Galois, $(x - u_1) \cdots (x - u_r) \in F[x]$. So, τ permutes the roots of $(x - u_1) \cdots (x - u_r)$. Therefore, $\tau(u) = \tau(u_1) = u_i \in L$ for some i.

($\Leftarrow$) For each $\tau \in F' = \mathrm{Aut}(K/F)$, we have $\tau(L) \subset L$. (For each $\sigma \in L'$, $\tau^{-1}\sigma\tau \in L'$. So, $\sigma\tau(v) = \tau(v)$ $\forall v \in L$. Hence $\tau(v) \in L$.) Thus $\tau|_L \in \mathrm{Aut}(L/F)$ (since we also have $\tau^{-1}(L) \subset L$).

Now assume that $u \in L \setminus F$. Since K/F is Galois, $\exists \tau \in \mathrm{Aut}(K/F)$ such that $\tau(u) \neq u$. Then $\tau|_L \in \mathrm{Aut}(L/F)$ and $\tau|_L(u) \neq u$. So, L/F is Galois.

Note that $\phi : F' \to \mathrm{Aut}(L/F)$, $\tau \mapsto \tau|_L$, is a homomorphism with $\ker\phi = L'$. Hence $F'/L' \hookrightarrow \mathrm{Aut}(L/F)$. Since $|F'/L'| = [L : F] = |\mathrm{Aut}(L/F)| < \infty$, $F'/L' \cong \mathrm{Aut}(L/F)$. □

Proposition 3.11 (Linear independence of characters). *Let G be a group and E a field. Let $\sigma_1,\dots,\sigma_n$ be distinct homomorphism from G to $E^\times$. Then $\sigma_1,\dots,\sigma_n$ are linearly independent over E as functions from G to E. (A homomorphism $\sigma : G \to E^\times$ is called an E-*character *of G.)*

Proof. Assume to the contrary that $\sigma_1,\dots,\sigma_n$ are linearly dependent. Choose a minimal linearly dependent subset of $\{\sigma_1,\dots,\sigma_n\}$, say, $\{\sigma_1,\dots,\sigma_m\}$. Then $\exists c_1,\dots,c_m \in E^\times$ such that $c_1\sigma_1 + \cdots + c_m\sigma_m = 0$, i.e.,

$$c_1\sigma_1(x) + \cdots + c_m\sigma_m(x) = 0 \qquad \text{for all } x \in G. \tag{3.1}$$

Clearly, $m \ge 2$. Choose $y \in G$ such that $\sigma_1(y) \ne \sigma_2(y)$. Replace x by yx in (3.1). We have

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_m\sigma_m(y)\sigma_m(x) = 0, \qquad x \in G. \tag{3.2}$$

$(3.1) - \sigma_1(y)^{-1} \cdot (3.2) \Rightarrow$

$$c_2\Bigl(1 - \frac{\sigma_2(y)}{\sigma_1(y)}\Bigr)\sigma_2(x) + \cdots + c_m\Bigl(1 - \frac{\sigma_m(y)}{\sigma_1(y)}\Bigr)\sigma_m(x), \qquad x \in G.$$

Then $\sigma_2,\dots,\sigma_m$ are linearly dependent, →←. □

Lemma 3.12. *Let $F \subset K$ be fields and $L, M \in \mathcal{F}(K/F)$, $L \subset M$. If $[M : L] < \infty$, then $[L' : M'] \le [M : L]$.*

Proof. Let $[M : L] = n$ and assume to the contrary that $[L' : M'] > n$. Let $\sigma_1,\dots,\sigma_{n+1} \in L'$ such that they represent distinct left cosets of M' in L'. Let $\epsilon_1,\dots,\epsilon_n$ be a basis of M/L. Then $\exists 0 \ne (c_1,\dots,c_{n+1}) \in K^{n+1}$ such that

$$\begin{bmatrix} \sigma_1(\epsilon_1) & \cdots & \sigma_{n+1}(\epsilon_1) \\ \vdots & & \vdots \\ \sigma_1(\epsilon_n) & \cdots & \sigma_{n+1}(\epsilon_n) \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_{n+1} \end{bmatrix} = 0.$$

For each $x \in M$, write

$$x = [a_1,\dots,a_n] \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix}, \qquad a_j \in L.$$

Then

$$\sigma_i(x) = [a_1,\dots,a_n] \begin{bmatrix} \sigma_i(\epsilon_1) \\ \vdots \\ \sigma_i(\epsilon_n) \end{bmatrix}, \qquad 1 \le i \le n+1.$$

So,

$$\begin{aligned} c_1\sigma_1(x)+\cdots+c_{n+1}\sigma_{n+1}(x) &= [\sigma_1(x),\dots,\sigma_{n+1}(x)]\begin{bmatrix} c_1\\ \vdots\\ c_{n+1}\end{bmatrix}\\ &= [a_1,\dots,a_n]\begin{bmatrix}\sigma_1(\epsilon_1) & \cdots & \sigma_{n+1}(\epsilon_1)\\ \vdots & & \vdots\\ \sigma_1(\epsilon_n) & \cdots & \sigma_{n+1}(\epsilon_n)\end{bmatrix}\begin{bmatrix} c_1\\ \vdots\\ c_{n+1}\end{bmatrix}\\ &= 0. \end{aligned}$$

Thus $\sigma_1|_M,\dots,\sigma_{n+1}|_M$ are linearly dependent over K.

Since $\sigma_1,\dots,\sigma_{n+1}$ belong to different left cosets of M' in L', $\sigma_1|_{M^\times},\dots,\sigma_{n+1}|_{M^\times}$ are distinct K-characters. By Proposition 3.11, $\sigma_1|_{M^\times},\dots,\sigma_{n+1}|_{M^\times}$ are linearly independent over K, →←. □

Lemma 3.13. *Let $F\subset K$ be fields and $H,J\in\mathcal{G}(K/F)$, $H\subset J$. If $[J:H]<\infty$, then $[H':J']\le[J:H]$.*

Proof. Let $[J:H]=n$ and let $\sigma_1(=\mathrm{id}),\dots,\sigma_n$ be a system of representatives of left cosets of H in J. Assume to the contrary that $[H':J']>n$. Let $\epsilon_1,\dots,\epsilon_{n+1}\in H'$ be linearly independent over J' and let

$$A=\begin{bmatrix}\sigma_1(\epsilon_1) & \cdots & \sigma_1(\epsilon_{n+1})\\ \vdots & & \vdots\\ \sigma_n(\epsilon_1) & \cdots & \sigma_n(\epsilon_{n+1})\end{bmatrix}\in M_{n\times(n+1)}(K).$$

Let $0\ne c\in K^{n+1}$ have the fewest nonzero components such that $Ac=0$. We may assume

$$c=\begin{bmatrix}1\\ c_2\\ \vdots\\ c_r\\ 0\\ \vdots\\ 0\end{bmatrix},\qquad c_i\ne 0.$$

The first equation in $Ac=0$ is $\epsilon_1+\epsilon_2c_2+\cdots+\epsilon_rc_r=0$. Hence, not all $c_2,\dots,c_r\in J'$. (Otherwise, $\epsilon_1,\dots,\epsilon_r$ would be linearly dependent over J'.) Say $c_2\notin J'$. Choose $\sigma\in J$ such that $\sigma(c_2)\ne c_2$. Apply σ to $Ac=0$. We have $\sigma(A)\sigma(c)=0$. Since $\sigma\sigma_1H,\dots,\sigma\sigma_nH$ is a permutation of $\sigma_1H,\dots,\sigma_nH$, $\sigma\sigma_1|_{H'},\dots,\sigma\sigma_n|_{H'}$ is a permutation of $\sigma_1|_{H'},\dots,\sigma_n|_{H'}$. (Here, note that $\alpha H=\beta H\Rightarrow\alpha^{-1}\beta\in H\subset H''\Rightarrow\alpha^{-1}\beta|_{H'}=\mathrm{id}\Rightarrow\alpha|_{H'}=\beta|_{H'}$.) So, $\sigma(A)=[\sigma\sigma_i(\epsilon_j)]$ is a row permutation of

A. Therefore, $\sigma(A)\sigma(c) = 0$ implies that $A\sigma(c) = 0$. Now, $A(c - \sigma(c)) = 0$, where

$$c - \sigma(c) = \begin{bmatrix} 0 \\ c_2 - \sigma(c_2) \\ \vdots \\ c_r - \sigma(c_r) \\ 0 \\ \vdots \\ 0 \end{bmatrix} \neq 0$$

has fewer nonzero components than c, →←. □

Note. Let K/F be a finite extension. Then $|\mathrm{Aut}(K/F)| \le [K : F]$. The equality holds ⇔ K/F is Galois.

Theorem 3.14 (Artin). *Let K be a field and $H < \mathrm{Aut}(K)$. Then K/H' is Galois. If $|H| < \infty$, then $\mathrm{Aut}(K/H') = H$.*

Proof. Since $H''' = H'$, K/H' is Galois. If $|H| < \infty$, by Proposition 3.9 (iv), $\mathrm{Aut}(K/H') = H'' = H$. □

3.3. Splitting Fields and Normal Extensions

Splitting fields. Let F be a field and $S \subset F[x] \setminus F$. An extension $K \supset F$ is called a *splitting field* of S over F if

(i) every $f \in S$ splits in K, i.e., every $f \in S$ is a product of linear polynomials in $K[x]$;
(ii) K is generated by F and the roots of all $f \in S$.

Namely, a splitting field of S over F is a smallest extension of F in which all $f \in S$ splits.

Algebraically closed fields. A field F is called *algebraically closed* if every $f \in F[x] \setminus F$ splits in F. The following statements are equivalent.

(i) F is algebraically closed.
(ii) Every $f \in F[x] \setminus F$ has a root in F.
(iii) The only algebraic extension of F is itself.

The fundamental theorem of algebra. *$\mathbb{C}$ is algebraically closed, i.e., every $f \in \mathbb{C}[x] \setminus \mathbb{C}$ has a root in $\mathbb{C}$.*

Proof. Assume to the contrary that $f(z) \neq 0$ for all $z \in \mathbb{C}$. Then $\frac{1}{f(z)}$ is a bounded entire function. By Liouville's theorem, $\frac{1}{f(z)}$ is a constant function, →←. □

Algebraic closure. Let F be a field. The following two conditions on an extension K/F are equivalent.

(i) K/F is algebraic and K is algebraically closed.
(ii) K is a splitting field of $F[x] \setminus F$ over F.

The field K in (i) and (ii) is called an *algebraic closure* of F.

Examples. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. If $F \subset K$ and K is algebraically closed, then the algebraic closure of F in K is an algebraic closure of F. The field of all algebraic numbers in $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$.

Theorem 3.15 (Existence of algebraic closure). *Every field F has an algebraic closure.*

Proof. For each $f \in F[x] \setminus F$, assign an indeterminate X_f. Let $\mathcal{X} = \{X_f : f \in F[x] \setminus F\}$ and consider the polynomial ring $F[\mathcal{X}]$. Let $I \subset F[\mathcal{X}]$ be the ideal generated by $f(X_f)$, $f \in F[x] \setminus F$. Then $1 \notin I$. (Otherwise, $\exists f_1, \dots, f_n \in F[x] \setminus F$, $g_1, \dots, g_n \in F[\mathcal{X}]$ such that

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1. \tag{3.3}$$

Let K/F be an extension such that each f_i $(1 \le i \le n)$ has a root $u_i \in K$. In (3.3), let $X_{f_i} = u_i$, $1 \le i \le n$, and $X_f = 0$ for $f \in (F[x] \setminus F) \setminus \{f_1, \dots, f_n\}$. Then $0 = 1$, $\rightarrow\leftarrow$.)

Let M be a maximal ideal of $F[\mathcal{X}]$ containing I and let $F_1 = F[\mathcal{X}]/M$. Then F_1 is an algebraic extension of F and every $f \in F[x] \setminus F$ has a root in F_1. By the same construction, there is an algebraic extension F_{i+1} of F_i such that every $f \in F_i[x] \setminus F_i$ has a root in F_i. Then $K = \bigcup_{i=1}^{\infty} F_i$ is an algebraic closure of F. □

An alternative proof. 1°. If K/F is algebraic, then $|K| \le \aleph_0 |F|$.

2° Choose a set $S \supset F$ such that $|S| > \aleph_0 |F|$. Let $\mathcal{A}$ be the class of all fields K such that $K \subset S$ and K is an algebraic extension of F. Then $\mathcal{A}$ is a *set*. For $K, L \in \mathcal{A}$, say $K \prec L$ if K is a subfield of L. Then $(\mathcal{A}, \prec)$ is a poset in which every chain has an upper bound (the union of the chain). By Zorn's lemma, $(\mathcal{A}, \prec)$ has a maximal element E. E is an algebraic closure of F. (Assume to the contrary that $\exists$ an algebraic extension E_1/E such that $E_1 \ne E$. Since E_1/F is algebraic, $|E_1| \le \aleph_0 |F| < |S|$. Thus $\exists$ a 1-1 map $f : E_1 \to S$ such that $f|_E = \text{id}$. Define $+$ and $\cdot$ in $f(E_1)$ by setting $f(a) + f(b) = f(a+b)$ and $f(a)f(b) = f(ab)$ for all $a, b \in E_1$. Then $f(E_1) \in \mathcal{A}$ and $E \precneqq f(E_1)$, $\rightarrow\leftarrow$.)

Note. We cannot simply consider the class of *all* algebraic extensions of F. It is too big to be a set. □

Corollary 3.16 (Existence of splitting field). *Let F be a field and $S \subset F[x] \setminus F$. The there is a splitting field of S over F.*

Proof. Let K be an algebraic closure of F and let R be the set of all roots in K of all polynomials in S. Then $F(R)$ is a splitting field of F. □

Theorem 3.17 (Uniqueness of splitting field). *Let F be a field and $S \subset F[x] \setminus F$. Then any two splitting fields of S over F are F-isomorphic. (An isomorphism between two extensions of F which is identity on F is called an* F-isomorphism*.) In particular, the algebraic closure of F is unique up to F-isomorphism.*

Proof. This follows from the next theorem. □

Theorem 3.18. *Let $\sigma : F_1 \to F_2$ be an isomorphism of fields and $S_1 \subset F_1[x] \setminus F_1$, $S_2 = \{\sigma f : f \in S_1\} \subset F_2[x] \setminus F_2$. Let K_1 be a splitting field of F_1 and K_2 a splitting field of F_2. Then σ can be extended to an isomorphism $K_1 \to K_2$.*

Proof. Let

$$\begin{aligned}\mathcal{A} = \{(L_1, L_2, \tau) : {}& L_i \text{ is a field between } F_i \text{ and } K_i \text{ and} \\ & \tau : L_1 \to L_2 \text{ is an isomorphism such that } \tau|_{F_1} = \sigma\}.\end{aligned}$$

For (L_1, L_2, τ), $(L_1', L_2', \tau') \in \mathcal{A}$, say $(L_1, L_2, \tau) \prec (L_1', L_2', \tau')$ if $L_1 \subset L_1'$, $L_2 \subset L_2'$ and $\tau'|_{L_1} = \tau$. By Zorn's lemma, $(\mathcal{A}, \prec)$ has a maximal element (E_1, E_2, α). It suffices to show that $E_1 = K_1$ and $E_2 = K_2$.

Assume to the contrary that $E_1 \neq K_1$ or $E_2 \neq K_2$, say $E_1 \neq K_1$. Then $\exists f \in S_1$ such that f does not split in E_1. Let $g \in E_1[x]$ be an irreducible factor of f with $\deg g \geq 2$ and let $u \in K_1 \setminus E_1$ be a root of g. Let $v \in K_2$ be a root of αg. ($\alpha g \in E_2[x]$ is the polynomial obtained by applying α to the coefficients of g.) By the next lemma, α can be extended to an isomorphism $\beta : E_1(u) \to E_2(v)$. Then $(E_1, E_2, \alpha) \precneqq (E_1(u), E_2(v), \beta)$, →←. □

Lemma 3.19. *Let $\sigma : F_1 \to F_2$ be an isomorphism of fields. Let K_i be an algebraic closure of F_i, $i = 1, 2$. Let $f \in F_1[x]$ be irreducible, $u \in K_1$ a root of f and $v \in K_2$ a root of σf. Then σ can be extended to an isomorphism $\tau : F_1(u) \to F_2(v)$ such that $\tau(u) = v$.*

Proof. f is the minimal polynomial of u over F_1 and σf is the minimal polynomial of v over F_2. Hence

$$\begin{array}{cccccc} \phi : & F_1(u) & \longrightarrow & F_2(v) & & \\ & g(u) & \longmapsto & (\sigma g)(v), & & g \in F_1[x] \end{array}$$

is a well defined isomorphism. □

Proposition 3.20. *Let $f \in F[x] \setminus F$ and let K be the splitting of f over F.*

(i) *If f is irreducible, the* Aut(K/F) *acts transitively on the roots of f.*

(ii) *If* Aut(K/F) *acts transitively on the roots of f and f has no multiple roots, then f is irreducible.*

Proof. (i) follows from Lemma 3.19.

(ii) Suppose to the contrary that $f = gh$, $g, h \in F[x] \setminus F$. Then g and h do not have common roots. Any $\sigma \in \mathrm{Aut}(K/F)$ maps a root of g to a root of g, not a root of h, →←. □

Proposition 3.21. *Let $f \in F[x] \setminus F$ and let K be the splitting field of f over F.*

(i) $[K : F] \mid (\deg f)!$.

(ii) *Let $f_1, \dots, f_k$ be the distinct irreducible factors of f. Then* $[K : F] \mid (\deg f_1)! \cdots (\deg f_k)!$.

Proof. (i) Induction on $\deg f$. If f is reducible, say $f = gh$, $g, h \in F[x] \setminus F$, let E be the splitting field of g over F. Then K is the splitting field of h over E. Thus $[K : F] = [K : E][E : F] \mid (\deg g)!(\deg h)! \mid (\deg f)!$. If f is irreducible, let $u \in K$ be a roots of f and write $f = (x - u)m$, $m \in (F(u))[x]$. Then $[F(u) : F] = \deg f$ and $[K : F(u)] \mid (\deg m)!$ since K is the splitting field of m over $F(u)$. So, $[K : F] \mid (\deg f)!$.

(ii) Let $E_0 = F$ and $E_i \subset K$ the splitting field of f_i over E_{i-1}. Then $E_k = K$ and by (i), $[E_i : E_{i-1}] \mid (\deg f_i)!$. □

Proposition 3.22 (Normal extension). *Let K/F be an algebraic extension. Then the following statements are equivalent.*

(i) *If $f \in F[x]$ is irreducible and has a root in K, then f splits in K.*
(ii) *K is a splitting field over F of some $S \subset F[x] \setminus F$.*
(iii) *Let $\bar{F}$ be an algebraic closure of F containing K. Then for every $\sigma \in \mathrm{Aut}(\bar{F}/F)$, $\sigma(K) = K$.*

The field K in (i) – (iii) *is called a* normal extension *of F.*

Proof. (i) ⇒ (ii). Let B be a basis of K/F. For each $b \in B$, let f_b be the minimal polynomial of b over F. Then K is the splitting field of $\{f_b : b \in B\}$ over F.

(ii) ⇒ (iii). Let X be the set of all roots of all $f \in S$. Then $K = F(X)$ and for each $\sigma \in \mathrm{Aut}(\bar{F}/F)$, $\sigma(X) = X$. So, $\sigma(K) = \sigma(F(X)) = F(\sigma(X)) = F(X) = K$.

(iii) ⇒ (i). By assumption, f has a root $u \in K$. Let $v \in \bar{F}$ be any root of f. Let $E \subset \bar{F}$ be the splitting field of f over F. By Proposition 3.20 (i), $\exists \tau \in \mathrm{Aut}(E/F)$ such that $\tau(u) = v$. By Theorem 3.18, τ can be extended to $\sigma \in \mathrm{Aut}(\bar{F}/F)$. Thus $v = \sigma(u) \in K$. So f splits in K. □

Proposition 3.23. *Let K/F be a normal extension. Then every F-isomorphism between two intermediate fields L_1 and L_2 ($F \subset L_i \subset K$) can be extended to an automorphism of K.*

Proof. K is a splitting field of some $S \subset F[x] \setminus F$. Thus K is also a splitting field of S over L_1 and over L_2. By Theorem 3.18, σ extends to some $\bar{\sigma} \in \mathrm{Aut}(K/F)$. □

The converse of Proposition 3.23 is false: $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not normal and has no proper intermediate subfields.

Separability. Let $f \in F[x]$ be irreducible. f is called *separable* if it has no multiple roots (in any extension of F). Note that f is separable iff $f' \neq 0$. Let K/F be an algebraic extension. $u \in K$ is called separable over F if its minimal polynomial over F is separable. K/F is called a *separable extension* if every $u \in K$ is separable over F.

Fact. If $\mathrm{char}\, F = 0$, every algebraic extension over F is separable.

Theorem 3.24 (Characterization of algebraic Galois extensions). *Let K/F be an algebraic extension. The following statements are equivalent.*

(i) *K/F is Galois.*
(ii) *K is a normal and separable extension over F.*
(iii) *K is a splitting field over F of a set of polynomials in $F[x]$ without multiple roots.*

Proof. (i) ⇒ (ii). For each $u \in K$, we want to show that the minimal polynomial f of u over F is separable and splits in K.

Let $\{u_1, \dots, u_n\}$ be the $\mathrm{Aut}(K/F)$-orbit of u. Let $g(x) = (x - u_1) \cdots (x - u_n)$. Then $\sigma g = g$ for all $\sigma \in \mathrm{Aut}(K/F)$; hence $g \in F[x]$. So, $f \mid g$. (In fact, $f = g$ since $\sigma(u)$ is a root of f for every $\sigma \in \mathrm{Aut}(K/F)$.) Thus f is separable and splits in K.

(ii) ⇒ (iii). Let B be a basis of K/F. For each $b \in B$, let $f_b \in F[x]$ be the minimal polynomial of b over F. Then f_b is separable and K is the splitting field of $\{f_b : b \in B\}$ over F.

(iii) $\Rightarrow$ (i). Let $S \subset F[x] \setminus F$ be a set of polynomials without multiple roots such that K is a splitting field of S over F.

1° Assume $[K : F] = n < \infty$. Use induction on n. The case $n = 1$ needs no proof. Assume $n > 1$. $\exists f \in S$ which does not split in F. Let $g \in F[x]$ be an irreducible factor of f with $\deg g = r \geq 2$. Let $u_1, \dots, u_r \in K$ be the roots of g. For each $1 \leq i \leq r$, $\exists$ F-isomorphism $\sigma_i : F(u_1) \to F(u_i)$ such that $\sigma(u_1) = u_i$. By Proposition 3.23, σ_i can be extended to an isomorphism $\tau_i \in \mathrm{Aut}(K/F)$. Clearly, $\tau_i^{-1}\tau_j \notin \mathrm{Aut}(K/F(u_1))$ for $i \neq j$. So, $\tau_1, \dots, \tau_r$ represent different left cosets of $\mathrm{Aut}(K/F(u_1))$ in $\mathrm{Aut}(K/F)$. Thus $[\mathrm{Aut}(K/F) : \mathrm{Aut}(K/F(u_1))] \geq r = [F(u_1) : F]$. Since $[K : F(u_1)] < n$, by the induction hypothesis, $K/F(u_1)$ is Galois. So,

$$\begin{aligned}|\mathrm{Aut}(K/F)| &= [\mathrm{Aut}(K/F) : \mathrm{Aut}(K/F(u_1))]|\mathrm{Aut}(K/F(u_1))| \\ &\geq [F(u_1) : F][K : F(u_1)] = [K : F].\end{aligned}$$

Hence K/F is Galois.

2° For each $T \subset S$, let $K_T \subset K$ be the splitting field of T over F. Then $K = \bigcup_{T \subset S,\, |T| < \infty} K_T$. $\forall u \in K \setminus F$, $\exists\, T \subset S$ with $|T| < \infty$ such that $u \in K_T$. Since $[K_T : F] < \infty$, by 1°, $\exists\, \sigma \in \mathrm{Aut}(K_T/F)$ such that $\sigma(u) \neq u$. Since K is the splitting field of S over K_T, by Theorem 3.18 (or Proposition 3.23), σ can be extended to an isomorphism $\tau \in \mathrm{Aut}(K/F)$. We have $\tau(u) \neq u$. So K/F is Galois. □

Theorem 3.25 (Normal closure). *Let K/F be an algebraic extension. Then there exists an extension L/K such that*

(i) *L is normal over F;*
(ii) *if $K \subset M \subset L$ such that M is normal over F, then $M = L$.*

If L_1 is another extension of K satisfying (i) *and* (ii)*, then L_1 is K-isomorphic to L. The field L is called a* normal closure *of K over F. Moreover,*

(iii) *if K/F is separable, then L/F is Galois;*
(iv) *if $[K : F] < \infty$, then $[L : F] < \infty$.*

$$\begin{tikzcd} L \arrow[d, dash] \\ K \arrow[d, dash] \\ F \end{tikzcd}$$

Proof. Let B be a basis of K over F. For each $b \in B$, let f_b be the minimal polynomial of b over F. Let L be a splitting field of $\{f_b : b \in B\}$ over K. Then (i) – (iv) are satisfied.

Assume L_1 is another extension of K satisfying (i) and (ii). Then L_1 is also a splitting field of $\{f_b : b \in B\}$ over K. By Theorem 3.17, L and L_1 are K-isomorphic. □

3.4. The Galois Group of a Polynomial

Let $f \in F[x]$ and K a splitting field of f over F. $\mathrm{Aut}(K/F)$ is called the *Galois group* of f over F. We also denote $\mathrm{Aut}(K/F)$ by $\mathrm{Aut}(f/F)$. Let $u_1, \dots, u_n \in K$ be the distinct roots of f. Then $\phi : \mathrm{Aut}(K/F) \to S_{\{u_1,\dots,u_n\}}$, $\sigma \mapsto \sigma|_{\{u_1,\dots,u_n\}}$ is an embedding. So, $\text{Aut}(K/F) \subset S_n$. If f is irreducible, $\text{Aut}(K/F)$ is a transitive subgroup of S_n.

THE DISCRIMINANT. Let $f \in F[x]$ be of the degree $n > 0$ and split as $f = a_0(x-u_1)\cdots(x-u_n)$ in a splitting field K of f. Then $\Delta := \prod_{i<j}(u_i - u_j) \in K$ and

$$D(f) := \Delta^2 = (-1)^{\frac{1}{2}n(n-1)} \prod_{i \neq j}(u_i - u_j) \in F.$$

Let $D = D(f)$. To see that $D \in F$, we may assume that $u_1, \dots, u_n$ are all distinct. For each $\sigma \in \text{Aut}(K/F)$, $\sigma(\Delta) = (\operatorname{sign}\sigma)\Delta$, so $\sigma(D) = D$. Since K/F is Galois, $D \in F$. $D(f)$ is called the *discriminant* of f.

PROPOSITION 3.26. *Let $f \in F[x]$ be a polynomial with no multiple roots and let K be the splitting field of f over F.*

(i) $\Delta := \sqrt{D(f)} \in K$ *and* $\text{Aut}(K/F) \cap A_n \subset \text{Aut}(K/F(\Delta))$.

(ii) *Assume* $\operatorname{char} F \neq 2$. *Then* $\text{Aut}(K/F) \cap A_n = \text{Aut}(K/F(\Delta))$. *In particular,* $\text{Aut}(K/F) \subset A_n \Leftrightarrow D(f)$ *is a square in* F *(*$\Leftrightarrow \Delta \in F$*).*

$$\begin{tikzcd}
 & K \arrow[r, leftrightarrow] \arrow[d, dash] & \{\text{id}\} \arrow[d, dash] \\
\text{Galois} & F(\Delta) \arrow[r, leftrightarrow] \arrow[d, dash] & F(\Delta)' = \text{Aut}(K/F) \cap A_n \arrow[d, dash] \\
 & F \arrow[r, leftrightarrow] & \text{Aut}(K/F)
\end{tikzcd}$$

PROOF. (i) If $\sigma \in \text{Aut}(K/F) \cap A_n$, then $\sigma(\Delta) = \Delta$, so $\sigma \in \text{Aut}(K/F(\Delta))$.

(ii) $\forall \sigma \in \text{Aut}(K/F)$, we have $\sigma(\Delta) = \text{sign}(\sigma)\Delta$. Thus $\sigma \in K(\Delta)' \Leftrightarrow \sigma(\Delta) = \Delta \Leftrightarrow \text{sign}(\sigma) = 1 \Leftrightarrow \sigma \in \text{Aut}(K/F) \cap A_n$. (Note. Since $\operatorname{char} F \neq 2$, $1 \neq -1$.) □

NOTE. Proposition 3.26 (ii) is false if $\operatorname{char} F = 2$. Example: $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible. Let K be the splitting field of f over $\mathbb{Z}_2$ and let $\alpha \in K$ be a root of f. The α^2 is also a root of f and $\alpha^2 \neq \alpha$. We have $\Delta = \alpha - \alpha^2 = 1$ ($\because \alpha^2 + \alpha + 1 = 0$). So, $\text{Aut}(K/F(\Delta)) = \text{Aut}(K/F) = S_2 \neq \text{Aut}(K/F) \cap A_2$.

THE RESULTANT. Let $\boldsymbol{a} = (a_0, \dots, a_n) \in F^{n+1}$ and $\boldsymbol{b} = (b_0, \dots, b_m) \in F^{m+1}$, where $m + n > 0$. Define

$$R(\boldsymbol{a},\boldsymbol{b}) = \left|\begin{array}{ccccccccc}
a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & & \\
 & a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & a_0 & a_1 & \cdot & \cdot & \cdot & a_n \\
b_0 & b_1 & \cdot & \cdot & b_m & & & & \\
 & b_0 & b_1 & \cdot & \cdot & b_m & & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & & b_0 & b_1 & \cdot & \cdot & b_m
\end{array}\right|
\begin{array}{l}
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \\
\left.\vphantom{\begin{array}{c}b\\b\\b\\b\\b\end{array}}\right\} n
\end{array}. \tag{3.4}$$

If $f = a_0x^n + a_1x^{n-1} + \cdots + a_0$, $g = b_0x^m + b_1x^{m-1} + \cdots + b_m$, where $m + n > 0$ and $a_0, b_0 \neq 0$, then $R(\boldsymbol{a}, \boldsymbol{b})$ is called the *resultant* of f and g and is denoted by $R(f, g)$.

Proposition 3.27. $\gcd(f, g) \neq 1 \Leftrightarrow R(f, g) = 0$.

Proof. ($\Rightarrow$) Let u be a common zero of f and g (in some extension of F). Then

$$\begin{bmatrix} a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & & \\ & a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ & & & a_0 & a_1 & \cdot & \cdot & \cdot & a_n \\ b_0 & b_1 & \cdot & \cdot & b_m & & & & \\ & b_0 & b_1 & \cdot & \cdot & b_m & & & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ & & & \cdot & \cdot & \cdot & \cdot & \cdot & \\ & & & & b_0 & b_1 & \cdot & \cdot & b_m \end{bmatrix} \begin{bmatrix} u^{m+n-1} \\ \vdots \\ u \\ 1 \end{bmatrix} = 0.$$

($\Leftarrow$) $\exists\, 0 \neq (\alpha_0, \dots, \alpha_{m-1}, \beta_0, \dots, \beta_{n-1}) \in F^{m+n}$ such that

$$(\alpha_0, \dots, \alpha_{m-1}, \beta_0, \dots, \beta_{n-1}) \begin{bmatrix} a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & & \\ & a_0 & a_1 & \cdot & \cdot & \cdot & a_n & & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ & & & a_0 & a_1 & \cdot & \cdot & \cdot & a_n \\ b_0 & b_1 & \cdot & \cdot & b_m & & & & \\ & b_0 & b_1 & \cdot & \cdot & b_m & & & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & & \\ & & & \cdot & \cdot & \cdot & \cdot & \cdot & \\ & & & & b_0 & b_1 & \cdot & \cdot & b_m \end{bmatrix} = 0. \tag{3.5}$$

Let $\alpha = \alpha_0x^{m-1} + \alpha_1x^{m-2} + \cdots + \alpha_{m-1}$ and $\beta = \beta_0x^{n-1} + \beta_1x^{n-2} + \cdots + \beta_{n-1}$. Then α, β are not both 0 and $\deg \alpha < m$, $\deg \beta < n$. Moreover, (3.5) is equivalent to $\alpha f + \beta g = 0$. So $(f, g) \neq 1$. □

Proposition 3.28. *Let $x_1, \dots, x_n, y_1, \dots, y_m, X$ be independent indeterminates. In $\big(F(x_1, \dots, x_n, y_1, \dots, y_n)\big)[X]$, write*

$$(X - x_1) \cdots (X - x_n) = X^n + a_1X^{n-1} + \cdots + a_n,$$
$$(X - y_1) \cdots (X - y_m) = X^m + b_1X^{m-1} + \cdots + b_m,$$

i.e., $a_i = (-1)^i s_{n,i}(x_1, \dots, x_n)$, $b_j = (-1)^j s_{m,j}(y_1, \dots, y_m)$, where $s_{n,i}$ is the ith elementary symmetric polynomial in n indeterminates. Let $\boldsymbol{a} = (1, a_1, \dots, a_n)$ and $\boldsymbol{b} = (1, b_1, \dots, b_m)$. Then

$$R(\boldsymbol{a}, \boldsymbol{b}) = \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j). \tag{3.6}$$

Proof. When $x_i = y_j$, by Proposition 3.27, $R(\boldsymbol{a}, \boldsymbol{b}) = 0$. So, in $F[x_1, \dots, x_n, y_1, \dots, y_m]$, $x_i - y_j \mid R(\boldsymbol{a}, \boldsymbol{b})$. Thus, the right side of (3.6) divides $R(\boldsymbol{a}, \boldsymbol{b})$. Note that

$$\deg_{(x_1,\dots,x_n)} R(\boldsymbol{a},\boldsymbol{b}) = m\deg_{(x_1,\dots,x_n)} a_n = mn.$$

So we must have $R(\boldsymbol{a},\boldsymbol{b}) = c\prod_{i=1}^n\prod_{j=1}^m(x_i-y_j)$ for some $c\in F[y_1,\dots,y_m]$. Compare the coefficients of $(x_1\cdots x_n)^m$ at both sides. We have $c=1$. □

Corollary 3.29. *Let $f,g\in F[x]\setminus F$. Suppose f and g split (in a splitting field of fg) as*

$$\begin{aligned} f &= a_0(x-u_1)\cdots(x-u_n), && a_0\in F^\times,\\ g &= b_0(x-v_1)\cdots(x-v_m), && b_0\in F^\times. \end{aligned}$$

Then

$$R(f,g) = a_0^m b_0^n \prod_{i=1}^n\prod_{j=1}^m(u_i-v_j). \tag{3.7}$$

Proof. In Proposition 3.28, let $x_i=u_i$, $y_j=v_j$. □

Note. (3.7) can be written as

$$R(f,g) = a_0^m\prod_{i=1}^n g(u_i) = (-1)^{mn}b_0^n\prod_{j=1}^m f(v_j). \tag{3.8}$$

These formulas can be generalized as follows.

Corollary 3.30. *Let f and g be as in Corollary 3.29 and write $f=a_0x^n+\cdots+a_n$, $g=b_0x^m+\cdots+b_m$. Let $h=c_0x^k+\cdots+c_k\in F[x]$, $k>0$. (Note that we do not assume that $c_0\neq 0$.) Put $\boldsymbol{a}=(a_0,\dots,a_n)$, $\boldsymbol{b}=(b_0,\dots,b_m)$, $\boldsymbol{c}=(c_0,\dots,c_k)$. Then*

$$R(\boldsymbol{a},\boldsymbol{c}) = a_0^k\prod_{i=1}^n h(u_i), \tag{3.9}$$

$$R(\boldsymbol{c},\boldsymbol{b}) = (-1)^{mk}b_0^k\prod_{j=1}^m h(v_j). \tag{3.10}$$

Proof. Assume $c_0=0$. (Otherwise, use (3.8).) Clearly,

$$R(\boldsymbol{a},\boldsymbol{c}) = a_0R\big(\boldsymbol{a},\,(c_1,\dots,c_k)\big), \tag{3.11}$$

$$R(\boldsymbol{c},\boldsymbol{b}) = (-1)^m b_0R\big((c_1,\dots,c_k),\,\boldsymbol{b}\big). \tag{3.12}$$

Use (3.11) and (3.12) repeatedly until $c_i\neq 0$. Then use (3.8). □

Theorem 3.31. *Let $f=a_0x^n+a_1x^{n-1}+\cdots+a_n\in F[x]$, $n\geq 2$, $a_0\neq 0$. Then*

$$D(f) = (-1)^{\frac12 n(n-1)}a_0^{-2n+1}R(\boldsymbol{a},\boldsymbol{a}'),$$

where $\boldsymbol{a}=(a_0,\dots,a_n)$ and $\boldsymbol{a}'=(na_0,(n-1)a_1,\dots,a_{n-1})$.

Proof. Write $f=a_0(x-u_1)\cdots(x-u_n)$. Then by Corollary 3.30,

$$R(\boldsymbol{a},\boldsymbol{a}') = a_0^{n-1}\prod_{i=1}^n f'(u_i) = a_0^{2n-1}\prod_{i=1}^n\prod_{j\neq i}(u_i-u_j) = a_0^{2n-1}(-1)^{\frac12 n(n-1)}D(f).$$

□

Example. $f = x^2 + bx + c \Rightarrow D(f) = b^2 - 4c$.
$f = x^3+bx^2+cx+d \Rightarrow D(f) = b^2c^2-4c^3-4b^3d-27d^2+18bcd$. If $\operatorname{char} F \neq 3$, $f = y^3 + qy + r$, where $y = x + \frac{b}{3}$. Hence $D(f) = -4q^3 - 27r^2$.

Galois groups of separable irreducible polynomials of degree ≤ 4.

If $f \in F[x]$ is a separable irreducible quadratic, clearly, $\operatorname{Aut}(f/F) \cong \mathbb{Z}_2$.

Proposition 3.32. *Let $f \in F[x]$ be a separable irreducible cubic.*

(i) *If* $\operatorname{char} F \neq 2$,

$$\operatorname{Aut}(f/F) = \begin{cases} A_3 & \text{if } D(f) \in F^2, \\ S_3 & \text{if } D(f) \notin F^2, \end{cases}$$

where $F^2 = \{a^2 : a \in F\}$.

(ii) *If* $\operatorname{char} F = 2$, *we may assume $f = x^3 + ax + b$. Then*

$$\operatorname{Aut}(f/F) = \begin{cases} A_3 & \text{if } y^2 + by + a^3 + b^2 \text{ has a root in } F, \\ S_3 & \text{otherwise.} \end{cases}$$

Proof. Since $\operatorname{Aut}(f/F)$ is a transitive subgroup of S_3, we have $\operatorname{Aut}(f/F) = S_3$ or A_3.

(i) follows from Proposition 3.26 (ii).

(ii) Let K be a splitting field of f over F and let $u_1, u_2, u_3 \in K$ be the roots of f. Put $G = \operatorname{Aut}(K/F)$. Let

$$\begin{cases} \alpha = u_1u_2^2 + u_2u_3^2 + u_3u_1^2, \\ \beta = u_1u_3^2 + u_3u_2^2 + u_2u_1^2. \end{cases}$$

Then $\alpha \neq \beta$ and every $\sigma \in G$ permutes α, β. Moreover, σ fixes α and β iff $\sigma \in A_3$. So, $F(\alpha,\beta)' = G \cap A_3$. Let $r(y) = (y-\alpha)(y-\beta) \in K[y]$. Since $r(y)$ is fixed by G, we have $r(y) \in F[x]$. In fact, direct computation shows that

$$r(y) = y^2 + by + a^3 + b^2.$$

So, $r(y)$ has a root in $F \Leftrightarrow F(\alpha,\beta) = F \Leftrightarrow G \cap A_3 = G \Leftrightarrow G = A_3$. □

$$\begin{tikzcd}
K \arrow[r, leftrightarrow] \arrow[d, dash] & \{\mathrm{id}\} \arrow[d, dash] \\
F(\alpha,\beta) \arrow[r, leftrightarrow] \arrow[d, dash] & G \cap A_3 \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

Lemma 3.33. *Let $f \in F[x]$ with* $\deg f = 4$ *such that f has 4 distinct roots $u_1, \dots, u_4$ in a splitting field K of f over F. Let*

$$\alpha = u_1u_2 + u_3u_4, \qquad \beta = u_1u_3 + u_2u_4, \qquad \gamma = u_1u_4 + u_2u_3.$$

(Note that α, β, γ are distinct.)

(i) $\mathrm{Aut}(K/F(\alpha,\beta,\gamma)) = \mathrm{Aut}(K/F)\cap V$, *where*

$$V = \{(1),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}.$$

(ii) *Assume* $f = x^4 + bx^3 + cx^2 + dx + e$. *Then*

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 - cx^2 + (bd-4e)x - b^2e + 4ce - d^2 \in F[x].$$

This polynomial is called the resolvant cubic *of* f.

Proof. (i) $\forall\,\sigma \in \mathrm{Aut}(K/F)\cap V$, clearly, σ fixes α,β,γ. So, $\sigma\in\mathrm{Aut}(K/F(\alpha,\beta,\gamma))$. It remains to show that $\mathrm{Aut}(K/F(\alpha,\beta,\gamma))\subset V$. Let $\sigma\in\mathrm{Aut}(K/F(\alpha,\beta,\gamma))$. There exists $\phi\in V$ such that $\phi\sigma(u_1)=u_1$. We claim that $\phi\sigma=\mathrm{id}$. (Then $\sigma=\phi^{-1}\in V$.) Assume to the contrary that $\phi\sigma\neq\mathrm{id}$. Without loss of generality, $\phi\sigma(u_2)=u_3$. Then $u_1u_2+u_3u_4=\alpha=\phi\sigma(\alpha)=u_1u_3+u_2u_4$. Then $(u_1-u_4)(u_2-u_3)=0$, $\rightarrow\leftarrow$.

(ii) The coefficients of $(x-\alpha)(x-\beta)(x-\gamma)$ are symmetric functions of α,β,γ, hence symmetric functions of $u_1,\dots,u_4$; hence polynomials in b,c,d,e. The actual computation of the coefficients of $(x-\alpha)(x-\beta)(x-\gamma)$ is tedious but straightforward. □

Proposition 3.34. *Let* $f = x^4+bx^3+cx^2+dx+e\in F[x]$ *be irreducible and separable and let* $g\in F[x]$ *be the cubic resolvant of* f. *Let* E *be a splitting filed of* g *over* F *and let* $m=[E:F]=|\mathrm{Aut}(g/F)|$.

(i) *If* $m=6$, *then* $\mathrm{Aut}(f/F)=S_4$.
(ii) *If* $m=3$, *then* $\mathrm{Aut}(f/F)=A_4$.
(iii) *If* $m=1$, *then* $\mathrm{Aut}(f/F)=V$.
(iv) *If* $m=2$, *then*

$$\mathrm{Aut}(f/F)\cong\begin{cases} D_4 & \text{if } f \text{ is irreducible over } E,\\ \mathbb{Z}_4 & \text{if } f \text{ is reducible over } E.\end{cases}$$

Proof. Let $K\supset E$ be a splitting field of f over F. Put $G=\mathrm{Aut}(F/F)$. By Lemma 3.33 (i), $[G:G\cap V]=[E:F]=m$. Since G is a transitive subgroup of S_4, we have $4\,\big|\,|G|$; hence $|G|=4,8,12,24$. More precisely, $G=S_4,A_4,D_4,V$ or $G\cong\mathbb{Z}_4$.

$$\begin{tikzcd}
K \arrow[d, dash] & \{\mathrm{id}\} \arrow[d, dash] \\
E \arrow[r, leftrightarrow] \arrow[d, dash] & G\cap V \arrow[d, dash] \\
F & G
\end{tikzcd}$$

(i) and (ii). Since $3\,\big|\,|G|$, $|G|=12$ or 24. So, $G=A_4$ or S_4. Thus $m=[G:G\cap V]=|G|/4$. So, $G=S_4$ when $m=6$; $G=A_4$ when $m=3$.

(iii) Since $G\subset V$, we have $G=V$.

(iv) Since $[G:G\cap V]=2$, we have $G=D_4$ or $G\cong\mathbb{Z}_4$. Moreover, f is irreducible over E $\Leftrightarrow$ $\mathrm{Aut}(f/E)$ $(=G\cap V)$ acts transitively on the roots of f $\Leftrightarrow$ $G\cap V=V\Leftrightarrow G=D_4$. □

The inverse Galois problem. Can every finite group G be realized as the Galois group of some finite Galois extension $K/\mathbb{Q}$? The answer is not known. The answer is affirmative for many families of finite groups.

- S_n (Proposition 3.36), A_n;
- finite solvable groups (Safarevich [**20**]);
- many finite simple groups ([**15**]).

Realization of S_n as a Galois group over $\mathbb{Q}$.

Proposition 3.35. *Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Let p be a prime and let $\bar{f} = x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0 \in \mathbb{Z}_p[x]$ be the reduction of f. Assume that $\bar{f}$ has n distinct roots $v_1, \dots, v_n$ in a splitting field $\bar{K}$ of $\bar{f}$ over $\mathbb{Z}_p$. Then f has n distinct roots $u_1, \dots, u_n$ in a splitting field K of f over $\mathbb{Q}$. Moreover, if $u_1, \dots, u_n$ are ordered suitably and $S_{\{u_1,\dots,u_n\}}$ is identified with $S_{\{v_1,\dots,v_n\}}$ in the obvious way, then* $\mathrm{Aut}(\bar{K}/\mathbb{Z}_p) \subset \mathrm{Aut}(K/\mathbb{Q})$.

$$\begin{tikzcd}
S_{\{v_1,\dots,v_n\}} \arrow[r, "\cong"] & S_{\{u_1,\dots,u_n\}} \\
\mathrm{Aut}(\bar{K}/\mathbb{Z}_p) \arrow[u, hook] \arrow[r, hook] & \mathrm{Aut}(K/\mathbb{Q}) \arrow[u, hook]
\end{tikzcd}$$

Proof. The reduction from $\mathbb{Z}$ to $\mathbb{Z}_p$ is denoted by $\overline{(\ )}$.

1° Since $(\bar{f}, \bar{f}') = 1$ in $\mathbb{Z}_p[x]$, we have $(f, f') = 1$ in $\mathbb{Q}[x]$. So f has n distinct roots in K.

2° Let

$$g(x) = \prod_{\sigma \in S_n} \Bigl(x - \sum_i u_{\sigma(i)} y_i\Bigr) \in K[y_1, \dots, y_n][x],$$

$$\mathfrak{g}(x) = \prod_{\sigma \in S_n} \Bigl(x - \sum_i v_{\sigma(i)} y_i\Bigr) \in \bar{K}[y_1, \dots, y_n][x].$$

Then $g(x) \in \mathbb{Z}[y_1, \dots, y_n][x]$. In fact, $\forall \tau \in S_n$, $\tau g = g$. So, each coefficient of $g(x, y_1, \dots, y_n)$ is a symmetric polynomial in $u_1, \dots, u_n$ with coefficients in $\mathbb{Z}$. Thus each coefficient of $g(x, y_1, \dots, y_n)$ is a polynomial over $\mathbb{Z}$ in the coefficients of f, i.e.,

$$g(x, y_1, \dots, y_n) = \sum_{i_0 + \cdots + i_n = n!} c_{i_0,\dots,i_n}(a_0, \dots, a_{n-1}) x^{i_0} y_1^{i_1} \cdots y_n^{i_n}, \tag{3.13}$$

where $c_{i_0,\dots,i_n} \in \mathbb{Z}[X_0, \dots, X_{n-1}]$. By the same argument,

$$\mathfrak{g}(x, y_1, \dots, y_n) = \sum_{i_0 + \cdots + i_n = n!} c_{i_0,\dots,i_n}(\overline{a_0}, \dots, \overline{a_{n-1}}) x^{i_0} y_1^{i_1} \cdots y_n^{i_n} \in \mathbb{Z}_p[y_1, \dots, y_n][x]. \tag{3.14}$$

By (3.13) and (3.14),

$$\bar{g}(x, y_1, \dots, y_n) = \mathfrak{g}(x, y_1, \dots, y_n). \tag{3.15}$$

3° Put $G = \mathrm{Aut}(K/\mathbb{Q})$ and $\bar{G} = \mathrm{Aut}(\bar{K}/\mathbb{Z}_p)$. For each $\sigma \in S_n$, let

$$g_\sigma(x) = \prod_{\tau \in G} \Bigl(x - \sum_i u_{\tau\sigma(i)} y_i\Bigr),$$

$$\mathfrak{g}_\sigma(x) = \prod_{\tau \in \bar{G}} \Bigl(x - \sum_i v_{\tau\sigma(i)} y_i\Bigr)$$

For each $\tau \in G$, we have $\tau(g_\sigma) = g_\sigma$, so $g_\sigma \in \mathbb{Q}[y_1,\dots,y_n][x]$. Since $g_\sigma \mid g$ in $\mathbb{Q}(y_1,\dots,y_n)[x]$, where $g_\sigma \in \mathbb{Q}(y_1,\dots,y_n)[x]$ and $g \in \mathbb{Z}[y_1,\dots,y_n][x]$ are both monic and $\mathbb{Q}(y_1,\dots,y_n)$ is the fractional field of the UFD $\mathbb{Z}[y_1,\dots,y_n]$, we have $g_\sigma \in \mathbb{Z}[y_1,\dots,y_n][x]$. In the same way, $\mathfrak{g}_\sigma \in \mathbb{Z}_p[y_1,\dots,y_n][x]$.

We claim that for each $\sigma \in S_n$, $\mathfrak{g}_\sigma$ is the irreducible factor of $\mathfrak{g}$ in $\mathbb{Z}_p(y_1,\dots,y_n)[x]$ divisible by $x - \sum_i v_{\sigma(i)} y_i$.

Proof of this claim. Let $\mathfrak{h}(x)$ be the (monic) irreducible factor of $\mathfrak{g}(x)$ in $\mathbb{Z}_p(y_1,\dots,y_n)[x]$ divisible by $x - \sum_i v_{\sigma(i)} y_i$. Then $\forall \tau \in \bar{G}$, $x - \sum_i v_{\tau\sigma(i)} y_i = \tau(x - \sum_i v_{\sigma(i)} y_i)$ divides $\mathfrak{h}$. So $\mathfrak{g}_\sigma(x) \mid \mathfrak{h}(x)$. Thus $\mathfrak{h} = \mathfrak{g}_\sigma$.

In fact, g_σ is also the irreducible factor of g in $\mathbb{Q}(y_1,\dots,y_n)[x]$ divisible by $x - \sum_i u_{\sigma(i)} y_i$. However, we do not need this.

4° We have $g = g_{\sigma_1} \cdots g_{\sigma_k}$, where σ_1 (= id)$,\dots,\sigma_k$ are representatives of the right cosets of G in S_n. By (3.15), $\mathfrak{g}_{\mathrm{id}} \mid \mathfrak{g} = \bar{g} = \bar{g}_{\sigma_1} \cdots \bar{g}_{\sigma_k}$, so $\mathfrak{g}_{\mathrm{id}} \mid \bar{g}_{\sigma_i}$ for some i. By relabeling u_i, we may assume $\mathfrak{g}_{\mathrm{id}} \mid \bar{g}_{\sigma_1} = \bar{g}_{\mathrm{id}}$.

$\forall \sigma \in \bar{G}$, we have

$$\begin{aligned}\mathfrak{g}_{\mathrm{id}}(x, y_1, \dots, y_n) &= \prod_{\tau \in \bar{G}} \Bigl(x - \sum_i v_{\tau\sigma(i)} y_i\Bigr) = \prod_{\tau \in \bar{G}} \Bigl(x - \sum_i v_{\tau(i)} y_{\sigma^{-1}(i)}\Bigr) \\ &= \mathfrak{g}_{\mathrm{id}}(x, y_{\sigma^{-1}(1)}, \dots, y_{\sigma^{-1}(n)}),\end{aligned}$$

which divides $\bar{g}_{\mathrm{id}}(x, y_{\sigma^{-1}(1)}, \dots, y_{\sigma^{-1}(n)}) = \bar{g}_\sigma(x, y_1, \dots, y_n)$. So $\mathfrak{g}_{\mathrm{id}} \mid \gcd(\bar{g}_\sigma, \bar{g}_{\mathrm{id}})$ in $\mathbb{Z}_p(y_1,\dots,y_n)[x]$. Thus $\gcd(\bar{g}_\sigma, \bar{g}_{\mathrm{id}}) \neq 1$. Write $G\sigma = G\sigma_i$ for some $1 \le i \le k$. Then $g_\sigma = g_{\sigma_i}$. So $\gcd(\bar{g}_{\sigma_i}, \bar{g}_{\mathrm{id}}) \neq 1$. Since $\mathfrak{g} = \bar{g}_{\sigma_1} \cdots \bar{g}_{\sigma_k}$ has no multiple roots, we must have $\sigma_i = \mathrm{id}$, i.e., $\sigma \in G$. So we have proved that $\bar{G} \subset G$. □

PROPOSITION 3.36. *Let $n > 3$. Let $f_1, f_2, f_3 \in \mathbb{Z}[x]$ be monic polynomials of degree n such that*

(i) *$\bar{f} \in \mathbb{Z}_2[x]$ is irreducible;*
(ii) *in $\mathbb{Z}_3[x]$, $\bar{f}_2 = gh$, where g is irreducible of degree $n-1$ and h is linear;*
(iii) *in $\mathbb{Z}_5[x]$,*

$$\bar{f}_3 = \begin{cases} kl & \text{if } n \text{ is odd}, \\ kl_1l_2 & \text{if } n \text{ is even}, \end{cases}$$

where k is irreducible of degree 2, l, l_1, l_2 are irreducible of odd degree and $(l_1, l_2) = 1$.

Let $f = -15f_1 + 10f_2 + 6f_3 \in \mathbb{Z}[x]$. Then the Galois group of f over $\mathbb{Q}$ is S_n.

PROOF. Let $G = \mathrm{Aut}(f/\mathbb{Q})$. Note that $f \equiv f_1 \pmod 2$, $f \equiv f_2 \pmod 3$, and $f \equiv f_3 \pmod 5$. Since $\mathrm{Aut}(\bar{f}_1/\mathbb{Z}_2) \subset G$, G contains an n-cycle α. Since $\mathrm{Aut}(\bar{f}_2/\mathbb{Z}_3) \subset G$, G contains an $(n-1)$-cycle β. Since $\mathrm{Aut}(\bar{f}_3/\mathbb{Z}_5) \subset G$, G contains an element of the form $\tau\sigma$, where τ is a transposition, $o(\sigma)$ is odd and $\tau\sigma = \sigma\tau$. It follows that $\tau \in G$. Therefore $G \supset \langle \alpha, \beta, \tau \rangle = S_n$. □

3.5. Finite Fields

EXISTENCE AND UNIQUENESS. Let F be a field with $|F| < \infty$. Define a ring homomorphism

$$\begin{aligned} f:\ \mathbb{Z} &\longrightarrow F \\ n &\longmapsto n1_F \end{aligned}$$

where 1_F is the identity of F. By the first isomorphism theorem, we have an embedding $\mathbb{Z}/\ker f \hookrightarrow F$. Thus $\mathbb{Z}/\ker f$ is an integral domain. Therefore, $\ker f$ is a prime ideal of $\mathbb{Z}$, i.e., $\ker f = p\mathbb{Z}$ for some prime p. Since the field $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ is embedded in F, we may simply assume that F contains $\mathbb{Z}_p$ as a subfield. Clearly, F is a vector space over $\mathbb{Z}_p$. Since F is finite, $[F : \mathbb{Z}_p] = \dim_{\mathbb{Z}_p} F < \infty$. Let $n = [F : \mathbb{Z}_p]$. Then $F \cong \mathbb{Z}_p^n$ as a $\mathbb{Z}_p$-vector space. In particular, $|F| = p^n$.

Conversely, given a prime p and an integer $n > 0$, up to isomorphism, there exists a unique field F with $|F| = p^n$.

THEOREM 3.37. *Let p be a prime and n a positive integer. The splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$ has precisely p^n elements.*

PROOF. Let $f = x^{p^n} - x$ and F the splitting field of f over $\mathbb{Z}_p$. Note that $(f', f) = (-1, f) = 1$. Thus, f has p^n distinct roots in F. Let

$$E = \{a \in F : f(a) = 0\}.$$

We will show that $F = E$. It suffices to show that E is a field. (Then f splits in E. Since F is the smallest field in which f splits, we must have $F = E$.)

In fact,

$$\begin{array}{cccc} \phi: & F & \longrightarrow & F \\ & a & \longmapsto & a^{p^n} \end{array}$$

is an automorphism of F. E is the fixed field of ϕ in F. Hence, E is a field. □

THEOREM 3.38. *Given a prime p and an integer $n > 0$, all finite fields of order p^n are isomorphic.*

PROOF. Let F be a finite field with $|F| = p^n$. As seen at the beginning of this section, $\mathbb{Z}_p \subset F$. Since $F \setminus \{0\}$ is a multiplicative group of order $p^n - 1$, we have $a^{p^n - 1} = 1$ for all $a \in F \setminus \{0\}$. Thus,

$$a^{p^n} = a \quad \text{for all } a \in F.$$

Namely, all elements of F are roots of $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Therefore, F is a splitting field of f over $\mathbb{Z}_p$.

Since all splitting fields of f over $\mathbb{Z}_p$ are isomorphic, the conclusion of the theorem follows. □

We denote the finite field with p^n elements by $\mathbb{F}_{p^n}$. Thus, $\mathbb{F}_p = \mathbb{Z}_p$. We have an $\mathbb{F}_p$-vector space isomorphism (not a ring isomorphism) $\mathbb{F}_{p^n} \cong \mathbb{F}_p^n$.

THE MULTIPLICATIVE GROUP OF $\mathbb{F}_{p^n}$.

THEOREM 3.39. *$\mathbb{F}_{p^n}^\times$ is cyclic. A generator of $\mathbb{F}_{p^n}^\times$ is called a* primitive element *of $\mathbb{F}_{p^n}$.*

PROOF. This follows from the next proposition. □

PROPOSITION 3.40. *Let F be any field and G a finite subgroup of the multiplicative group of F. Then G is cyclic.*

PROOF. Assume to the contrary that G is not cyclic. By the fundamental theorem of finite abelian groups, $G \cong G_1 \times G_2$, where $|G_1| = m$, $|G_2| = n$ and $(m, n) > 1$. Let $k = \operatorname{lcm}(m, n)$. Then $k < mn = |G|$ and

$$x^k = 1 \quad \text{for all } x \in G.$$

However, $x^k - 1$ cannot have more than k roots in F. We have a contradiction. □

Corollary 3.41. *Let p be a prime and $n > 0$ an integer. Then there exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n.*

Proof. Let $\alpha \in \mathbb{F}_{p^n}$ be a primitive element. Clearly, $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Let $f \in \mathbb{F}_p[x]$ be the minimal polynomial of α over $\mathbb{F}_p$. Then f is irreducible and $\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. □

Representation of elements of $\mathbb{F}_{p^n}$.

- Let $f \in \mathbb{F}_p[x]$ be irreducible of degree n. Then $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f)$. So each element in $\mathbb{F}_{p^n}$ is uniquely of the form
$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + (f), \qquad c_i \in \mathbb{F}_p;$$
this element is usually denoted by $(c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_p^n$. See Table 3.1 for the multiplication table of $\mathbb{F}_{2^3} = \mathbb{F}_2[x]/(x^3 + x + 1)$.
- Let α be a primitive element of $\mathbb{F}_{p^n}$. Then $\mathbb{F}_{p^n} = \{0, 1, \alpha, \dots, \alpha^{p^n-2}\}$. Representing elements of $\mathbb{F}_{p^n}$ this way is convenient for multiplication but not for addition.

Table 3.1. Multiplication Table of $\mathbb{F}_{2^3} = \mathbb{F}_2[x]/(x^3 + x + 1)$

·	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	011	001	111	101
011	000	011	110	101	111	100	001	010
100	000	100	011	111	110	010	101	001
101	000	101	001	100	010	111	011	110
110	000	110	111	001	101	011	010	100
111	000	111	101	010	001	110	100	011

Lattice of finite fields.

Theorem 3.42. *Let p be a prime and let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$.*

(i) *For each integer $n > 0$, $\overline{\mathbb{F}}_p$ has a unique subfield of order p^n.*

(ii) *Let $\mathbb{F}_{p^m} \subset \overline{\mathbb{F}}_p$ and $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$. Then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m \mid n$. In general,*

$$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{(m,n)}}, \tag{3.16}$$

$$\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^{[m,n]}}, \tag{3.17}$$

where $\mathbb{F}_{p^m}\mathbb{F}_{p^n}$ is the subfield of $\overline{\mathbb{F}}_p$ generated $\mathbb{F}_{p^m} \cup \mathbb{F}_{p^n}$, $(m,n) = \gcd(m,n)$ and $[m,n] = \operatorname{lcm}(m,n)$.

Note. We already know that a finite field of order p^n is unique up to isomorphism. However, Theorem 3.42 (i) states that in a given algebraic closure of $\mathbb{F}_p$, a finite field of order p^n is not only unique up to isomorphism, but also unique as a set.

Proof of Theorem 3.42. (i) By the proof of Theorem 3.38, a subfield of $\overline{\mathbb{F}}_p$ of order p^n must be $\{a \in \overline{\mathbb{F}}_p : a^{p^n} = a\}$.

(ii) If $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is an $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$-dimensional vector space over $\mathbb{F}_{p^m}$. Hence,

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]} = p^{m[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]}.$$

Thus $n = m[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$.

If $m \mid n$, then

$$\begin{aligned} x^{p^n} - x &= x(x^{p^n-1} - 1) = x\Big(x^{\frac{p^n-1}{p^m-1}(p^m-1)} - 1\Big) \\ &= x(x^{p^m-1} - 1)\sum_{i=0}^{\frac{p^n-1}{p^m-1}-1} x^{(p^m-1)i} = (x^{p^m} - x)\sum_{i=0}^{\frac{p^n-1}{p^m-1}-1} x^{(p^m-1)i}. \end{aligned}$$

Therefore, in $\overline{\mathbb{F}}_p$, the splitting field of $x^{p^m} - x$ is contained in the splitting field of $x^{p^n} - x$, i.e., $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.

To prove (3.16), first observe that $\mathbb{F}_{p^{(m,n)}} \subset \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$. Let $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^s}$. Since $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^m}$ and $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^n}$, from the above, $s \mid m$ and $s \mid n$; hence $s \mid (m, n)$. Therefore, $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^s} \subset \mathbb{F}_{p^{(m,n)}}$. Equation (3.17) is proved in the same way. □

Proposition 3.43. *Let $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, where $m \mid n$. If α is a primitive element of $\mathbb{F}_{p^n}$, then $\alpha^{\frac{p^n-1}{p^m-1}}$ is a primitive element of $\mathbb{F}_{p^m}$.*

Proof. Since $o(\alpha) = p^n - 1$, $o(\alpha^{\frac{p^n-1}{p^m-1}}) = p^m - 1$. Since $\mathbb{F}_{p^n}^{\times}$ is cyclic, $\mathbb{F}_{p^m}^{\times}$ is the only subgroup of $\mathbb{F}_{p^n}^{\times}$ of order $p^m - 1$. Thus, $\mathbb{F}_{p^m}^{\times} = \langle \alpha^{\frac{p^n-1}{p^m-1}} \rangle$. □

The automorphism group. Define a map

$$\begin{aligned} \sigma : \ \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ a &\longmapsto a^p. \end{aligned}$$

Clearly, $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. σ is called the *Frobenius map* of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.

Theorem 3.44. *The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$. More generally, if $m \mid n$, then the extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \sigma^m \rangle$.*

Proof. Since $x^{p^n} - x \in \mathbb{F}_p[x]$ has no multiple roots and since $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$. Thus, $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Since $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, to prove that $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$, it suffices to show that $o(\sigma) = n$, or, equivalently, $o(\sigma) \geq n$. Since $\sigma^{o(\sigma)} = \mathrm{id}$, we have

$$0 = \sigma^{o(\sigma)}(a) - a = a^{p^{o(\sigma)}} - a \quad \text{for all } a \in \mathbb{F}_{p^n}. \tag{3.18}$$

The polynomial $x^{p^{o(\sigma)}} - x$, being of degree $p^{o(\sigma)}$, has at most $p^{o(\sigma)}$ roots in $\mathbb{F}_{p^n}$. Thus, (3.18) implies that $p^n \leq p^{o(\sigma)}$, i.e., $n \leq o(\sigma)$.

If $m \mid n$, then $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, so is $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$. Moreover, $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is a subgroup of $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of order $\frac{n}{m}$. Since $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$ is cyclic, its only subgroup of order $\frac{n}{m}$ is $\langle \sigma^m \rangle$. Thus, $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \sigma^m \rangle$. □

Note. The automorphism $\sigma^m \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \sigma^m \rangle$ is defined by $\sigma^m(a) = a^{p^m}$, $a \in \mathbb{F}_{p^n}$, and is called the *Frobenius map* of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$.

3.6. Separability

Definition 3.45. Let K/F be an extension of fields and let $u \in K$ be algebraic over F. u is called *purely inseparable* over F is the minimal polynomial of u over F is $(x-u)^n$ for some $n > 0$. K/F is called a *purely inseparable extension* if every $u \in K$ is purely inseparable over F.

Example. Let $\operatorname{char} F = p$. Consider fields $F(x) \supset F(x^p)$. The minimal polynomial of x over $F(x^p)$ is $f(y) = y^p - x^p \in [F(x^p)][y]$. Since $f(y) = (y-x)^p$, x is purely inseparable over $F(x^p)$.

Fact. If u is both separable and purely inseparable over F, then $u \in F$.

Proposition 3.46. *Let K/F be an extension with* $\operatorname{char} F = p > 0$ *and let $u \in K$ be algebraic over F. Then u^{p^n} is separable over F for some $n \geq 0$.*

Proof. Let $f = a_0 + a_1 x + \cdots$ be the minimal polynomial of u over F. Use induction on $\deg f$.

Assume u is not separable over F. Then $0 = f' = a_1 + 2a_2 x + 3a_3 x^2 + \cdots$. It follows that $a_i = 0$ whenever $p \nmid i$. So $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p)$, where $g \in F[x]$ with $\deg g = \frac{1}{p} \deg f < \deg f$. Since $g(u^p) = 0$, by the induction hypothesis, $(u^p)^{p^m}$ is separable over F for some $m \geq 0$. Note that $(u^p)^{p^m} = u^{p^{m+1}}$. □

Proposition 3.47. *Let K/F be an extension with* $\operatorname{char} F = p > 0$ *and let $u \in K$ be algebraic over F. Then the following statements are equivalent.*

(i) *u is purely inseparable over F.*
(ii) *$u^{p^n} \in F$ for some $n \geq 0$.*
(iii) *The minimal polynomial of u over F is of the form $x^{p^n} - a$.*

Proof. (i) ⇒ (iii). Let $f = (x-u)^m \in F[x]$ be the minimal polynomial of u over F. Write $m = kp^n$, where $(k,p) = 1$. Then

$$f = (x^{p^n} - u^{p^n})^k = (x^{p^n})^k - ku^{p^n}(x^{p^n})^{k-1} + \cdots \in F[x].$$

So, $ku^{p^n} \in F$, hence $u^{p^n} \in F$. Thus $x^{p^n} - u^{p^n}$ belongs $F[x]$ and divides f. It follows that $f = x^{p^n} - u^{p^n}$.

(iii) ⇒ (ii). We have $u^{p^n} = a \in F$.

(ii) ⇒ (i). Let f be the minimal polynomial of u over F. $\exists\, n \geq 0$ such that $f \mid x^{p^n} - u^{p^n} = (x-u)^{p^n}$. So, $f = (x-u)^m$ for some $1 \leq m \leq p^n$. Thus u is purely inseparable over F. □

Corollary 3.48. *Let K/F be a finite purely inseparable extension, where* $\operatorname{char} F = p > 0$. *Then $[K : F]$ is a power of p.*

Proof. Use induction on $[K : F]$. Assume $[K : F] > 1$. Choose $u \in K \setminus F$. By Proposition 3.47 (iii), $[F(u) : F] = p^n$. Since $K/F(u)$ is purely inseparable and $[K : F(u)] < [K : F]$, by the induction hypothesis, $[K : F(u)]$ is a power of p. So $[K : F]$ is a power of p. □

Proposition 3.49. *Let K/F be an algebraic extension where* $\operatorname{char} F = p > 0$. *Then the following statements are equivalent.*

(i) *K is purely inseparable over F.*
(ii) *If $u \in K$ is separable over F, then $u \in F$.*

(iii) *K is generated over F by a set of purely inseparable elements over F.*

Proof. (i) $\Rightarrow$ (ii). Obvious.

(ii) $\Rightarrow$ (i). Let $u \in K$. By Proposition 3.46, u^{p^n} is separable over F for some $n \geq 0$. By (ii), $u^{p^n} \in F$. By Proposition 3.47, u is purely inseparable over F.

(i) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (i). Assume $K = F(X)$, where $X \subset K$ is a set of purely inseparable elements over F. Let $P = \{u \in K : u \text{ is purely inseparable over } F\}$. By Proposition 3.47,

$$P = \{u \in K : u^{p^n} \in F \text{ for some } n \geq 0\}. \tag{3.19}$$

It is clear from (3.19) that P is a subfield of K. Since $P \supset F$ and $P \supset X$, we have $P \supset F(X) = K$. □

Proposition 3.50. *Let K/F be an extension and let $X \subset K$ be a set of separable elements over F. Then $F(X)/F$ is separable.*

Proof. $\forall u \in X$, let $f_u \in F[x]$ be the minimal polynomial of u over F. Then f_u is separable. Let $L \supset F(X)$ be a splitting field of $\{f_u : u \in X\}$ over F. By Theorem 3.24, L/F is Galois hence separable. So $F(X)/F$ is separable. □

Theorem 3.51. *Let K/F be an algebraic extension. Let*

$$S = \{u \in K : u \text{ is separable over } F\},$$
$$P = \{u \in K : u \text{ is purely inseparable over } F\}.$$

(i) *S and P are subfields of K. S is separable over F; P is purely inseparable over F.*
(ii) *K is purely inseparable over S.*
(iii) *$P \cap S = F$.*
(iv) *K is separable over $P \Leftrightarrow K = SP$.*
(v) *If K is normal over F, then S/F and K/P are Galois and* $\mathrm{Aut}(S/F) \cong \mathrm{Aut}(K/P) = \mathrm{Aut}(K/F)$.

$$\begin{tikzcd}
& K \arrow[dl, dash, "\text{in}"'] \arrow[dr, dash, "?"] & \\
S \arrow[dr, dash, "\text{sep}"'] & & P \arrow[dl, dash, "\text{in}"] \\
& F &
\end{tikzcd}$$

Proof. Assume $\operatorname{char} F = p > 0$ since if $\operatorname{char} F = 0$, all the conclusions are obvious.

(i) By Propositions 3.50 and 3.49, S and P are subfields of K.

(ii) $\forall u \in K$, by Proposition 3.46, $\exists n \geq 0$ such that u^{p^n} is separable over F, i.e., $u^{p^n} \in S$. By Proposition 3.47, u is separable over S.

(iii) Obvious.

(iv) ($\Rightarrow$) K is both separable and purely inseparable over SP. Thus $K = SP$.

($\Leftarrow$) Every $u \in S$ is separable over F hence separable over P. So, $K = P(S)$ is separable over P.

(v) 1° $\mathrm{Aut}(K/F) = \mathrm{Aut}(K/P)$.

Let $\sigma \in \text{Aut}(K/F)$ and $u \in P$. Let $f = (x-u)^m$ be the minimal polynomial of u over F. Then $\sigma(u)$ is also a root of f. So, $\sigma(u) = u$. Thus $\sigma \in \text{Aut}(K/P)$.

2° K/P is Galois.

Let $u \in K \setminus P$. Let f be the minimal polynomial of u over F. Since u is not purely inseparable over F, f has a root $v \in K$ such that $v \neq u$. $\exists\, F$-isomorphism $\tau : F(u) \to F(v)$ such that $\tau(u) = v$. By Proposition 3.23, τ extends to some $\sigma \in \text{Aut}(K/F) = \text{Aut}(K/P)$. We have $\sigma(u) = v \neq u$. So K/P is Galois.

3° $\text{Aut}(S/F) \cong \text{Aut}(K/F)$.

$\forall \sigma \in \text{Aut}(K/F)$, clearly, $\sigma(S) = S$. So $\sigma|_S \in \text{Aut}(S/F)$. The group homomorphism

$$\begin{array}{rccc} \theta: & \text{Aut}(K/F) & \longrightarrow & \text{Aut}(S/F) \\ & \sigma & \longmapsto & \sigma|_S \end{array}$$

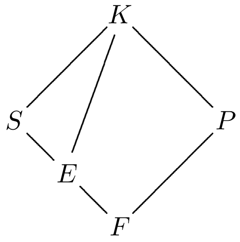
is onto. (Since K/F is normal, every $\tau \in \text{Aut}(S/F)$ extends to some $\sigma \in \text{Aut}(K/F)$.) θ is also 1-1. Assume $\sigma \in \ker\theta$. Then $\sigma|_S = \text{id}$. By 1°, $\sigma|_P = \text{id}$. Thus $\sigma|_{SP} = \text{id}$. However, by 2°, K/P is separable. By (iv), $SP = K$. So $\sigma = \text{id}$.

4° S/F is Galois.

$\forall u \in S \setminus F$, we have $u \in K \setminus P$ ($\because S \cap P = F$). By 2°, $\exists \sigma \in \text{Aut}(K/P)$ such that $\sigma(u) \neq u$. We have $\sigma|_S \in \text{Aut}(S/F)$ and $\sigma|_S(u) \neq u$. □

Corollary 3.52. *Let $F \subset E \subset K$ be fields such that both E/F and K/E are separable. Then K/F is separable.*

Proof. Let $S = \{u \in K : u \text{ is separable over } F\}$. Since K is separable over E, K is separable over S. By Theorem 3.51 (ii), K is purely inseparable over S. So $K = S$. □



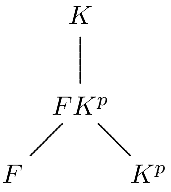
Corollary 3.53. *Let K/F be an algebraic extension with* $\text{char}\, F = p > 0$.

(i) *If K/F is separable, then $K = FK^p$, where $K^p = \{a^p : a \in K\}$.*

(ii) *If $K = FK^p$ and $[K : F] < \infty$, then K/F is separable.*

(iii) *$u \in K$ is separable over $F \Leftrightarrow F(u^p) = F(u)$.*

Proof. (i) Since K is separable over F, K is separable over FK^p. Since K is purely inseparable over K^p, K is purely inseparable over FK^p. Thus $K = FK^p$.



(ii) We have $K = FK^{p^n}$ for all $n \geq 1$. (See the remark below.) Since $[K : F] < \infty$, we can write $K = F(u_1, \dots, u_m)$ for some $u_1, \dots, u_m \in K$. $\exists n > 0$ such that $u_i^{p^n}$ is separable over F for all $1 \le i \le m$. Thus $K^{p^n} = F^{p^n}(u_1^{p^n}, \dots, u_n^{p^n})$ is separable over F. So $K = FK^{p^n}$ is separable over F.

(iii) In fact,

$$\begin{aligned} u \text{ is separable over } F &\Leftrightarrow F(u)/F \text{ is separable} \\ &\Leftrightarrow F(u) = F(F(u)^p) = F(u^p) \qquad \text{(by (i) and (ii)).} \end{aligned}$$

□

Remark. Let K/F be an extension with $\operatorname{char} F = p > 0$.

- $K = FK^{p^n}$ for *some* $n \ge 1 \Leftrightarrow K = FK^{p^n}$ for *all* $n \ge 1$.
- Let $u \in K$. Then $F(u^{p^n}) = F(u)$ for *some* $n \ge 1 \Leftrightarrow F(u^{p^n}) = F(u)$ for *all* $n \ge 1$.

Proof. Assume $K = FK^{p^n}$ for some $n \ge 1$. Then $K = FK^{p^n} \subset FK^p$. So $K = FK^p$. It follows that $K = F(FK^p)^p = F(F^pK^{p^2}) = FK^{p^2}$, etc. For the second claim, let $L = F(u)$. Then $FL^{p^n} = F(u^{p^n})$. □

Simple extensions. An extension K/F is called *simple* if $K = F(a)$ for some $a \in K$.

Theorem 3.54. *Let K/F be an algebraic extension. Then K/F is a simple extension if and only if there are only finitely many intermediate fields between F and K.*

Proof. ($\Leftarrow$) Let $u \in K$ such that $F(u)$ is a maximal simple extension of F in K. Assume to the contrary that $F(u) \ne K$. Choose $v \in K \setminus F(u)$. If $|F| < \infty$, then $|F(u, v)| < \infty$. So $F(u, v)$ is a simple extension over F, which is a contradiction. So assume $|F| = \infty$. Among the intermediate fields $F(u + av)$, $a \in F$, at least two are equal, say $F(u + a_1v) = F(u + a_2v)$, where $a_1, a_2 \in F$, $a_1 \ne a_2$. Then $F(u, v) = F(u + a_1v)$ which is a simple extension over F, $\rightarrow\leftarrow$.

($\Rightarrow$) Let $K = F(u)$ and let $f(x) \in F[x]$ be the minimal polynomial of u over F. For any intermediate field B between F and $F(u)$, let $f_B(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0 \in B[x]$ be the minimal polynomial of u over B. We claim that

$$B = F(b_0, \dots, b_{n-1}).$$

Clearly, $B \supset F(b_0, \dots, b_{n-1})$. Let $B' = F(b_0, \dots, b_{n-1})$. Since B' and B are between F and $F(u)$, we have $B'(u) = B(u) = F(u)$. Note that

$$\begin{aligned} [F(u) : B] = [B(u) : B] &= \deg f_B \\ &= [B'(u) : B'] \quad \text{(since } f_B \text{ is also the minimal polynomial of } B'\text{)} \\ &= [F(u) : B']. \end{aligned}$$

It follows that $B = B'$.

Therefore, B is determined by f_B. f_B is a monic minimal factor of $f(x)$. $f(x)$ has only finitely many monic factors. Thus there are only finitely many intermediate fields B between F and $F(u)$.

□

Corollary 3.55. *Every finite separable extension is a simple extension.*

Proof. Let K/F be a finite separable extension. Let L be the normal closure of K over F. Then L is a finite Galois extension over F. So there are only finitely many fields between F and L. Same is true between F and K. □

Separable and inseparable degrees. Let K/F be an algebraic extension and $S \subset K$ the largest separable extension over F. $[K:F]_s := [S:F]$ is the *separable degree* of K over F; $[K:F]_i := [K:S]$ is the *inseparable degree* of K over F. Note that $[K:F] = [K:F]_i[K:F]_s$.

$$\begin{tikzcd}
K \arrow[d, dash, "{[K:F]_i}"] \\
S \arrow[d, dash, "{[K:F]_s}"] \\
F
\end{tikzcd}$$

Lemma 3.56. *Let $F \subset L \subset M \subset K$ be fields such that K/F is normal. Let*

$$\begin{aligned}
\mathrm{Iso}(M/F) &= \textit{the set of all } F\textit{-isomorphisms } M \to K,\\
\mathrm{Iso}(L/F) &= \textit{the set of all } F\textit{-isomorphisms } L \to K,\\
\mathrm{Iso}(M/L) &= \textit{the set of all } L\textit{-isomorphisms } M \to K.
\end{aligned}$$

Then $|\mathrm{Iso}(M/F)| = |\mathrm{Iso}(M/L)||\mathrm{Iso}(L/F)|$.

$$\begin{tikzcd}
K \arrow[d, dash] \\
M \arrow[d, dash] \\
L \arrow[d, dash] \\
F
\end{tikzcd}$$

Note. The sets $\mathrm{Iso}(M/F)$, $\mathrm{Iso}(L/F)$ and $\mathrm{Iso}(M/L)$ do not depend on K. One can let K be an algebraic closure of F.

Proof of Lemma 3.56. Since K/F is normal, every $\sigma \in \mathrm{Iso}(L/F)$ extends to some $\bar\sigma \in \mathrm{Aut}(K/F)$. Define

$$\begin{array}{rccc}
\theta: & \mathrm{Iso}(L/F) \times \mathrm{Iso}(M/L) & \longrightarrow & \mathrm{Iso}(M/F)\\
& (\sigma, \tau) & \longmapsto & \bar\sigma|_{\tau(M)} \circ \tau.
\end{array}$$

1° θ is 1-1. Assume $\bar\sigma_1|_{\tau_1(M)} \circ \tau_1 = \bar\sigma_2|_{\tau_2(M)} \circ \tau_2$, where $\sigma_1, \sigma_2 \in \mathrm{Iso}(L/F)$ and $\tau_1, \tau_2 \in \mathrm{Iso}(M/L)$. Then

$$\sigma_1 = \bar\sigma_1|_L = (\bar\sigma_1|_{\tau_1(M)} \circ \tau_1)|_L = (\bar\sigma_2|_{\tau_2(M)} \circ \tau_2)|_L = \bar\sigma_2|_L = \sigma_2.$$

Now $\bar\sigma_1|_{\tau_1(M)} \circ \tau_1 = \bar\sigma_1|_{\tau_2(M)} \circ \tau_2$ implies that $\sigma_1(\tau_1(a)) = \sigma_1(\tau_2(a))$ $\forall a \in M$. So, $\tau_1(a) = \tau_2(a)$ $\forall a \in M$, i.e., $\tau_1 = \tau_2$.

2° θ is onto. Let $\alpha \in \mathrm{Iso}(M/F)$. Then $\sigma := \alpha|_L \in \mathrm{Iso}(L/F)$. Let $\tau = \bar\sigma^{-1}|_{\alpha(M)} \circ \alpha$. Then $\tau \in \mathrm{Iso}(M/L)$ and $\alpha = \bar\sigma|_{\tau(M)} \circ \tau$. □

Proposition 3.57. *Let $F \subset L \subset K$ be fields such that $[L:F]_s < \infty$ and K/F is normal. Then $|\mathrm{Iso}(L/F)| = [L:F]_s$, where $\mathrm{Iso}(L/F)$ is the set of all F-isomorphisms $L \to K$.*

$$\begin{tikzcd} K \arrow[d, dash] \\ L \arrow[d, dash] \\ S \arrow[d, dash] \\ F \end{tikzcd}$$

Proof. Let $S \subset L$ be the largest separable extension over F. Since L/S is purely inseparable, it is easy to see that $\text{Iso}(L/S) = \{\text{id}\}$. (Let $\sigma \in \text{Iso}(L/S)$ and let $u \in L$. Since u is purely inseparable over S, the minimal polynomial of u over S is $f(x) = (x-u)^m$ for some $m > 0$. Since $\sigma(u)$ is a root of f, we have $\sigma(u) = u$.) By Lemma 3.56, $|\text{Iso}(L/F)| = |\text{Iso}(L/S)||\text{Iso}(S/F)| = |\text{Iso}(S/F)|$. Thus it suffices to show that $[S : F] = |\text{Iso}(S/F)|$.

Use induction on $[S : F]$. Assume $[S : F] > 1$. Choose $u \in S \setminus F$. Let f be the minimal polynomial of u over F. Then f has $n = \deg f$ distinct roots $u_1, \dots, u_n \in K$. Then $\text{Iso}(F(u)/F) = \{\sigma_1, \dots, \sigma_n\}$, where $\sigma_i : F(u) \to F(u_i)$ is the F-isomorphism such that $\sigma_i(u) = u_i$. So $|\text{Iso}(F(u)/F)| = n = [F(u) : F]$. Since $S/F(u)$ is separable and $[S : F(u)] < [S : F]$, by the induction hypothesis, $|\text{Iso}(S/F(u))| = [S : F(u)]$. So

$$|\text{Iso}(S/F)| = |\text{Iso}(S/F(u))||\text{Iso}(F(u)/F)| = [S : F(u)][F(u) : F] = [S : F].$$

□

Proposition 3.57 is false when $[L : F]_s = \infty$.

Proposition 3.58. *Let $F \subset L \subset K$ be fields such that $[L : F]_s = \infty$ and K/F is normal. Then $|\text{Iso}(L/F)| = 2^{[L:F]_s}$.*

Proof. For each $Y \subset L$, let $C(Y) \subset K$ be the set of all conjugates of elements in Y over F. (Two algebraic elements over F are called *conjugates* if they have the same minimal polynomial over F.)

1° Let S be the largest separable extension of F in L. Let X be a basis of S over F. Define

$$\begin{array}{rccc} \theta : & \text{Iso}(S/F) & \longrightarrow & \prod_{\epsilon \in X} C(\epsilon) \\ & \sigma & \longmapsto & \big(\sigma(\epsilon)\big)_{\epsilon \in X}. \end{array}$$

θ is 1-1. So,

$$|\text{Iso}(L/F)| = |\text{Iso}(S/F)| \le \Big|\prod_{\epsilon \in X} C(\epsilon)\Big| \le \aleph_0^{|X|} \le (2^{\aleph_0})^{|X|} = 2^{\aleph_0 |X|} = 2^{|X|} = 2^{[L:F]_s}.$$

($|\text{Iso}(L/F)| = |\text{Iso}(S/F)|$ since $|\text{Iso}(L/S)| = 1$; see the proof of Proposition 3.57.)

2° Let

$$\begin{aligned} \mathcal{Y} = \big\{ (Y, \le) : Y \subset S;\ \le \text{ is a linear order on } Y; \\ \text{for each } y \in Y,\ y \notin F\big(C(\{z \in Y : z < y\})\big)\big\}. \end{aligned}$$

For $(Y_1, \le_1),\ (Y_2, \le_2) \in \mathcal{Y}$, say $(Y_1, \le_1) \prec (Y_2, \le_2)$ if $Y_1 \subset Y_2$ and $\le_1$ is the restriction of $\le_2$. Then $(\mathcal{Y}, \prec)$ is a poset in which every chain has an upper bound. By Zorn's lemma, $(\mathcal{Y}, \prec)$ has a maximal element $(Y, \le)$.

We claim that $|Y| \geq [S : F] = [L : F]_s$. Otherwise,

$$[F(C(Y)) : F] \begin{cases} < \aleph_0 \leq [S : F] & \text{if } |Y| < \infty, \\ \leq |Y|\aleph_0 = |Y| < [S : F] & \text{if } |Y| = \infty. \end{cases}$$

So $F(C(Y)) \subsetneq S$. Choose $y_0 \in S \setminus F(C(Y))$ and define $y \leq y_0$ for all $y \in Y$. Then $(Y \cup \{y_0\}, \leq) \in \mathcal{Y}$, contradicting the maximality of $(Y, \leq)$.

For each $y \in Y$, since y is separable over F and $y \notin F\big(C(\{z \in Y : z < y\})\big)$, y has a conjugate $\bar{y} \in K$ over $F\big(C(\{z \in Y : z < y\})\big)$ such that $\bar{y} \neq y$. Using Zorn's lemma, it is easy to see that for every $(f_y)_{y \in Y} \in \prod_{y \in Y} \{y, \bar{y}\}$, $\exists\, \sigma \in \mathrm{Iso}(L/F)$ such that $\sigma(y) = f_y$ for all $y \in Y$. Thus

$$|\mathrm{Iso}(L/F)| \geq \Big| \prod_{y \in Y} \{y, \bar{y}\} \Big| = 2^{|Y|} \geq 2^{[L:F]_s}.$$

□

Corollary 3.59. *Let $F \subset L \subset K$ be fields such that K/F is algebraic. Then*

$$[K : F]_s = [K : L]_s [L : F]_s, \tag{3.20}$$

$$[K : F]_i = [K : L]_i [L : F]_i. \tag{3.21}$$

Proof. 1° We first prove (3.20). Let $S_{K/F}$ be the largest separable extension of F in K.

(3.22)

$$\begin{tikzcd}
& & K \arrow[dl, dash, "\text{in}"'] \arrow[dd, dash] \\
& S_{K/L} \arrow[dl, dash, "\text{in}"'] \arrow[dr, dash, "\text{sep}"'] & \\
S_{K/F} \arrow[dr, dash, "\text{sep}"'] & & L \arrow[dl, dash, "\text{in}"'] \arrow[dd, dash] \\
& S_{L/F} \arrow[dr, dash, "\text{sep}"'] & \\
& & F
\end{tikzcd}$$

Since $[K : F]_s = [S_{K/L} : S_{L/F}][S_{L/F} : F]$, $[K : L]_s = [S_{K/L} : L]$, and $[L : F]_s = [S_{L/F} : F]$, it suffices to show $[S_{K/F} : S_{L/F}] = [S_{K/L} : L]$. Apply Theorem 3.51 (iv) to

(3.23)

$$\begin{tikzcd}
& S_{K/L} \arrow[dl, dash, "\text{in}"'] \arrow[dr, dash, "\text{sep}"] & \\
S_{K/F} \arrow[dr, dash, "\text{sep}"'] & & L \arrow[dl, dash, "\text{in}"] \\
& S_{L/F} &
\end{tikzcd}$$

we have $S_{K/L} = S_{K/F}L$.

Let $X \subset S_{K/F}$ be linearly independent over $S_{L/F}$ with $|X| < \infty$. We claim that X is also linearly independent over L. (This means that $S_{K/F}$ and L are *linearly disjoint* over $S_{L/F}$. Also, this implies that $[S_{K/L} : L] = [S_{K/F} : S_{L/F}]$.) We have

$$\begin{tikzcd} & L(X) \arrow[dl, dash, "\text{in}"'] \arrow[dr, dash, "\text{sep}"] & \\ S_{L/F}(X) \arrow[dr, dash, "\text{sep}"'] & & L \arrow[dl, dash, "\text{in}"] \\ & S_{L/F} & \end{tikzcd}$$

Since $[S_{L/F}(X) : S_{L/F}]$ and $[L(X) : L]$ are finite, by Proposition 3.57 and Lemma 3.56,

$$\begin{aligned} [L(X) : L] &= |\mathrm{Iso}(L(X)/L)| = |\mathrm{Iso}(L(X)/S_{L/F})| \\ &= |\mathrm{Iso}(S_{L/F}(X)/S_{L/F})| = [S_{L/F}(X) : S_{L/F}] = |X|. \end{aligned}$$

So, X is linearly independent over L.

2° Proof of (3.21). It suffices to show that in diagram (3.22), $[S_{K/L} : S_{K/F}] = [L : S_{L/F}]$. Since we have proved that in diagram (3.23), $S_{K/F}$ and L are linearly disjoint over $S_{L/F}$, it follows that L and $S_{K/F}$ are linearly disjoint over $S_{L/F}$ ([**11**, p.318, Theorem 2.2]). So, $[S_{K/L} : S_{K/F}] = [S_{K/F}L : S_{K/F}] = [L : S_{L/F}]$. □

Corollary 3.60. *Let $f \in F[x]$ be monic and irreducible and let K be a splitting field of f over F. Let $u_1 \in K$ be any root of f. Then*

(i) $f = [(x-u_1)\cdots(x-u_n)]^{[F(u_1):F]_i}$*, where $u_1, \dots, u_n \in K$ are the distinct roots of f and $n = [F(u_1) : F]_s$;*

(ii) $u_1^{[F(u_1):F]_i}$ *is separable over F.*

Proof. May assume $\operatorname{char} F = p > 0$.

(i) Let $u_1, \dots, u_n \in K$ be all the distinct roots of f. Then

$$[F(u_1) : F]_s = |\mathrm{Iso}(F(u_1)/F)| = n.$$

Write $f = (x-u_1)^{r_1}\cdots(x-u_n)^{r_n}$. For each $1 \le i \le n$, $\exists\, F$-isomorphism $\sigma_i : F(u_1) \to F(u_i)$ such that $\sigma_i(u_1) = u_i$. Then

$$(x-u_1)^{r_1}\cdots(x-u_n)^{r_n} = f = \sigma_i f = (x-\sigma_i(u_1))^{r_1}\cdots(x-\sigma_i(u_n))^{r_n}.$$

It follow that $r_i = r_1$. So $f = [(x-u_1)\cdots(x-u_n)]^{r_1}$. We have $nr_1 = \deg f = [F(u_1) : F] = [F(u_1) : F]_s[F(u_1) : F]_i$, so $r_1 = [F(u_1) : F]_i$.

(ii) In the notation of (i), we have $f = (x^{r_1} - u_1^{r_1})\cdots(x^{r_1} - u_n^{r_1})$ since r_1 is a power of p. Thus $g := (x - u_1^{r_1})\cdots(x - u_n^{r_1}) \in F[x]$, where $u_1^{r_1}, \dots, u_n^{r_1}$ are all distinct. Since u^{r_1} is a root of g, u^{r_1} is separable over F. □

3.7. Cyclotomic Extensions

Let F be a field. A splitting of $x^n - 1$ over F is called a *cyclotomic extension* of order n over F. If $\operatorname{char} F = p > 0$ and $n = mp^t$, $(m,p) = 1$, then $x^n - 1 = (x^m - 1)^{p^t}$. So, a splitting field of $x^n - 1$ over F is a splitting field of $x^m - 1$ over F. Therefore, we assume that $\operatorname{char} F \nmid n$.

Let K be a cyclotomic extension of order n over F ($\operatorname{char} F \nmid n$) and let $U_n = \{u \in K : u^n = 1\}$. Then $|U_n| = n$ since $x^n - 1$ has no multiple roots. Since U_n is a finite subgroup of $K^\times$, U_n is cyclic. A generator of U_n is called a *primitive nthe root of unity*.

Proposition 3.61. *Let K be a cyclotomic extension of order n over F, where $\operatorname{char} F \nmid n$.*

(i) *K/F is Galois.*
(ii) *$K = F(\zeta)$, where ζ is any primitive nth root of unity.*
(iii) *Let*

$$\begin{array}{cccc} \theta: & \operatorname{Aut}(K/F) & \longrightarrow & \mathbb{Z}_n^\times \\ & \sigma & \longmapsto & i \end{array}$$

where $\sigma(\zeta) = \zeta^i$. Then θ is a 1-1 group homomorphism. In particular, $[K : F] \mid \phi(n)$, where ϕ is the Euler function.

Cyclotomic polynomials. Let $K = F(\zeta)$, where ζ is a primitive nth root of unity and $\operatorname{char} F \nmid n$.

$$\Phi_n(x) = \prod_{\substack{u \in \langle \zeta \rangle \\ o(u)=n}} (x - u)$$

is called the nth *cyclotomic polynomial* over F.

Facts.

(i) $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.
(ii)

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d \mid n,\, d<n} \Phi_d(x)} = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)},$$

where μ is the Möbius function.
(iii) If $\operatorname{char} F = 0$, $\Phi_n(x) \in \mathbb{Z}[x]$; if $\operatorname{char} F = p > 0$, $\Phi_n(x) \in \mathbb{Z}_p[x]$.

Proof. (i)

$$x^n - 1 = \prod_{u \in \langle \zeta \rangle} (x - u) = \prod_{d \mid n} \prod_{\substack{u \in \langle \zeta \rangle \\ o(u)=d}} (x - u) = \prod_{d \mid n} \Phi_d(x).$$

(ii) The formula $\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$ follows from (i) and the Möbius inversion.

(iii) Assume $\operatorname{char} F = 0$. (The proof in the case $\operatorname{char} F = p$ is the same.) Use induction on n. We have

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d \mid n \\ d<n}} \Phi_d(x).$$

Since $x^n - 1 \in \mathbb{Z}[x]$ and since $\prod_{d \mid n,\, d<n} \Phi_d(x) \in \mathbb{Z}[x]$ is monic (by the induction hypothesis), we have $\Phi_n(x) \in \mathbb{Z}[x]$. □

Cyclotomic extensions in characteristic 0.

Theorem 3.62. *Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.*

(i) *Φ_n (the nth cyclotomic polynomial over $\mathbb{Q}$) is irreducible over $\mathbb{Q}$ and is the minimal polynomial of ζ_n over $\mathbb{Q}$.*
(ii) *$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ and $\operatorname{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.*

Proof. We only have to show that Φ_n is irreducible in $\mathbb{Q}[x]$. Let $f \in \mathbb{Q}[x]$ be a monic irreducible factor of Φ_n and write $\Phi_n = fg$, where $g \in \mathbb{Q}[x]$ is monic. Since $\Phi_n(x) \in \mathbb{Z}[x]$, it follows that $f, g \in \mathbb{Z}[x]$ (Write $f = \frac{k}{l} f_1$, $g = \frac{s}{t} g_1$, where $k, l, s, t \in \mathbb{Z}^+$, $(k, l) = 1$, $(s, t) = 1$ and $f_1, g_1 \in \mathbb{Z}[x]$ are primitive. Since f and g are monic, $k = s = 1$. So $\frac{1}{lt} f_1 g_1 = fg \in \mathbb{Z}[x]$. Thus $l = t = 1$.)

Let p be a prime such that $p \nmid n$. We claim that if u is a root of f, then so is u^p. Suppose to the contrary that u^p is not a root of f. Then u^p is a root of g, i.e., u is a root of $g(x^p)$. So, $f(x) \mid g(x^p)$. Let $\bar{f}$ denote the reduction of f in $\mathbb{Z}_p[x]$. Then in $\mathbb{Z}_p[x]$, $\bar{f}(x) \mid \bar{g}(x^p) = \bar{g}(x)^p$. Hence $(\bar{f}, \bar{g}) \neq 1$. Then $\overline{\Phi}_n = \bar{f}\bar{g}$ has multiple roots. Since $\overline{\Phi}_n \mid x^n - 1$, it follows that $x^n - 1 \in \mathbb{Z}_p[x]$ has multiple roots. But this is impossible since $p \nmid n$. So the claim is proved.

By the above claim, if u is a root of f, then so is u^r for all r with $(r, n) = 1$. Thus $\deg f \geq \phi(n)$. So $f = \Phi_n$. □

Corollary 3.63. *Let F be a field with $\operatorname{char} F = 0$. Let ζ be a primitive nth root of unity in some extension of F. Then*

$$[F(\zeta) : F] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta) \cap F] = \frac{\phi(n)}{[\mathbb{Q}(\zeta) \cap F : \mathbb{Q}]}.$$

$$\begin{tikzcd}
& F(\zeta) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta) \arrow[dr, dash] \arrow[ddr, dash, "\phi(n)"'] & & F \arrow[dl, dash] \\
& \mathbb{Q}(\zeta) \cap F \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Proof. It suffices to show that $[F(\zeta) : F] \geq [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta) \cap F]$. Let $f \in F[x]$ be the minimal polynomial of ζ over F. Since f is a factor of $x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta^i)$, we have $f \in \mathbb{Q}(\zeta)[x]$. So $f \in \big(\mathbb{Q}(\zeta) \cap F\big)[x]$. Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta) \cap F] \leq \deg f = [F(\zeta) : F]$. □

Example. Let $\zeta_8 = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$, $F = \mathbb{Q}(\sqrt{2})$. Then $\mathbb{Q}(\zeta_8) \cap F = F$. So $[F(\zeta_8) : F] = \frac{\phi(8)}{[F:\mathbb{Q}]} = 2$.

Cyclotomic extensions in characteristic p.

Fact. Assume $p \nmid n$ and let ζ_n be a primitive nth root of unity in some extension of $\mathbb{F}_p$. Let $o_n(p)$ be the order of p in $\mathbb{Z}_n^{\times}$. Then $\mathbb{F}_p(\zeta_n) = \mathbb{F}_{p^{o_n(p)}}$. More generally, $\mathbb{F}_{p^m}(\zeta_n) = \mathbb{F}_{p^{[m, o_n(p)]}}$.

Proof. $\zeta_n \in \mathbb{F}_{p^k} \Leftrightarrow n \mid p^k - 1 \Leftrightarrow o_n(p) \mid k$. □

Corollary 3.64. *Let $\operatorname{char} F = p > 0$. Let ζ be a primitive nth root of unity in some extension of F, where $p \nmid n$. Assume $\mathbb{F}_{p^{o_n(p)}} \cap F = \mathbb{F}_{p^m}$. Then $[F(\zeta) : F] = \frac{o_n(p)}{m}$.*

$$\begin{tikzcd}
 & F(\zeta) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{F}_{p^{o_n(p)}} = \mathbb{F}_p(\zeta) \arrow[dr, no head] & & F \arrow[dl, no head] \\
 & \mathbb{F}_p(\zeta) \cap F = \mathbb{F}_{p^m} &
\end{tikzcd}$$

Proof. Same as the proof of Corollary 3.63 □

Abelian extensions. An *abelian extension* is an algebraic Galois extension K/F such that $\mathrm{Aut}(K/F)$ is abelian. Subextensions of an abelian extension are abelian (Exercise 3.2). Cyclotomic extensions are abelian. Thus an extension K of F contained in a cyclotomic extension of F is a finite abelian extension over F. The converse is true for $F = \mathbb{Q}$.

The Kronecker-Weber Theorem. *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subset \mathbb{Q}(\zeta_n)$ for some $n > 0$, where $\zeta_n = e^{2\pi i/n}$.*

The proof is difficult and needs algebraic number theory ([**22**, Ch.14]).

Ruler and compass construction of regular polygon and Fermat primes. Let $F_k = 2^{2^k} + 1$, $k \geq 0$. $F_0, \dots, F_4$ are primes (the only known primes in the sequence F_k). For $5 \leq i \leq 23$ and many other values of i, F_i are known to be composite. A primes of the form F_k is called a *Fermat prime.*

Proposition 3.65. *$\zeta_n = e^{2\pi i/n}$ is constructible by ruler and compass iff $n = 2^a p_1 \cdots p_s$, where $p_1, \dots, p_s$ are distinct Fermat primes.*

Proof. 1° We first show that ζ_n is constructible $\Leftrightarrow$ $\phi(n)$ is a power of 2.

($\Rightarrow$) By Theorem 3.62 (ii) and Corollary 3.6, $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is a power of 2.

($\Leftarrow$) Let $\phi(n) = 2^m$. By Theorem 3.62 (ii), $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension where $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian group of order 2^m. Thus there are subgroups

$$1 = H_0 < H_1 < \cdots < H_m = \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

such that $[H_i : H_{i-1}] = 2$. So we have a tower of fields

$$\mathbb{Q} = H'_m \subset \cdots \subset H'_1 \subset H'_0 = \mathbb{Q}(\zeta_n)$$

such that $[H'_{i-1} : H'_i] = 2$. Hence by Theorem 3.5, ζ_n is constructible.

2° Let $n = 2^a p_1^{e_1} \cdots p_s^{e_s}$, where $p_1, \dots, p_s$ are distinct odd primes and $e_j > 0$. Then

$$\phi(n) = 2^{a-1} p_1^{e_1 - 1}(p_1 - 1) \cdots p_s^{e_s - 1}(p_s - 1).$$

So $\phi(n)$ is a power of 2 $\Leftrightarrow$ $e_1 = \cdots = e_s = 1$ and $p_j = 2^{t_j} + 1$, $1 \leq j \leq s$. Note that if $2^t + 1$ is a prime, then t is a power of 2. (If $t = uv$, where u is odd, then $2^v + 1 \mid 2^{uv} + 1$.) So $p_j = 2^{t_j} + 1$ is a prime $\Leftrightarrow$ p_j is a Fermat prime. □

3.8. Trace and Norm, Cyclic Extensions

Let $F \subset K \subset \bar{F}$ be fields such that $[K : F] < \infty$ and $\bar{F}$ is an algebraic closure of F. Let $r = [K : F]_s$ and $\mathrm{Iso}(K/F) = \{\sigma_1, \dots, \sigma_r\}$. For each $u \in K$, define

$$\mathrm{Tr}_{K/F}(u) = [K : F]_i\big(\sigma_1(u) + \cdots + \sigma_r(u)\big) \qquad \text{(the } \textit{trace} \text{ of } u\text{)},$$

$$\mathrm{N}_{K/F}(u) = \big(\sigma_1(u) \cdots \sigma_r(u)\big)^{[K:F]_i} \qquad \text{(the } \textit{norm} \text{ of } u\text{)}.$$

It follows from the next proposition that $\mathrm{Tr}_{K/F}(u), \mathrm{N}_{K/F}(u) \in F$ $\forall u \in K$.

Proposition 3.66. *Let $[K : F] < \infty$ and $u \in K$. Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$ be the minimal polynomial of u over F. Then*

$$\mathrm{Tr}_{K/F}(u) = -[K : F(u)]a_{n-1}, \tag{3.24}$$

$$\mathrm{N}_{K/F}(u) = \big[(-1)^n a_0\big]^{[K:F(u)]}. \tag{3.25}$$

Proof. Let $r = [F(u) : F]_s$ and let $\mathrm{Iso}(F(u)/F) = \{\sigma_1, \dots, \sigma_r\}$. By Corollary 3.60 (i),

$$f = \big[(x - \sigma_1(u)) \cdots (x - \sigma_r(u))\big]^{[F(u):F]_i}.$$

So,

$$a_{n-1} = -[F(u) : F]_i \sum_j \sigma_j(u), \qquad a_0 = \Big[(-1)^r \prod_j \sigma_j(u)\Big]^{[F(u):F]_i}.$$

Let $\mathrm{Iso}(K/F(u)) = \{\tau_1, \dots, \tau_t\}$, where $t = [K : F(u)]_s$. Let $\bar{\sigma}_j \in \mathrm{Aut}(\bar{F}/F)$ be an extension of σ_j. By the proof of Lemma 3.56, $\mathrm{Iso}(K/F) = \{\bar{\sigma}_j|_{\tau_k(K)} \circ \tau_k : 1 \le j \le r,\ 1 \le k \le t\}$.

$$\begin{tikzcd}
\bar{F} \arrow[d, dash] \\
K \arrow[d, dash] \\
F(u) \arrow[d, dash] \\
F
\end{tikzcd}$$

Then

$$\begin{aligned}
\mathrm{Tr}_{K/F}(u) &= [K : F]_i \sum_{\alpha \in \mathrm{Iso}(K/F)} \alpha(u) \\
&= [K : F]_i \sum_{\substack{1 \le j \le r \\ 1 \le k \le t}} \bar{\sigma}_j(\tau_k(u)) \\
&= [K : F]_i \cdot t \sum_{1 \le j \le r} \sigma_j(u) \\
&= t\,[K : F(u)]_i\,[F(u) : F]_i \sum_j \sigma_j(u) \\
&= -[K : F(u)]a_{n-1}.
\end{aligned}$$

The proof of (3.25) is the same. □

Facts. Let $[K : F] < \infty$.

(i) For $u, v \in K$ and $a, b \in F$,

$$\begin{aligned}\operatorname{Tr}_{K/F}(au+bv) &= a\operatorname{Tr}_{K/F}(u) + b\operatorname{Tr}_{K/F}(v),\\ \mathrm{N}_{K/F}(uv) &= \mathrm{N}_{K/F}(u)\mathrm{N}_{K/F}(v).\end{aligned}$$

(ii) If $u \in F$, then $\operatorname{Tr}_{K/F}(u) = [K : F]u$ and $\mathrm{N}_{K/F}(u) = u^{[K:F]}$.

(iii) (Transitivity) Let $F \subset K \subset L$ where $[L : F] < \infty$. Then for each $u \in L$,

$$\begin{aligned}\operatorname{Tr}_{L/F}(u) &= \operatorname{Tr}_{K/F}\big(\operatorname{Tr}_{L/K}(u)\big),\\ \mathrm{N}_{L/F}(u) &= \mathrm{N}_{K/F}\big(\mathrm{N}_{L/K}(u)\big).\end{aligned}$$

Proof. (iii) Let $\operatorname{Iso}(K/F) = \{\sigma_1, \dots, \sigma_r\}$, $\operatorname{Iso}(L/K) = \{\tau_1, \dots, \tau_t\}$. Extend σ_j to $\bar{\sigma}_j \in \operatorname{Aut}(\bar{F}/F)$. Then $\operatorname{Iso}(L/F) = \{\bar{\sigma}_j|_{\tau_k(K)} \circ \tau_k : 1 \le j \le r,\ 1 \le k \le t\}$.

$$\begin{tikzcd}\bar{F} \arrow[d, dash] \\ L \arrow[d, dash] \\ K \arrow[d, dash] \\ F\end{tikzcd}$$

So,

$$\begin{aligned}\operatorname{Tr}_{K/F}\big(\operatorname{Tr}_{L/K}(u)\big) &= \operatorname{Tr}_{K/F}\Big(\frac{[L:K]}{t}\sum_k \tau_k(u)\Big)\\ &= \frac{[L:K]}{t}\operatorname{Tr}_{K/F}\Big(\sum_k \tau_k(u)\Big)\\ &= \frac{[L:K]}{t}\,\frac{[K:F]}{r}\sum_j \sigma_j\Big(\sum_k \tau_k(u)\Big)\\ &= [L:F]_i \sum_{j,k} \bar{\sigma}_j(\tau_k(u))\\ &= \operatorname{Tr}_{L/F}(u).\end{aligned}$$

□

Cyclic extensions: algebraic Galois extensions K/F such that $\operatorname{Aut}(K/F)$ is cyclic.

Theorem 3.67. *Let K/F be a finite cyclic extension with* $\operatorname{Aut}(K/F) = \langle\sigma\rangle$. *Let $u \in K$.*

(i) $\operatorname{Tr}_{K/F}(u) = 0 \Leftrightarrow u = v - \sigma(v)$ *for some* $v \in K$.

(ii) (Hilbert's Theorem 90) $\mathrm{N}_{K/F}(u) = 1 \Leftrightarrow u = \frac{v}{\sigma(v)}$ *for some* $v \in K^\times$.

Proof. Let $n = [K : F]$.

(i) We show that the sequence of F-maps

$$0 \longrightarrow F \hookrightarrow K \xrightarrow{\mathrm{id}-\sigma} K \xrightarrow{\operatorname{Tr}_{K/F}} F \longrightarrow 0$$

is exact.

1° $\mathrm{Tr}_{K/F} : K \to F$ is onto. Since $\sigma^0, \dots, \sigma^{n-1}$ are distinct automorphisms of K, by Proposition 3.11, they are linearly independent over K as K-valued functions. So $\mathrm{Tr}_{K/F} = \sigma^0 + \cdots + \sigma^{n-1} \neq 0$. Hence $\mathrm{Tr}_{K/F} : K \to F$ is onto.

2° $\ker(\mathrm{id} - \sigma) = \{v \in K : \sigma(v) = v\} = F$ since K/F is Galois.

3° Clearly, $\mathrm{im}(\mathrm{id} - \sigma) \subset \ker \mathrm{Tr}_{K/F}$. However, by 1° and 2°,

$$\dim_F(\ker \mathrm{Tr}_{K/F}) = n - 1 = \dim_F\big(\mathrm{im}(\mathrm{id} - \sigma)\big).$$

So $\mathrm{im}(\mathrm{id} - \sigma) = \ker \mathrm{Tr}_{K/F}$.

(ii) We show that

$$1 \longrightarrow F^\times \hookrightarrow K^\times \xrightarrow{\frac{\mathrm{id}}{\sigma}} K^\times \xrightarrow{\mathrm{N}_{K/F}} F^\times$$

is exact. It suffices to show that $\ker \mathrm{N}_{K/F} \subset \mathrm{im}(\frac{\mathrm{id}}{\sigma})$.

Let $u \in \ker \mathrm{N}_{K/F}$. Define

$$\begin{array}{cccc} \alpha : & K & \longrightarrow & K \\ & x & \longmapsto & u\sigma(x). \end{array}$$

Then $\alpha^i = u\sigma(u)\cdots\sigma^{i-1}(u)\sigma^i$ and $\alpha^n = \mathrm{id}$. Since $\sigma^0, \dots, \sigma^{n-1}$ are linearly independent over K, so are $\alpha^0, \dots, \alpha^{n-1}$. Hence $\exists x \in K$ such that

$$v := (\alpha^0 + \cdots + \alpha^{n-1})(x) \neq 0.$$

Clearly, $\alpha(v) = v$, i.e., $u\sigma(v) = v$. So $u = \frac{v}{\sigma(v)}$.

Note. In general, $\mathrm{N}_{K/F} : K^\times \to F^\times$ is not onto. Example: $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = |z|^2$, $z \in \mathbb{C}$. □

Proposition 3.68. *Let F be a field containing a primitive nth root of unity ζ (so $\mathrm{char} F \nmid n$).*

(i) *K/F is a cyclic extension of degree $n \Leftrightarrow K = F(u)$ where u is a root of an irreducible polynomial of the form $x^n - a \in F[x]$.*

(ii) *If $u^n \in F$, then $\mathrm{Aut}(F(u)/F) \hookrightarrow \mathbb{Z}_n$.*

Note. In (ii) of the above Proposition, if F does not contain a primitive nth root of unity, $\mathrm{Aut}(F(u)/F)$ may not be abelian. See Exercise 3.5.

Proof of Proposition 3.68. (i) ($\Leftarrow$) Obvious.

($\Rightarrow$) Let $\mathrm{Aut}(K/F) = \langle\sigma\rangle$. Since $\mathrm{N}_{K/F}(\zeta) = \zeta^n = 1$, by Hilbert's Theorem 90, $\zeta = \frac{\sigma(u)}{u}$ for some $u \in K$. So $\sigma(u) = \zeta u$. Since $\sigma^i(u) = \zeta^i u$, $0 \leq i \leq n-1$, are distinct conjugates of u over F, $[F(u) : F] \geq n$. Thus $K = F(u)$. Since $\sigma(u^n) = \sigma(u)^n = (\zeta u)^n = u^n$, we have $u^n \in F$. Let $a = u^n$. Then $x^n - a \in F[x]$ is the minimal polynomial of u over F.

(ii) $\forall \sigma \in \mathrm{Aut}(F(u)/F)$, $\sigma(u) = \zeta^i u$ for some $i \in \mathbb{Z}_n$. The embedding $\mathrm{Aut}(F(u)/F) \hookrightarrow \mathbb{Z}_n$ is given by $\sigma \mapsto i$. □

Theorem 3.69 (Artin-Schreier). *Assume* $\mathrm{char} F = p > 0$. *Then K/F is a cyclic extension of degree $p \Leftrightarrow K = F(u)$ where u is a root of an irreducible polynomial of the form $x^p - x - a \in F[x]$.*

Proof. ($\Leftarrow$) It is easy to see that $u + i$, $i \in \mathbb{F}_p$, are all roots of $x^p - x - a$. So $F(u)$ is the splitting field of $x^p - x - a$ over F. Hence K/F is Galois. Since $[K : F] = p$, K/F must be cyclic.

($\Rightarrow$) Let $\text{Aut}(K/F) = \langle\sigma\rangle$. Since $\text{Tr}_{K/F}(1) = p = 0$, by Theorem 3.67 (i), $1 = \sigma(u) - u$ for some $u \in K$. Clearly $u \notin F$. We have

$$\sigma(u^p - u) = \sigma(u)^p - \sigma(u) = (u+1)^p - (u+1) = u^p - u.$$

So $u^p - u \in F$. Let $a = u^p - u$. Then u is a root of $x^p - x - a \in F[x]$. It remains to show that $x^p - x - a$ is irreducible in $F[x]$. Note that the roots of $x^p - x - a$ are $u + i$, $i \in \mathbb{F}_p$. Let $f \in F[x]$ be a monic irreducible factor of $x^p - x - a$. Then $f = \prod_{i \in S}[x - (u+i)]$ for some $\emptyset \neq S \subset \mathbb{F}_p$. Since

$$f = x^{|S|} - \Big(|S|u + \sum_{i \in S} i\Big)x^{|S|-1} + \cdots,$$

we have $|S|u \in F$. Since $u \notin F$, we must have $|S| = p$. So $f = x^p - x - a$. □

Note. It follows from the proof of Theorem 3.69 that if $\text{char}\, F = p$, a polynomial of the form $x^p - x - a \in F[x]$ is either irreducible or splits in F.

3.9. Radical Extensions

Definition 3.70. Let K/F be a finite extension. K is called a *radical extension* over F if $K = F(u_1, \dots, u_n)$ such that for each $1 \le i \le n$,

(i) $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$ for some $m_i > 0$ or
(ii) $\text{char}\, F = p$ and $u_i^p - u_i \in F(u_1, \dots, u_{i-1})$.

Assume $\text{char}\, F = 0$. If K/F is a radical extension, then every element in K can be expressed in terms of elements in F using $+, -, \times, \div, \sqrt[m]{\ }$. Let $f \in F[x]$. If the splitting field of f over F is contained in a radical extension over F, then the equation $f(x) = 0$ is solvable by radicals.

Call an extension K/F (with non assumption on $\text{char}\, F$) *solvable by radicals* if K is contained in a radical extension of F.

Fact. Let E_1, E_2 be intermediate fields of $F \subset K$ such that both E_1 and E_2 are radical over F. The E_1E_2 is also radical over F.

Proof. Let $E_1 = F(u_1, \dots, u_m)$ and $E_2 = (F(v_1, \dots, v_n)$ such that $u_1, \dots, u_m$ and $v_1, \dots, v_n$ satisfy the conditions on Definition 3.70. Let $(w_1, \dots, w_{m+n}) = (u_1, \dots, u_m, v_1, \dots, v_n)$. Then $E_1E_2 = F(w_1, \dots, w_{m+n})$ and $w_1, \dots, w_{m+n}$ satisfy the conditions in Definition 3.70. □

Theorem 3.71 (Galois). *Let K/F be a finite extension and K' the normal closure of K over F. Then K/F is solvable by radicals $\Leftrightarrow$ $\text{Aut}(K'/F)$ is solvable.*

Proof. ($\Rightarrow$) 1° Assume $F \subset K \subset L$, where L is a radical extension over F. Let $L = F(u_1, \dots, u_n)$, where u_i satisfies (i) or (ii) in Definition 3.70. We may assume that each m_i in (i) of Definition 3.70 is a prime.

Let N be a normal closure of L over F. We claim that N is radical over F. Let $v_1, \dots, v_m$ be all the conjugates of $u_1, \dots, u_n$ over F. Then $N = F(v_1, \dots, v_m)$. For each $1 \le j \le m$, $\exists u \in \{u_1, \dots, u_n\}$ such that u and v_j are conjugates over F. So $\exists\, F$-isomorphism $\sigma_j : F(u) \to F(v_j)$. Extend σ_j to $\bar{\sigma}_j \in \text{Aut}(N/F)$. Let $L_j = \bar{\sigma}_j(L)$. Then L_j is radical over F. Since $v_j \in F(v_j) \subset \bar{\sigma}_j(L) = L_j$, we have

$N = L_1 \cdots L_m$. By the above fact, N is radical over F. Replacing L with N, we may assume that L/F is radical and normal. We may assume $K' \subset L$.

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[dd, dash, bend right=60, "\text{normal}"'] \\
K' \arrow[d, dash, "\text{normal}"] \\
F
\end{tikzcd}$$

2° By 1°, $\mathrm{Aut}(K'/F) \cong \mathrm{Aut}(L/F)/\mathrm{Aut}(L/K')$. So it suffices to show that $\mathrm{Aut}(L/F)$ is solvable. Let $P \subset L$ be the largest purely inseparable extension over F. Then L/P is Galois and $\mathrm{Aut}(L/P) = \mathrm{Aut}(L/F)$ (Theorem 3.51). Note that L/P is still radical. Replacing F with P, we may assume that L/F is Galois. Hence we may assume that the m_i's are primes $\neq \mathrm{char}\, F$.

3° Let m be the product of all m_i's. Let ζ be a primitive mth root of unity. Since $\mathrm{Aut}(L/F) \cong \mathrm{Aut}(L(\zeta)/F)/\mathrm{Aut}(L(\zeta)/L)$, it suffices to show that $\mathrm{Aut}(L(\zeta)/F)$ is solvable. Since $\mathrm{Aut}(L(\zeta)/F)/\mathrm{Aut}(L(\zeta)/F(\zeta)) \cong \mathrm{Aut}(F(\zeta)/F)$ is abelian, it suffices to show that $\mathrm{Aut}(L(\zeta)/F(\zeta))$ is solvable.

$$\begin{tikzcd}
 & L(\zeta) \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & F(\zeta) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

Let $H_i = \mathrm{Aut}(F(u_1, \dots, u_i)/F)$. Since $F(\zeta, u_1, \dots, u_i)$ is normal over $F(\zeta, u_1, \dots, u_{i-1})$, $H_{i-1} \lhd H_i$ and $H_i/H_{i-1} \cong \mathrm{Aut}(F(\zeta, u_1, \dots, u_i)/F(\zeta, u_1, \dots, u_{i-1}))$. By Proposition 3.68 (i) and Theorem 3.69, $\mathrm{Aut}(F(\zeta, u_1, \dots, u_i)/F(\zeta, u_1, \dots, u_{i-1}))$ is cyclic. So H_n is solvable. Note that $H_n = \mathrm{Aut}(F(\zeta, u_1, \dots, u_n)/F(\zeta)) = \mathrm{Aut}(L(\zeta)/F(\zeta))$.

($\Leftarrow$) 1° It suffices to show that K'/F is solvable by radicals. Let $S \subset K'$ be the largest separable extension over F. Then S is Galois over F and $\mathrm{Aut}(S/F) \cong \mathrm{Aut}(K'/F)$ (Theorem 3.51). K'/S is purely inseparable, hence radical. Thus it suffices to show that S/F is solvable by radicals.

2° Let m be the product of all prime factors of $[S : F]$ different from $\mathrm{char}\, F$. Let ζ be a primitive mth root of unity. We claim that $[S(\zeta) : F(\zeta)] \mid [S : F]$. (By Corollaries 3.63 and 3.64, we have $[S(\zeta) : S] \mid [F(\zeta) : F]$, so the claim follows.) We show that $S(\zeta)/F$ is radical. It suffices to show that $S(\zeta)/F(\zeta)$ is radical. Since both $\mathrm{Aut}(S(\zeta)/S)$ and $\mathrm{Aut}(S(\zeta)/F)/\mathrm{Aut}(S(\zeta)/S) \cong \mathrm{Aut}(S/F)$ are solvable, $\mathrm{Aut}(S(\zeta)/F)$ is solvable. So $\mathrm{Aut}(S(\zeta)/F(\zeta))$ is solvable. Let $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = \mathrm{Aut}(S(\zeta)/F(\zeta))$ such that H_i/H_{i-1} is cyclic of prime order. Then H'_{i-1}/H'_i is a cyclic extension of prime degree. By Proposition 3.68 (i) and Theorem 3.69, H'_{i-1}/H'_i is radical. Therefore $H'_0 = S(\zeta)$ is radical over $H'_n = F(\zeta)$. □

$$\begin{tikzcd}
 & S(\zeta) \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash] & & F(\zeta) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

$$\begin{tikzcd}
S(\zeta) \arrow[r, leftrightarrow] \arrow[d, dash] & 1 \arrow[d, dash] \\
H'_{i-1} \arrow[r, leftrightarrow] \arrow[d, dash] & H_{i-1} \arrow[d, dash] \\
H'_i \arrow[r, leftrightarrow] \arrow[d, dash] & H_i \arrow[d, dash] \\
F(\zeta) \arrow[r, leftrightarrow] & H_n
\end{tikzcd}$$

Proposition 3.72. *Let $F \subset K \subset N$ such that N/F is normal and* $\text{Aut}(N/F)$ *is solvable. Then* $\text{Aut}(K/F)$ *is also solvable.*

Proof. Let $H = \text{Aut}(K/F)$ and $H' = \{u \in K : \sigma(u) = u \ \forall \sigma \in H\}$. By Theorem 3.14, K/H' is Galois. Since $H \subset \text{Aut}(K/H')$ and since

$$\text{Aut}(K/H') \cong \text{Aut}(N/H')\big/\text{Aut}(N/K),$$

which is solvable, we conclude that H is solvable. □

$$\begin{tikzcd}
N \arrow[d, dash] \arrow[dd, dash, bend right=60, "\text{normal}"'] \\
K \arrow[d, dash, "\text{Galois}"] \\
H'
\end{tikzcd}$$

Corollary 3.73. *If K/F is solvable by radicals, then* $\text{Aut}(K/F)$ *is solvable.*

Proof. Combine Theorem 3.71 and Proposition 3.72. □

Example. Let $f = x^5 - 4x - 2 \in \mathbb{Q}[x]$ and let K be a splitting field of f over $\mathbb{Q}$. Then $\text{Aut}(K/\mathbb{Q}) \cong S_5$ (Exercise 3.3 (i)), which is not solvable. So the equation $f(x) = 0$ is not solvable by radicals over $\mathbb{Q}$.

Note. Let K/F be algebraic and K' the normal closure of K over F. If $\text{Aut}(K/F)$ is solvable, $\text{Aut}(K'/F)$ is not necessarily solvable. Example: Let u be a root of $f(x) = x^5 - 4x - 2 \in \mathbb{Q}[x]$ and let $K = \mathbb{Q}(u)$. Then $\text{Aut}(K/\mathbb{Q}) = 1$ but $\text{Aut}(K'/\mathbb{Q}) = S_5$. (Proof that $\text{Aut}(K/\mathbb{Q}) = 1$. If $K = \mathbb{Q}(u)$ contains more than one root of f, then $[K' : \mathbb{Q}] \le 3!\,[\mathbb{Q}(u) : \mathbb{Q}] < 5!$, $\rightarrow\leftarrow$.)

3.10. Transcendental Extensions

Algebraic dependence and independence. Let K/F be an extension and $S \subset K$. S is called *algebraically dependent* over F if $\exists s_1, \dots, s_n \in S$ distinct and $0 \ne f \in F[x_1, \dots, x_n]$ such that $f(s_1, \dots, s_n) = 0$. S is called *algebraically independent* over F if it is not algebraically dependent over F.

Fact. Let $S \subset K$ be algebraically independent over F. Then the ring homomorphism $\phi : F(\{x_s : s \in S\}) \to F(S)$ mapping x_s to s is an isomorphism.

Transcendence basis. Let K/F be an extension. A *transcendence basis* of K over F is a maximal subset of K that is algebraically independent over F. By Zorn's lemma, transcendence bases exist.

PROPOSITION 3.74. *Let K/F be an extension and $S \subset K$ algebraically independent over F. Let $u \in K \setminus F(S)$. Then u is transcendental over $F(S) \Leftrightarrow S \cup \{u\}$ is algebraically independent over F.*

PROOF. ($\Rightarrow$) Assume to the contrary that $\exists\, s_1, \dots, s_n \in S$ distinct and $0 \neq f \in F[x_1, \dots, x_n, x_{n+1}]$ such that $f(s_1, \dots, s_n, u) = 0$. Write $f = \sum_{i=0}^m f_i(x_1, \dots, x_n)x_{n+1}^i$, $f_i \in F[x_1, \dots, x_n]$. Then $\sum_{i=0}^m f_i(s_1, \dots, s_n)u^i = 0$. Since u is transcendental over $F(S)$, we have $f_i(s_1, \dots, s_n) = 0$, $1 \le i \le m$. Since $s_1, \dots, s_n$ are algebraically independent over F, $f_i = 0$, $1 \le i \le m$. So $f = 0$, $\rightarrow\leftarrow$.

($\Leftarrow$) Assume $\exists f \in F(S)[x]$ such that $f(u) = 0$. Write

$$f(x) = \sum_{i=1}^m \frac{f_i(s_1, \dots, s_n)}{g_i(s_1, \dots, s_n)}x^i, \qquad f_i, g_i \in F[x_1, \dots, x_n],\ g_i(s_1, \dots, s_n) \neq 0.$$

Let

$$h = \Big(\prod_{i=1}^m g_i(x_1, \dots, x_n)\Big) \sum_{i=1}^m \frac{f_i(x_1, \dots, x_n)}{g_i(x_1, \dots, x_n)}x^i \in F[x_1, \dots, x_n, x].$$

Then $h(s_1, \dots, s_n, u) = 0$. So $h = 0$. Hence

$$0 = h(s_1, \dots, s_n, x) = \Big(\prod_{i=1}^m g_i(s_1, \dots, s_n)\Big)f(x) = 0.$$

So $f = 0$. Therefore u is transcendental over $F(S)$. □

COROLLARY 3.75. *Let K/F be an extension. A subset $S \subset K$ is a transcendence basis of K over F iff*

(i) *S is transcendental over F and*
(ii) *K is algebraic over $F(S)$.*

THEOREM 3.76. *Let K/F be an extension. Then two transcendence bases of K over F have the same cardinality.*

PROOF. Let S and T be two transcendence bases of K/F.

Case 1. $|S| < \infty$, say $S = \{s_1, \dots, s_n\}$.

1° We claim that $\exists\, t_1 \in T$ such that $\{t_1, s_2, \dots, s_n\}$ is a transcendence basis of K/F.

First, $\exists\, t_1 \in T$ such that t_1 is transcendental over $F(s_2, \dots, s_n)$. (Otherwise, $F(s_2, \dots, s_n)(T)/F(s_2, \dots, s_n)$ is algebraic. Since $K/F(T)$ is algebraic, $K/F(s_2, \dots, s_n)(T)$ is algebraic. So $K/F(s_2, \dots, s_n)$ is algebraic. But $s_1 \in K$ is not algebraic over $F(s_2, \dots, s_n)$, $\rightarrow\leftarrow$.) By Proposition 3.74, $\{t_1, s_2, \dots, s_n\}$ is algebraically independent over F.

Next, s_1 is algebraic over $F(t_1, s_2, \dots, s_n)$. (Otherwise, $t_1, s_1, s_2, \dots, s_n$ would be algebraically independent over F, $\rightarrow\leftarrow$.) By Corollary 3.75, $\{t_1, s_2, \dots, s_n\}$ is a transcendence basis of K/F.

2° Using 1° repeatedly, $\exists\, t_1, \dots, t_n \in T$ such that $\{t_1, \dots, t_n\}$ is a transcendence basis of K/F. Thus $T = \{t_1, \dots, t_n\}$. So $|T| = n = |S|$.

Case 2. $|S| = \infty$ and $|T| = \infty$.

$\forall s \in S$, s is algebraic over $F(T)$. Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in F(T)[x]$ be the minimal polynomial of s over $F(T)$. Since $F(T) = \bigcup_{T' \subset T, |T'| < \infty} F(T')$, $\exists\, T_s \subset T$ with $|T_s| < \infty$ such that $a_0, \dots, a_{m-1} \in F(T_s)$. So s is algebraic over $F(T_s)$.

We claim that $\bigcup_{s\in S} T_s$ is a transcendental basis of K/F. First, $\bigcup_{s\in S} T_s$ is algebraically independent over F since it is contained in T. Since $K/F(S)$ and $F(S)/F(\bigcup_{s\in S} T_s)$ are both algebraic, $K/F(\bigcup_{s\in S} T_s)$ is algebraic. Thus $\bigcup_{s\in S} T_s$ is a transcendence basis of K/F. Hence $T = \bigcup_{s\in S} T_s$. Now we have

$$|T| \le \sum_{s\in S} |T_s| \le |S|\aleph_0 = |S|.$$

By symmetry, $|S| \le |T|$. □

Transcendence degree. The *transcendence degree* of K/F, denoted by $\operatorname{tr.d.} K/F$, is the cardinality of any transcendence basis of K/F.

Theorem 3.77. *Let $F \subset K \subset L$ be fields. Then*

$$\operatorname{tr.d.} L/F = \operatorname{tr.d.} L/K + \operatorname{tr.d.} K/F.$$

Proof. Let S be a transcendence basis of K/F and T a transcendence basis of L/K. Then clearly $S \cap T = \emptyset$. It is easy to check that $S \cup T$ is a transcendence basis of L/F. □

Example. $\operatorname{tr.d.} \mathbb{C}/\mathbb{Q} = \aleph$ and $|\operatorname{Aut}(\mathbb{C}/\mathbb{Q})| = \aleph!$ ($= |S_{\mathbb{C}}|$, where $S_{\mathbb{C}}$ is the symmetric group on $\mathbb{C}$).

Proof. Let T be a transcendence basis of $\mathbb{C}/\mathbb{Q}$. Clearly, $|T| = \infty$. Since $\mathbb{C}/\mathbb{Q}(T)$ is algebraic, $|\mathbb{C}| \le |\mathbb{Q}(T)|\aleph_0 = |\mathbb{Q}(T)|$. Let $\mathcal{P}_0(T)$ be the set of all finite subsets of T. Then

$$|\mathbb{Q}(T)| = \Big|\bigcup_{T'\in\mathcal{P}_0(T)} \mathbb{Q}(T')\Big| \le \sum_{T'\in\mathcal{P}_0(T)} |\mathbb{Q}(T')| \le |\mathcal{P}_0(T)|\aleph_0 = |T|\aleph_0 = |T|.$$

So $|\mathbb{C}| \le |T|$. Of course, $|T| \le |\mathbb{C}|$. So $|T| = |\mathbb{C}| = \aleph$.

Every $\rho \in S_T$ induces an automorphism $\bar\rho$ of $\mathbb{Q}(T)$. Since $\mathbb{C}$ is the algebraic closure of $\mathbb{Q}(T)$, $\bar\rho$ extends to an automorphism $\tilde\rho$ of $\mathbb{C}$. The mapping $S_T \to \operatorname{Aut}(\mathbb{C}/\mathbb{Q})$, $\rho \mapsto \tilde\rho$ is 1-1. So $|\operatorname{Aut}(\mathbb{C}/\mathbb{Q})| \ge |S_T| = |S_{\mathbb{C}}| = \aleph!$. Since $\operatorname{Aut}(\mathbb{C}/\mathbb{Q}) < S_{\mathbb{C}}$, we have $|\operatorname{Aut}(\mathbb{C}/\mathbb{Q})| \le \aleph!$. □

3.11. Transcendence of e and π

Entire functions of order $\le \rho$ on $\mathbb{C}$. An entire function $f(z)$ is said to have order $\le \rho$ if $\exists\, C > 0$ such that

$$|f(z)| \le e^{C|z|^\rho} \qquad \text{for all } z \in \mathbb{C}.$$

Equivalently, $|f(z)| = O(C_1^{|z|^\rho})$ as $|z| \to \infty$ for some $C_1 > 1$.

Meromorphic functions of order $\le \rho$ on $\mathbb{C}$. $\frac{f(z)}{g(z)}$ where $f(z)$ and $g(z)$ ($g \ne 0$) are entire functions of order $\le \rho$.

Theorem 3.78 (Lang). *Let K be a number field. Let $f_1, \dots, f_N$ be meromorphic functions of order $\le \rho$ such that*

(i) $\operatorname{tr.d.} K(f_1, \dots, f_N)/K \ge 2$;

(ii) $Df_\alpha \in K[f_1, \dots, f_N]$, $1 \le \alpha \le N$, ($D = \frac{d}{dz}$).

Assume that $w_1, \dots, w_m \in \mathbb{C}$ are distinct such that $f_\alpha(w_j) \in K$ for all $1 \le \alpha \le N$ and $1 \le j \le m$. Then $m \le 10\rho[K : \mathbb{Q}]$.

Proof (Gelfond, Schneider, Lang). 1° *Notation and assumptions.* Let $\mathfrak{o}_K$ be the ring of integers of K. We may assume that $f_\alpha(w_j) \in \mathfrak{o}_K$. (Otherwise, multiply f_α by a suitable integer in $\mathfrak{o}_K$.)

Let $t \in \mathbb{Z}^+$, $n = 2mt^2$, $r = 2mt$. $O(\ )$ means $O(\ )$ as $t \to +\infty$. Constants, denoted by $C_1, C_2, \dots$, are positive real numbers depending only on the data in the statement of the theorem. Let $\operatorname{Iso}(K/\mathbb{Q})$ denote the set of all isomorphisms of K into $\mathbb{C}$. For each $x \in K$, let

$$||x|| = \max\{|\phi(x)| : \phi \in \operatorname{Iso}(K/\mathbb{Q})\}.$$

Assume that f_1 and f_2 are algebraically independent over K.

2° We claim that there exists a constant $C_1 >$ such that

$$||D^k(f_1^u f_2^v)(w_j)|| \le k! r^k C_1^{k+r} \quad \text{for all } k \ge 0,\ 1 \le u, v \le r,\ 1 \le j \le m. \tag{3.26}$$

Let $h_1 = \cdots = h_u = f_1$ and $h_{u+1} = \cdots = h_{u+v} = f_2$. Then

$$\begin{aligned}(3.27)\quad & ||D^k(f_1^u f_2^v)(w_j)|| \\ &= \Big|\Big| \sum_{k_1+\cdots+k_{u+v}=k} \binom{k}{k_1, \cdots, k_{u+v}} D^{k_1}h_1(w_j)\cdots D^{k_{u+v}}h_{u+v}(w_j)\Big|\Big| \\ &\le (u+v)^k \max\big\{||D^{k_1}h_1(w_j)||\cdots||D^{k_{u+v}}h_{u+v}(w_j)|| : k_1+\cdots+k_{u+v}=k\big\}.\end{aligned}$$

Let

$$D\begin{bmatrix} f_1 \\ \vdots \\ f_N \end{bmatrix} = \begin{bmatrix} P_1(f_1, \dots, f_N) \\ \vdots \\ P_N(f_1, \dots, f_N) \end{bmatrix}, \qquad P_\alpha \in K[X_1, \dots, X_N].$$

By induction (or by Theorem 3.81), for each $l > 0$, $(D^l f_\alpha)(w_j)$ is a sum of $(l-1)!N^{l-1}$ terms of the form

$$\Big[\frac{\partial^{i_1} P_{\alpha_1}}{\partial X_{\beta(1,1)}\cdots\partial X_{\beta(1,i_1)}} \cdots \frac{\partial^{i_{l-1}} P_{\alpha_{l-1}}}{\partial X_{\beta(l-1,1)}\cdots\partial X_{\beta(l-1,i_{l-1})}} P_{\alpha_l}\Big](f_1(w_j), \dots, f_N(w_j)), \tag{3.28}$$

where $i_1, \dots, i_{l-1} \in \mathbb{N}$ and $i_1 + \cdots + i_{l-1} = l-1$. Put

$$\begin{aligned} C = \max\Big\{ \Big|\Big| \frac{\partial^i P_\alpha}{\partial X_{\beta_1}\cdots\partial X_{\beta_i}}(f_1(w_j), \dots, f_N(w_j))\Big|\Big| : \\ i \ge 0,\ 1 \le \alpha, \beta_1, \dots, \beta_i \le N,\ 1 \le j \le m\Big\}. \end{aligned}$$

Then

$$||D^l f_\alpha(w_j)|| \le (l-1)!N^{l-1}C^l, \quad l > 0,\ 1 \le \alpha \le N,\ 1 \le j \le m.$$

Including the case $l = 0$, we have

$$||D^l f_i(w_j)|| \le l!N^l(C + C')^{l+1}, \quad l \ge 0,\ 1 \le i \le N,\ 1 \le j \le m, \tag{3.29}$$

where

$$C' = \max\{||f_\alpha(w_j)|| : 1 \le \alpha \le N,\ 1 \le j \le m\}.$$

By (3.27) and (3.29),

$$\begin{aligned}&||D^k(f_1^u f_2^v)(w_j)||\\ &\le (2r)^k \max\{k_1!\cdots k_{u+v}!N^{u+v}(C+C')^{k+u+v} : k_1+\cdots+k_{u+v}=k\}\\ &\le k!r^k C_1^{k+r}.\end{aligned}$$

3° Choose $0 \ne \lambda \in \mathfrak{o}_K$ such that

$$\lambda \frac{\partial^i P_\alpha}{\partial X_{\beta_1}\cdots\partial X_{\beta_i}}(f_1(w_j),\dots,f_N(w_j)) \in \mathfrak{o}_K$$

for all $i \ge 0$, $1 \le \alpha, \beta_1, \dots, \beta_i \le N$, $1 \le j \le m$. By (3.28), we have

$$\lambda^l D^l f_\alpha(w_j) \in \mathfrak{o}_K, \qquad l \ge 0,\ 1 \le \alpha \le N,\ 1 \le j \le m. \tag{3.30}$$

(Recall that we assumed $f_\alpha(w_j) \in \mathfrak{o}_K$.) It follows that

$$\lambda^k D^k(f_1^u f_2^v)(w_j) \in \mathfrak{o}_K, \qquad k \ge 0,\ 1 \le u,v \le r,\ 1 \le j \le m.$$

By 2°,

$$\begin{aligned}||\lambda^k D^k(f_1^u f_2^v)(w_j)|| \le ||\lambda||^k k! r^k C_1^{k+r} \le k! r^k C_2^{k+r},&\\ k \ge 0,\ 1 \le u,v \le r,\ 1 \le j \le m.&\end{aligned} \tag{3.31}$$

4° We claim that $\exists\, b_{uv} \in \mathfrak{o}_K$ $(1 \le u,v \le r)$ not all 0 such that

$$\sum_{u,v=1}^{r} b_{uv} D^k(f_1^u f_2^v)(w_j) = 0, \qquad 0 \le k < n,\ 1 \le j \le m, \tag{3.32}$$

and

$$\max\{||b_{uv}|| : 1 \le u,v \le r\} = O(n^{2n}). \tag{3.33}$$

Write $\Delta_{uv,kj} = \lambda^k D^k(f_1^u f_2^v)(w_j) \in \mathfrak{o}_K$. Then (3.32) is equivalent to

$$\sum_{u,v=1}^{r} \Delta_{uv,kj} b_{uv} = 0, \qquad 0 \le k < n,\ 1 \le j \le m. \tag{3.34}$$

$\mathfrak{o}_K$ is a free $\mathbb{Z}$-module of rank $M := [K:\mathbb{Q}]$. Let $\epsilon_1, \dots, \epsilon_M$ be a basis of $\mathfrak{o}_K$ over $\mathbb{Z}$. Write

$$\Delta_{uv,kj} = \sum_{l=1}^{M} \xi_{uv,kj,l}\epsilon_l, \qquad \xi_{uv,kj,l} \in \mathbb{Z},$$

$$b_{uv} = \sum_{l=1}^{M} c_{uv,l}\epsilon_l, \qquad c_{uv,l} \in \mathbb{Z}. \tag{3.35}$$

Then (3.34) is a system of nmM linear equations in r^2M unknowns $c_{uv,l}$, i.e.,

$$A[c_{uv,l}] = 0, \tag{3.36}$$

where $[c_{uv,l}]$ is an $r^2M \times 1$ column and A is an $nmM \times r^2M$ matrix whose entries are linear combinations of $\xi_{uv,kj,l}$ over $\mathbb{Z}$. More precisely, the $((k,j,l),(u,v,l''))$ entry of A is $\sum_{l'=1}^{M} a_l^{l'l''}\xi_{uv,kj,l'}$, where $a_l^{l'l''}$ is defined by

$$\epsilon_{l'}\epsilon_{l''} = \sum_{l=1}^{M} a_l^{l'l''}\epsilon_l.$$

Let $\epsilon_1',\dots,\epsilon_M'$ be the dual basis of $\epsilon_1,\dots,\epsilon_M$ with respect $\mathrm{Tr}_{K/\mathbb{Q}}$. Then $\xi_{uv,kj,l} = \mathrm{Tr}_{K/\mathbb{Q}}(\Delta_{uv,kj}\epsilon_l')$. So, by (3.31),

$$\begin{aligned} |\xi_{uv,kj,l}| &\le C_3||\Delta_{uv,kj}|| \le k!r^kC_4^{k+r} \le n!r^nC_4^{n+r}, \\ &0 \le k < n,\ 1 \le u,v \le r,\ 1 \le j \le m. \end{aligned}$$

Thus all the entries of A have $|\ | \le n!r^nC_5^{n+r}$. Let $L \in \mathbb{Z}^+$ to be chosen. $A : \mathbb{Z}^{r^2M} \to \mathbb{Z}^{nmM}$ maps $[-L,L]^{r^2M}$ to $[-n!r^nC_5^{n+r}r^2ML,\ n!r^nC_5^{n+r}r^2ML]^{nmM} \subset [-Ln!r^{n+2}C_6^{n+r},\ Ln!r^{n+2}C_6^{n+r}]^{nmM}$. Therefore, if

$$(2L+1)^{r^2M} > (2Ln!r^{n+2}C_6^{n+r}+1)^{nmM}, \tag{3.37}$$

(3.36) has a nonzero integer solution $[c_{uv,l}] \in [-L,L]^{r^2M}$. (3.37) holds when

$$(2L)^{r^2M} > (3Ln!r^{n+2}C_6^{n+r})^{nmM},$$

i.e.,

$$2^{r^2M}L^{(r^2-nm)M} > (3n!r^{n+2}C_6^{n+r})^{nmM}. \tag{3.38}$$

Since $r^2 - nm = nm$, (3.38) holds when we choose

$$L = 3n!r^{n+2}C_6^{n+r} = 3n!(2nm)^{\frac{1}{2}(n+2)}C_6^{n+r} = O(n^{2n}).$$

Then by (3.35),

$$\max\{||b_{uv}|| : 1 \le u,v \le r\} = O(n^{2n}).$$

5° Define a meromorphic function

$$F = \sum_{u,v=1}^{r} b_{uv}f_1^uf_2^v.$$

(Note. F depends on r hence on t.) By 4°,

$$D^kF(w_j) = 0 \qquad \text{for all } 0 \le k < n,\ 1 \le j \le m.$$

But $F \neq 0$ since f_1, f_2 are algebraically independent over K. Let $s \ge n$ be the smallest integer such that

$$D^kF(w_j) = 0 \qquad \text{for all } 0 \le k < s,\ 1 \le j \le m.$$

Assume, without loss of generality, that

$$\gamma := D^sF(w_1) \neq 0.$$

By (3.30), $\lambda^s\gamma \in \mathfrak{o}_K$; hence

$$1 \le |\mathrm{N}_{K/\mathbb{Q}}(\lambda^s\gamma)| \le ||\lambda||^{s[K:\mathbb{Q}]}|\mathrm{N}_{K/\mathbb{Q}}(\gamma)|. \tag{3.39}$$

By (3.26) and (3.33),

$$||\gamma|| = \Big|\Big| \sum_{u,v=1}^{r} b_{uv}D^s(f_1^uf_2^v)(w_j)\Big|\Big| = O(r^2n^{2n}s!r^sC_1^{n+s}) = O(s^{5s}). \tag{3.40}$$

By (3.39) and (3.40),

$$1 \le ||\lambda||^{s[K:\mathbb{Q}]}O(s^{5s})^{[K:\mathbb{Q}]-1}|\gamma|. \tag{3.41}$$

6° There exist entire functions $p(z)$ and $q(z)$ of order $\le \rho$ such that pf_1 and qf_2 are entire functions of order $\le \rho$. We may assume that $p(w_1) \neq 0$ and $q(w_1) \neq 0$.

Let $\theta = pq$. Then θ is an entire function of order $\le \rho$ and $\theta f_1, \theta f_2$ are both entire functions order $\le \rho$. Clearly,

$$H(z) := \frac{\theta(z)^{2r} F(z)}{\prod_{j=1}^{m} (z - w_j)^s} \tag{3.42}$$

is an entire function. Let $R > 0$ be large. When $|z| = R$,

$$\begin{aligned} |\theta(z)^{2r} F(z)| &= \Big| \sum_{u,v=1}^{r} b_{uv} \big[(\theta f_1)(z)\big]^u \big[(\theta f_2)(z)\big]^v \big[\theta(z)\big]^{2r-(u+v)} \Big| \\ &\le r^2 O(n^{2n}) C_7^{2rR^\rho} \\ &\le O(s^{2s} C_8^{2rR^\rho}). \end{aligned}$$

By the maximum modulus principle,

$$\max\{|H(z)| : |z| \le R\} \le O\Big(\frac{s^{2s} C_8^{2rR^\rho}}{R^{ms}}\Big).$$

Let $R = s^{\frac{1}{2\rho}}$ and $z = w_1$, we have

$$|H(w_1)| \le O\Big(\frac{s^{2s} C_8^{2rs^{\frac{1}{2}}}}{s^{\frac{ms}{2\rho}}}\Big) = O\Big(\frac{s^{2s} C_8^{2\sqrt{2mns}}}{s^{\frac{ms}{2\rho}}}\Big) \le O\Big(\frac{s^{2s} C_9^s}{s^{\frac{ms}{2\rho}}}\Big).$$

From (3.42), it is clear that

$$|\gamma| = |D^s F(w_1)| = O(s! C_{10}^s) |H(w_1)| \le O\Big(\frac{s^{3s} C_{11}^s}{s^{\frac{ms}{2\rho}}}\Big). \tag{3.43}$$

Now combine (3.41) and (3.43), we have

$$1 \le O\Big(C_{12}^s \frac{s^{5s([K:\mathbb{Q}]-1)+3s}}{s^{\frac{ms}{2\rho}}}\Big) \le O(C_{12}^s s^{s(5[K:\mathbb{Q}]-\frac{m}{2\rho})}).$$

So, $5[K:\mathbb{Q}] - \frac{m}{2\rho} \ge 0$, i.e., $m \le 10\rho[K:\mathbb{Q}]$. □

Corollary 3.79 (Hermite-Lindemann). *If $\alpha \in \mathbb{C}^\times$ is algebraic, then e^α is transcendental.*

Proof. In Theorem 3.78, let $f_1(z) = z$, $f_2(z) = e^z$. Assume to the contrary that e^α is algebraic. Then in Theorem 3.78, we can let $w_j = j\alpha$, $j = 0, 1, 2, \dots$, $\rightarrow\leftarrow$. □

Corollary 3.80. *e and π are transcendental.*

Proof. If π were algebraic, by Corollary 4.1, $e^{2\pi i} = 1$ would be transcendental. □

Derivatives of the solution of the Cauchy problem. For $k \in \mathbb{Z}^+$, let

$$\mathfrak{I}_k = \big\{(i_1, \dots, i_k) \in \mathbb{N}^k : i_1 + \dots + i_t \ge t,\ 1 \le t \le k,\ i_1 + \dots + i_k = k\big\}.$$

Also define $\mathfrak{I}_0 = \{\emptyset\}$. For $(j_1, \dots, j_{k-1}) \in \mathbb{N}^{k-1}$ and $(i_1, \dots, i_k) \in \mathbb{N}^k$, say $(j_1, \dots, j_{k-1}) \prec (i_1, \dots, i_k)$ if $(i_1, \dots, i_k) = (j_1, \dots, j_{l-1}, j_l + 1, 0, j_{l+1}, \dots, j_{k-1})$ for some $1 \le l \le k-1$ or $(i_1, \dots, i_k) = (j_1, \dots, j_{k-1}, 1)$.

Note. If $(j_1, \dots, j_{k-1}) \prec (i_1, \dots, i_k)$, then $(j_1, \dots, j_{k-1}) \in \mathfrak{I}_{k-1} \Leftrightarrow (i_1, \dots, i_k) \in \mathfrak{I}_k$.

THEOREM 3.81. *Let $D = \frac{d}{dz}$, where z is either a real or a complex variable. Consider the Cauchy problem*

$$D\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} P_1(y_1,\dots,y_n) \\ \vdots \\ P_n(y_1,\dots,y_n) \end{bmatrix}, \qquad \begin{bmatrix} y_1(0) \\ \vdots \\ y_n(0) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{3.44}$$

where $P_1, \dots, P_n$ have continuous partial derivatives of total order up to k in a neighborhood of $(0, \dots, 0)$. Then the $(k+1)$st derivatives of a solution of (3.44) *in a neighborhood of $(0, \dots, 0)$ is given by*

(3.45)

$$D^{k+1}\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} =$$

$$\sum_{(i_1,\dots,i_k)\in\mathfrak{I}_k} a(i_1,\dots,i_k)\frac{\partial^{i_1}\boldsymbol{P}}{\partial\boldsymbol{y}^{i_1}}\Big(I_{n^{i_1-1}} \otimes \frac{\partial^{i_2}\boldsymbol{P}}{\partial\boldsymbol{y}^{i_2}}\Big)\cdots\Big(I_{n^{i_1+\cdots+i_{k-1}-(k-1)}} \otimes \frac{\partial^{i_k}\boldsymbol{P}}{\partial\boldsymbol{y}^{i_k}}\Big)\boldsymbol{P},$$

where

(i)

$$\boldsymbol{P} = \begin{bmatrix} P_1(y_1,\dots,y_n) \\ \vdots \\ P_n(y_1,\dots,y_n) \end{bmatrix};$$

(ii) $\frac{\partial^i \boldsymbol{P}}{\partial \boldsymbol{y}^i}$ *is an $n \times n^i$ matrix whose columns are indexed by $(\beta_1, \dots \beta_i) \in \{1, \dots, n\}^i$ lexicographically and whose $(\alpha, (\beta_1, \dots, \beta_i))$-entry is*

$$\frac{\partial^i P_\alpha}{\partial y_{\beta_1} \cdots \partial y_{\beta_i}};$$

(iii) *$a(i_1, \dots, i_k) \in \mathbb{Z}^+$, $(i_1, \dots, i_k) \in \mathfrak{I}_k$, are defined inductively by*

$$\begin{cases} a(i_1,\dots,i_k) = \sum_{(j_1,\dots,j_{k-1})\prec(i_1,\dots,i_k)} a(j_1,\dots,j_{k-1}), \\ a(\emptyset) = 1. \end{cases}$$

Moreover,

$$\sum_{(i_1,\dots,i_k)\in\mathfrak{I}_k} a(i_1,\dots,i_k) = k!.$$

PROOF. For $(i_1, \dots, i_k) \in \mathfrak{I}_k$, let $i_{k+1} = 0$ and let

$$F_{(i_1,\dots,i_k,0)} = \prod_{l=1}^{k+1}\Big(I_{n^{i_1+\cdots+i_{l-1}-(l-1)}} \otimes \frac{\partial^{i_l}\boldsymbol{P}}{\partial\boldsymbol{y}^{i_l}}\Big), \tag{3.46}$$

where the factors in the product appear from left to right in the order of $l = 1, 2, \dots, k+1$. Then (3.45) can be written as

$$D^{k+1}\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \sum_{(i_1,\dots,i_k)\in\mathfrak{I}_k} a(i_1,\dots,i_k)F_{(i_1,\dots,i_k,0)}. \tag{3.47}$$

To prove (3.47), we use induction on k. The initial case $k = 0$ needs no proof. Since

$$D\Big(\frac{\partial^i P_\alpha}{\partial y_{\beta_1} \cdots \partial y_{\beta_i}}\Big) = \sum_{\beta_{i+1}} \frac{\partial^{i+1} P_\alpha}{\partial y_{\beta_1} \cdots \partial y_{\beta_i} \partial y_{\beta_{i+1}}} D y_{\beta_{i+1}} = \sum_{\beta_{i+1}} \frac{\partial^{i+1} P_\alpha}{\partial y_{\beta_1} \cdots \partial y_{\beta_i} \partial y_{\beta_{i+1}}} P_{\beta_{i+1}},$$

we have

$$D\Big(\frac{\partial^i \boldsymbol{P}}{\partial \boldsymbol{y}^i}\Big) = \frac{\partial^{i+1} \boldsymbol{P}}{\partial \boldsymbol{y}^{i+1}} (I_{n^i} \otimes \boldsymbol{P}).$$

Thus

$$\begin{aligned} & D\Big[I_{n^{i_1+\cdots+i_{l-1}-(l-1)}} \otimes \frac{\partial^{i_l} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_l}}\Big] \\ &= I_{n^{i_1+\cdots+i_{l-1}-(l-1)}} \otimes \Big[\frac{\partial^{i_l+1} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_l+1}} (I_{n^{i_l}} \otimes \boldsymbol{P})\Big] \\ &= \Big[I_{n^{i_1+\cdots+i_{l-1}-(l-1)}} \otimes \frac{\partial^{i_l+1} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_l+1}}\Big] \big[I_{n^{i_1+\cdots+i_{l-1}+(i_l+1)-l}} \otimes \boldsymbol{P}\big]. \end{aligned} \tag{3.48}$$

By (3.46) and (3.48), we have

$$\begin{aligned} & DF_{(i_1,\ldots,i_k,0)} \\ &= \sum_{l=1}^{k+1} \Big[\prod_{s=1}^{l-1} \Big(I_{n^{i_1+\cdots+i_{s-1}-(s-1)}} \otimes \frac{\partial^{i_s} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_s}}\Big)\Big] \Big[D\Big(I_{n^{i_1+\cdots+i_{l-1}-(l-1)}} \otimes \frac{\partial^{i_l} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_l}}\Big)\Big] \\ & \quad \Big[\prod_{s=l+1}^{k+1} \Big(I_{n^{i_1+\cdots+i_{s-1}-(s-1)}} \otimes \frac{\partial^{i_s} \boldsymbol{P}}{\partial \boldsymbol{y}^{i_s}}\Big)\Big] \\ &= \sum_{l=1}^{k+1} F_{(i_1,\ldots,i_{l-1},i_l+1,0,i_{l+1},\ldots,i_k,0)}. \end{aligned}$$

Therefore, assuming (3.47), we have

$$\begin{aligned} D^{k+2} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} &= \sum_{(i_1,\ldots,i_k)\in\mathfrak{I}_k} a(i_1,\ldots,i_k) \sum_{l=1}^{k+1} F_{(i_1,\ldots,i_{l-1},i_l+1,0,i_{l+1},\ldots,i_k,0)} \\ &= \sum_{(j_1,\ldots,j_{k+1})\in\mathfrak{I}_{k+1}} a(j_1,\ldots,j_{k+1}) F_{(j_1,\ldots,j_{k+1},0)}, \end{aligned}$$

where

$$a(j_1,\ldots,j_{k+1}) = \sum_{(i_1,\ldots,i_k)\prec(j_1,\ldots,j_{k+1})} a(i_1,\ldots,i_k).$$

So the induction is complete.

Since $a(i_1,\ldots,i_k)$ is the number of chains $\emptyset = \alpha_0 \prec \alpha_1 \prec \cdots \prec \alpha_k = (i_1,\ldots,i_k)$, where $\alpha_l \in \mathfrak{I}_l$, $0 \le l \le k$, and since for each $\alpha_l \in \mathfrak{I}_l$, there are exactly l $\alpha_{l+1} \in \mathfrak{I}_{l+1}$ such that $\alpha_l \prec \alpha_{l+1}$, we have

$$\sum_{(i_1,\ldots,i_k)\in\mathfrak{I}_k} a(i_1,\ldots,i_k) = k!.$$

□

NOTE. For a formula for $a(i_1,\ldots,i_k)$, see [**10**].

Exercises

3.1. Let $F \subset K$ be fields and let M, N be two intermediate fields between F and K such that $[M : F] = m < \infty$ and $[N : F] = n < \infty$. Let $[M \cap N : F] = l$. Prove that

$$[MN : F] \le mn - (l-1)(m+n-l).$$

3.2. Let $F \subset L \subset K$ be fields such that K/F is algebraic and Galois. Then the following hold.

(i) K/L is Galois.

(ii) L/F is Galois $\Leftrightarrow$ $\mathrm{Aut}(K/L) \lhd \mathrm{Aut}(K/F)$. Moreover, if L/F is Galois, then $\mathrm{Aut}(L/F) \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$.

3.3. (i) Let p be a prime. Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p which has precisely two non real roots in $\mathbb{C}$. Prove that the Galois group of f over $\mathbb{Q}$ is S_p.

(ii) Show that for every prime p, there is an $f \in \mathbb{Q}[x]$ satisfying the conditions in (i).

3.4. Let $\mathrm{char}\, F = 2$. Assume that $f(x) = x^4 + ax^2 + b \in F[x]$ is irreducible such that $b \notin F^2$ and $a + c^2 b \notin F^2$ for all $c \in F$. (Example. $F = \mathbb{F}_2(y, z)$, where y, z are independent indeterminates. $f(x) = x^4 + yx^2 + z$.) Let u be a root of f. Prove that in $F(u)$, the largest separable extension over F is $F(u^2)$ and the largest purely inseparable extension over F is F.

3.5. Determine the Galois group $\mathrm{Aut}(\mathbb{Q}(i, 3^{1/6})/\mathbb{Q}(i))$.

3.6. Compute the cyclotomic polynomial Φ_{30} over $\mathbb{Q}$.

3.7. Let $n > 2$ and let ζ be a primitive nth root of unity over $\mathbb{Q}$. Prove that $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \phi(n)/2$. (Hint: Let $u = \zeta + \zeta^{-1}$. Then $\zeta^2 - u\zeta + 1 = 0$.)

3.8. Prove that $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ is onto.

3.9. Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n. Prove that in $\mathbb{F}_{q^m}[x]$, $f(x)$ factors as a product of t irreducible polynomials of degree n/t where $t = (n, m)$.

3.10. (Compare with Proposition 3.9 (v) and the fundamental theorem of Galois theory (ii).) Let $F \subset K$ be fields and $L, M \in \mathcal{F}(K/F)$, $H, J \in \mathcal{G}(K/F)$.

(i) Prove that $(L \cap M)' \supset \langle L' \cup M' \rangle$ and give an example in which $(L \cap M)' \supsetneq \langle L' \cup M' \rangle$.

(ii) Prove that $(H \cap J)' \supset H'J'$ and give an example in which $(H \cap J)' \supsetneq H'J'$.

3.11. (Lagrange theorem on natural irrationalities) Let $F \subset K$ be fields and let L and M be two intermediate fields such that L/F is finite and Galois. The LM is a finite Galois extension over M and $\mathrm{Aut}(LM/M) \cong \mathrm{Aut}(L/L \cap M)$.

3.12. (Irreducibility of $x^n - a$) Let F be a field, $a \in F$, and $n \in \mathbb{Z}^+$. Then $x^n - a$ is irreducible in $\mathbb{F}[x]$ if and only the following two conditions both hold.

(i) For every prime $p \mid n$, $a \notin F^p = \{u^p : u \in F\}$.

(ii) If $4 \mid n$, then $a \notin -4F^4$.

CHAPTER 4

Noncommutative Rings

4.1. The Jacobson Radical

Definition 4.1. Let R be a ring. The *Jacobson radical* of R is

$$J(R)=\bigcap_{\substack{I\text{ is a max.}\\ \text{left ideal of }R}} I.$$

It will be shown that $J(R)$ is a two-sided ideal (Corollary 4.3). R is called *J-semisimple* if $J(R)=0$.

Fact. $J(R/J(R))=0$, i.e., $R/J(R)$ is always J-semisimple.

Proof. Let $\mathcal{I}$ be the set of all maximal left ideals of R. Then $\{I/J(R) : I\in\mathcal{I}\}$ is the set of all maximal left ideals of $R/J(R)$. So,

$$J\big(R/J(R)\big)=\bigcap_{I\in\mathcal{I}}\big(I/J(R)\big)=\Big(\bigcap_{I\in\mathcal{I}}I\Big)/J(R)=0.$$

□

Example. Let $R=M_n(D)$ be the ring of $n\times n$ matrices over a division ring D. For each $1\le j\le n$, let

$$J_j=\big\{[a_1\ \cdots\ a_{j-1}\ 0\ a_{j+1}\ \cdots\ a_n]\in M_n(D)\big\}.$$

Then J_j is a left ideal of R. $R/J_j\cong D^n$. We claim that R/J_j is a simple R-module. Let $0\ne\alpha\in R/J_j$. Then $\alpha=[0\ \ldots\ \underset{j}{a}\ \ldots\ 0]+J_j$, where $0\ne a\in D^n$. For each $x\in D^n$, $\exists A\in R$ such that $Aa=x$. Then $[0\ \ldots\ \underset{j}{x}\ \ldots\ 0]+J_j=A\alpha\in R\alpha$. So $R\alpha=R/J_j$.

Therefore, J_j is a maximal left ideal of R. Thus $J(R)\subset\bigcap_{j=1}^n J_j=0$.

Proposition 4.2. *Let R be a ring and let $x\in R$. Then the following statements are equivalent.*

(i) *$x\in J(R)$.*
(ii) *$\forall r\in R$, $1-rx$ has a left inverse in R.*
(iii) *For each simple module ${}_RM$, $xM=0$.*

Proof. (i) $\Rightarrow$ (ii) Suppose to the contrary that $1-rx$ does not have a left inverse. Then $R(1-rx)$ is a proper left ideal of R. So $R(1-rx)$ is contained in a maximal left ideal I of R. Then $1=(1-rx)+rx\in I+J(R)\subset I$, $\rightarrow\leftarrow$.

(ii) $\Rightarrow$ (iii) Assume to the contrary that $xM\ne0$. Choose $m\in M$ such that $xm\ne0$. Since M is simple, we have $Rxm=M$. So $\exists r\in R$ such that $rxm=m$, i.e. $(1-rx)m=0$. Then $1-rx$ is not left invertible, $\rightarrow\leftarrow$.

(iii) $\Rightarrow$ (i) Let I be a maximal left ideal of R. Then R/I is a simple R-module. So $x(R/I)=0$. Thus $x\in I$. So $x\in\bigcap_{I\text{ is a max. left ideal of }R}I=J(R)$. □

Corollary 4.3. *We have*

$$J(R) = \bigcap_{\substack{{}_RM \text{ is a simple} \\ \text{left } R\text{-module}}} \operatorname{ann}(M). \tag{4.1}$$

In particular, $J(R)$ is a two-sided ideal of R.

Proof. Proposition 4.2 (i) $\Leftrightarrow$ (iii). □

Proposition 4.4. *Let R be a ring and $x \in R$. Then $x \in J(R) \Leftrightarrow \forall r \in R$, $1 - rx$ is a unit of R.*

Proof. ($\Rightarrow$) By Proposition 4.2 (ii), $\exists u \in R$ such that $u(1-rx) = 1$. So, $u = 1 + urx$, which has a left inverse by Proposition 4.2 (ii). Thus u is a unit of R and $1 - rx = u^{-1}$. □

Corollary 4.5. *In Definition 4.1, Proposition 4.2 and Corollary 4.3, "left" can be replaced with "right".*

Proof. In Proposition 4.2 (ii), "left" can be dropped (Proposition 4.4). Also $1 - rx$ is a unit $\Leftrightarrow$ $1 - xr$ is a unit. □

Nil and nilpotent ideals. A left ideal I of R is called *nil* if for each $a \in I$, $\exists n > 0$ such that $a^n = 0$; I is called *nilpotent* if $I^n = 0$ for some $n > 0$. (I^n is the left ideal generated by $\{a_1 \cdots a_n : a_i \in I\}$.) I is nilpotent $\Rightarrow$ I is nil.

Proposition 4.6 (Levitsky). *Let R be a left noetherian ring and I a left or right ideal of R. Then I is nil $\Leftrightarrow$ I is nilpotent.*

Proof. Exercise. □

Nil radical. The *nil radical* of a ring R, denoted by $N(R)$, is the sum of all nil ideals of R. If R is commutative, $N(R)$ is the set all nilpotent elements of R.

Proposition 4.7.

(i) *$N(R) \subset J(R)$.*

(ii) *Assume R is left artinian. Then $J(R)$ is nilpotent and $J(R) = N(R)$. Moreover, $J(R) = N(R)$ is the unique maximal nil left (right) ideal of R.*

Proof. (i) Let I be a nil ideal of R. $\forall x \in I$ and $r \in R$, $rx \in I$. So, $(rx)^n = 0$ for some $n > 0$. Then $1 - rx$ has a left inverse since $\big(1 + rx + \cdots + (rx)^{n-1}\big)(1 - rx) = 1$. So $x \in J(R)$. Thus $I \subset J(R)$.

(ii) We first show that $J(R)$ is a nilpotent ideal. Let $J = J(R)$. Apply DCC to $J \supset J^2 \supset \cdots$. We have $J^m = J^{m+1}$ for some $m > 0$. Let $I = J^m$. Then $I^2 = I$. It suffices to show that $I = 0$. Assume to the contrary that $I \neq 0$. Let $\mathcal{A}$ be the set of all left ideals A of R such that $IA \neq 0$. Then $\mathcal{A} \neq \emptyset$ ($I \in \mathcal{A}$). Since R is left artinian, $\mathcal{A}$ has a minimal element A_0. Choose $a \in A_0$ such that $Ia \neq 0$. Then $I(Ia) \neq 0$, i.e., $Ia \in \mathcal{A}$. By the minimality of A_0, we have $Ia = A_0$. So $\exists r \in I$ such that $ra = a$. Then $(1 - r)a = 0$, so $1 - r$ is not left invertible. This is a contradiction since $r \in I \subset J(R)$.

Since $J(R)$ is nilpotent, $J(R) \subset N(R)$. By (i), $J(R) = N(R)$. Let I be a maximal nil left (or right) ideal of R. Then for all $x \in I$ and $r \in R$, rx is nilpotent. Thus $1 - rx$ is invertible, so $x \in J(R)$. Hence $I \subset J(R)$. Since $J(R)$ is nilpotent, we must have $I = J(R)$. □

Example. Let R be a PID and $a = p_1^{e_1} \cdots p_n^{e_n} \in R$, where $p_1, \dots, p_n$ are distinct primes in R and $e_i > 0$, $1 \le i \le n$. Then

$$N\big(R/(a)\big) = J\big(R/(a)\big) = (p_1 \cdots p_n)/(a).$$

Proof. $(p_1 \cdots p_n)/(a)$ is the set of all nilpotent elements of $R/(a)$, so $N(R/(a)) = (p_1 \cdots p_n)/(a)$. $R/(a)$ has DCC, so $J(R/(a)) = N(R/(a))$. □

Theorem 4.8 (Nakayama's Lemma). *Let ${}_RM$ be a finitely generated R-module such that $J(R)M = M$. Then $M = 0$.*

Proof. Assume to the contrary that $M \neq 0$. Let $m_1, \dots, m_n$ be a minimal set of generators of M. Since $J(R)M = M$, we have

$$m_1 = r_1 m_1 + \cdots + r_n m_n, \qquad r_i \in J(R).$$

The $(1 - r_1)m_1 = r_2 m_2 + \cdots + r_n m_n$. Since $r_1 \in J(R)$, $1 - r_1$ has a left inverse u. Then $m_1 = ur_2 m_2 + \cdots + ur_n m_n$. So $M = \langle m_2, \dots, m_n \rangle$, $\rightarrow\leftarrow$. □

4.2. Structure of Semisimple Rings

Definition 4.9. A module ${}_RM$ is called *semisimple* if it is a direct sum of simple modules. A ring R is called left semisimple if ${}_RR$ is a semisimple modules, i.e., ${}_RR$ is a direct sum of certain minimal left ideals of R.

Proposition 4.10. *Let M be a left R-module. The following statements are equivalent.*

(i) *M is semisimple.*
(ii) *M is a sum of simple submodules.*
(iii) *Every submodule of M is a direct summand of M.*

Proof. (i) $\Rightarrow$ (ii). Obvious.

(ii) $\Rightarrow$ (iii) Assume $M = \sum_{i \in I} M_i$, where each M_i is a simple submodule of M. Let N be a submodule of M. By Zorn's lemma, $\exists$ a maximal subset $J \subset I$ such that $N + \sum_{i \in J} M_i = N \oplus \sum_{i \in J} M_i$. It suffices to show that $N \oplus \sum_{i \in J} M_i = M$. Assume the contrary. Then $\exists k \in I$ such that $M_k \not\subset N + \sum_{\in J} M_i$. Then $M_k \cap (N \oplus \sum_{i \in J} M_i) = \{0\}$. So $N + (M_k + \sum_{i \in J} M_i) = N \oplus (M_k \oplus \sum_{i \in J} M_i)$, which contradicts the maximality of J.

(iii) $\Rightarrow$ (i).

1° Every nonzero submodule A of M contains a simple submodule.

Let $0 \neq a \in A$. We may assume $A = Ra$ (since it suffices to show that Ra contains a simple submodule). Then $A \cong R/L$, where $L = \text{ann}(a)$. L is contained in a maximal left ideal K of R. Then K/L is a maximal submodules of R/L. So A contains a maximal submodules B. Write $M = B \oplus C$. Then $A = B \oplus (C \cap A)$. Since B is a maximal submodule of A, $C \cap A$ must be a minimal submodules of A.

2° M is semisimple.

Let $\{M_i : i \in I\}$ be the set of all simple submodules of M. By Zorn's lemma, $\exists$ a maximal subset $J \subset I$ such that $\sum_{i \in J}$ is a direct sum. We claim that $\sum_{i \in J} M_i = M$. Otherwise, $M = A \oplus \sum_{i \in J} M_i$ for some nonzero submodule A of M. By 1°, $A \supset M_k$ for some $k \in I$. Then $\sum_{i \in J \cup \{k\}} M_i$ is a direct sum, which contradicts the maximality of J. □

Proposition 4.11.

(i) *Submodules and quotient modules of a semisimple module are semisimple.*

(ii) *If R is a left semisimple ring, then every left R-module is semisimple.*

Proof. (i) Let ${}_RM$ be a semisimple module. Let A be a submodule of M. Let B be a submodule of A. By Proposition 4.10, $M = B \oplus C$ for some submodule C of M. Then $A = B \oplus (A \cap C)$, so B is a direct summand of A. Hence A is semisimple. Also, $M = A \oplus D$ for some submodule D of M. Thus $M/A \cong D$ is semisimple.

(ii) Every left R-module is isomorphic to a quotient of a free R-module; the free R module is semisimple since ${}_RR$ is semisimple. □

Proposition 4.12. *If a ring R is left semisimple, then ${}_RR$ has a composition series.*

Proof. We have $R = \bigoplus_{i \in I} L_i$, where each L_i is a minimal left ideal of R. Write

$$1 = \sum_{i \in I} e_i,$$

where $e_i \in L_i$ and only finitely many $e_i \neq 0$. $\forall j \in I$, choose $0 \neq r \in L_j$. We have

$$r = r \sum_{i \in I} e_i = \sum_{i \in I} r e_i.$$

Since $\bigoplus_{i \in I} L_i$ is a direct sum, we have $r = re_j$. So, $e_j \neq 0$. Therefore $|I| < \infty$. So $R = L_1 \oplus \cdots \oplus L_n$, where each L_i is a minimal left ideal of R. Thus

$$\{0\} \subset L_1 \subset L_1 \oplus L_2 \subset \cdots \subset L_1 \oplus \cdots \oplus L_n = R$$

is a composition series of ${}_RR$. □

Note. If M is a semisimple R-modules, M may not have a composition series. A vector space over a division ring D is a semisimple D-module. However, if $\dim_D V = \infty$, then ${}_DV$ does not have ACC or DCC.

Theorem 4.13. *A ring R is left semisimple $\Leftrightarrow$ R is left artinian and $J(R) = 0$.*

Proof. ($\Rightarrow$) By Proposition 4.12, R is left artinian. By Proposition 4.10, $R = J(R) \oplus I$, where I is a left ideal of R. So $1 = e + f$, where $e \in J(R)$ and $f \in I$. Then $f = 1 - e$ has a left inverse. So $I = R$. Thus $J(R) = 0$.

($\Leftarrow$) Since R has DCC, R has a minimal left ideal I_1. Since $I_1 \not\subset \{0\} = J(R)$, $\exists$ a maximal left ideal B_1 such that $I_1 \not\subset B_1$. Then $R = I_1 + B_1 = I_1 \oplus B_1$. If $B_1 \neq 0$, B_1 contains a minimal left ideal I_2 of R. By the same argument, $\exists$ a maximal left ideal M of R such that $R = I_2 \oplus M$. Then it is easy to see that $B_1 = I_2 \oplus (B_1 \cap M)$. Let $B_2 = B_1 \cap M$. Then $R = I_1 \oplus I_2 \oplus B_2$. Continuing this way, we have

$$R = I_1 \oplus B_1 = I_1 \oplus I_2 \oplus B_2 = \cdots,$$

where I_i's are minimal left ideals of R and $R \supsetneq B_1 \supsetneq B_2 \supsetneq \cdots$ unless $B_n = 0$ for some n. Since R has DCC, $B_n = 0$ for some n. So $R = I_1 \oplus \cdots \oplus I_n$. □

Simple rings. A ring R is called *simple* if it does not have any nontrivial ideal. If D is a division ring, then $M_n(D)$ is a simple ring.

Fact. If R is a simple ring and is left artinian, then R is semisimple.

Proof. $J(R)$ is a proper ideal of $R \Rightarrow J(R) = 0$. □

Lemma 4.14 (Schur's lemma). *If ${}_RM$ is a simple R-module, then* $\mathrm{End}_R(M)$ *is a division ring.*

PROOF. Let $0 \neq f \in \mathrm{End}_R(M)$. We want to show that f is an isomorphism of M. Since $0 \neq f(M) \subset M$ and M is simple, we have $f(M) = M$. Since $\ker f \subsetneq M$, we have $\ker f = 0$. □

PROPOSITION 4.15. *Let ${}_RL$ be an R-module and* $V = \overbrace{L \oplus \cdots \oplus L}^{n}$. *Then*

$$\mathrm{End}_R(V) \cong M_n\big(\mathrm{End}_R(L)\big).$$

PROOF. Let $\iota_i : L \to L\oplus\cdots\oplus L$, $x \mapsto (0, \dots, 0, \underset{i}{x}, 0, \dots, 0)$ and $\pi_i : L\oplus\cdots\oplus L \to L$, $(x_1, \dots, x_n) \mapsto x_i$. Define

$$\begin{array}{rccc} \theta : & \mathrm{End}_R(V) & \longrightarrow & M_n\big(\mathrm{End}_R(L)\big) \\ & f & \longrightarrow & [\pi_i f \iota_j]_{1\le i,j\le n}. \end{array}$$

Then it is easy to show that θ is an abelian group isomorphism. It remains to show that θ preserves multiplication.

$\forall f, g \in \mathrm{End}_R(V)$, we have $\theta(fg)_{ij} = \pi_i f g \iota_j$, $\theta(f)_{ik} = \pi_i f \iota_k$ and $\theta(g)_{kj} = \pi_k g \iota_j$. Therefore,

$$\begin{aligned} \big[\theta(f)\,\theta(g)\big]_{ij} &= \sum_k \pi_i f \iota_k \pi_k g \iota_j \\ &= \pi_i f\Big(\sum_k \iota_k \pi_k\Big) g \iota_j \\ &= \pi_i f g \iota_j \qquad\qquad (\because \sum_k \iota_k \pi_k = \mathrm{id}_V) \\ &= \theta(fg)_{ij}. \end{aligned}$$

So $\theta(fg) = \theta(f)\theta(g)$. □

THE OPPOSITE RING. Let $(R, +, \cdot)$ be a ring. The *opposite ring* R is $R^{\mathrm{op}} = (R, +, *)$, where $a * b = ba$ $\forall a, b \in R$.

PROPOSITION 4.16. *Let R be a ring. Then* $\mathrm{End}_R({}_RR) \cong R^{\mathrm{op}}$.

PROOF. Define

$$\begin{array}{rccc} \phi : & \mathrm{End}_R({}_RR) & \longrightarrow & R^{\mathrm{op}} \\ & f & \longmapsto & f(1). \end{array}$$

1° ϕ is a ring homomorphism. Let $f, g \in \mathrm{End}_R({}_RR)$. Clearly, $\phi(f+g) = \phi(f) + \phi(g)$. Also,

$$\phi(f \circ g) = (f \circ g)(1) = f(g(1)) = f(g(1)1_R) = g(1)f(1) = \phi(f) * \phi(g).$$

Clearly, $\phi(\mathrm{id}_R) = 1_{R^{\mathrm{op}}}$.

2° ϕ is onto. $\forall r \in R^{\mathrm{op}}$, let $f : {}_RR \to {}_RR$, $x \mapsto xr$. Then $f \in \mathrm{End}_R({}_RR)$ and $f(1) = r$.

3° $\ker\phi = \{0\}$. Let $f \in \ker\phi$. Then $f(1) = 0$. $\forall r \in R$, we have $f(r) = f(r1_R) = rf(1) = 0$. So $f = 0$. □

PROPOSITION 4.17. *Let R be a ring. Then* $M_n(R)^{\mathrm{op}} \cong M_n(R^{\mathrm{op}})$.

Proof. Let $*$ denote the multiplication in $(\ )^{\mathrm{op}}$ and let $\diamond$ denote the multiplication in $M_n(R^{\mathrm{op}})$. Define

$$\begin{array}{cccc} f: & M_n(R)^{\mathrm{op}} & \longrightarrow & M_n(R^{\mathrm{op}}) \\ & A & \longmapsto & A^T. \end{array}$$

Clearly, f is an abelian group isomorphism. It remains to show that $f(A*B) = f(A)\diamond f(B)\ \forall A, B \in M_n(R)^{\mathrm{op}}$. Let $A = [a_{ij}]$, $B = [b_{ij}]$. Then

$$\begin{aligned} f(A*B)_{ij} &= f(BA)_{ij} = \big[(BA)^T\big]_{ij} = (BA)_{ji} = \sum_k b_{jk}a_{ki}, \\ \big[f(A)\diamond f(B)\big]_{ij} &= [A^T \diamond B^T]_{ij} = \sum_k a_{ki} * b_{jk} = \sum_k b_{jk}a_{ki}. \end{aligned}$$

So the proof is complete. □

Proposition 4.18. *Let R be a ring. The column module R^n is a left $M_n(R)$-module. We have* $\mathrm{End}_{M_n(R)}(R^n) \cong R^{\mathrm{op}}$.

Proof. Define

$$\begin{array}{cccc} \theta: & R^{\mathrm{op}} & \longrightarrow & \mathrm{End}_{M_n(R)}(R^n) \\ & a & \longmapsto & \theta(a), \end{array}$$

where

$$\begin{array}{cccc} \theta(a): & R^n & \longrightarrow & R^n \\ & \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} & \longmapsto & \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} a. \end{array}$$

It is easy to see that θ is 1-1 ring homomorphism. It remains to show that θ is onto. Let $f \in \mathrm{End}_{M_n(R)}(R^n)$. We have

$$f(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}) = f(\begin{bmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}) = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} f(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}) = \begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

for some $a \in R$. Then

$$f(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}) = f(\begin{bmatrix} x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}) = \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{bmatrix} f(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}) = \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{bmatrix}\begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} a,$$

i.e., $f = \theta(a)$. □

Theorem 4.19 (Wedderburn-Artin, structure of semisimple rings). *Every left semisimple ring R is isomorphic to*

$$M_{n_1}(D_1) \times \cdots M_{n_k}(D_k),$$

where $n_i \geq 1$ and D_i is a division ring. Moreover, $(n_1, D_1), \dots, (n_k, D_k)$ are uniquely determined by R.

Proof. *Existence of the isomorphism.*

Since R is left semisimple, $R = J_1 \oplus \cdots \oplus J_n$, where each J_i is a minimal left ideal of R. Group $J_1, \dots, J_n$ into isomorphism classes. We can write

$$R = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{n_i} L_{ij},$$

where $\{L_{ij} : 1 \le i \le k,\ 1 \le j \le n_i\} = \{J_1, \dots, J_n\}$ and $L_{ij} \cong L_{i'j'}$ iff $i = i'$. Put $A_i = \bigoplus_{j=1}^{n_i} L_{ij}$. Then $R = \bigoplus_{i=1}^{k} A_i$.

1° We claim that all simple submodules of A_i are isomorphic to L_{i1}. A_i has a composition series $0 \subset L_{i1} \subset L_{i1} \oplus L_{i2} \subset \cdots \subset L_{i1} \oplus \cdots \oplus L_{in_i} = A_i$ whose factors are all $\cong L_{i1}$. Let B be a simple submodule of A_i. Then $0 \subset B \subset A_i$ can be refined to a composition series of A_i; B is a factor of this composition series. By the Jordan-Hölder theorem, $B \cong L_{i1}$.

2° We claim that

$$\mathrm{End}_R(R) = \mathrm{End}_R(A_1 \oplus \cdots \oplus A_k) \cong \mathrm{End}_R(A_1) \times \cdots \times \mathrm{End}_R(A_k).$$

Let $f \in \mathrm{End}_R(R)$. We first show that $f(A_i) \subset A_i$. Assume to the contrary that $f(A_1) \not\subset A_1$. Let $\pi_i : A_1 \oplus \cdots \oplus A_k \to A_i$ be the projection. Then $\exists i > 1$ such that $\pi_i f(A_1) \neq 0$. So $\exists j$ such that $\pi_i f(L_{1j}) \neq 0$. Since L_{1j} is simple, $\pi_i f|_{L_{1j}} : L_{1j} \to \pi_i f(L_{1j})$ is an isomorphism. Since $\pi_i f(L_{1j}) \subset A_i$, by 1°, $\pi_i f(L_{1j}) \cong L_{i1} \ncong L_{1j}$, $\rightarrow\leftarrow$.

Now define

$$\begin{array}{cccc} \phi : & \mathrm{End}_R(A_1 \oplus \cdots \oplus A_k) & \longrightarrow & \mathrm{End}_R(A_1) \times \cdots \times \mathrm{End}_R(A_k) \\ & f & \longmapsto & (f|_{A_1}, \dots, f|_{A_k}). \end{array}$$

Clearly, f is an isomorphism.

3° Since $A_i \cong \overbrace{L_{i1} \oplus \cdots \oplus L_{i1}}^{n_i}$, we have

$$\mathrm{End}_R(A_i) \cong \mathrm{End}_R(L_{i1} \oplus \cdots \oplus L_{i1}) \cong M_{n_i}(\mathrm{End}_R(L_{i1})) = M_{n_i}(\Delta_i),$$

where $\Delta_i = \mathrm{End}_R(L_{i1})$ is a division ring (Schur's lemma). Therefore,

$$\begin{aligned} R^{\mathrm{op}} \cong \mathrm{End}_R(R) &\cong \mathrm{End}_R(A_1) \times \cdots \times \mathrm{End}_R(A_k) \\ &\cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_k}(\Delta_k). \end{aligned}$$

So

$$R \cong M_{n_1}(\Delta_1)^{\mathrm{op}} \times \cdots \times M_{n_k}(\Delta_k)^{\mathrm{op}} \cong M_{n_1}(\Delta_1^{\mathrm{op}}) \times \cdots \times M_{n_k}(\Delta_k^{\mathrm{op}}),$$

where Δ_i^{op} is also a division ring.

Uniqueness of $(n_1, D_1), \dots, (n_k, D_k)$.

Assume that

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k) \cong M_{m_1}(D_1') \times \cdots \times M_{m_l}(D_l'),$$

where $m_i > 0$ and D_i' is a division ring. Let R_i and R_i' denote the image of $M_{n_i}(D_i)$ and $M_{m_i}(D_i')$ in R respectively. Then R_i and R_i' are ideals of R and are simple rings themselves. We claim that $\forall 1 \le i \le k$, $\exists 1 \le j \le l$ such that $R_i = R_j'$. (Then it follows that $k = l$ and, after a permutation of the indices, $R_i = R_i'$, $1 \le i \le k$.) Write $1_{R_i} = a_1 + \cdots + a_l$, where $a_j \in R_j'$. $\exists 1 \le j \le l$ such that $a_j \neq 0$. Then $a_j = 1_{R_i} 1_{R_j'} \in R_i \cap R_j'$, so $R_i \cap R_j'$ is a nonzero ideal of R_i and of R_j'. Thus $R_i = R_i \cap R_j' = R_j'$.

Therefore, we have $k = l$ and $M_{n_i}(D_i) \cong M_{m_i}(D_i')$, $1 \le i \le k$. It remains to show that if $M_n(D) \cong M_m(D')$, where $m, n > 0$ and D, D' are division rings, then $n = m$ and $D \cong D'$.

Let $L_i = \{[0, \dots, 0, \underset{i}{a}, 0, \dots, 0] \in M_n(D) : a \in D^n\}$, $1 \le i \le n$. Each L_i is a minimal left ideal of $M_n(D)$ and $M_n(D) = L_1 \oplus \cdots \oplus L_n$. Using composition series, it is clear that all minimal left ideals of $M_n(D)$ are $\cong L_1 \cong D^n$. By Proposition 4.18, $D^{\mathrm{op}} \cong \mathrm{End}_{M_n(D)}(L_1)$. Under the isomorphism $M_n(D) \cong M_m(D')$, L_1 is isomorphic to a minimal left ideal L' of D' and by Proposition 4.18, $D'^{\text{op}} \cong \text{End}_{M_m(D')}(L')$. So

$$D^{\text{op}} \cong \text{End}_{M_n(D)}(L_1) \cong \text{End}_{M_m(D')}(L') \cong D'^{\text{op}}.$$

Hence $D \cong D'$. Finally,

$$n^2 = \dim_D M_n(D) = \dim_{D'} M_m(D') = m^2.$$

So $n = m$. □

COROLLARY 4.20. *A ring R is left semisimple $\Leftrightarrow$ R is right semisimple.*

4.3. Theorems of Wedderburn, Hopkins-Levitzki and Maschke

This section contains several classical theorems in ring theory.

- Wedderburn's theorem asserts that finite division rings are fields.
- Hopkins-Levitzki's theorem postulates that for a ring, DCC $\Rightarrow$ ACC.
- Maschke's theorem claims that the group ring $k[G]$ of a finite group over a filed k is semisimple $\Leftrightarrow$ $\text{char}\, k \nmid |G|$.

THEOREM 4.21 (Wedderburn). *Every finite division ring D is a field.*

PROOF. Let Z be the center of D. Then $Z = \mathbb{F}_q$. Assume to the contrary that D is not a field. Then $\dim_Z D = n > 1$. $\forall a \in D^\times \setminus Z^\times$, $\text{cent}_D(a) = \{x \in D : xa = ax\}$ is a proper sub division ring of D. Let $d(a) = \dim_Z\bigl(\text{cent}_D(a)\bigr)$. Then $d(a) \mid n$ and $d(a) < n$. So

$$|\text{cent}_{D^\times}(a)| = |\text{cent}_D(a)| - 1 = q^{d(a)} - 1.$$

Let $[a_1], \dots [a_k]$ be the conjugacy classes of $D^\times$ not contained in $Z(D^\times) = Z^\times$. By the class equation,

$$q^n - 1 = |D^\times| = |Z(D^\times)| + \sum_{i=1}^{k} |[a_i]| = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d(a_i)} - 1}. \tag{4.2}$$

Let $\zeta = e^{2\pi i/n}$ and let $\Phi_n(x) = \prod_{1 \le k \le n,\, (k,n)=1} (x - \zeta^k) \in \mathbb{Z}[x]$ be the nth cyclotomic polynomial over $\mathbb{Q}$. Since $x^n - 1 = \prod_{c|n} \Phi_c(x)$, $\Phi_n \mid \frac{x^n-1}{x^d-1}$ in $\mathbb{Z}[x]$ for all $d \mid n$, $d < n$. Thus in $\mathbb{Z}$, $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$ for all $d \mid n$, $d < n$. By (4.2), we have $\Phi_n(q) \mid q - 1$. However, since $|q - \zeta^k| > |q - 1|$ for $1 \le k \le n - 1$, we have

$$|\Phi_n(q)| = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} |q - \zeta^k| > \prod_{\substack{1 \le k \le n \\ (k,n)=1}} |q - 1| \ge q - 1,$$

which is a contradiction. □

Wedderburn's theorem has several generalizations. (In Theorems 4.22 – 4.24, the ring is not assumed to have identity.)

THEOREM 4.22 (Jacobson). *Let R be a ring such that for each $a \in R$, $\exists$ integer $n(a) > 1$ such that $a^{n(a)} = a$. Then R is commutative.*

THEOREM 4.23 (Herstein [**9**]). *Let R be a ring such that $\forall x, y \in R$, $\exists$ integer $n(x, y) > 1$ such that $(xy - yx)^{n(x,y)} = xy - yx$. Then R is commutative.*

THEOREM 4.24 (Herstein [**8**]). *Let R be a ring such that $\forall a \in R$, $\exists\, p(x) \in \mathbb{Z}[x]$ such that $a - a^2 p(a) \in Z(R)$. Then R is commutative.*

Modules over a quotient ring. Let R be a ring and I an ideal of R. If M is a left R/I-module, M is automatically an R-modules. ($ra := (r+I)a\ \forall r \in R,\ a \in M$.) Submodules of ${}_RM$ are precisely submodules of ${}_{R/I}M$. If M is a left R-module such that $I \subset \operatorname{ann}(M)$, then M is also an R/I-modules. ($(r+I)a := ra\ \forall r \in R,\ a \in M$.)

Theorem 4.25 (Hopkins-Levitzki). *If a ring R is left artinian, it is left noetherian.*

Proof. We show that ${}_RR$ has a composition series. Let $J = J(R)$. By Proposition 4.7, $J^m = 0$ for some $m > 0$. Since

$$R = J^0 \supset J^1 \supset \cdots \supset J^m = 0,$$

it suffices to show that for each $0 \le i \le m-1$, J^i/J^{i+1} has a composition series.

Clearly, R/J is left artinian. Since $J(R/J) = 0$, R/J is semisimple. J^i/J^{i+1} is an R/J-modules. By Proposition 4.11 (ii), J^i/J^{i+1} is a semisimple R/J-modules. Thus J^i/J^{i+1} is a direct sum of simple R/J-modules. Since J^i/J^{i+1} has DCC as an R-modules, J^i/J^{i+1} has DCC as an R/J-module. Therefore, J^i/J^{i+1} is a direct sum of finitely many simple R/J-modules. Thus J^i/J^{i+1}, as an R/J-module, has a composition series

$$J^i/J^{i+1} = M_0 \supset \cdots \supset M_k = 0. \tag{4.3}$$

(4.3) is also a composition series of J^i/J^{i+1} as an R-module. □

Theorem 4.26 (Maschke). *Let G be a finite group and k a field. Then $k[G]$ is semisimple* $\Leftrightarrow \operatorname{char} k \nmid |G|$.

Proof. ($\Leftarrow$) Let I be a left ideal of $k[G]$. We want to show that I is a direct summand of $k[G]$. Since I is a k-subspace of $k[G]$, $\exists$ k-linear projection $\pi : k[G] \twoheadrightarrow I$. Define

$$\rho(x) = \frac{1}{|G|}\sum_{y \in G} y\pi(y^{-1}x), \qquad x \in k[G].$$

It is easy to see that $\rho : k[G] \to I$ is also a k-linear projection. We claim that ρ is a $k[G]$-map. It suffices to show that $\rho(ax) = a\rho(x)\ \forall a \in G,\ x \in k[G]$. We have

$$\rho(ax) = \frac{1}{|G|}\sum_{y \in G} y\pi(y^{-1}ax) = a\frac{1}{|G|}\sum_{y \in G} a^{-1}y\pi((a^{-1}y)^{-1}x) = a\rho(x).$$

Therefore $k[G] = I \oplus \ker\rho$ and I is a direct summand of $k[G]$.

($\Rightarrow$) Define

$$\begin{array}{cccc} \epsilon: & k[G] & \longrightarrow & k \\ & \sum_{g \in G} a_g g & \longmapsto & \sum_{g \in G} a_g. \end{array}$$

ϵ is a k-linear map (called the *augmentation map*). $\ker\epsilon$ is an ideal of $k[G]$. Since $k[G]$ is semisimple, we have $k[G] = \ker\epsilon \oplus L$ for some left ideal L of $k[G]$. Note that $\dim_k L = |G| - \dim_k \ker\epsilon = 1$. So $L = k[G]v$ for some $v = \sum_{g \in G} a_g g \in k[G]$. Since $v \notin \ker\epsilon$, $\epsilon(v) \ne 0$. $\forall h \in G$, $\exists \lambda \in k$ such that $hv = \lambda v$. So $\epsilon(v) = \epsilon(hv) = \lambda\epsilon(v)$, which implies that $\lambda = 1$. Since

$$\sum_{g \in G} a_{h^{-1}g} g = h\sum_{g \in G} a_g g = hv = v = \sum_{g \in G} a_g g,$$

we have $a_{h^{-1}g} = a_g\ \forall g, h \in G$. So $a_g = a_1\ \forall g \in G$. Then $|G|a_1 = \epsilon(v) \ne 0$. So $\operatorname{char} k \nmid |G|$. □

Exercises

4.1. Let R be a ring. Prove that all ideals of $M_n(R)$ are of the form $M_n(I)$, where I is an ideal of R. (It follows that if R is a division ring, then $M_n(R)$ is simple.)

4.2. Let R be a ring. Prove that $J(M_n(R)) = M_n(J(R))$.

4.3. Let F be a field, $n_1, \ldots, n_k \in \mathbb{Z}^+$, $n = n_1 + \cdots + n_k$, and let

$$R = \left\{ \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ 0 & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{kk} \end{bmatrix} : A_{ij} \in M_{n_i \times n_j}(F),\ 1 \le i \le j \le k \right\} \subset M_n(F).$$

Prove that

$$J(R) = \left\{ \begin{bmatrix} 0 & A_{12} & \cdots & A_{1,k-1} & A_{1k} \\ 0 & 0 & \cdots & A_{2,k-1} & A_{2k} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & A_{k-1,k} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} : A_{ij} \in M_{n_i \times n_j}(F),\ 1 \le i < j \le k \right\}.$$

4.4. Let p be a prime and $n \ge 0$ an integer. Let a_n denote the number of nonisomorphic semisimple rings of order p^n. Prove that

$$\sum_{n=0}^{\infty} a_n x^n = \prod_{k=1}^{\infty} \frac{1}{1 - x^{k^2}}.$$

4.5. Let R be a ring. Then the following statements are equivalent.
(i) R is semisimple.
(ii) Every left R-module is projective.
(iii) Every left R-module is injective.

4.6. Prove Proposition 4.6

4.7. (i) Give an example of a ring R such that $R \not\cong R^{\mathrm{op}}$. Prove your claim.
(ii) Prove that every ring R is isomorphic to a subring of a ring E such that $E \cong E^{\mathrm{op}}$.

4.8. Let R be a left artinian ring and let $J = J(R)$. Let A be a left R-module. Prove that A is semisimple if and only if $JA = 0$.