Abstract Algebra

HHH

December 9, 2025

Contents

Part I

Group Theory

Chapter I

Group

Contents

§1 Basic Definition

§1.1 Basic Definition

Definition 1.1. *Let G be a set.*

1. *A **binary operation** $\cdot$ on G is a function $\cdot : G \times G \to G$. For any $a, b \in G$ we shall write $a \cdot b$ for $\cdot(a, b)$.*

2. *A binary operation $\cdot$ on G is **associative** if for all $a, b, c \in G$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

3. *If $\cdot$ is a binary operation on G we say elements a and b of G **commute** if $a \cdot b = b \cdot a$. We say $\cdot$ is **commutative** if for all $a, b \in G$, $a \cdot b = b \cdot a$.*

Definition 1.2. *A **semigroup** is a nonempty set G together with a binary operation on G which is associative*

*A **monoid** is a semigroup G which contains a identity element $e \in G$ such that $ge = eg = g$ for all $g \in G$.*

*A **group** is a monoid G such that for every $g \in G$ there exists a inverse element $g^{-1} \in G$ such that $g^{-1}g = gg^{-1} = e$.*

A semigroup G is said to be abelian or commutative if its binary operation is (iv) commutative: ab = ba *for all $a, b \in G$.*

*The **order** of a group G is the cardinal number $|G|$. G is said to be finite [resp. infinite] if $|G|$ is finite [resp. infinite].*

Proposition 1.3. *If G is a semigroup, then*

1. *for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ is independent of how the expression is bracketed (this is called the generalized associative law).*

2. $x^{a+b} = x^a x^b$

3. $(x^a)^b = x^{ab}$

If G is a monoid,

4. *the identity of G is unique*

If G is a group,

5. *for each $a \in G$, a^{-1} is unique*

6. $(a^{-1})^{-1} = a$ *for all $a \in G$*

7. $(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$

8. *a^{-n} is defined to be $(a^{-1})^n = (a^n)^{-1}$*

9. *for all $a, b, c \in G$, $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ (left and right. cancellation);*

10. *for $a, b \in G$ the equations $ax = b$ and $ya = b$ have unique solutions in G: $x = a^{-1}b$ and $y = ba^{-1}$.*

Proposition 1.4. *Let G be a semigroup. Then the following conditions on G are equivalent*

1. *G is a group*

2. *There exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (left identity clement); for each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = ea$ (left inverse).*

3. *There exists an element $e \in G$ such that $ae = a$ for all $a \in G$ (right identity clement); for each $a \in G$, there exists an element $a^{-1} \in G$ such that $aa^{-1} = ea$ (right inverse).*

4. *For all $a, b \in G$ the equations $ax = b$ and $yb = a$ have solutions in G .*

Theorem 1.5. *Let $\sim$ be an equivalence relation on a monoid G. Then the set $G/\sim$ is a monoid under the binary operation defined by $\bar{a} \cdot \bar{b} = \bar{ab}$,*

If G is an [abelian] group, then so is G/R.

An equivalence relation on a monoid G that satisfies the hypothesis of the theorem is called a congruence relation on G.

Order

Definition 1.6. *For G a group and $x \in G$ define the **order** of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of order n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of **infinite order**.*

Theorem 1.7. *If x and g are elements of the group G, then*

(1) $|x| = |g^{-1}xg|$

(2) $|ab| = |ba|$ for all $a, b \in G$

(3) If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$.

(4) If $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

§1.2 Subgroup

Definition 1.8. *Let G be a group. The subset H of G is a **subgroup** of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.*

Theorem 1.9 (The subgroup criterion)**.** *Let G be a group, then*

(1) A subset H of a group G is a subgroup if and only if

(i) $H \neq \varnothing$, and

(ii) for all $x, y \in H, xy^{-1} \in H$. Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

(2) If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

(3) If $\mathcal{B}$ is a chain (with respect to set inclusion) in the family of all subgroups of G, then the union of all members in $\mathcal{B}$ is also a subgroup of G

Proposition 1.10. *Let H and K be subgroups of G. THen $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.*

Subgroup generated by sets

Definition 1.11. *If X is any subset of the group G define*

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

*This is called the **subgroup of** G **generated by** X. When X is the finite set $\{a_1, a_2, \ldots, a_n\}$ we write $\langle a_1, a_2, \ldots, a_n \rangle$ for the group generated by $a_1, a_2, \ldots, a_n$. If A and B are two subsets of G we shall write $\langle A, B \rangle$ in place of $\langle A \cup B \rangle$.*

*If H and K are subgroups, $\langle H \cup K \rangle$ is called the **join** of H and K and is denoted $H \bigvee K$ (additive notation: $H + K$)*

Theorem 1.12. *Suppose a group G and subset $A \subset G$, then*

$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$$

($\langle A \rangle = \{e\}$ if $A = \varnothing$)

Normal Subgroup and Normalizer

Definition 1.13. *Let G be a group.*

1. *A subgroup N of a group G is called **normal subgroup** if every element of G normalizes N, i.e. $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.*
2. *Define the **normalizer of** X **in** G to be the set (subgroup)*

$$N_G(X) = \left\{g \in G \mid gXg^{-1} = X\right\}$$

*If K is any subset of $N_G(X)$, we shall say K **normalizes** X.*

Theorem 1.14. *Let N be a subgroup of the group G. The following conditions are equivalent:*

1. *$N \trianglelefteq G$*
2. *$N_G(N) = G$*
3. *$gN = Ng$ for all $g \in G$*
4. *$gNg^{-1} \subseteq N$ for all $g \in G$.*
5. *Left and right congruence modulo N coincide (that is, define the same equivalence relation on G);*
6. *every left coset of N in G is a right coset of N in G*
7. *for any $x, y \in G$, $xy \in N \Leftrightarrow yx \in N$.*

Theorem 1.15. *Let K and N be subgroups of a group G with N normal in G . Then*

(1) $N \cap K$ is a normal subgroup of K;

(2) N is a normal subgroup of $N \vee K$;

(3) $NK = N \vee K = KN$;

(4) if K is normal in G and $K \cap N = \langle e \rangle$, then $nk = kn$ for all $k \in K$ and $n \in N$.

Definition 1.16. *If N is a normal subgroup of a group G and G/N is the set of all (left) cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)\cdot(bN) = abN$. Then the group G/N is called the **quotient group of** G **by** N.*

Center and Centralizers

Definition 1.17. *Let X be any nonempty subset of G. Define*

$$C_G(X) = \left\{ g \in G : gxg^{-1} = x \text{ for all } x \in X \right\}$$

*This subset of G is called the **centralizer of** X **in** G. $C_G(X)$ is a subgroup of G which consists of element commute with every element of X. Define*

$$Z(G) = C_G(G) = \left\{ g \in G : gag^{-1} = a \text{ for all } a \in G \right\}$$

*the set of elements commuting with all the elements of G. This subset of G is called the **center of** G.*

Proposition 1.18. *Suppose a group G.*

1. $C_G(Z(G)) = G$

2. $N_G(Z(G)) = G$

3. *If A and B are subsets of G with $A \subseteq B$ then $C_G(B) \leq C_G(A)$.*

§1.3 Coset

Definition 1.19. *For any $H \leq G$ and any $g \in G$ let*

$$gH = \{gn : n \in H\} \quad \text{and} \quad Hg = \{ng : n \in H\}$$

*called respectively a **left coset** and a **right coset of** N **in** G. Any element of a coset is called a representative for the coset.*

Theorem 1.20. *Let H be any subgroup of the group G. Then*

1. *The set $\{gH : g \in G\}$ of left cosets of H in G form a partition of G.*

2. *For all* $u, v \in G, uH = vH$ *if and only if* $v^{-1}u \in N$, *denoted*

$$a \equiv_l b \,(\mathrm{mod} H)$$

This is a congruence relation.

3. *Right [resp. left] congruence modulo* H *is an equivalence relation on* G

Theorem 1.21. *If* K, H, G *are groups with* $K < H < G$, *then* $[G : K] = [G : H][H : K]$. *If any two of these indices are finite, then so is the third.*

Theorem 1.22 (Lagrange's Theorem)**.** *If* G *is a finite group and* H *is a subgroup of* G, *then the order of* H *divides the order of* G *and the number of left cosets of* H *in* G *equals* $\frac{|G|}{|H|}$ *called the* ***index of*** H ***in*** G *and is denoted by* $[G : H]$.

Corollary 1.23. *If* G *is a finite group and* $x \in G$, *then the order of* x *divides the order of* G. *In particular* $x^{|G|} = 1$ *for all* x *in* G.

Corollary 1.24. *If* G *is a group of prime order* p, *then* G *is cyclic, hence* $G \cong Z_p$.

Definition 1.25. *Let* H *and* K *be subsets of a group and define*

$$HK = \{hk \mid h \in H, k \in K\}.$$

Theorem 1.26. *If* H *and* K *are finite subgroups of a group then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proposition 1.27. *If* H *and* K *are subgroups of a group,* HK *is a subgroup if and only if* $HK = KH$.

Corollary 1.28. *If* H *and* K *are subgroups of* G *and* $H \leq N_G(K)$, *then* HK *is a subgroup of* G. *In particular, if* $K \trianglelefteq G$ *then* $HK = KH \leq G$ *for any* $H \leq G$.

Definition 1.29. *The* ***quotient group***, G/N *(read* G *modulo* N*), is*

$$\{gN : g \in G\}$$

with the operation defined by

$$g_1N \cdot g_2N = g_1Ng_2N = g_1g_2N$$

Proposition 1.30. *(1) If* $N \leq Z(G)$, *then* $N \trianglelefteq G$.
(2) $Z(G) \trianglelefteq G$.

§1.4 Cyclic Groups

Definition 1.31. *A group G is **cyclic** if H can be generated by a single element, i.e., there is some element $x \in H$ such that $G = \{x^n : n \in \mathbb{Z}\}$.*

Theorem 1.32. *Any two cyclic groups of the same order are isomorphic. More specifically,*

(1) If $n \in \mathbb{Z}_{>0}$and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism.

(2) If $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

§2 Homomorphisms

§2.1 Homomorphisms

Definition 2.1. *Let $(G, \cdot)$ and $(H, \times)$ be groups. A map $\varphi : G \to H$ such that*

$$\varphi(x \cdot y) = \varphi(x) \times \varphi(y), \quad \text{for all } x, y \in G$$

*is called a **group homomorphism**.*

*If f is injective as a map of sets, f is said to be a **monomorphism**. If f is surjective, f is called an **epimorphism**. If f is bijective, f is called an **isomorphism**. In this case G and H are said to be **isomorphic** (written $G \cong H$). A homomorphism $f : G \to G$ is called an **endomorphism** of G and an isomorphism $f : G \to G$ is called an **automorphism** of G.*

Definition 2.2. *Let f is a homomorphism $f : G \to H$. The **kernel** of homomorphism f is the set*

$$\{g \in G \mid f(g) = e\}$$

and will be denoted by $\operatorname{Ker} f$.

Theorem 2.3. *Let $f : G \to H$ be a homomorphism of groups. Then*

(1) f is a monomorphism if and only if $\operatorname{Ker} f = e$;

(2) f is an isomorphism if and only if there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

Proposition 2.4. *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.*

1. $\varphi(1_G) = 1_H$*, where 1_G and 1_H are the identities of G and H, respectively.*
2. $\varphi(g^n) = \varphi(g)^n$ *for all $n \in \mathbb{Z}$.*
3. $\ker\varphi \trianglelefteq G$.
4. $\mathrm{Im}(\varphi)$ *is a subgroup of H.*

Natural Projection

Definition 2.5. *Let $N \trianglelefteq G$. The homomorphism*

$$\pi : G \to G/N$$

defined by

$$\pi(g) = gN = Ng$$

is called the ***natural projection*** *(homomorphism) of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the* ***complete preimage*** *of $\bar{H}$ in G is the preimage of $\bar{H}$ under the natural projection homomorphism.*

Theorem 2.6. *A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.*

§2.2 Isomorphism Theorem

Theorem 2.7 (The First Isomorphism Theorem)**.** *If $\varphi : G \to H$ is a homomorphism of groups,then*

$$G/\ker\varphi \cong \varphi(G)$$

and

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \varphi(G) \\ G/\ker\varphi \arrow[ur] & \end{tikzcd}$$

Corollary 2.8. *Let $\varphi : G \to H$ be a homomorphism of groups.*

1. *φ is injective if and only if* $\ker\varphi = 1$.
2. $|G : \ker\varphi| = |\varphi(G)|$.

Proposition 2.9. *If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.*

Proposition 2.10. *Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$(particularly, $B \trianglelefteq A$ or $A, B \trianglelefteq G$). Then*

(1) $B \trianglelefteq AB = BA \leq G$

(2) $A \cap B \trianglelefteq A$

Theorem 2.11 (The Second Isomorphism Theorem)**.** *Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then*

$$AB/B \cong A/A \cap B$$

Theorem 2.12 (The Third Isomorphism Theorem)**.** *Let G be a group and $H \trianglelefteq G$. Then for each $H \leq K \trianglelefteq G$ we have $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K$$

If we denote the quotient by H with a bar, this can be written

$$\bar{G}/\bar{K} \cong G/K$$

Theorem 2.13 (The Fourth or Lattice Isomorphism Theorem)**.** *Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set $\mathcal{U} = \{H : N < H < G\}$ onto the set $\mathcal{V} = \left\{\bar{H} : \bar{H} < \bar{G}\right\}$. This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$*

1. *$A \leq B$ if and only if $\bar{A} \leq \bar{B}$,*
2. *if $A \leq B$, then $|B : A| = |\bar{B} : \bar{A}|$,*
3. *$\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$,*
4. *$\overline{A \cap B} = \bar{A} \cap \bar{B}$*
5. *$A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$.*

§2.3 Automorphism

Definition 2.14. *Let G be a group. An isomorphism from G onto itself is called an* ***automorphism*** *of G. The set of all automorphisms of G is denoted by* $\mathrm{Aut}(G)$.

$\mathrm{Aut}(G)$ *is a subgroup of S_G.*

Proposition 2.15. *Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H*

$$\sigma_g : h \mapsto ghg^{-1} \quad \textit{for each } h \in H$$

For each $g \in G$, conjugation by g is an automorphism of H.

The permutation representation $\sigma : g \mapsto \sigma_g$ afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ *with kernel $C_G(H)$ that*

$$G/C_G(H) \cong \sigma(G) \leq Aut(H)$$

In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Corollary 2.16. *If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.*

Corollary 2.17. *For $H \leq G$, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$. *(Observe that $H \trianglelefteq N_G(H) = G'$ and $C_{G'}(H) = C_G(H)$)*

In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Definition 2.18. *Let G be a group and let $g \in G$. Conjugation by g is called an **inner automorphism** of G and the subgroup of* $\mathrm{Aut}(G)$ *consisting of all inner automorphisms is denoted by* $\mathrm{Inn}(G)$.

$$G/Z(G) \cong Inn(G) \leq \mathrm{Aut}(H)$$

Definition 2.19. *A subgroup H of a group G is called **characteristic** in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in$* $\mathrm{Aut}(G)$.

Chapter II

Group Action

Contents

§1 Basic Definition

Definition 1.1. *A* ***group action*** *of a group G on a set X is a map from $G \times X$ to X (written as $g \cdot x$, for all $g \in G$ and $x \in X$) satisfying the following properties:*

(i) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$*, for all* $g_1, g_2 \in G, x \in X$

(ii) $e \cdot x = x$ *for all* $x \in X$.

If G acts on a set X and distinct elements of X induce distinct permutations of X, the action is said to be ***faithful****.*

The ***kernel of the action*** *of G on X is defined as*

$$\{g \in G : g \cdot x = x, \text{ for all } x \in X\}$$

Proposition 1.2. *Let G acts on X, then*

1. *for each fixed $g \in G$*
$$\sigma_g : x \mapsto g \cdot x$$
is a permutation of X.

2. *the map*
$$\sigma : G \to \mathfrak{S}_X \quad \text{provided that } g \mapsto \sigma_g$$
is a homomorphism called the ***permutation representation associated to the action****.*

3. *Conversely, if $\varphi : G \to \mathfrak{S}_X$ is any homomorphism, then the map from $G \times X$ to X defined by*
$$g \cdot a = \varphi(g)(a) \quad \text{for all } g \in G, \text{ and all } x \in X$$
satisfies the properties of a group action of G on X.

4. *Thus the action of G on X and $\operatorname{Hom}(G, \mathfrak{S}_X)$ are in bijective correspondence. And the kernel of an action of the group G on the set X is the same as the kernel of the corresponding permutation representation $\sigma : G \to \mathfrak{S}_X$.*

Corollary 1.3. *Let G acts on X, then*

1. *the action is faithful if and only if the associated permutation representation is injective.*

2. *the action is faithful if and only if the kerel of the action is $\{e\}$*

3. *if G be a group acting on X and K be the kernel of the action, then G/K acts on X by*
$$(g + K) \cdot x = g \cdot x$$
faithfully

§1.1 Orbits and Stabilizer

Definition 1.4. *Let G be a group acting on the nonempty set X.*

1. *The equivalence class*
$$\mathcal{O}_x = \{g \cdot x : g \in G\}$$
is called the ***orbit*** *of G containing x.*

2. *If $|\mathcal{O}_x| = 1$, i.e. $g \cdot x = x$ for all $g \in G$, then we call x* ***fixed element*** *of X.*

3. *The action of G on X is called* ***transitive*** *if there is only one orbit, i.e. given any two elements $x, y \in X$ there is some $g \in G$ such that $y = g \cdot x$.*

Definition 1.5. *If G is a group acting on a set X and x is some fixed element of X, the* ***stabilizer of*** *x* ***in*** *G is the subgroup*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Proposition 1.6. *Let G act on the set X and $x, y \in X$*

1. *The kernel of the action is $\bigcap_{x \in X} G_x$*
2. *If $y = g \cdot x$, then $G_y = gG_xg^{-1}$.*
3. *Thus if G acts transitively on X then the kernel of the action is*

$$\bigcap_{g \in G} gG_xg^{-1}$$

where x is any element in X.

§1.2 The Class Equation

Definition 1.7. *Let G be a group acts on X and X' respectively. If there exists a one-to-one map φ that*

$$\varphi(g \cdot x) = g \cdot \varphi(x)$$

for all $g \in G$ and $x \in X$. We say the two action are ***equivalent****.*

Theorem 1.8. *Let G be a group acting on the nonempty set X, $x \in X$. Then the action on $\{gG_x : g \in G\}$ by left multiplication and the action of G on $\mathcal{O}_x$ are equivalent.*

Proof. We define

$$\psi : \{gG_x : g \in G\} \longrightarrow \mathcal{O}_x \text{ given that } gG_x \mapsto g \cdot x$$

Then for any $a \in G$,

$$\psi\left(a \cdot gG_x\right) = \psi\left(agG_x\right) = ag \cdot x = a \cdot (g \cdot x) = a \cdot \psi\left(G_x\right)$$

□

Corollary 1.9 (The Class Equation)**.** *Let G be group acting on a finite X. Then*

1. *The number of elements in the orbit of $x \in G$ is*

$$\#\mathcal{O}_x = [G : G_x]$$

2. *let $x_1, x_2, \ldots, x_r$ be representatives of the distinct orbit of X, we have partition*

$$X = \bigsqcup \mathcal{O}_{x_1}$$

Furthermore,

$$\#X = \sum_{i=1}^{r} [G : G_x]$$

§2 Group Actions by Left multiplication

§2.1 Left regular action

Definition 2.1. *Let G be any group and acts on itself defined by*

$$g \cdot x = gx$$

for each $g \in G$ and $x \in G$. This action is called the ***left regular action*** *of G on itself. Associated to the left regular action, the homomorphism*

$$\varphi : G \to \mathrm{Aut}(G)$$

defined by

$$g \to \sigma_g$$

is called ***left regular representation****.*

Corollary 2.2 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.*

§2.2 G acts on (left) coset space by (left) multiplication

Theorem 2.3. *Let G be a group, H be a subgroup of G. If G act on the set $X = \{xH : x \in G\}$ by left multiplication. Then*

1. *G acts transitively on X*
2. *The stabilizer of $xH \in X$ is the subgroup xHx^{-1}*
3. *the kernel of the action π_H is*

   $$\bigcap_{x \in G} G_{xH} = \bigcap_{x \in G} xHx^{-1}$$

   thus $\mathrm{Ker}\, \pi_H$ *is the largest normal subgroup of G contained in H.*
4. *The set of all fixed elements in X is*

   $$\left\{xH : xHx^{-1} = H\right\} = \{xH : x \in N_G(H)\}$$

   Thus the number of all distinct fixed elements are

   $$\# \{xH : x \in N_G(H)\} = [N_G(H) : H]$$

Corollary 2.4. *If H is a subgroup of index n in a group G and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of $\mathfrak{S}_n$.*

Corollary 2.5. *If H is a subgroup of a finite group G of index p, where p is the smallest prime dividing $|G|$, then H is normal in G.*

Proof. Let X be the set of all left cosets of H in G and $\pi_H : G \to X$ be the associated permutation representation. By 2.3, $\operatorname{Ker}\pi_H$ is normal in G and contained in H. Furthermore $G/\operatorname{Ker}\pi_H$ is isomorphic to a subgroup of $\mathfrak{S}_X \cong \mathfrak{S}_p$ by 1.3 and **??**. Hence $|G/\operatorname{Ker}\pi_H| = [H : \operatorname{Ker}\pi_H]\,[G : H]$ divides $p!$, we must have $[H : \operatorname{Ker}\pi_H] = 1$ since $[H : \operatorname{Ker}\pi_H]$ divide $|G|$ and the minimality of p. Thus $H = \operatorname{Ker}\pi_H$ is normal in G. □

§3 Group Actions by Conjugation

§3.1 G acts on itself by conjugation

Definition 3.1. *Suppose G is any group and we consider G acting on itself by conjugation:*

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G$$

Two elements a and b of G are said to be ***conjugate*** *in G if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called the* ***conjugacy classes of*** *G.*

Proposition 3.2. *Let G be a finite group and act on itself by conjugation.*

1. *For each $g \in G$, conjugation by g induces an automorphism of G.*

$$\sigma_g : x \mapsto gxg^{-1}$$

   Thus there is a homomorphism $\sigma : G \to \operatorname{Aut} G$ whose kernel is $C(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. The automorphism σ_g is called the ***inner automorphism*** *induced by g.*

2. *The stabilizer of $s \in G$ is*

$$G_s = \left\{g \in G : g \cdot s = gsg^{-1} = s\right\} = C_G(s)$$

   is the centralizer of s in G.

3. $$\#\mathcal{O}_s = [G : C_G(s)]$$

4. *Let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

§3.2 G acts on $\mathcal{P}(G)$ by conjugation

Definition 3.3. *A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining*

$$g \cdot S = gSg^{-1}$$

for any $g \in G$ and $S \in \mathcal{P}(G)$. Two subsets S and T of G are said to be ***conjugate*** *in G if there is some $g \in G$ such that $T = gSg^{-1}$.*

Proposition 3.4. *For action by conjugation,*

1. *The stabilizer G_S of S*

$$G_S = \left\{g \in G : g \cdot S = gSg^{-1} = S\right\} = N_G(S)$$

   is the normalizer of S in G.

2. *The number of conjugates of a subset S in a group G is the index of the normalizer of S, that is, $\#\mathcal{O}_S = [G : N_G(S)]$.*

Corollary 3.5. *If H is any a nontrivial normal subgroup of G then $H \cap Z(G) \neq 1$. In particular, every normal subgroup of order p is contained in the center.*

§4 Sylow's Theorem

Definition 4.1. *Let G be a group and let p be a prime.*

1. *A group of order p^α for some $\alpha \geq 1$ is called a* ***p-group****. Subgroups of G which are p-groups are called* ***p-subgroups****.*

2. *If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a* ***Sylow p-subgroup of*** *G.*

3. *The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$.*

Lemma 4.2. *If a p-group G acts on a finite set X, then the number of all fixed elements in X*

$$\#\left\{x \in X : \#\mathcal{O}_x = 1\right\} \equiv \#X(\text{mod} p)$$

Corollary 4.3. *The center $C(G)$ of a nontrivial finite p-group G contains more than one element.*

Theorem 4.4 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. (J. H. McKay) It is equivalent that equations $x^p = e$ has at least a solution in G. Let S be the set of p-tuples of group elements $\{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$. Since a_p is uniquely determined as $(a_1 a_2 \cdots a_{p-1})^{-1}$, it follows that $|S| = n^{p-1}$, where $|G| = n$. Since $p|n, |S| \equiv 0(\text{mod} p)$.

Let the group $\mathbb{Z}_p$ act on S by cyclic permutation; that is, for $k \in \mathbb{Z}_p$,

$$k\,(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k)$$

Verify that $(a_{k+1}, a_{k+2}, \ldots, a_k) \in S$; for $0, k, k' \in \mathbb{Z}_p$ and $x \in S, 0x = x$ and $(k + k')\,x = k\,(k'x)$. Therefore the action of $\mathbb{Z}_p$ on S is well defined.

Now $(a_1, \ldots, a_p) \in S_0$ if and only if $a_1 = a_2 = \cdots = a_p$; clearly $(e, e, \ldots, e) \in S_0$ and hence $|S_0| \neq 0$. By 4.2, $0 \equiv |S| \equiv |S_0|\,(\text{mod} p)$. Since $|S_0| \neq 0$ there must be at least p elements in S_0; that is, there is $a \neq e$ such that $(a, a, \ldots, a) \in S_0$ and hence $a^p = e$. Since p is prime, $|a| = p$. □

Corollary 4.5. *A finite group G is a p-group if and only if every element has a order of p.*

Lemma 4.6. *If H is a p -subgroup of a finite group G , then $[N_G(H) : H] \equiv [G : H](\text{mod} p)$.*

Proof. Consider G acts on $X = \{xH\}$ by left multiplication. It follows from 2.3 and 4.2 that

$$[N_G(H) : H] = \#\,\{xH : \#\mathcal{O}_{xH} = 1\} \equiv \#X = [G : H]\,(\text{mod} p)$$

□

Corollary 4.7. *If H is p-subgroup of a finite group G such that p divides $[G : H]$, then $N_G(H) \neq H$.*

Theorem 4.8 (First Sylow Theorem)**.** *Let G be a group of order $p^n m$, with $n \geq 1, p$ prime, and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order $p^i (i < n)$ is normal in some subgroup of order p^{i+1}.*

Proof. Since $p||G|, G$ contains an element a, and therefore, a subgroup $\langle a \rangle$ of order p by Cauchy's Theorem. Proceeding by induction assume H is a subgroup of G of order $p^i (1 \leq i < n)$. Then $p \mid [G : H]$ and by Lemma 5.5 and Corollary $5.6 H$ is normal in $N_G(H), H \neq N_G(H)$ and $1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0\ (\text{mod} p)$. Hence $p\,||N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup of order p as above. By 1.12 this group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since H is normal in $N_G(H), H$ is necessarily normal in H_1. Finally $|H_1| = |H|\,|H_1/H| = p^i p = p^{i+1}$. □

Corollary 4.9. *Let G be a group of order $p^n m$ with p prime, $n \geq 1$ and $(m, p) = 1$.*

(1) H is a Sylow p-subgroup of G if and only if H is a maximal p-subgroup of G.

(2) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(3) If there is only one Sylow p-subgroup P, then P is normal in G .

Theorem 4.10 (Second Sylow theorem)**.** *If H is a p-subgroup of a finite group G, and P is any Sylow p -subgroup of G, then there exists $x \in G$ such that $H < xPx^{-1}$. In particular, any two Sylow p -subgroups of G are conjugate.*

Proof. Let X be the set of left cosets of P in G and let H act on X by (left) translation.

$$\#X_0 \equiv \#X = [G : P] (\mathrm{mod} p)$$

by 4.2. But $p \nmid [G : P]$; therefore $\#X_0 \neq 0$ and there exists $xP \in X_0$, that is, the stabilizer of xP in H

$$H_{xP} = xPx^{-1} \cap H = H$$

by 2.3 and 1.9. Thus $H < xPx^{-1}$. □

Theorem 4.11 (Third Sylow Theorem)**.** *If G is a finite group and p a prime, then the number of Sylow p-subgroups of G, $n_p = [G : N_G(P)]$ divides $|G|$ and $n_p \equiv 1 \, (\mathrm{mod} p)$.*

Proof. (1) By the second Sylow Theorem the number of Sylow p-subgroups is the number of conjugates of any one of them, say P. But this number is $[G : N_G(P)]$, a divisor of $|G|$.

(2) Let X be the set of all Sylow p-subgroups of G and let P act on X by conjugation. Then the set of all fixed elements in X

$$X_0 = \left\{ Q : gQg^{-1} = Q \text{ for all } g \in P \right\} = \{ Q : P < N_G(Q) \}$$

Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$ and are therefore conjugate in $N_G(Q)$. But since Q is normal in $N_G(Q)$, this can only occur if $Q = P$ by 4.10. Therefore, $X_0 = \{P\}$ and by 4.2, $n_p = \#X \equiv \#X_0 = 1 (\mathrm{mod} p)$. □

Corollary 4.12. *If P is a Sylow p-subgroup of a finite group G, then $N_G(N_G(P)) = N_G(P)$.*

Proof. Every conjugate of P is a Sylow p-subgroup of G and of any subgroup of G that contains it. Since P is normal in $N = N_G(P)$, P is the only Sylow p-subgroup of N by 4.9. Therefore,

$$x \in N_G(N) \Rightarrow xNx^{-1} = N \Rightarrow xPx^{-1} < N \Rightarrow xPx^{-1} = P \Rightarrow x \in N.$$

Hence $N_G(N_G(P)) < N$; the other inclusion is obvious. □

§4.1

Lemma 4.13. *Lemma 19. Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.*

Proof. Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$ it is clear that $P \cap Q \leq H$, so we must prove the reverse inclusion. Since by definition $H \leq Q$, this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p-subgroup of G containing both P and H; but P is a p-subgroup of G of largest possible order, so we must have $PH = P$, i.e., $H \leq P$.

Since $H \leq N_G(P)$, by Corollary 15 in Section 3.2, PH is a subgroup. By Proposition 13 in the same section

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

All the numbers in the above quotient are powers of p, so PH is a p-group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^α, the largest power of p which divides $|G|$. These two facts force $|PH| = p^\alpha = |P|$. This in turn implies $P = PH$ and $H \leq P$. This establishes the lemma. $\square$

Corollary 4.14. *Let P be a Sylow p-subgroup of G. Then the following are equivalent:*

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$

(2) P is normal in G

(3) P is characteristic in G

(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Definition 4.15. *A **maximal subgroup** of a group G is a proper subgroup M of G such that there are no subgroups H of G with $M < H < G$.*

Chapter III

Symmetric Group

§1 Basic Definition

Definition 1.1. *Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself (i.e., the set of all permutations of Ω).*

*The set S_Ω is a group under function composition: o. Note that $\circ$ is a binary operation on S_Ω since if $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$ are both bijections, then $\sigma \circ \tau$ is also a bijection from Ω to Ω. Since function composition is associative in general, o is associative. The identity of S_Ω is the permutation 1 defined by $1(a) = a$, for all $a \in \Omega$. For every permutation σ there is a (2 -sided) inverse function, $\sigma^{-1} : \Omega \to \Omega$ satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Thus, all the group axioms hold for ($S_\Omega, \circ$). This group is called the **symmetric group** on the set Ω.*

In the special case when $\Omega = \{1, 2, 3, \ldots, n\}$, the symmetric group on Ω is denoted S_n

*A **cycle** is a string of integers which represents the element of S_n which cyclically permutes these integers and fixes all other integers. The cycle $(a_1 a_2 \ldots a_m)$ is the permutation which sends a_i to $a_{i+1}, 1 \leq i \leq m-1$ and sends a_m to a_1.*

*We can represent this description of σ by **cycle decomposition**.*

*The length of a cycle is the number of integers which appear in it. A cycle of length t is called a **t-cycle**. A 2-cycle is called a **transposition**.*

$$(a_1 a_2 \ldots a_m) = (a_1 a_m)(a_1 a_{m-1})(a_1 a_{m-2}) \ldots (a_1 a_2)$$

Two cycles are called disjoint if they have no numbers in common.

Proposition 1.2. *The order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.*

Proposition 1.3. *Let σ, τ be elements of the symmetric group S_n and*

(1) suppose σ has cycle decomposition

$$(a_1 a_2 \ldots a_{k_1})(b_1 b_2 \ldots b_{k_2}) \ldots$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\,\tau(a_2)\ldots\tau(a_{k_1}))\,(\tau(b_1)\,\tau(b_2)\ldots\tau(b_{k_2}))\ldots,$$

(2) Suppose σ has the form

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

then $\tau\sigma\tau^{-1}$ is

$$\begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(n) \\ \tau(a_1) & \tau(a_2) & \cdots & \tau(a_n) \end{pmatrix}$$

Definition 1.4. *(1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, \ldots, n_r$ are called the **cycle type** of σ.*

(2) If $n \in \mathbb{Z}^+$, a partition of n is any nondecreasing sequence of positive integers whose sum is n.

Proposition 1.5. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.*

§2 The Alternating Group

Definition 2.1. *Let $x_1, \ldots, x_n$ be independent variables and let Δ be the polynomial*

$$\Delta = \prod_{1\leq i<j\leq n} (x_i - x_j)$$

For each $\sigma \in S_n$ let σ act on Δ by permuting the variables in the same way it permutes their indices:

$$\sigma(\Delta) = \prod_{1\leq i<j\leq n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right)$$

or each $\sigma \in S_n$ let

$$\in(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

Then

(1) $\in(\sigma)$ is called the sign of σ.

*(2) σ is called an **even permutation** if $\in(\sigma) = 1$ and an **odd permutation** if $\in(\sigma) = -1$*

Proposition 2.2. *(1) The map $\in : S_n \to \{\pm 1\}$ is a homomorphism.*

(2) Transpositions are all odd permutations and ϵ is a surjective homomorphism.

(3) An m-cycle is an odd permutation if and only if m is even.

(4) The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

Definition 2.3. ***The alternating group of degree*** *n, denoted by A_n, is the kernel of the homomorphism ϵ (i.e., the set of even permutations).*

Chapter IV

Group Series

Contents

§1 Nilpotent Group

Definition 1.1. *Let G be a group. The center $Z(G)$ of G is a normal subgroup. Let $Z_2(G)$ be the inverse image of $Z(G/Z(G))$ under the canonical projection $G \to G/Z(G)$. Then $Z_2(G)$ is normal in G and contains $Z(G)$. Continue this process by defining inductively: $Z_1(G) = Z(G)$ and $Z_i(G)$ is the inverse image of $Z(G/Z_{i-1}(G))$ under the canonical projection $G \to G/Z_{i-1}(G)$. Thus we obtain a sequence of normal subgroups of G, called the* ***ascending central series*** *of G :*

$$\langle e \rangle < Z_1(G) < Z_2(G) < \cdots$$

A group G is ***nilpotent*** *if $Z_n(G) = G$ for some n.*

Theorem 1.2. *Every finite p-group is nilpotent.*

Proof. G and all its nontrivial quotients are p-groups, and therefore, have nontrivial centers by Corollary 5.4. This implies that if $G \neq C_i(G)$, then $C_i(G)$ is strictly contained in $C_{i+1}(G)$. Since G is finite, $C_n(G)$ must be G for some n. $\square$

Theorem 1.3. *The direct product of a finite number of nilpotent groups is nilpotent.*

Proof. Suppose for convenience that $G = H \times K$, the proof for more than two factors being similar. Assume inductively that $C_i(G) = C_i(H) \times C_i(K)$ (the case $i = 1$ is obvious). Let π_H

be the canonical epimorphism $H \to H/C_i(H)$ and similarly for π_K. Verify that the canonical epimorphism $\varphi : G \to G/C_i(G)$ is the composition

$$G = H \times K \xrightarrow{\pi} H/C_i(H) \times K/C_i(K) \xrightarrow{\psi} \frac{H \times K}{C_i(H) \times C_i(K)} = \frac{H \times K}{C_i(H \times K)} = G/C_i(G),$$

where $\pi = \pi_H \times \pi_K$ (Theorem I.8.10), and ψ is the isomorphism of Corollary I.8.11. Consequently,

$$\begin{aligned} C_{i+1}(G) &= \varphi^{-1}\left[C\left(G/C_i(G)\right)\right] = \pi^{-1}\psi^{-1}\left[C\left(G/C_i(G)\right)\right] \\ &= \pi^{-1}\left[C\left(H/C_i(H) \times K/C_i(K)\right)\right] \\ &= \pi^{-1}\left[C\left(H/C_i(H)\right) \times C\left(K/C_i(K)\right)\right] \\ &= \pi_H^{-1}\left[C\left(H/C_i(H)\right)\right] \times \pi_K^{-1}\left[C\left(K/C_i(K)\right)\right] \\ &= C_{i+1}(H) \times C_{i+1}(K). \end{aligned}$$

Thus the inductive step is proved and $C_i(G) = C_i(H) \times C_i(K)$ for all i. Since H, K are nilpotent, there exists $n \in$ N* such that $C_n(H) = H$ and $C_n(K) = K$, whence $C_n(G) = H \times K = G$. Therefore, G is nilpotent. □

Proposition 1.4. *If H is a proper subgroup of a nilpotent group G, then H is a proper subgroup of its normalizer $N_G(H)$.*

Proof. Let $C_0(G) = \langle e \rangle$ and let n be the largest index such that $C_n(G) < H$; (there is such an n since G is nilpotent and H a proper subgroup). Choose $a \in C_{n+1}(G)$ with $a \notin H$. Then for every $h \in H$,

$$C_n ah = (C_n a)(C_n h) = (C_n h)(C_n a) = C_n ha$$

in $G/C_n(G)$ since $C_n a$ is in the center of $C_{n+1}(G)$. Thus $ah = h'ha$, where $h' \in C_n(G) < H$. Hence $aha^{-1} \in H$ and $a \in N_G(H)$. Since $a \notin H, H$ is a proper subgroup of $N_G(H)$. □

Theorem 1.5. *A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Proof. If G is the direct product of its Sylow p-subgroups, then G is nilpotent by Theorems 7.2 and 7.3.

If G is nilpotent and P is a Sylow p-subgroup of G for some prime p, then either $P = G$ (and we are done) or P is a proper subgroup of G. In the latter case P is a proper subgroup of $N_G(P)$ by Lemma 7.4. Since $N_G(P)$ is its own normalizer by Theorem 5.11, we must have $N_G(P) = G$ by Lemma 7.4. Thus P is normal in G, and hence the unique Sylow p-subgroup of G by Theorem 5.9.

Let $|G| = {p_1}^{n_1} \cdots {p_k}^{n_k}$ (p_i distinct primes, $n_i > 0$) and let $P_1, P_2, \dots, P_k$ be the corresponding (proper normal) Sylow subgroups of G. Since $|P_i| = {p_i}^{n_i}$ for each i, $P_i \cap P_j = \langle e \rangle$ for $i \neq j$. By Theorem I.5.3 $xy = yx$ for every $x \in P_i, y \in P_j (i \neq j)$. It follows that for each $i, P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k$ is a subgroup in which every element has order dividing $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$. Consequently, $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = \langle e \rangle$ and $P_1 P_2 \cdots P_k =$

$P_1 \times \cdots \times P_k$. Since $|G| = {p_1}^{n_1} \cdots {p_k}^{n_k} = |P_1 \times \cdots \times P_k| = |P_1 \cdots P_k|$ we must have $G = P_1 P_2 \cdots P_k = P_1 \times \cdots \times P_k$. $\square$

§2 Solvable Group

§2.1 Commutator Subgroup

Definition 2.1. *Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.*

1. *Define $[x, y] = x^{-1}y^{-1}xy$, called the **commutator of** x **and** y.*
2. *Define $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$, the group generated by commutators of elements from A and from B.*
3. *Define $G^{(1)} = [G, G]$, the subgroup of G generated by commutators of elements from G, called the **commutator subgroup of** G.*
4. *$G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$*

Proposition 2.2. *Let G be a group and $N \trianglelefteq G$.*

1. *$G^{(1)} \trianglelefteq G$*
2. *G/N is abelian if and only if $G^{(1)} \leq N$*

Proposition 2.3. *Let G be a group, let $x, y \in G$ and let $H \leq G$. Then*

1. *$xy = yx[x, y]$.*
2. *$H \trianglelefteq G$ if and only if $[H, G] \leq H$.*
3. *$\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G, G' char G and G/G' is abelian.*
4. *$G/G^{(1)}$ is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.*
5. *If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G' i.e., $G' \leq \ker \varphi$ and the following diagram commutes:*

§2.2 Solvable

Definition 2.4. *A group G is **solvable** if there is a $n > 0$ such that $G^{(n)} = \langle e \rangle$.*

Theorem 2.5. *The finite group G is solvable if and only if for every divisor n of $|G|$ such that $\left(n, \frac{|G|}{n}\right) = 1$, G has a subgroup of order n.*

Theorem 2.6. *If N and G/N are solvable, then G is solvable.*

Proof. To see this let $\bar{G} = G/N$, let $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N$ be a chain of subgroups of N such that N_{i+1}/N_i is abelian, $0 \le i < n$ and let $\overline{1} = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \ldots \trianglelefteq \overline{G_m} = \bar{G}$ be a chain of subgroups of $\bar{G}$ such that $\overline{G_{i+1}}/\overline{G_i}$ is abelian, $0 \le i < m$.

By the Lattice Isomorphism Theorem there are subgroups G_i of G with $N \le G_i$ such that $G_i/N = \overline{G_i}$ and $G_i \trianglelefteq G_{i+1}, 0 \le i < m$. By the Third Isomorphism Theorem

$$G_{i+1}/G_i \cong (G_{i+1}/N) \,/\, (G_i/N) = \overline{G_{i+1}}/\overline{G_i}$$

is abelian. Thus

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m = G$$

is a chain of subgroups of G all of whose successive quotient groups are abelian. This proves G is solvable. □

§3 Normal and Subnormal Series

Definition 3.1. *A **subnormal series** of a group G is a chain of subgroups*

$$G = G_0 > G_1 > \cdots > G_n$$

*such that G_{i+1} is normal in G_i for $0 \le i < n$. The **factors** of the series are the quotient groups G_i/G_{i+1}. The **length** of the series is the number of strict inclusions. A subnormal series such that G_i is normal in G for all i is said to be **normal**.*

Definition 3.2. *Let $G = G_0 > G_1 > \cdots > G_n$ be a subnormal series. A one-step refinement of this series is any subnormal series of the form $G = G_0 > \cdots > G_i > N > G_{i+1} > \cdots > G_n$ or $G = G_0 > \cdots > G_n > N$, where N is a normal subgroup of G_i and (if $i < n$) G_{i+1} is normal in N .*

*A **refinement** of a subnormal series S is any subnormal series obtained from S by a finite sequence of one-step refinements. A refinement of S is said to be **proper** if its length is larger than the length of S.*

*Two subnormal series S and T of a group G are **equivalent** if there is a one-to-one correspondence between the nontrivial factors of S and the nontrivial factors of T such that corresponding factors are isomorphic groups.*

Definition 3.3. *A subnormal series $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ is a **composition series** if each factor G_i/G_{i+1} is simple.*

*A subnormal series $G = G_0 > G_1 > \cdots > G_n = \langle \mathrm{e} \rangle$ is a **solvable series** if each factor is abelian.*

Theorem 3.4. *(1) Every finite group G has a composition series.*

(2) Every refinement of a solvable series is a solvable series.

(3) A subnormal series is a composition series if and only if it has no proper refinements.

Proof. (1) Let G_1 be a maximal normal subgroup of G; then G/G_1 is simple by Corollary I.5.12. Let G_2 be a maximal normal subgroup of G_1, and so on. Since G is finite, this process must end with $G_n = \langle e \rangle$. Thus $G > G_1 > \cdots > G_n = \langle e \rangle$ is a composition series.

(2) If G_i/G_{i+1} is abelian and $G_{i+1} \triangleleft H \triangleleft G_i$, then H/G_{i+1} is abelian since it is a subgroup of G_i/G_{i+1} and G_i/H is abelian since it is isomorphic to the quotient $(G_i/G_{i+1}) \,/\, (H/G_{i+1})$ by the Third Isomorphism Theorem I.5.10. The conclusion now follows immediately.

(iii) If $G_{i+1} \underset{\ntriangleright}{\trianglelefteq} \underset{\ntriangleright}{\trianglelefteq} G_i$ are groups, then H/G_{i+1} is a proper normal subgroup of G_i/G_{i+1} and every proper normal subgroup of G_i/G_{i+1} has this form by Corollary I.5.12. The conclusion now follows from the observation that a subnormal series $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ has a proper refinement if and only if there is a subgroup H such that for some $i, G_{i+1} \underset{\ntriangleright \neq G_i.}{\forall}$ □

Theorem 3.5. *(1) A group G is solvable if and only if it has a solvable series.*

(2) A finite group G is solvable if and only if G has a composition series whose factors are $\mathbb{Z}_p$ of order prime number p.

Proof. (1) If G is solvable, then the derived series $G > G^{(1)} > G^{(2)} > \cdots > G^{(n)} = \langle e \rangle$ is a solvable series by Theorem 7.8.

If $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ is a solvable series for G, then G/G_1 abelian implies that $G_1 > G^{(1)}$ by Theorem 7.8; G_1/G_2 abelian implies $G_2 > G_1{}' > G^{(2)}$. Continue by induction and conclude that $G_2 > G^{(i)}$ for all i; in particular $\langle e \rangle = G_n > G^{(n)}$ and G is solvable.

(2) A composition series with cyclic factors is a solvable series. Conversely, assume $G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$ is a solvable series for G. If $G_0 \neq G_1$, let H_1 be a maximal normal subgroup of $G = G_0$ which contains $G_{1:}$ If $H_1 \neq G_1$, let H_2 be a maximal normal subgroup of H_1 which contains G_1, and so on. Since G is finite, this gives a series $G > H_1 > H_2 > \cdots > H_k > G_1$ with each subgroup a maximal normal subgroup of the preceding, whence each factor is simple. Doing this for each pair (G_i, G_{i+1}) gives a solvable refinement $G = N_0 > N_1 > \cdots > N_r = \langle e \rangle$ of the original series by Theorem 8.4 (ii). Each factor of this series is abelian and simple and hence cyclic of prime order (Exercise I.4.3). Therefore, $G > N_1 > \cdots > N_r = \langle e \rangle$ is a composition series. □

Lemma 3.6 (Zassenhaus)**.** *Let A_2, A_1, B_2, B_1 be subgroups of a group G such that A_2 is normal in A_1 and B_2 is normal in B_1 .*

(1) $A_2\,(A_1 \cap B_2)$ is a normal subgroup of $A_2(A_1 \cap B_1)$;

(2) $B_2\,(A_2 \cap B_1)$ is a normal subgroup of $B_2(A_1 \cap B_1)$;

(3) $A_2(A_1 \cap B_1)/A_2\,(A_1 \cap B_2) \cong B_2(A_1 \cap B_1)/B_2(A_2 \cap B_1)$.

Theorem 3.7 (Schreier)**.** *Any two subnormal [resp. normal] series of a group G have subnormal [resp. normal] refinements that are equivalent.*

Proof. Let $G = G_0 > G_1 > \cdots > G_n$ and $G = H_0 > H_1 > \cdots > H_m$ be subnormal [resp. normal] series. Let $G_{n+1} = \langle e \rangle = H_{m+1}$ and for each $0 \le i \le n$ consider the groups

$$G_i = G_{i+1}(G_i \cap H_0) > G_{i+1}(G_i \cap H_1) > \cdots > G_{i+1}(G_i \cap H_j) > G_{i+1}(G_i \cap H_{j+1})$$
$$> \cdots > G_{i+1}(G_i \cap H_m) > G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}.$$

For each $0 \le j \le m$, the Zassenhaus Lemma (applied to G_{i+1}, G_i, H_{j+1}, and H_j) shows that $G_{i+1}(G_i \cap H_{j+1})$ is normal in $G_{i+1}(G_i \cap H_j)$. [If the original series were both normal, then each $G_{i+1}(G_i \cap H_j)$ is normal in G by Theorem I.5.3 (iii) and Exercises I.5.2 and I.5.13.] Inserting these groups between each G_i and G_{i+1}, and denoting $G_{i+1}(G_i \cap H_j)$ by $G(i,j)$ thus gives a subnormal [resp. normal] refinement of the series $G_0 > G_1 > \cdots > G_n$:

$$G = G(0,0) > G(0,1) > \cdots > G(0,m) > G(1,0) > G(1,1) >$$
$$G(1,2) > \cdots > G(1,m) > G(2,0) > \cdots > G(n-1,m) > G(n,0) > \cdots > G(n,m),$$

where $G(i,0) = G_i$. Note that this refinement has $(n+1)(m+1)$ (not necessarily distinct) terms. A symmetric argument shows that there is a refinement of $G = H_0 > H_1 > \cdots > H_m$ (where $H(i,j) = H_{j+1}(G_i \cap H_j)$ and $H(0,j) = H_j$) :

$$G = H(0,0) > H(1,0) > \cdots > H(n,0) > H(0,1) > H(1,1) > H(2,1) > \cdots >$$
$$H(n,1) > H(0,2) > \cdots > H(n,m-1) > H(0,m) > \cdots > H(n,m).$$

8. NORMAL AND SUBNORMAL SERIES 111

This refinement also has $(n+1)(m+1)$ terms. For each pair $(i,j)(0 \le i \le n, 0 \le j \le m)$ there is by the Zassenhaus Lemma 8.9 (applied to G_{i+1}, G_i, H_{j+1}, and H_j) an isomorphism:

$$\frac{G(i,j)}{G(i,j+1)} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)} = \frac{H(i,j)}{H(i+1,j)}.$$

This provides the desired one-to-one correspondence of the factors and shows that the refinements are equivalent. □

Theorem 3.8 (Jordan-Hölder)**.** *Any two composition series of a group G are equivalent. Therefore every group having a composition series determines a unique list of simple groups.*

Chapter V

Structure of Groups

Contents

§1 Free Groups

§1.1 Words on Free Group

Theorem 1.1. *Let G be a group, X a set and $\varphi : S \to G$ a map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:*

$$\begin{tikzcd} S \arrow[r, "i"] \arrow[dr, "\phi"'] & F(S) \arrow[d, "\Phi"] \\ & G \end{tikzcd}$$

Corollary 1.2. *Every group G is a homomorphic image of a free group.*

Corollary 1.3. *$F(S)$ is unique up to a unique isomorphism which is the identity map on the set S.*

Definition 1.4. *The group $F(S)$ is called the* ***free group on the set*** *S. A group F is a free group if there is some set S such that $F = F(S)$ - in this case we call S a set of* ***free generators (or a free basis) of*** *F. The cardinality of S is called the* ***rank of the free group****.*

Theorem 1.5 (Schreier)**.** *Subgroups of a free group are free.*

§1.2 Presentations

Lemma 1.6. *Let G be a group and a subset S of G, the normal closure of S (****normal subgroup generated by*** *S) is defined by the*

$$\bigcap_{S \subset N \trianglelefteq G} N$$

Definition 1.7. *Let X be a set and Y a set of (reduced) words on X. A group G is said to be the group determined by the* ***generators*** *$x \in X$ and* ***relations*** *$w = e(w \in Y)$ provided $G \cong G/N$, where F is the free group on X and N the normal subgroup of F generated by Y. One says that $(X \mid Y)$ is a* ***presentation*** *of G.*

We say G is ***finitely generated*** *if there is a presentation (S, R) such that S is finite. And we say G is* ***finitely presented*** *if there is a presentation (S, R) with both S and R are finite.*

If G is finitely presented with $S = \{s_1, \dots, s_n\}$ and $R = \{w_1, \dots, w_k\}$, we write:

$$G = \langle s_1, s_2, \dots, s_n \mid w_1 = w_2 = \dots = w_k = 1 \rangle$$

Theorem 1.8 (Van Dyck)**.** *Let X be a set, Y a set of (reduced) words on X and G the group defined by the generators $x \in X$ and relations $w = e(w \in Y)$. If H is any group such that $H = \langle X \rangle$ and H satisfies all the relations $w = e(w \in Y)$, then there is an epimorphism $G \to H$.*

Proof. If F is the free group on X then the inclusion map $X \to H$ induces an epimorphism $\varphi : F \to H$ by Corollary 9.3. Since H satisfies the relations $w = e(w \in Y), Y \subset \operatorname{Ker} \varphi$. Consequently, the normal subgroup N generated by Y in F is contained in Ker φ. By Corollary 5.8φ induces an epimorphism $F/N \to \mathbf{H}/0$. Therefore the composition $G \cong F/N \to \mathbf{H}/0 \cong H$ is an epimorphism. □

Theorem 1.9. *Every finite group is finitely presented.*

Proof: To see this let $G = \{g_1, \dots, g_n\}$ be a finite group. Let $S = G$ and let $\pi : F(S) \to G$ be the homomorphism extending the identity map of S. Let

$$R_0 = \{g_i g_j g_k^{-1} : i, j, k = 1, \dots, n \text{ and } g_i g_j = g_k\}$$

Clearly $R_0 \leq \ker \pi$.

If N is the normal closure of R_0 in $F(S)$ and $\widetilde{G} = F(S)/N$, then $N \leq \ker \pi$ and G is a homomorphic image of $\widetilde{G}$ (i.e., π factors through N). Moreover, the set of elements $\{\widetilde{g}_i \mid i = 1, \dots, n\}$ is closed under multiplication. Since this set generates $\widetilde{G}$, it must equal $\widetilde{G}$. Thus $|\widetilde{G}| = |G|$ and so $N = \ker \pi$ and (S, R_0) is a presentation of G.

This illustrates a sufficient condition for (S, R) to be a presentation for a given finite group G : (i) S must be a generating set for G, and (ii) any group generated by S satisfying the relations in R must have order $\leq |G|$.

§2 Product and Coproduct

§2.1 Direct Product

Definition 2.1. *Let $\{G_i \mid i \in I\}$ be an arbitrary family of groups. Define a binary operation on the Cartesian product*

$$\prod_{i \in I} G_i = \left\{ (g_i)_{i \in I} : g(i) \in G_i \right\}$$

by

$$(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_i \cdot h_i)_{i \in I}$$

is called the ***direct product*** *of the family of groups $\{G_i \mid i \in I\}$.*

Remark. *It equivalent that*

$$\prod_{i \in I} G_i \cong \left\langle \bigsqcup_{i \in I} G_i \mid \bigsqcup_{i \in I} R_i, g_i g_j \right\rangle$$

isomorphism.

Proposition 2.2. *If $\{G_i \mid i \in I\}$ is a family of groups, then*

1. *The direct product $\prod_{i \in I} G_i$ is a group;*
2. *For each $k \in I$, the map $\pi_k : \prod_{i \in I} G_i \to G_k$ given by $f \mapsto f(k)$ is an epimorphism of groups. The maps π_k are called the* ***canonical projections*** *of the direct product.*

Theorem 2.3. *Let $\{G_i : i \in I\}$ be a family of groups and $\{f_i : G \to G_i \mid i \in I\}$ a family of group homomorphisms. Then there is a unique homomorphism $f : G \to \prod_{i \in I} G_i$ such that the following diagram*

$$\begin{tikzcd}
G \arrow[d, "\exists! f"] \arrow[dr, "f_j"] & \\
\prod_{i \in I} G_i \arrow[r, "\pi_j"] & G_j
\end{tikzcd}$$

is commutative for all $i \in I$ and this property determines $\prod_{i \in I} G_i$ uniquely up to isomorphism. In other words, $\prod_{i \in I} G_i$ is a product in the category of groups.

§2.2 Free Product

Definition 2.4. *Let $\{G_i \mid i \in I\}$ be an arbitrary family of groups with presentation $\langle S_i \mid R_i \rangle$. We define*

$$*_{i \in I} G_i = \left\langle \bigsqcup_{i \in I} S_i \mid \bigsqcup_{i \in I} R_i \right\rangle$$

§2.3 Weak Direct Product

Definition 2.5. *Let $\{G_i \mid i \in I\}$ be an arbitrary family of groups. The **weak direct product** of a family of groups $\{G_i \mid i \in I\}$, denoted*

$$\prod_{i\in I}^{w} G_i = \left\{ f \in \prod_{i\in I} G_i : f(i) = e_i \text{ for all but a finite number of } i \in I \right\}$$

*If all the groups G_i are (additive) abelian, $\prod_{i\in I}^{w} G_i$ is usually called the **direct sum** and is denoted $\sum_{i\in I} G_i$.*

Theorem 2.6. *If $\{G_i \mid i \in I\}$ is a family of groups, then*

(1) $\prod_{i\in I}^{w} G_i$ is a normal subgroup of $\prod_{i\in I} G_i$

(2) for each $k \in I$, the map

$$\iota_k : G_k \to \prod_{i\in I}^{w} G_i$$

given by $\iota_k(a) = \{a_i\}_{i\in I}$, where $a_i = e$ for $i \neq k$ and $a_k = a$, is a monomorphism of groups;

(3) for each $i \in I, \iota_i(G_i)$ is a normal subgroup of $\prod_{i\in I} G_i$.

*The maps ι_i are called the **canonical injections***

Theorem 2.7. *Let $\{A_i : i \in I\}$ be a family of abelian groups (written additively). If A is an abelian group and $\{f_i : A_i \to A : i \in I\}$ a family of homomorphisms, then there is a unique homomorphism $f : \sum_{i\in I} A_i \to A$ such that*

$$\begin{tikzcd}
A & \\
\sum\limits_{i\in I} A_i \arrow[u, "f"] & G_j \arrow[l, "\iota_j"] \arrow[ul, "f_j"']
\end{tikzcd}$$

for all $j \in I$ and this property determines $\sum_{i\in I} A_i$ uniquely up to isomorphism. In other words, $\sum_{i\in I} A_i$ is a coproduct in the category of abelian groups.

Theorem 2.8. *Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G such that*

(i) $G = \left\langle \bigcup_{i\in I} N_i \right\rangle$;

(ii) for each $k \in I, N_k \cap \left\langle \bigcup_{i\neq k} N_i \right\rangle = \langle e \rangle$.

*Then $G \cong \prod_{i\in I}^{w} N_i$, G is said to be the **internal weak direct product** of the family $\{N_i \mid i \in I\}$.(or the **internal direct sum** if G is abelian)*

Corollary 2.9. *If $N_1, N_2, \ldots, N_r$ are normal subgroups of a group G such that $G = N_1N_2\cdots N_r$ and for each $1 \leq k \leq r, N_k \cap (N_1 \cdots N_{k-1}N_{k+1} \cdots N_r) = \langle e \rangle$, then $G \cong N_1 \times N_2 \times \cdots \times N_r$.*

Theorem 2.10. *Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G. Then G is the internal weak direct product of the family $\{N_i \mid i \in I\}$ if and only if every nonidentity element of G is a unique product*

$$n_{i_1}n_{i_2}\cdots n_{i_k}$$

with $i_1, \ldots, i_k$ distinct indexs of I and $e \neq n_{i_s} \in N_{i_s}$ for each $s = 1, 2, \ldots, k$.

§3 The Krull-Schmidt Theorem

Definition 3.1. *A group G is **indecomposable** if $G \neq \langle e \rangle$ and G is not the (internal) direct product of two of its proper subgroups.*

Proposition 3.2. *Let G be group.*

1. *G is indecomposable if and only if $G \neq \langle e \rangle$ and $G \cong H \times K$ implies $H = \langle e \rangle$ or $K = \langle e \rangle$.*
2. *Every simple group is indecomposable.*
3. *However indecomposable groups need not be simple: $\mathbb{Z}, \mathbb{Z}_{p^n}$ (p prime) and S_n are indecomposable but not simple.*

Definition 3.3. *A group G is said to satisfy the **ascending chain condition (ACC) on subgroups [resp. normal subgroup]** if for every chain $G_1 < G_2 < \cdots$ of subgroups [resp. normal subgroups] of G there is an integer n such that $G_i = G_n$ for all $i \geq n$.*

G is said to satisfy the descending chain condition (DCC) on subgroups [resp. normal subgroup] if for every chain $G_1 > G_2 > \cdots$ of subgroups [resp. normal subgroup] of G there is an integer n such that $G_i = G_n$ for all $i \geq n$.

Theorem 3.4 (Krull-Schmidt Theorem)**.** *If a group G satisfies either the ascending or descending chain condition on normal subgroups, then G is the direct product of a finite number of indecomposable subgroups.*

§4 The Fundentmental Theorem of Finitely Generated Abelain Groups

Part II

Ring Theory

Chapter VI

Ring Theory

Contents

§1 Basic Definition

Definition 1.1. *A **ring** R is a set together with two binary operations $+$ and $\times$ satisfying the following axioms:*

(i) $(R, +)$ *is an abelian group,*

(ii) $\times$ *is associative*

(iii) the distributive laws hold in R *: for all* $a, b, c \in R$

$$(a+b) \times c = (a \times c) + (b \times c) \quad \textit{and} \quad a \times (b+c) = (a \times b) + (a \times c)$$

The ring R *is **commutative** if*

(iv) multiplication $\times$ *is commutative.*

*The ring R is called unital if it has an **identity** 1_R s.t.*

(v) $1_R \times a = a \times 1_R = a$ *for all* $a \in R$.

Remark. *In this book, we usually use the term "ring" to refer a unital ring.*

Definition 1.2. *A **subring** of R is a subgroup of R that is closed under multiplication and contains the identity element 1_R. .*

Proposition 1.3. *Let R be a ring. Then*

1. $0a = a0 = 0$ *for all* $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$.
3. $(-a)(-b) = ab$ *for all* $a, b \in R$.
4. *the identity is unique and* $-a = (-1)a$.

Definition 1.4. *Let R be a ring.*

1. *A nonzero element a of R is called a **zero divisor** if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.*
2. *An element u of R is called a **unit** in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.*

Definition 1.5. *A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.*

Proposition 1.6 (Cancellation property)**.** *Let R be a ring. Then*

1. *Assume a, b and c are elements of R with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.*
2. *In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.*
3. *Any finite integral domain is a field.*

Definition 1.7. *Let R be a ring. If there is a least positive integer n such that $nr = 0$ for all $r \in R$, then R is said to have **characteristic** n . If no such n exists R is said to have characteristic zero. (Notation:* $\operatorname{char} R = n$*).*

Theorem 1.8. *Let R be a ring with identity 1_R and characteristic $n > 0$.*

1. *If $\varphi : \mathbb{Z} \to R$ is the map given by $m \mapsto m1_R$, then φ is a homomorphism of rings with kernel $\langle n \rangle = n\mathbb{Z}$.*
2. *n is the least positive integer such that $n1_R = 0$.*
3. *If R has no zero divisors (in particular if R is an integral domain), then n is prime.*

§2 Ideal

§2.1 Definition and Quotient Ring

Definition 2.1. *Let R be a ring. A subset $\mathfrak{a}$ of R is a* ***left ideal*** *of R if*

(i) $\mathfrak{a}$ *is an additive subgroup of R,*

(ii) $\mathfrak{a}$ *is closed under left multiplication by elements from R, i.e., $r\mathfrak{a} \subseteq \mathfrak{a}$ for all $r \in R$.*

A subset $\mathfrak{b}$ that is both a left ideal and a right ideal is called an ***ideal*** *(or a* ***two-sided ideal****) of R. An ideal $\mathfrak{b}$ is* ***proper*** *if $\mathfrak{b} \neq R$ and $\mathfrak{b} \neq 0$. The ideal $\{0\}$ is called the* ***trivial ideal*** *and is denoted by* 0.

Theorem 2.2. *Let R be a ring. A nonempty subset $\mathfrak{a}$ of a ring R is a left [resp. right] ideal if and only if for all $a, b \in \mathfrak{a}$ and $r \in R$:*

(i) $a, b \in \mathfrak{a} \quad \Rightarrow \quad a - b \in \mathfrak{a}$

(ii) $a \in \mathfrak{a}, r \in R \quad \Rightarrow \quad ra \in \mathfrak{a}$ [*resp.* $ar \in \mathfrak{a}$]

Corollary 2.3. *Let R be a ring.*

1. *If $\{I_\alpha\}$ is a family of ideals [resp. left ideal] in a ring R, then*

$$\bigcap I_\alpha$$

is also a ideal [resp. left ideal].

2. *If $\{J_\beta\}$ is a chain of ideals [resp. left ideal] in $\mathcal{P}(R)$ i.e. either $J_\beta \subset$ or $J_{\beta'} \subset J_\beta$ holds for all β, β', then*

$$\bigcup J_\beta$$

is also a ideal [resp. left ideal] of R.

Definition 2.4. *Let R be a ring and let $\mathfrak{a}$ be an ideal of R. Then the (additive) quotient group $R/\mathfrak{a}$ is a ring called the* ***quotient ring of** R **by*** $\mathfrak{a}$ *under the binary operations:*

$$(r + \mathfrak{a}) + (s + \mathfrak{a}) = (r + s) + \mathfrak{a} \quad \textit{and} \quad (r + \mathfrak{a}) \times (s + \mathfrak{a}) = (rs) + \mathfrak{a}$$

for all $r, s \in R$.

Conversely, if $\mathfrak{b}$ is any subgroup such that the above operations are well defined, then $\mathfrak{b}$ is an ideal of R.

Remark. *If $\mathfrak{a}$ is a left [resp. right] ideal of R, then the quotient group $R/\mathfrak{a}$ is left [resp. right] R-module under the operation*

§2.2 Ideals generated by a set

Definition 2.5. *Let $A_1, A_2, \ldots, A_n$ be nonempty subsets of a rng R. Then*

1. *Denote by $A_1 + A_2 + \cdots + A_n$ the set*

$$\{a_1 + a_2 + \cdots + a_n : a_i \in A_i, i = 1, 2, \ldots, n\}$$

2. *If A and B are nonempty subsets of R let AB denote the set of all finite sums*

$$\{a_1 b_1 + \cdots + a_n b_n : n \in \mathbb{Z}_{\geq 1}; a_i \in A, b_i \in B\}$$

If A consists of a single element a, we write aB for AB. Similarly if $B = \{b\}$, we write Ab for AB.

Theorem 2.6. *Let $A, A_1, A_2, \ldots, A_n, B$ and C be subsets of ring R. Then*

1. *$(A + B) + C = A + (B + C)$; $A + B = B + A$*

2. *$(AB)C = A(BC)$*

3. *$B(A_1 + A_2) = BA_1 + BA_2$; and $(A_1 + A_2)C = A_1 C + A_2 C$.*

Definition 2.7. *Let X be a subset of a rng R. Let $\{I_\alpha\}$ be the family of all (left) ideals in R which contain X. Then $\bigcap I_\alpha$ is called the **(left) ideal generated by** X. This ideal is denoted (X). The elements of X are called **generators** of the ideal (X).*

*If $X = \{x_1, \ldots, x_n\}$, then the ideal (X) is denoted by $(x_1, x_2, \ldots, x_n)$ and said to be **finitely generated**.*

*An ideal (x) generated by a single element is called a **principal ideal**. A principal ideal ring is a ring in which every ideal is principal. A principal ideal ring which is an integral domain is called a **principal ideal domain**.*

Theorem 2.8. *Let R be a rng and $X \subset R$, then*

1. *the left [resp. right] ideal generated by X is*

$$(X)_l = RX \quad \text{[resp.]} \quad (X)_r = +XR$$

the (two-sided) ideal generated by X is

$$(X) = RX + XR + RXR$$

2. *if R has identity, we have $(X)_l = RX$,$(X)_r = RX$ and $(X) = RX + XR + RXR$*

3. *if R is commutative, $(X)_l = (X)_r = (X) = RX$*

§2.3 Prime ideal

Definition 2.9. *Let R be a ring. An ideal $\mathfrak{p}$ in R is said to be* ***prime*** *if*

(i) $\mathfrak{p} \neq R$

(ii) for any ideals A, B in R, $\mathfrak{ab} \subset \mathfrak{p} \Rightarrow \mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$

The set of all prime ideals in a ring R is called the ***spectrum*** *of R, denoted by* $\operatorname{Spec}(R)$.

Theorem 2.10. *Let R be a ring and an ideal $\mathfrak{p} \neq R$.*

1. *If $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ for all $a, b \in R$, then $\mathfrak{p}$ is prime.*

If R is commutative,

2. *ideal $\mathfrak{p}$ is prime if and only if then $\mathfrak{p}$ satisfies the above condition.*

Corollary 2.11. *Let R be a commutative ring and $\mathfrak{p}$ be an ideal in R. The following conditions are equivalent.*

1. *Ideal $\mathfrak{p}$ is prime*
2. *$R - \mathfrak{p}$ is a multiplicative set.*
3. *$R/\mathfrak{p}$ is an integral domain.*

Theorem 2.12. *Let K be a subring of a commutative ring R. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_\mathrm{n}$ are prime ideals of R such that $K \subset \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \ldots \cup \mathfrak{p}_\mathrm{n}$, then $K \subset \mathfrak{p}_i$ for some i .*

Proof. Assume $K \not\subset \mathfrak{p}_i$ for every i. It then suffices to assume that $n > 1$ and n is minimal; that is, for each i, $K \not\subset \bigcup_{j \neq i} \mathfrak{p}_j$. For each i there exists $a_i \in K - \bigcup_{j \neq i} \mathfrak{p}_1$. Since $K \subset \bigcup_i \mathfrak{p}_i$, each $a_i \in \mathfrak{p}_i$. The element $a_1 + a_2 a_3 \cdots a_n$ lies in K and hence in $\bigcup_i \mathfrak{p}_i$. Therefore $a_1 + a_2 a_3 \cdots a_n = b_j$ with $b_j \in \mathfrak{p}_j$. If $j > 1$, then $a_1 \in \mathfrak{p}_j$, which is a contradiction. If $j = 1$, then $a_2 a_3 \cdots a_n \in \mathfrak{p}_1$, whence $a_i \in \mathfrak{p}_1$ for some $i > 1$ by 2.11. □

§2.4 Maximal ideal

Definition 2.13. *Let R be a ring. An ideal $\mathfrak{m}$ is called a* ***maximal ideal*** *[resp. maximal left ideal] if*

(i) $\mathfrak{m} \neq R$

(ii) the only ideals[resp. left ideal] containing $\mathfrak{m}$ are R and $\mathfrak{m}$.

Theorem 2.14. *In a ring R with identity $1_R \neq 0$, every ideal [resp. left ideal] in R (except R itself) is contained in a [resp. left ideal] maximal ideal.*

Proof. It follows from Zorn's lemma and corollary 2.3 □

Theorem 2.15. *If R is a commutative ring, then every maximal ideal $\mathfrak{m}$ is prime.*

Theorem 2.16. *Let $\mathfrak{m}$ be an ideal in a ring R with identity $1_R \neq 0$.*

1. *If $\mathfrak{m}$ is maximal and R is commutative, then the quotient ring R/M is a field.*

2. *If the quotient ring $R/\mathfrak{m}$ is a division ring, then $\mathfrak{m}$ is maximal.*

Remark.

Corollary 2.17. *The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent.*

1. *R is a field.*

2. *R has only trivial ideals.*

3. *0 is a maximal ideal in R.*

4. *R is simple.*

5. *every nonzero homomorphism of rings $R \to S$ is a monomorphism.*

§2.5 Chinese Remainder Theorem

Definition 2.18. *The ideals $\mathfrak{a}$ and $\mathfrak{b}$ of the ring R are said to be* ***comaximal*** *if $\mathfrak{a} + \mathfrak{b} = R$.*

Theorem 2.19 (Chinese Remainder Theorem)**.** *Let R be a commutative ring with $1_R \neq 0$ and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k$ be ideals in R. Then*

1. *The map*
$$R \to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_k$$
defined by
$$r \mapsto (r + \mathfrak{a}_1, r + \mathfrak{a}_2, \ldots, r + \mathfrak{a}_k)$$
is a ring homomorphism with kernel $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_k$.

2. *If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are comaximal, then this map is surjective and*
$$R/\left(\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_k\right) = R/\left(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_k\right) \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_k$$

Corollary 2.20. *Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then*

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times .$$

§3 Homomorphisms

Definition 3.1. *Let R and S be ring.*

1. *A **ring homomorphism** is a map $f : R \to S$ satisfying*
$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$
for all $a, b \in R$ and $f(1_R) = 1_S$.

2. *The **kernel** of the ring homomorphism f, denoted* $\operatorname{Ker} f$*, is the set of elements of R that map to 0 in S.*

3. *A bijective ring homomorphism is called an **isomorphism**.*

Theorem 3.2 (The First Isomorphism Theorem for Rings)**.** *If $f : R \to S$ is a homomorphism of rings, then*

1. *The kernel of f is an ideal of R.*

2. *The image of f is a subring of S and $R/\operatorname{Ker} f \cong f(R)$.*

Corollary 3.3. *If I is any ideal of R, then the **natural projection***
$$R \to R/I \quad \text{defined by} \quad r \mapsto r + I$$
is a surjective ring homomorphism with kernel I. Thus every ideal is the kernel of a ring homomorphism.

Theorem 3.4 (The Second Isomorphism Theorem for Rings)**.** *Let R be a ring. Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and*
$$(A+B)/B \cong A/(A \cap B)$$

Theorem 3.5 (The Third Isomorphism Theorem for Rings)**.** *Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and*
$$(R/I)/(J/I) \cong R/J$$

Theorem 3.6 (The Fourth or Lattice Isomorphism Theorem for Rings)**.** *Let $\mathfrak{a}$ be an ideal of ring R.*

1. *The correspondence*
$$R \leftrightarrow R/\mathfrak{a} \tag{1}$$
is an inclusion preserving bijection between the collection of subrings of R that contain I and the collection of subrings of $R/\mathfrak{a}$.

2. *Furthermore, a subring A containing $\mathfrak{a}$ is an ideal of R if and only if $A/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$.*

§4 Rings of Polynomial and Formal Power Series

We only consider $R\,[x]$ where R is a commutative ring with identity.

Proposition 4.1. *Let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.*

1. *f is a unit in $R[[x]]$ if and only if its constant term a_0 is a unit in R*
2. *If a_0 is irreducible in R, then f is irreducible in $R[[x]]$.*

Corollary 4.2. *If R is a division ring, then*

1. *$R[[x]]^\times$ are precisely those power series with nonzero constant term.*
2. *The principal ideal (x) consists precisely of the nonunits in $R[[x]]$ and is the unique maximal ideal of $R[[x]]$.*
3. *Thus if R is a field, $R[[x]]$ is a local ring.*

Chapter VII

Factorization in Integral Domaina

Contents

§1 Divisor Decomposition

§1.1 Basic definition

Definition 1.1. *Let R be a integral domain and let $a, b \in R$ with $b \neq 0$.*

1. *a is said to be a* ***multiple*** *of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to divide a or be a* ***divisor*** *of a, written $b \mid a$.*

2. *If $a \mid b$ and $b \mid a$, then a and b are said to be* ***associates***

3. *If $b \mid a$ and $a \nmid b$ then b called* ***proper divisor*** *of a. Every element a has two* ***trivial divisor****: units and associate elements of a.*

Theorem 1.2. *Let R be a integral domain, and a, b, u be elements of R.*

1. *$a \mid b$ if and only if $(b) \subset (a)$.*

2. *a and b are associates $\Leftrightarrow (a) = (b) \Leftrightarrow a = bu$ for some unit u.*

Definition 1.3. *Let R be an commutative ring with $1_R \neq 0$.*

1. *Suppose $r \in R$, then r is called **irreducible** in R if*

   (i) $r \neq 0$ *and* $r \notin R^\times$

   (ii) $r = ab \Rightarrow a$ *or* b *is a unit.*

   The only divisors of an irreducible element are its associates and the units of R .

2. *The element $p \in R$ is called **prime** in R if*

   (i) $p \neq 0$ *and* $p \notin R^\times$

   (ii) if $p \mid ab$ for any $a, b \in R$, then $p \mid a$ or $p \mid b$.

Remark. *Every associate of an irreducible [resp. prime] element is irreducible [resp. prime].*

Theorem 1.4. *Let p and c be nonzero elements in an integral domain R.*

1. *p is prime if and only if (p) is nonzero prime ideal*

2. *c is irreducible if and only if (c) is maximal in the set $\mathcal{S}$ of all proper principal ideals of R.*

3. *Every prime element of R is irreducible.*

Definition 1.5. *Let X be a nonempty subset of a integral domain R*

1. *An element $d \in R$ is a **greatest common divisor** of X provided*

   (i) $d \mid x$ *for all* $x \in X$

   (ii) if $d' \mid x$ for all $x \in X$ then $d' \mid d$.

   A greatest common divisor of a and b will be denoted by $\gcd(a, b)$*, or* (a, b).

2. *An element $l \in R$ is a **least common multiple** of X such that*

   (i) $x \mid l$ *for all* $x \in X$

   (ii) if $x \mid l'$ for all $x \in X$, then $l \mid l'$

   A least common multiple of a and b will be denoted by $\operatorname{lcm}(a, b)$*, or* $[a, b]$.

Remark. *The greatest common divisor and least common multiple are unique up to association.*

Definition 1.6. *Let R be a integral domain, and $a_1, a_2, \ldots, a_n$ have 1_R as a greatest common divisor, then $a_1, a_2, \ldots a_n$ are said to be **relatively prime**.*

Theorem 1.7. *Let $a_1, \ldots, a_n$ be elements of a commutative ring R with identity. Then $d \in R$ is a greatest common divisor of $\{a_1, \ldots, a_n\}$ and $d \in (a_1) + (a_2) + \cdots + (a_n)$ if and only if $(d) = (a_1) + (a_2) + \cdots + (a_n)$;*

If F is a field, then x and y are relatively prime in the polynomial domain $F[x, y]$, but $F[x, y] = (1_F) \supsetneq (x) + (y)$

§2 E.D $\Rightarrow$ P.I.D $\Rightarrow$ U.F.D

§2.1 Unique Factorization Domain

Definition 2.1. *A* ***unique factorization domain*** *is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:*

(i) every nonzero nonunit element a of R can be written $a = c_1 c_2 \cdots c_n$, with $c_1, \ldots, c_n$ irreducible.

(ii) If $a = c_1 c_2 \cdots c_n$ and $a = d_1 d_2 \cdots d_n$ (c_i, d_i irreducible), then $n = m$ and for some permutation $\sigma \in \mathfrak{S}_n$, c_i and $d_{\sigma(i)}$ are associates for every i.

Proposition 2.2. *If R is a unique factorization domain then*

1. *Irreducible and prime elements coincide.*
2. *for any $a_1, a_2, \ldots, a_n$, there exists an unique greatest common divisor of $a_1, \ldots, a_n$ in the sense of associationa and $(d) = (a_1) + (a_2) + \cdots + (a_n)$,*

§2.2 Principal rings and principal domains

Definition 2.3. *A* ***principal ideal ring*** *is a ring in which every ideal is principal.*

Theorem 2.4. *If R is principal ideal domain*

1. *R is a unique factorization domain thus proposition 2.2 holds.*
2. *maximal ideals and prime ideals coincide.*
3. *if $(a) + (b) = (c)$, then c is a greatest common divisor of a and b.*

Definition 2.5. *Define N to be a* ***Dedekind-Hasse norm*** *in commutative ring R if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element in the ideal $(a, b) = (a) + (b)$ of norm strictly smaller than the norm of b. (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).*

Theorem 2.6. *The integral domain R is a P.I.D. if and only if R has a Dedekind-Hasse norm.*

Proof. Suppose that R has a Dedekind-Hasse norm N. Let $\mathfrak{a}$ be a nonzero ideal in R and let b be a nonzero element of $\mathfrak{a}$ of minimum norm. If $a \in \mathfrak{a}$, then either $a \in (b)$ or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$. The latter is impossible since $sa - tb \in \mathfrak{a}$ and b has minimum norm in $\mathfrak{a}$. Therefore, $a \in (b)$ and consequently, $\mathfrak{a} = (b)$. Thus R is a principal ideal domain.

The converse is obvious. □

§2.3 Euclidean Ring and Euclidean domain

Definition 2.7. *Let R a commutative ring. R is a **Euclidean ring** if there is a function $\varphi : R - \{0\} \to \mathbb{N}$ such that:*

(i) if $a, b \in R$ and $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$;

(ii) if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$, or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

*A Euclidean ring which is an integral domain is called a **Euclidean domain**.*

Theorem 2.8. *If R is a Euclidean ring, then*

1. *R is a principal ideal ring with identity.*

2. *if $\mathfrak{a}$ is any nonzero ideal in the Euclidean ring R with φ and $\mathfrak{a} = (a)$, then a is a nonzero element of $\mathfrak{a}$ of minimum norm.*

Proof. If I is a nonzero ideal in R, choose $a \in I$ such that $\varphi(a)$ is the least integer in the set of nonnegative integers $\{\varphi(x) \mid x \neq 0; x \in I\}$. If $b \in I$, then $b = qa$. Consequently, $I \subset Ra \subset (a) \subset I$. Therefore $I = Ra = (a)$ and R is a principal ideal ring.

Conversely, if $\mathfrak{a} = (a)$ and b is a nonzero element of $\mathfrak{a}$ of minimum norm, then $a = xy$ and $b = ya$ for some $x, y \in R$, whence $\varphi(a) = \varphi(xb) \geq \varphi(b)$ and $\varphi(b) = \varphi(ya) \geq \varphi(a)$. Thus a is also a nonzero element of $\mathfrak{a}$ of minimum norm.

Since R itself is an ideal, $R = Ra$ for some $a \in R$. Consequently, $a = ea = ae$ for some $e \in R$. If $b \in R = Ra$, then $b = xa$ for some $x \in R$. Therefore, $be = (xa)e = x(ae) = xa = b$, whence e is a multiplicative identity element for R. $\square$

Corollary 2.9. *Let R be a Euclidean ring and $a \in R$. Then $\varphi(1_R)$ is minimum and element a is a unit in R if and only if $\varphi(a) = \varphi(1_R)$.*

§3 Factorization in Polynomial Rings

Definition 3.1.

Theorem 3.2. *Let R be a ring and $f, g \in R[x_1, \ldots, x_n]$.*

1. $\deg(f + g) \leq \max\{\deg f, \deg g\}$.

2. $\deg(fg) \leq \deg f + \deg g$.

3. *If R has no zero divisors,* $\deg(fg) = \deg f + \deg g$.

4. *If $n = 1$ and the leading coefficient of f or g is not a zero divisor, then* $\deg(fg) = \deg f + \deg g$.

Theorem 3.3 (The division algorithm). *Let R be a ring and $f, g \in R[x]$ nonzero polynomials such that the leading coefficient of g is a unit in R. Then there exist unique polynomials $q, r \in R[x]$ such that*

$$f = qg + r \text{ and } \deg r < \deg g$$

Corollary 3.4 (Remainder Theorem). *Let R be a ring with identity and*

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x].$$

For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

Corollary 3.5. *If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain.*

Definition 3.6. *Let R be a subring of a commutative ring S, $c_1, c_2, \ldots, c_n \in S$ and $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}} \in R[x_1, \ldots, x_n]$ a polynomial such that $f(c_1, c_2, \ldots c_n) = 0$. Then $(c_1, c_2, \ldots, c_n)$ is said to be a root or zero of f (or a solution of the polynomial equation $f(x_1, \ldots, x_n) = 0$).*[4]

Theorem 3.7. *Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.*

Theorem 3.8. *If D is an integral domain contained in an integral domain E and $f \in D[x]$ has degree n, then f has at most n distinct roots in E.*

Definition 3.9. *Let D be an integral domain and $f \in D[x]$. If $c \in D$ and c is a root of f, then there is a greatest integer $m (0 \leq m \leq \deg f)$ such that*

$$f(x) = (x - c)^m g(x)$$

*where $g(x) \in R[x]$ and $x - c \nmid g(x)$. The integer m is called the **multiplicity** of the root c of f. If c has multiplicity 1, c is said to be a **simple root**. If c has multiplicity $m > 1$, c is called a multiple root.*

Theorem 3.10. *Let D be an integral domain which is a subring of an integral domain E. Let $f \in D[x]$ and $c \in E$.*

1. *c is a multiple root of f if and only if $f(c) = 0$ and $f'(c) = 0$.*
2. *If D is a field and f is relatively prime to f', then f has no multiple roots in E.*
3. *If D is a field, f is irreducible in $D[x]$ and E contains a root of f, then f has no multiple roots in E if and only if $f' \neq 0$.*

§3.1 Over U.F.D

Definition 3.11. *Let D be a unique factorization domain and*

$$f=\sum_{i=0}^{n} a_i x^i$$

a nonzero polynomial in $D[x]$. A greatest common divisor of the coefficients $a_0, a_1, \ldots, a_n$ is called a ***content*** *of f and is denoted* $\operatorname{Cont}(f)$.

If $f \in D[x]$ and $\operatorname{Cont}(f)$ *is a unit in D, then f is said to be* ***primitive***. *Clearly for any polynomial $g \in D[x], g=\operatorname{Cont}(g) g_1$ with g_1 primitive.*

Theorem 3.12 (Gauss)**.** *If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) \approx C(f)C(g)$. In particular, the product of primitive polynomials is primitive.*

Proof. $f=\operatorname{Cont}(f) f_1$ and $g=\operatorname{Cont}(g) g_1$ with f_1, g_1 primitive. Consequently, $\operatorname{Cont}(g)=C\left(\operatorname{Cont}(f) f_1 \operatorname{Cont}(g) g_1\right) \approx \operatorname{Cont}(f) \operatorname{Cont}(g) C\left(f_1 g_1\right)$. Hence it suffices to prove that $f_1 g_1$ is primitive (that is, $C\left(f_1 g_1\right)$ is a unit).

If $f_1=\sum_{i=0}^n a_i x^i$ and $g_1=\sum_{j=0}^m b_j x^j$, then $f_1 g_1=\sum_{k=0}^{m+n} c_k x^k$ with $c_k=\sum_{i+j=k} a_i b_j$. If $f_1 g_1$ is not primitive, then there exists an irreducible element p in R such that $p \mid c_k$ for all k. Since $C\left(f_1\right)$ is a unit $p \nmid C\left(f_1\right)$, whence there is a least integer s such that

$$p \mid a_i \text{ for } i<s \text{ and } p \nmid a_s .$$

Similarly there is a least integer t such that

$$p \mid b_j \text{ for } j<t \text{ and } p \nmid b_t .$$

Since p divides $c_{s+t}=a_0 b_{s+t}+\cdots+a_{s-1} b_{t+1}+a_s b_t+a_{s+1} b_{t-1}+\cdots+a_{s+t} b_0, p$ must divide $a_s b_t$. Since every irreducible element in D is prime, $p \mid a_s$ or $p \mid b_t$. This is a contradiction. Therefore $f_1 g_1$ is primitive. □

Corollary 3.13. *Let D be a unique factorization domain with quotient field F*

1. *If f is a primitive polynomial of positive degree in $D[x]$, then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.*
2. *If f and g are primitive polynomials in $D[x]$. Then f and g are associates in $D[x]$ if and only if they are associates in $F[x]$.*

Theorem 3.14. *Let D be a unique factorization domain with quotient field F and let $f=\sum_{i=0}^n a_i x^i \in D[x]$. If $u=c/d \in F$ with c and d relatively prime, and u is a root of f, then c divides a_0 and d divides a_n.*

Theorem 3.15. *If D is a Unique Factorization Domain, then so $D[x]$.*

Proof. We have indicated above that $R[x]$ a Unique Factorization Domain forces R to be a Unique Factorization Domain. Suppose conversely that R is a Unique Factorization Domain, F is its field of fractions and $p(x)$ is a nonzero element of $R[x]$. Let d be

the greatest common divisor of the coefficients of $p(x)$, so that $p(x) = dp'(x)$, where the g.c.d. of the coefficients of $p'(x)$ is 1 . Such a factorization of $p(x)$ is unique up to a change in d (so up to a unit in R), and since d can be factored uniquely into irreducibles in R (and these are also irreducibles in the larger ring $R[x]$), it suffices to prove that $p'(x)$ can be factored uniquely into irreducibles in $R[x]$. Thus we may assume that the greatest common divisor of the coefficients of $p(x)$ is 1 . We may further assume $p(x)$ is not a unit in $R[x]$, i.e., degree $p(x) > 0$.

Since $F[x]$ is a Unique Factorization Domain, $p(x)$ can be factored uniquely into irreducibles in $F[x]$. By Gauss' Lemma, such a factorization implies there is a factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of the factors in $F[x]$. Since the greatest common divisor of the coefficients of $p(x)$ is 1 , the g.c.d. of the coefficients in each of these factors in $R[x]$ must be 1 . By Corollary 6 , each of these factors is an irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducibles in $R[x]$.

The uniqueness of the factorization of $p(x)$ follows from the uniqueness in $F[x]$. Suppose

$$p(x) = q_1(x) \cdots q_r(x) = q'_1(x) \cdots q'_s(x)$$

are two factorizations of $p(x)$ into irreducibles in $R[x]$. Since the g.c.d. of the coefficients of $p(x)$ is 1 , the same is true for each of the irreducible factors above in particular, each has positive degree. By Corollary 6, each $q_i(x)$ and $q'_j(x)$ is an irreducible in $F[x]$. By unique factorization in $F[x]$, $r = s$ and, possibly after rearrangement, $q_i(x)$ and $q'_i(x)$ are associates in $F[x]$ for all $i \in \{1, \ldots, r\}$. It remains to show they are associates in $R[x]$. Since the units of $F[x]$ are precisely the elements of $F^\times$we need to consider when $q(x) = \frac{a}{b}q'(x)$ for some $q(x), q'(x) \in R[x]$ and nonzero elements a, b of R, where the greatest common divisor of the coefficients of each of $q(x)$ and $q'(x)$ is 1 . In this case $bq(x) = aq'(x)$; the g.c.d. of the coefficients on the left hand side is b and on the right hand side is a. Since in a Unique Factorization Domain the g.c.d. of the coefficients of a nonzero polynomial is unique up to units, $a = ub$ for some unit u in R. Thus $q(x) = uq'(x)$ and so $q(x)$ and $q'(x)$ are associates in R as well. This completes the proof. □

Corollary 3.16. *If R is a Unique Factorization Domain, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a Unique Factorization Domain.*

Theorem 3.17 (Eisenstein's Criterion)**.** *Let D be a unique factorization domain with quotient field F . If $f = \sum_{i=0}^n a_i x^i \in D[x]$,* deg $f \geq 1$ *and p is an irreducible element of D such that*

(i) $p \nmid a_n$

(ii) $p \mid a_i$ *for* $i = 0, 1, \ldots, n-1$

(iii) $p^2 \nmid a_0$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Part III

Modules Theory

Chapter VIII

Modules

Contents

§1 Basic Definition

Definition 1.1. *Let R be a ring. A **left** R**-module** is an additive abelian group M together with a function $R \times M \to M$ such that for all $r, s \in R$ and $a, b \in M$:*

(i) $r(a+b) = ra + rb$.

(ii) $(r+s)a = ra + sa$

(iii) $r(sa) = (rs)a$

(iv) $1_R a = a$ *for all* $a \in M$

*then M is said to be a R**-module**. If R is a division ring, then a R-module is called a (left) **vector space**.*

Remark. *If R has no identity or (iv) fails, we call M **non-unital module** or **pseudo-module**. In the vast majority of cases, the objects we study are modules.*

Definition 1.2. *Let R be a ring, M an R-module and N a nonempty subset of M. Then N is a **submodule** of M provided that $N < M$ and $rb \in N$ for all $r \in R$, $b \in N$. A submodule of a vector space over a division ring is called a **subspace**.*

Proposition 1.3. *Let M be an R-module.*

1. *If N is a nonempty subset of M, then N is a submodule of M if and only if for all $x, y \in N$ and $r \in R$, $x - y \in N$ and $rx \in N$*
2. *If $\{N_\alpha\}$ is a chain of submodules, then so $\bigcup N_\alpha$.*
3. *If $\{N_\alpha\}$ is a family of submodules, then so $\bigcap N_\alpha$.*

§1.1 Submodule generated by sets

Definition 1.4. *Let M be a R-module.*

1. *If X is a subset of M, then the intersection of all submodules of M containing X is called the **submodule generated by** X (or spanned by X).*
2. *If X is finite, and X generates the submodule N, then N is said to be **finitely generated** and X spans N. If $X = \{a\}$, then the submodule generated by X is called the **cyclic module generated by** a.*
3. *if $\{B_i : i \in I\}$ is a family of submodules of M, then the submodule generated by $X = \bigcup_{i \in I} B_i$ is called the **sum of the modules** B_i, denoted by $\sum_{i \in I} B_i$.*

4. *If I is a left ideal of R and S is a nonempty subset of M. Then*

$$IS = \left\{ \sum_{i=1}^{n} r_i a_i : r_i \in I; a_i \in S; n \in \mathbb{N}^* \right\}$$

is a submodule of M. Similarly if $a \in M$, then $Ia = \{ra \mid r \in I\}$ is a submodule of M.

Theorem 1.5. *Let R be a ring, M an R-module, X a subset of M, $\{M_\alpha\}$ a family of submodules of M.*

1. *The submodule generated by X is*

$$RX = \left\{ \sum_{i=1}^{s} r_i a_i : s \in \mathbb{Z}_{\geq 1}; a_i \in X; r_i \in R \right\}$$

2. *The submodule generated by the family $\{M_\alpha\}$ consists of all finite sums that is*

$$\sum M_\alpha = \{x_{i_1} + \cdots + x_{i_n} : n \in \mathbb{Z}_{\geq 1}; x_{i_k} \in M_{\alpha_k}\}$$

§1.2 Quotient module and homomorphism

Definition 1.6. *Let M and N be modules over a ring R.*

1. *A function $f : M \to N$ is an R-**module homomorphism** provided that for all $x, y \in M$ and $r \in R$:*

$$f(x + y) = f(x) + f(y) \text{ and } f(rx) = rf(x)$$

*If R is a division ring, then an R-module homomorphism is called a **linear transformation**.*

2. *Four submodules* $\operatorname{Ker} f = f^{-1}(0)$, $\operatorname{Im}(F) = f(M)$, $\operatorname{Coker}(f) = N/\operatorname{Im}(f)$, $\operatorname{Coim}(f) = M/\operatorname{Ker}(f)$

3. *define* $\operatorname{Hom}_R(M, N)$ *to be the set of all R-module homomorphisms from M into N, which forms a R-module.*

Proposition 1.7. *The following conditions of module-homomorphism $f : M \to N$ are equivalent*

1. *f is injective*

2. $\operatorname{Ker}(f) = 0$

3. *f is monomorphism ($fg = fh \Rightarrow g = h$)*

4. $fg = 0 \Rightarrow g = 0$

Definition 1.8. *Let N be a submodule of a module M over a ring R. Then the quotient group M/N is an R-module with the action of R on M/N given by:*

$$r(x+N) = rx + N \quad \textit{for all } r \in R, a \in M$$

called quotient module. The map $\pi : M \to M/N$ given by $x \mapsto x+N$ is an R-module epimorphism with kernel N. The map π is called the ***canonical epimorphism (or projection)***.

Theorem 1.9. *Let R be a ring, $f : M \to N$ an R-module homomorphism and L is a submodule of* $\operatorname{Ker} f$*, then*

1. *There is a unique R-module homomorphism*

$$\overline{f} : M/L \to N \quad \textit{such that } \overline{f}(x+L) = f(x) \textit{ for all } x \in M$$

with $\operatorname{Im} \overline{f} = \operatorname{Im} f$ *and* $\operatorname{Ker} \overline{f} = \operatorname{Ker} f/L$.

2. *$\overline{f}$ is an R-module isomorphism if and only if f is an R-module epimorphism and $C = \operatorname{Ker} f$. In particular, $M/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Corollary 1.10. *If R is a ring and M' is a submodule of the R-module M and N' a submodule of the R-module N and $f : M \to N$ is an R-module homomorphism such that $f(A') \subset B'$, then*

(1) f induces an R-module homomorphism $\overline{f} : A/A' \to B/B'$ given by $a + A' \mapsto f(a) + B'$. $\overline{f}$ is an R -module isomorphism if and only if $\operatorname{Im} f + B' = B$ and $f^{-1}(B') \subset A'$.

In particular if f is an epimorphism such that $f(A') = B'$ and $\operatorname{Ker} f \subset A'$, then $\overline{f}$ is an R-module isomorphism.

Theorem 1.11. *Let B and C be submodules of a module A over a ring R .*

(1) There is an R -module isomorphism $B/(B \cap C) \cong (B+C)/C$;

(2) if $C \subset B$, then B/C is a submodule of A/C, and there is an R -module isomorphism $(A/C)/(B/C) \cong A/B$.

Theorem 1.12. *Let R be a ring and N is a submodule of an R-module M, then*

1. *There is a one-to-one correspondence between the set of all submodules of M containing N and the set of all submodules of M/N, given by $L \mapsto L/N$.*

2. *Hence every submodule of M/N is of the form L/N, where L is a submodule of M which contains N.*

§1.3 Annihilator

Definition 1.13. *Let R be a ring and M an left R-module. If X be a subset of M*

1. *The left ideal*
$$\operatorname{Ann}(X) = \{r \in R \mid rX = 0\}$$
is called the ***annihilator*** *of X in R.*

2. *If* $\operatorname{Ann}(u) \neq 0$*, u is called to be* ***torsion element****.*

   If $\operatorname{Ann}(u) = 0$*, u is called to be* ***free-torsion element****.*

3. *If* $\operatorname{Ann}(u) = 0$ *for all $u \in M$, then M is called to be a* ***torsion-free*** module.

   If $\operatorname{Ann}(u) \neq 0$ *for all $u \in M$, then M is called to be a* ***torsion module****.*

4. *If R is a integral domain, the set $T(M)$ consists of all torsion element is called the* ***torsion submodule*** *of M*

Proposition 1.14. *Let N, N_1, N_2 be submodule of M.*

1. $\operatorname{Ann}(N_1 + N_2) = \operatorname{Ann}(N_1) + \operatorname{Ann}(N_2)$

2. $\operatorname{Ann}(M/N) = (N : M)$

3. $(N_1 : N_2) = (N_1 : (N_1 + N_2)) = \operatorname{Ann}((N_1 + N_2)/N_1)$

Definition 1.15. *The module M is said to be a* ***faithful*** *R-module if* $\operatorname{Ann}(M) = 0$.

Remark. *It's obvious that M is a faithful $R/\operatorname{Ann}(M)$-module*

§2 Modules Category

We only consider left module in this section.

§2.1 Direct Products and Direct Sums

Definition 2.1. *Let R be a ring and $\{M_i : i \in I\}$ a nonempty family of left R-modules, $\prod_{i\in I} M_i$ the direct product of the abelian groups M_i, and $\bigoplus_{i\in I} M_i$ the direct sum of the abelian groups M_i.*

1. *$\prod_{i\in I} M_i$ is an left R-module with the action of R given by $r\{a_i\} = \{ra_i\}$.*

2. *$\bigoplus_{i\in I} M_i$ is a submodule of $\prod_{i\in I} M_i$.*

3. *For each $k \in I$, the canonical projection $\pi_k : \prod M_i \to M_k$ is an left R-module epimorphism.*

4. *For each $k \in I$, the canonical injection $\iota_k : M_k \to \bigoplus M_i$ is an left R-module monomorphism.*

The ring $\prod_{i\in I} M_i$ is called the ***(external) direct product*** *of the family of R-modules $\{M_i \mid i \in I\}$ and $\bigoplus_{i\in I} M_i$ is its* ***(external) direct sum****. The maps π_k are called the* ***canonical projections*** *ang ι_k are called* ***canonical injections****.*

Theorem 2.2. *Let R be a ring.*

1. *If $\{M_i \mid i \in I\}$ a family of R-modules, M an R-module, and $\{f_i : M \to M_i \mid i \in I\}$ a family of R-module homomorphisms, then there is a unique R-module homomorphism $f : M \to \prod_{i\in I} M_i$ such that the diagram*

$$\begin{tikzcd} M \arrow[r, "\exists! f"] \arrow[d, "f_i"'] & \prod\limits_{i\in I} M_i \\ M_i \arrow[ur, "\pi_i"] & \end{tikzcd}$$

   is commutative for all $i \in I$. $\prod_{i\in I} M_i$ is uniquely determined up to isomorphism by this property. In other words, $\prod_{i\in I} M_i$ is a product in the category of left R-modules.

2. *If $\{N_i\}_{i\in I}$ is a family of R-modules, N an R-module, and $g_i \in \mathrm{Hom}_R(N_i, N)$ $i \in I$, then there is a unique R-module homomorphism $g : \oplus_{i\in I} N_i \to N$ such that the diagram*

$$\begin{tikzcd} \bigoplus\limits_{i\in I} N_i \arrow[r, "\exists! g"] \arrow[d, "\iota_i"'] & N \\ N_i \arrow[ur, "g_i"] & \end{tikzcd}$$

   is commutative for all $i \in I$. $\bigoplus_{i\in I} N_i$ is uniquely determined up to isomorphism by this property. In other words, $\bigoplus_{i\in I} N_i$ is a coproduct in the category of R-modules.

Remark. *It follows that*

$$\prod \mathrm{Hom}_R(A, A_i) \cong \mathrm{Hom}_R\left(A, \prod A_i\right)$$

$$\prod \mathrm{Hom}_R(A_i, A) \cong \mathrm{Hom}_R\left(\bigoplus A_i, A\right)$$

Theorem 2.3. *Let R be a ring and $M, M_1, M_2, \ldots, M_n$, R-modules. Then $M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_n$ if and only if for each $i = 1, 2, \ldots, n$ there are R-module homomorphisms $\pi_i : M \to M_i$ and $\iota_i : M_i \to M$ such that*

(i) $\pi_i \iota_i = 1_{M_i}$ *for* $i = 1, 2, \ldots, n$

(ii) $\pi_j \iota_i = 0$ *for* $i \neq j$

(iii) $\iota_1\pi_1 + \iota_2\pi_2 + \cdots + \iota_n\pi_n = 1_M$.

Theorem 2.4. *Let R be a ring and $\{M_i : i \in I\}$ a family of submodules of an R-module M such that*

(i) $M = \sum_i M_i$

(ii) for each $k \in I$, $M_k \cap \sum_{i \neq k} M_i = 0$

Then there is an isomorphism $M \cong \bigoplus_{i \in I} M_i$. The module M is said to be the ***internal direct sum*** *of $\{M_i : i \in I\}$.*

Corollary 2.5. *Let R be a ring and $\{R_i : i \in I\}$ a family of subrings of an R such that*

(i) $R = \sum_i R_i$

(ii) for each $k \in I$, $R_k \cap \sum_{i \neq k} R_i = 0$

Then there is an isomorphism $M \cong \bigoplus_{i \in I} R_i$.

§2.2 Free Modules

Definition 2.6. *Let R be a ring and M an left R-module*

1. *A subset X of M is said to be* ***linearly independent*** *provided that for some finite distinct $x_1, \ldots, x_n \in X$ and $r_i \in R$.*

$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n = 0 \Rightarrow r_i = 0 \textit{ for every } i$$

   Conversely, a set that is not linearly independent is said to be ***R-linearly dependent****.*

2. *The $\{u_i\}_{i \in I}$ is called to be a* ***maximal linearly independent subset*** *of M provided that it is not contained in any larger linearly independent subset of M.*

3. *A linearly independent subset that spans M is called a* ***(Hamel) basis*** *of M.*

Remark. *A basis must be a maximal linearly independent subset.*

Definition 2.7. *Let R be a ring and X a nonempty set. An left R-module F is called a* ***free module*** *on X if F is a free object on X in the category of all left R-modules, i.e. there is a function $\iota : X \to F$ such that the diagram*

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr, "f"'] & F(X) \arrow[d, dashed, "\exists! \tilde{f}"] \\ & M \end{tikzcd}$$

is commutative for any left R-module M and function $f : X \to M$ there is a unique R-module homomorphism $\tilde{f} : F(X) \to M$ with $\tilde{f}\iota = f$.

Theorem 2.8. *Let R be a ring. The following conditions on a R-module F are equivalent:*

1. *F has a nonempty basis;*

2. *F is the internal direct sum of a family of cyclic R-modules, each of which is isomorphic as a left R-module to R,*

3. *F is R-module isomorphic to a direct sum of copies of the left R-module R*

Corollary 2.9. .

1. *Every module M over a ring R is the homomorphic image of a free R-module F.*

2. *M is a finitely generated $\Leftrightarrow$ M is isomorphic to a quotient of free module R^n for some integer $n > 0$.*

Dimension and invariant dimension property

Definition 2.10. *Let R be a ring. If any two bases of free R-module F have the same cardinality, then R is said to have the* ***invariant dimension property*** *and the cardinal number of any basis of F is called the* ***dimension*** *of* ***rank*** *of F.*

Proof of invariant dimension property

Theorem 2.11. *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. Step 1. If Y is another basis of F, then we claim that Y is infinite. Suppose on the contrary that Y were finite. Since Y generates F and every element of Y is a linear combination of a finite number of elements of X, it follows that there is a finite subset $\{x_1, \ldots, x_m\}$ of X, which generates Y, thus generates F. Since X is infinite, there exists

$$x \in X - \{x_1, \ldots, x_m\}$$

Then for some $r_i \in R, x = r_1x_1 + \cdots + r_mx_m$, which contradicts the linear independence of X. Therefore, Y is infinite.

Step 2. Let $K(Y)$ be the set of all finite subsets of Y. Define a map

$$f : X \to K(Y)$$

by

$$x \mapsto \{y_1, \ldots, y_n\}$$

where $x = r_1y_1 + \cdots + r_ny_n$ and $r_i \neq 0$ for all i. Since Y is a basis, the y_i are uniquely determined and f is a well-defined function.

Step 3. If $\operatorname{Im} f$ were finite, then

$$\bigcup_{S \in \operatorname{Im} f} S$$

would be a finite subset of Y that would generate X and hence F. This leads to a contradiction of the linear independence of Y as in the preceding paragraph. Hence $\operatorname{Im} f$ is infinite.

Step 4. Next we show that $f^{-1}(T)$ is a finite subset of X for every $T \in \operatorname{Im} f \subset K(Y)$. If $x \in f^{-1}(T)$, then x is contained in the submodule $\langle T\rangle$ of F generated by T; that is,

$$f^{-1}(T) \subset \langle T\rangle$$

Since T is finite and each $y \in T$ is a linear combination of a finite number of elements of X, there is a finite subset S of X such that $\langle T\rangle \subset \langle S\rangle$. Thus $x \in f^{-1}(T)$ implies $x \in \langle S\rangle$ and x is a linear combination of elements of S. Since $x \in X$ and $S \subset X$, this contradicts the linear independence of X unless $x \in S$. Therefore, $f^{-1}(T) \subset S$, whence $f^{-1}(T)$ is finite.

Step 5. Verify that the sets $f^{-1}(T)$ form a partition of X,

$$X = \bigsqcup_{T \in \operatorname{Im} f} f^{-1}(T)$$

For each $T \in \operatorname{Im} f$, order the elements of $f^{-1}(T)$, say $x_1, \ldots, x_n$, and define an injective map

$$g_T : f^{-1}(T) \to \operatorname{Im} f \times N \quad \text{by } x_k \mapsto (T, k).$$

It follows that the map $X \to \operatorname{Im} f \times N$ defined by $x \mapsto g_T(x)$, where $x \in f^{-1}(T)$, is a well-defined injective function, whence $|X| \leq |\operatorname{Im} f \times N|$. Therefore

$$|X| \leq |\operatorname{Im} f \times N| = |\operatorname{Im} f| \leq |K(Y)| = |Y|$$

since $|\operatorname{Im} f|$ is infinite.

Step 6. Interchanging X and Y in the preceding argument shows that $|Y| \leq |X|$. Therefore $|Y| = |X|$ by the Schroeder-Bernstein Theorem. □

Lemma 2.12. *Let R be a ring, $I (\neq R)$ an ideal of R, F a free R-module with basis X. Then F/IF is a free R/I-module with basis $\pi(X)$ and $|\pi(X)| = |X|$ where $\pi : F \to F/IF$ is the canonical epimorphism.*

Proof. If $u + IF \in F/IF$, then $u = \sum_{j=1}^{n} r_j x_j$ with $r_j \in R, x_j \in X$ since $u \in F$ and X is a basis of F. Consequently,

$$u + IF = \sum_j (r_j x_j + IF) = \sum_j (r_j + I)(x_j + IF) = \sum_j (r_j + I)\,\pi(x_j)$$

whence $\pi(X)$ generates F/IF as an R/I-module.

On the other hand, if $\sum_{k=1}^{m} (r_k + I)\,\pi(x_k) = 0$ with $r_k \in R$ and $x_1, \ldots, x_m$ distinct elements of X, then

$$0 = \sum_k (r_k + I)\,\pi(x_k) = \sum_k (r_k + I)(x_k + IF) = \sum_k r_k x_k + IF$$

whence $\sum_k r_k x_k \in IF$. Thus $\sum_k r_k x_k = \sum_j s_j u_j$ with $s_j \in I, u_j \in F$. Since each u_j is a linear combination of elements of X and I is an ideal, $\sum_j s_j u_j$ is a linear combination of elements of X with coefficients in I. Consequently,

$$\sum_{k=1}^{m} r_k x_k = \sum_j s_j u_j = \sum_{t=1}^{d} c_t y_t$$

with $c_t \in I, y_t \in X$. The linear independence of X implies that $r_k \in I$ for every k. Hence $r_k + I = 0$ in R/I for every k and $\pi(X)$ is linearly independent over R/I. Thus F/IF is a free R/I-module with basis $\pi(X)$.

Finally if $x, x' \in X$ and $\pi(x) = \pi(x')$ in F/IF, then

$$0 = (1_R + I)\,\pi(x) - (1_R + I)\,\pi(x') = (1_R + I)(x + IF) - (1_R + I)(x' + IF)$$

If $x \neq x'$, the preceding argument implies that $1_R + I = 0$ in R/I, which contradicts the fact that $I \neq R$. Therefore, $x = x'$ and the map $\pi : X \to \pi(X)$ is a bijection, whence $|X| = |\pi(X)|$. □

Theorem 2.13. .

1. *Division ring has the invariant dimension property.*
2. *Let $f : R \to S$ be a nonzero epimorphism of rings. If S has the invariant dimension property, then so does R .*
3. *If R is a ring that has a homomorphic image which is a division ring, then R has the invariant dimension property.*
4. *Every commutative ring has the invariant dimension property.*

Proof. (2) Let $I = \operatorname{Ker} f$; then $S \cong R/I$. Let X and Y be two bases of the free unitary R-module F and $\pi : F \to F/IF$ the canonical epimorphism. By Lemma F/IF is a free R/I-module (and hence a free unitary S-module) with bases $\pi(X)$ and $\pi(Y)$ such that $|X| = |\pi(X)|, |Y| = |\pi(Y)|$. Since S has the invariant dimension property, $|\pi(X)| = |\pi(Y)|$. Therefore, $|X| = |Y|$ and R has the invariant dimension property.

(3) It is obvious from (1) and (2)

(4) Consider the maximal ideal $\mathfrak{m}$ in R and canonical projective

$$R \to R/\mathfrak{m}$$

□

Theorem 2.14. *Let R be a ring and M a module over R. Let I be a non-empty set, and let $\{x_i\}_{i\in I}$ be a basis of M. Let N be an R-module, and let $\{y_i\}_{i\in I}$ be a family of elements of N. Then there exists a unique homomorphism $f : M \to N$ such that $f(x_i) = y_i$ for all i.*

§2.3 Vector Space

Theorem 2.15. *Let D be a division ring.*

1. *A maximal linearly independent subset X of a vector space V over a division ring D is a basis of V.*
2. *Basis Extension Theorem. Let V be a vector space, T spans V and S be a subset of T which is linearly independent. Then there exists a basis B of V such that $S \subset B \subset T$.*
3. *Every vector space V over a division ring D has a basis and is therefore a free D-module.*
4. *Let V be a vector space over D. Then two bases of V over D have the same cardinality.*

Definition 2.16. *If V is a finitely generated D-module the cardinality of any basis is called the* ***dimension of*** *V and is denoted by $\dim_D V$, or just $\dim V$, and V is said to be finite dimensional over D. If V is not finitely generated, V is said to be* ***infinite dimensional*** *(written $\dim V = \infty$).*

Theorem 2.17. *Let W be a subspace of a vector space V over a division ring D.*

1. $\dim_D W \leq \dim_D V$
2. *if* $\dim_D W = \dim_D V < \infty$*, then* $W = V$
3. $\dim_D V = \dim_D W + \dim_D(V/W)$.
4. *If V_1 and V_2 are finite dimensional subspaces of a vector space over D, then*

$$\dim_D V_1 + \dim_D V_2 = \dim_D(V_1 \cap V_2) + \dim_D(V_1 + V_2)$$

Corollary 2.18. *If $f : V \to V'$ is a linear transformation of vector spaces over a division ring D, then there exists a basis X of V such that $X \cap \operatorname{Ker} f$ is a basis of $\operatorname{Ker} f$ and $X \cap f^{-1}(\operatorname{Im} f)$ is a basis of $\operatorname{Im} f$. In particular,*

$$\dim_D V = \dim_D(\operatorname{Ker} f) + \dim_D(\operatorname{Im} f)$$

Theorem 2.19. *Let R, S, T be division rings such that $R \subset S \subset T$. Then*

$$\dim_R T = (\dim_S T)\,(\dim_R S)$$

Furthermore, $\dim_R T$ is finite if and only if $\dim_S T$ and $\dim_R S$ are finite.

§2.4 Pullbacks and Pushout

Definition 2.20. *Let R be a ring and in R-***Mod***.*

1. *Given a diagram*

$$A_1 \xrightarrow{f_1} B \xleftarrow{f_2} A_2$$

*The **pullback** of f_1 and f_2 is the submodule*

$$P = \{(a_1, a_2) \in A_1 \oplus A_2 \mid f_1(a_1) = f_2(a_2)\}$$

of the direct product $A_1 \oplus A_2$ together with the canonical projections $\pi_1 : P \to A_1$ and $\pi_2 : P \to A_2$. That is,

$$\begin{tikzcd}
X \arrow[drr, bend left, "q_2"] \arrow[ddr, bend right, "q_1"'] \arrow[dr, dashed, "\exists! u"] & & \\
& P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & A_2 \arrow[d, "f_2"] \\
& A_1 \arrow[r, "f_1"] & B
\end{tikzcd}$$

2. *Given a diagram*

$$B_1 \xleftarrow{f_1} A \xrightarrow{f_2} B_2$$

*The **pushout** of f_1 and f_2 is the quotient module*

$$P = (B_1 \oplus B_2)/K$$

where K is the submodule of $B_1 \oplus B_2$ generated by all elements of the form $(f_1(a), -f_2(a))$ with $a \in A$, together with the canonical injections $\iota_1 : B_1 \to P$ and $\iota_2 : B_2 \to P$. That is,

$$\begin{tikzcd}
A \arrow[r, "f_2"] \arrow[d, "f_1"'] & B_2 \arrow[d, "\iota_2"] \arrow[ddr, bend left] & \\
B_1 \arrow[r, "\iota_1"'] \arrow[drr, bend right] & P \arrow[dr, dashed] & \\
& & Y
\end{tikzcd}$$

§3 Tensor Products

§3.1 Basic definition

Definition 3.1. *Let R be a ring, A_R be a right module and ${}_RB$ a left module. Let F be the free abelian group on the set $A \times B$. Let K be the subgroup of F generated by all elements of the following forms :*

$$(a + a', b) - (a, b) - (a', b)\,,\ (a, b + b') - (a, b) - (a, b')\,, (ar, b) - (a, rb)$$

The quotient group F/K is called the ***tensor product*** *of A_R and ${}_RB$; it is denoted $A \otimes_R B$. The coset $(a, b) + K$ of the element (a, b) in F is denoted $a \otimes b$; the coset of $(0, 0)$ is denoted 0 .*

Theorem 3.2. *Let R and S be rings and ${}_SA_R$, ${}_RB$, C_R, ${}_RD_S$ bimodules as indicated.*

1. *$A \otimes_R B$ is a left S-module such that*

$$s(a \otimes b) := sa \otimes b$$

for all $s \in S, a \in A$, $b \in B$.

2. *$C \otimes_R D$ is a right S-module such that $(c \otimes d)s = c \otimes ds$ for all $c \in C$, $d \in D, s \in S$.*

Remark. *An important special case occurs when R is a commutative ring and hence every R-module A is an R-R bimodule. In this case $A \otimes_R B$ is also an R-R bimodule with*

$$r(a \otimes b) = ra \otimes b = ar \otimes b = a \otimes rb = a \otimes br = (a \otimes b)r$$

for all $r \in R, a \in A, b \in B$.

Definition 3.3. *If A_R and ${}_RB$ are modules over a ring R, and C is an abelian group, then a* ***middle linear (or banlanced) map*** *from $A \times B$ to C is a function $f : A \times B \to C$ such that for all $a, a_i \in A, b, b_i \in B$, and $r \in R$:*

$$\begin{aligned} f(a_1 + a_2, b) &= f(a_1, b) + f(a_2, b) \\ f(a, b_1 + b_2) &= f(a, b_1) + f(a, b_2) \\ f(ar, b) &= f(a, rb) \end{aligned}$$

Remark. *The map $i : A \times B \to A \otimes_R B$ given by $(a, b) \mapsto a \otimes b$ is a middle linear map, that is, for all $a, a_i \in A, b, b_i \in B$, and $r \in R$*

$$\begin{aligned} (a_1 + a_2) \otimes b &= a_1 \otimes b + a_2 \otimes b \\ a \otimes (b_1 + b_2) &= a \otimes b_1 + a \otimes b_2 \\ ar \otimes b &= a \otimes rb \end{aligned}$$

The map i is called the ***canonical middle linear map****.*

Theorem 3.4 (Universal property of canonical middle linear map)**.** *Let A_R and ${}_RB$ be modules over a ring R, and let C be an abelian group. If $g : A \times B \to C$ is a middle linear map, then there exists a unique group homomorphism $\overline{g} : A \otimes_R B \to C$ such that*

$$\begin{tikzcd} A \times B \arrow[r, "g"] \arrow[d, "i"] & C \\ A \otimes_R B \arrow[ur, dashed, "\exists! \overline{g}"'] & \end{tikzcd}$$

is commutative. This proves that $i : A \times B \to A \otimes_R B$ is a universal object in the category of all middle linear maps on $A \times B$, whence $A \otimes_R B$ is uniquely determined up to isomorphism.

Definition 3.5. *Let A, B, C be modules over a commutative ring R. A **bilinear map** from $A \times B$ to C is a function $f : A \times B \to C$ such that for all $a_i \in A, b_i \in B$, and $r \in R$:*

$$\begin{aligned} f(a_1 + a_2, b) &= f(a_1, b) + f(a_2, b) \\ f(a, b_1 + b_2) &= f(a, b_1) + f(a, b_2) \\ f(ra, b) &= rf(a, b) = f(a, rb) \end{aligned}$$

*If A and B are modules over a commutative ring R, then so is $A \otimes_R B$ and the canonical middle linear map $i : A \times B \to A \otimes_R B$ is easily seen to be bilinear. In this context i is called the **canonical bilinear map**.*

Theorem 3.6 (Universal property of canonical bilinear map)**.** *If A, B, C are modules over a commutative ring R and $g : A \times B \to C$ is a bilinear map, then there is a unique R-module homomorphism $\overline{g} : A \otimes_R B \to C$ such that*

$$\begin{tikzcd} A \times B \arrow[r, "g"] \arrow[d, "i"] & C \\ A \otimes B \arrow[ur, dashed, "\exists! \overline{g}"'] & \end{tikzcd}$$

where $i : A \times B \to A \otimes_R B$ is the canonical bilinear map. The module $A \otimes_R B$ is uniquely determined up to isomorphism by this property.

Proposition 3.7. *If $A_R, A'_R, {}_RB$ and ${}_RB'$ are modules over a [resp. commutative] ring R and $f : A \to A'$, $g : B \to B'$ are R-module homomorphisms, then there is a unique group [resp. R-module] homomorphism*

$$f \otimes g : A \otimes_R B \to A' \otimes_R B' \quad \text{such that } a \otimes b \mapsto f(a) \otimes g(b)$$

for all $a \in A, b \in B$.

§3.2 Operation of tensor products

Theorem 3.8. *Let R and S be rings and ${}_SA_R$, ${}_RB$, C_R, ${}_RD_S$ (bi)modules as indicated.*

1. *If $f : A \to A'$ is a homomorphism of S-R bimodules and $g : B \to B'$ is an R-module homomorphism, then the induced map $f \otimes g : A \otimes_R B \to A' \otimes_R B'$ is a homomorphism of left S-modules.*

2. *If $h : C \to C'$ is an R -module homomorphism and $k : D \to D'$ a homomorphism of R-S bimodules, then the induced map $h : C \otimes_R D \to C' \otimes_R D'$ is a homomorphism of right S-modules.*

Theorem 3.9. *Let R, S be ring. Then*

1. *If A_R, $_RB_S$, $_SC$ are (bi)modules, then there is an abelian group isomorphism.*

$$(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C)$$

If A is an S-R module, there is a left S-module isomorphism $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$.

2. *Let A and $\{A_i \mid i \in I\}$ right R-modules, B and $\{B_j \mid j \in J\}$ left R-modules. Then there are abelian group isomorphisms:*

$$\left(\bigoplus_{i \in I} A_i\right) \otimes_R B \cong \bigoplus_{i \in I} (A_i \otimes_R B)$$

and

$$A \otimes_R \left(\bigoplus_{j \in J} B_j\right) \cong \bigoplus_{j \in J} (A \otimes_R B_j)$$

Proof. 1. By definition, we have

$$v = \sum_i u_i \otimes c_i = \sum_i \left(\sum_j a_{ij} \otimes b_{ij}\right) \otimes c_i = \sum_i \sum_j \left[(a_{ij} \otimes b_{ij}) \otimes c_i\right].$$

Therefore, $(A \otimes_R B) \otimes_S C$ is generated by all elements of the form $(a \otimes b) \otimes c$ $(a \in A, b \in B, c \in C)$. Similarly, $A \otimes_R (B \otimes_S C)$ is generated by all $a \otimes (b \otimes c)$ with $a \in A, b \in B, c \in C$.

Verify that the assignment $(\sum_{i=1}^n a_i \otimes b_i, c) \mapsto \sum_{i=1}^n [a_i \otimes (b_i \otimes c)]$ defines an S-middle linear map $(A \otimes_R B) \times C \to A \otimes_R (B \otimes_S C)$. Therefore, by 3.4 there is a homomorphism

$$\alpha : (A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$$

with $\alpha[(a \otimes b) \otimes c] = a \otimes (b \otimes c)$ for all $a \in A, b \in B, c \in C$. Similarly there is an homomorphism

$$\beta : A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$$

such that $\beta[a \otimes (b \otimes c)] = (a \otimes b) \otimes c$ for all $a \in A, b \in B, c \in C$. Therefore, α and β are isomorphisms.

2. Let ι_k, π_k be the canonical injections and projections of $\bigoplus_{i \in I} A_i$. The family of homomorphisms

$$\iota_k \otimes 1_B : A_k \otimes_R B \to \left(\bigoplus_{i \in I} A_i\right) \otimes_R B$$

induce a homomorphism

$$\alpha : \bigoplus_{i\in I} (A_i \otimes_R B) \to \left(\bigoplus_{i\in I} A_i\right) \otimes_R B$$

such that $\alpha(\{a_i \otimes b\}) = \bigoplus(\iota_i(a_i) \otimes b) = (\bigoplus \iota_i(a_i)) \otimes b$ (Note that the summation here is finite.) The assignment $(u, b) \mapsto \{\pi_i(u) \otimes b\}$ defines a middle linear map $\left(\bigoplus_{i\in I} A_i\right) \times B \to \bigoplus_{i\in I}(A_i \otimes_R B)$ and thus induces a homomorphism $\beta : (\bigoplus A_i) \otimes_R B \to \bigoplus(A_i \otimes_R B)$ such that $\beta(u \otimes b) = \{\pi_i(u) \otimes b\}$. We can show that $\alpha\beta$ and $\beta\alpha$ are the respective identity maps, whence α is an isomorphism. □

Theorem 3.10 (Adjoint Associativity). *Let R and S be rings and $A_R, {}_RB_S, C_S$ modules. Then there is an isomorphism of abelian groups*

$$\alpha : \mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)),$$

defined for each S-module homomorphism $f : A \otimes_R B \to C$ by

$$f \mapsto f(- \otimes -)$$

where $f(- \otimes -) : A \to \mathrm{Hom}_S(B, C)$ is the map defined by $a \mapsto f(a \otimes -)$

§3.3

Theorem 3.11. *If R is a ring and $A_R, {}_RB$ are R-modules, then there are right R-module isomorphisms*

$$A \otimes_R R \cong A$$

and left R-module isomorphisms

$$R \otimes_R B \cong B$$

Theorem 3.12. *Let R be a ring. If A is a right R-module and F is a free left R-module with basis Y. Then every element u of $A \otimes_R F$ may be written uniquely in the form $u = \sum_{i=1}^n a_i \otimes y_i$, where $a_i \in A$ and the y_i are distinct elements of Y.*

Proof. For each $y \in Y$, let A_y be a copy of A and consider the direct sum $\bigoplus_{y\in Y} A_y$. We first construct an isomorphism

$$\theta : A \otimes_R F \cong \bigoplus_{y\in Y} A_y$$

as follows. Since Y is a basis, $\{y\}$ is a linearly independent set for each $y \in Y$. Consequently, the R-module epimorphism

$$\varphi : R \to Ry \quad \text{given by } r \mapsto ry$$

is actually an isomorphism. Therefore there is for each $y \in Y$ an isomorphism

$$A \otimes_R Ry \xrightarrow{1_A \otimes \varphi^{-1}} A \otimes_R R \cong A = A_y.$$

Thus by 3.9 and I.8.10 there is an isomorphism θ :

$$A \otimes_R F = A \otimes_R \left(\bigoplus_{y \in Y} Ry \right) \cong \bigoplus_{y \in Y} A \otimes_R Ry \cong \bigoplus_{y \in Y} A_y$$

Verify that for every $a \in A, z \in Y$,

$$\theta(a \otimes z) = \{u_y\} \in \bigoplus A_y$$

where $u_z = a$ and $u_y = 0$ for $y \neq z$; in other words, $\theta(a \otimes z) = \iota_z(a)$, with $\iota_z : A_z \to \bigoplus A_y$ the canonical inection. Now every nonzero $v \in \bigoplus A_y$ is a finite sum $v = \iota_{y_1}(a_1) + \cdots + \iota_{y_n}(a_n)$ $= \theta(a_1 \otimes y_1) + \cdots + \theta(a_n \otimes y_n)$ with $y_1, \ldots, y_n$ distinct elements of Y and a_i uniquely determined nonzero elements of A. It follows that every element of $A \otimes_R F$ (which is necessarily $\theta^{-1}(v)$ for some v) may be written uniquely as $\bigoplus_{i=1}^n a_i \otimes y_i$. □

Corollary 3.13. *If R is a ring with identity and A_R and ${}_RB$ are free R-modules with bases X and Y respectively, then $A \otimes_R B$ is a free (right) R-module with basis $W = \{x \otimes y \mid x \in X, y \in Y\}$ of cardinality $|X||Y|$.*

REMARKS. Since R is an $R - R$ bimodule, so is every direct sum of copies of R. In particular, every free left R-module is also a free right R-module and vice versa. However, it is not true in general that a free (left) R-module is a free object in the category of $R - R$ bimodules (Exercise 12).

Proof. By the proof of Theorem 5.11 and by Theorem 2.1 (for right R-modules) there is a group isomorphism

$$\theta : A \otimes_R B \cong \bigoplus_{y \in Y} A_y = \sum_{y \in Y} A = \sum_{y \in Y} \left(\sum_{x \in X} xR \right).$$

Since B is an $R - R$ bimodule by the remark preceding the proof, $A \otimes_R B$ is a right R-module by Theorem 5.5. Verify that θ is an isomorphism of right R-modules such that $\theta(W)$ is a basis of the free right R-module $\sum_Y (\sum_X xR)$. Therefore, $A \otimes_R B$ is a free right R-module with basis W. Since the elements of W are all distinct by Theorem 5.11, $|W| = |X||Y|$. □

§4 Algebra

Definition 4.1. *Let K be a commutative ring. The abelian group $(A, +)$ is a R-**algebra** if*

(i) $(A, +, \cdot)$ *is a R-module*

(ii) $(A, +, \times)$ *is a ring*

(iii) $r \cdot (a \times b) = (ra)b = a(rb)$ *for all* $r \in R$ *and* $a, b \in A$.

If A *which, as a ring, is a division ring, is called a* ***division algebra***.

Remark. *Condition (ii) may fail to hold if* A *does not have an identity of noassociativity. In this case, we say that* A *is a* ***nonunital*** R***-algebra*** *or* ***noassociativity*** R***-algebra*** *respectively.*

An algebra over a field F *that is finite dimensional as a vector space over* K *is called a* ***finite dimensional algebra*** *over* F.

Definition 4.2. *Let* K *be a commutative ring with identity* 1 *and* A, B K*-algebras.*

1. *A* ***subalgebra*** *of* A *is a subring of* A *that is also a* K*-submodule of* A.
2. *A (left, right, two-sided)* ***algebra ideal*** *of* A *is a (left, right, two-sided) ideal of the ring* A *(in this case it is also a* K*-submodule of* A*).*
3. *A homomorphism [resp. isomorphism] of* K*-algebras* $f : A \to B$ *is a ring homomorphism [isomorphism] that is also a* K*-module homomorphism [isomorphism].*

Theorem 4.3 (Tensor product of algebras)**.** *Let* A *and* B *be algebras over a commutative ring* K. *Let* π *be the composition*

$$(A \otimes_K B) \otimes_K (A \otimes_K B) \xrightarrow{1_A \otimes \alpha \otimes 1_B} (A \otimes_K A) \otimes_K (B \otimes_K B) \xrightarrow{\pi_A \otimes \pi_B} A \otimes_K B$$

where π_A, π_B *are the product maps of* A *and* B *respectively. Then* $A \otimes_K B$ *is a* K*-algebra with product map* $\pi = \pi_A \otimes \pi_B$. *The* K*-algebra* $A \otimes_K B$ *is called the* ***tensor product of the*** K***-algebras*** A *and* B.

Proof. note that for generators $a \otimes b$ and $a_1 \otimes b_1$ of $A \otimes_K B$ the product is defined to be

$$(a \otimes b)(a_1 \otimes b_1) = \pi(a \otimes b \otimes a_1 \otimes b_1) = aa_1 \otimes bb_1$$

Thus if A and B have identities $1_A, 1_B$ respectively, then $1_A \otimes 1_B$ is the identity in $A \otimes_K B$. □

§5 Modules over Principal Ideal Domains

Rings are P.I.D and R-module M.

§5.1 Preparatory Lemmas

Theorem 5.1. *Let* F *be a free module over* R *and* N *a submodule of* F. *Then* N *is a free* R*-module and* rank $N \leq$ rank M.

Proof. Let $\{x_1, x_2, \ldots, x_n\}$ be a basis of F. We proceed by induction on n.

If $n = 1$, then $F \cong R$ and $N \cong I$ for some ideal I of R. Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. Therefore, $N \cong R$ or $N = 0$ is free and rank $N \leq$ rank F.

Suppose the theorem is true for $n - 1$ and let F be generated by n elements. Let $\pi : F \to R$ be the projection defined by

$$\pi\left(r_1 x_1 + r_2 x_2 + \cdots + r_n x_n\right) = r_n$$

for all $r_i \in R$. Then $\pi(N)$ is an ideal of R, whence $\pi(N) = (a)$ for some $a \in R$ since R is a principal ideal domain.

If $\pi(N) = 0$, then $N \subseteq \operatorname{Ker} \pi = \langle x_1, x_2, \ldots, x_{n-1} \rangle$. By the induction hypothesis, N is free and rank $N \leq n - 1 <$ rank F.

If $\pi(N) \neq 0$, let $z \in N$ such that $\pi(z) = a$. For each $y \in N$, there exists $r \in R$ such that $\pi(y) = ra = \pi(rz)$. Thus $y - rz \in \operatorname{Ker} \pi \cap N$. It follows that

$$N = Rz \oplus (\operatorname{Ker} \pi \cap N)$$

Since $\operatorname{Ker} \pi \cap N$ is a submodule of the free module $\operatorname{Ker} \pi = x_1, x_2, \ldots, x_{n-1}$, $\operatorname{Ker} \pi \cap N$ is free and rank$(\operatorname{Ker} \pi \cap N) \leq n - 1$ by the induction hypothesis. Therefore, N is free and

$$\operatorname{rank} N = 1 + \operatorname{rank}(\operatorname{Ker} \pi \cap N) \leq 1 + (n - 1) = n = \operatorname{rank} F$$

□

Corollary 5.2. *If M is a finitely generated by n elements, then every submodule of M may be generated by m elements with $m \leq n$.*

Corollary 5.3. *A module M over a principal ideal domain R is free if and only if M is projective.*

§5.2

Theorem 5.4. *A finitely generated torsion-free module M over a principal ideal domain R is free.*

Proof. Let M be generated by n elements. By Corollary 6.2, every submodule of M may be generated by m elements with $m \leq n$. We proceed by induction on n.

If $n = 1$, then $M \cong R/\operatorname{Ann}(M)$ is torsion-free, whence $\operatorname{Ann}(M) = 0$ and $M \cong R$ is free.

Suppose the theorem is true for $n - 1$ and let M be generated by n elements. Let N be a maximal submodule of M; then N may be generated by m elements with $m \leq n$. Since M/N is cyclic, there exists an epimorphism

$$f : R \to M/N$$

with $\operatorname{Ker} f = \operatorname{Ann}(M/N)$. If $\operatorname{Ann}(M/N) \neq 0$, then M/N has torsion, which contradicts the fact that M is torsion-free. Therefore, $\operatorname{Ann}(M/N) = 0$ and $M/N \cong R$ is free.

By the induction hypothesis, N is free since it is generated by at most $n-1$ elements. Consequently, the exact sequence

$$0 \to N \xrightarrow{\subseteq} M \to M/N \to 0$$

is split exact and $M \cong N \oplus M/N$ by Theorem 2.6 and Proposition 2.7. Therefore, M is free. □

Theorem 5.5. *If M is a finitely generated module over R, then*

$$M = \text{Tor}\,(M) \oplus F$$

where F is a free left R-module of finite rank and $F \cong M/\,\text{Tor}\,(M)$.

Proof. The quotient module M/M_t is torsion-free since for each $r \neq 0$,

$$r\,(a + M_t) = M_t \Rightarrow ra \in M_t \Rightarrow r_1(ra) = 0 \text{ for some } r_1 \neq 0 \Rightarrow a \in M_t$$

Furthermore, M/M_t is finitely generated since M is. Therefore, M/M_t is free of finite rank by Theorem 6.5. Consequently, the exact sequence

$$0 \to M_t \xrightarrow{\subseteq} M \to M/M_t \to 0$$

is split exact and $M \cong M_t \oplus (M/M_t)$ by 2.8 and **??**.

Under the isomorphism $M_t \oplus M/M_t \cong M$ of Theorem 3.4 the image of M_t is M_t and the image of M/M_t is a submodule F of M, which is necessarily free of finite rank. It follows that M is the internal direct sum $M = M_t \oplus F$ (see Theorem 1.15). □

§5.3 Torsion module decomposition

Theorem 5.6. *Let M be a torsion module over a principal ideal domain R and for each prime $p \in R$ let $M_p = \{m \in M \mid m$ has order a power of $p\}$.*

1. *M_p is a submodule of M for each prime $p \in R$.*

2. *$M = \bigoplus M_p$ where the sum is over all primes $p \in R$. If A is finitely generated, only finitely many of the M_p are nonzero.*

Proof. Let $0 \neq a \in M$ with $\text{Ann}\,(a) = (r)$. By Theorem III.3.7 $r = {p_1}^{n_1} \cdots {p_k}^{nk}$ with p_i distinct primes in R and each $n_i > 0$. For each i, let $r_i = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$. Then $r_1, \ldots, r_k$ are relatively prime and there exist $s_1, \ldots, s_k \in R$ such that $s_1 r_1 + \cdots + s_k r_k = 1_R$ by 2.2. Consequently, $a = 1_R a = s_1 r_1 a + \cdots + s_k r_k a$, and we have proved that the submodules M_p generate the module M.

Let $p \in R$ be prime and let M_1 be the submodule of M generated by all M_q with $q \neq p$. Suppose $a \in M(p) \cap A_1$. Then $p^m a = 0$ for some $m \geq 0$ and $a = a_1 + \cdots + a_t$ with $a_i \in A\,(q_i)$ for some primes $q_1, \ldots, q_t$ all distinct from p. Since $a_i \in A\,(q_i)$, there are integers m_i such that ${q_i}^{m_i} a_i = 0$, whence $({q_1}^{m_1} \cdots {q_t}^{m_t})\, a = 0$. If $d = {q_1}^{m_1} \cdots {q_t}^{m_t}$, then p^m and d are relatively prime and $rp^m + sd = 1_R$ for some $r, s \in R$. Consequently, $a = 1_R a = rp^m a + sda = 0$. Therefore, $A(p) \cap A_1 = 0$ and $A = \sum A(p)$ by Theorem 1.15. The last statement of the Theorem is a consequence of the easily verified fact that a direct sum of modules with infinitely many nonzero summands cannot be finitely generated. For each generator has only finitely many nonzero coordinates. □

Lemma 5.7. *Let M be a unitary module over a principal ideal domain R such that $p^n M = 0$ and $p^{n-1} M \neq 0$ for some prime $p \in R$ and positive integer n. Let a be an element of M of order p^n.*

1. *If $M \neq Ra$, then there exists a nonzero $b \in M$ such that $Ra \cap Rb = 0$.*
2. *There is a submodule N of M such that $M = Ra \oplus N$.*

Theorem 5.8. *Let M be a finitely generated unitary module over a principal ideal domain R such that every element of M has order a power of some prime $p \in R$. Then M is a direct sum of cyclic R-modules of orders $p^{n_1}, \ldots, p^{n_k}$ respectively, where $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.*

§5.4

Theorem 5.9. *Let M be a finitely generated unitary module over a principal ideal domain R.*

1. *M is the direct sum of a free submodule F of finite rank and a finite number of cyclic torsion modules. The cyclic torsion summands (if any) are of orders $r_1, \ldots, r_t$, where $r_1, \ldots, r_t$ are (not necessarily distinct) nonzero nonunit elements of R such that $r_1 \,|r_2| \cdots \mid r_t$. The rank of F and the list of ideals $(r_1), \ldots, (r_t)$ are uniquely determined by M.*
2. *M is the direct sum of a free submodule E of finite rank and a finite number of cyclic torsion modules. The cyclic torsion summands (if any) are of orders $p_1^{s_1}, \ldots, p_k^{s_k}$, where $p_1, \ldots, p_k$ are (not necessarily distinct) primes in R and $s_1, \ldots, s_k$ are (not necessarily distinct) positive integers. The rank of E and the list of ideals $(p_1^{s_1}), \ldots, (p_k^{s_k})$ are uniquely determined by M.*

The elements $r_1, \ldots, r_t$ are called the ***invariant factors*** *of the module M just as in the special case of abelian groups. Similarly $p_1^{s_1}, \ldots, p_k^{s_k}$ are called the* ***elementary divisors*** *of M.*

Part IV

Field and Galois Theory

Chapter IX

Field Theory

Contents

§1 Field Extension

§1.1 Basic Definition

Definition 1.1. *Let K be a fixed field. We define the category of field extensions* **Field**$/K$ *as follows:*

- *An object, called* ***extension****, is field L together with a fixed embedding $i_L : K \hookrightarrow L$. We typically suppress i_L and simply write L/K.*

- *A morphism from F/K to L/K is a field homomorphism $\phi : F \to L$ such that the following diagram commutes:*

$$\begin{tikzcd} K \arrow[r, "i_F"] \arrow[dr, "i_L"'] & F \arrow[d, "\phi"] \\ & L \end{tikzcd}$$

*simply denoted as $\phi|_K = \mathrm{id}_K$. The morphism ϕ is called a K-**homomorphism (embedding)** and field F is called an **intermediate field** of L/K. The all morphisms from L_1/K to L_2/K is denoted as $\mathrm{Hom}_K(L_1, L_2)$.*

Remark. *Let $L_1 = \mathbb{Q} \times \{1\}$ and $L_2 = \mathbb{Q} \times \{2\}$, then $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ are both field extensions but $L_1 \cap L_2 = \varnothing$.*

§1.2 Composition fields

Definition 1.2. *Let **Field**$/K$ be the category of field extensions of K and L_1/K, L_2/K be two extension. The **composition** of L_1/K and L_2/K is an extension Ω/K such that*

*(i) L_i is an intermediate field of Ω/K (Ω is a **overfield** of both L_1 and L_2).*

(ii) If extension Ω'/K satisfies the above condition, then Ω is an intermediate field of Ω'/K.

Theorem 1.3. *The composition of two field extensions L_1/K and L_2/K in **Field**$/K$ exists and uniquely up to K-isomorphism (is isomorphic in **Field**$/K$).*

Proof. Let $A = L_1 \otimes_K L_2$ be the pushout (tensor product of K-algebra L_i) of $L_1 \leftarrow K \to L_2$ in the category **CRing** and there is a prime ideal $\mathfrak{p}$ of A such that $A/\mathfrak{p}$ is an integral domain with fractions field $\Omega = \mathrm{Frac}\left((L_1 \otimes_K L_2)/\mathfrak{p}\right)$. The following diagram commutes:

$$\begin{tikzcd} K \arrow[r] \arrow[d] & L_2 \arrow[d] \arrow[ddr, bend left] & \\ L_1 \arrow[r] \arrow[drr, bend right] & A \arrow[dr] & \\ & & \Omega \end{tikzcd}$$

thus L_i can be imbedded into Ω by

$$L_i \to A \to A/\mathfrak{p} \to \Omega$$

respectively, Ω is an overfield of both L_1 and L_2.

If there is another overfield Ω' of both L_1 and L_2, then by the universal property of pushout, Ω can be imbedded into Ω'. □

By theorem 1.3 , when studying a collection of extensions L_i/K, we can have an overfield Ω and a common embedding ι such that $\iota(K) \subset \iota(L_i) \subset \Omega$ for each i.

§2 Extension tower

Definition 2.1. *In the category of field extensions* **Field**$/K$*,*

1. *The* ***degree*** *of a field extension* L/K*, denoted* $[L : K]$*, is the dimension of* L *as a vector space over* K*.*
2. L *is said to be a* ***finite dimensional extension*** *or* ***infinite dimensional extension*** *of* K *according as* $[L : K]$ *is finite or infinite.*

It follows that $[L : K] = [L : F][F : K]$*. Furthermore* $[L : K]$ *is finite if and only if* $[L : F]$ *and* $[F : K]$ *are finite.*

Theorem 2.2. *Let field extension* $K \subset L, M$*. The following statements hold:*

1. *If* $[LM : K]$ *is finite, then* $[L : K]$ *and* $[M : K]$ *divide* $[LM : K]$ *and*

$$\begin{aligned} [LM : K] &= [LM : L]\,[L : K] \\ &= [M : L \cap M]\,[L : K] \\ &\leq [M : K] \leq [L : K] \end{aligned}$$

Corollary 2.3. *Let* L *and* M *be intermediate fields in the extension* F/K*.*

1. $[LM : K]$ *is finite if and only if* $[L : K]$ *and* $[M : K]$ *are finite.*
2. *If* $[L : K]$ *and* $[M : K]$ *are finite and relatively prime, then*

$$[LM : K] = [L : K][M : K]$$

3. *If* L *and* M *are algebraic over* K*, then so is* LM*.*
4. *Assume that* $[LM : K] = [L : K][M : K]$*, then* $L \cap M = K$*.*

§3 Generation

Definition 3.1. *Let* L/K *be a field extension and a subset* $X \subset L$

1. *the* ***subfield generated by*** X ***over*** K *is the intersection of all subfields of* L *that contain* $X \cup K$*, denoted by* $K(X)$*.*
2. *If* $X = \{u_1, \ldots, u_n\}$*, then the subfield* $F(X)$ *of* K *is denoted* $K(u_1, \ldots, u_n)$*. The field* $K(u_1, \ldots, u_n)$ *is said to be a* ***finitely generated extension of*** K*. If* $X = \{u\}$*, then* $F(u)$ *is said to be a* ***simple extension of*** F *and* u *is said* ***primitive element****.*

3. *If F is a field and $X \subset F$, then the subring generated by X is the intersection of all subrings of F that contain X. If F is an extension field of K and $X \subset F$, then the subring generated by $K \cup X$ is called the subring generated by X over K and is denoted $K[X]$.*

4. *If $X = \{u_1, \ldots, u_n\}$, then the subring $K[X]$ of F is denoted $K\left[u_1, \ldots, u_n\right]$.*

Theorem 3.2. *Let L/K be a field extension, $u, u_i \in L$, and $X \subset L$, then*

1. *The subring $K[X]$ consists of all elements of the form $h\left(u_1, \ldots, u_n\right)$, where each $u_i \in X, n$ is a positive integer, and $h \in K\left[x_1, \ldots, x_n\right]$.*

2. *The subfield $K(X)$ consists of all elements of the form*

$$f\left(u_1, \ldots, u_n\right) / g\left(u_1, \ldots, u_n\right) = f\left(u_1, \ldots, u_n\right) g\left(u_1, \ldots, u_n\right)^{-1}$$

where $n \in \mathbb{Z}_{>0}, f, g \in K\left[x_1, \ldots, x_n\right], u_1, \ldots, u_n \in X$ and $g\left(u_1, \ldots, u_n\right) \neq 0$.

3. *For each $v \in\ K(X)$ (resp. $K[X]$) there is a finite subset X' of X such that $v \in K\left(X'\right)$ (resp. $K\left[X'\right]$). Furthermore, we have that*

$$K(X) = \bigcup_{\#X'<\infty} K(X'), \quad K[X] = \bigcup_{\#X'<\infty} K[X']$$

Corollary 3.3. *For any $u_1, \ldots, u_n \in F$ and any permutation $\sigma \in S_n$.*

1. $K\left(u_1, \ldots, u_n\right) = K\left(u_{\sigma(1)}, \ldots, u_{\sigma(n)}\right)$.

2. $K\left(u_1, \ldots, u_{n-1}\right)\left(u_n\right) = K\left(u_1, \ldots, u_n\right)$.

3. $K\left[u_1, \ldots, u_n\right] = K\left[u_{\sigma(1)}, \ldots, u_{\sigma(n)}\right]$.

4. $K\left[u_1, \ldots, u_{n-1}\right]\left[u_n\right] = K\left[u_1, \ldots, u_n\right]$.

§3.1 Finitely Generated Extensions

Definition 3.4. *Let F be an extension field of K.*

1. *An element u of F is said to be* ***algebraic over*** *K provided that u is a root of some nonzero polynomial $f \in K[x]$. F is called an* ***algebraic extension*** *of K if every element of F is algebraic over K.*

2. *If u is not a root of any nonzero $f \in K[x]$, u is said to be* ***transcendental over*** *K. F is called a* ***transcendental extension*** *if at least one element of F is transcendental over K .*

3. *Let $u_1, \ldots u_n$ be element of F, then u_i are* ***algebraically independent*** *provided that there is no nonzero polynomial $f \in K\left[x_1, \ldots, x_n\right]$ such that $f\left(u_1, \ldots, u_n\right) = 0$.*

   Remark. *It follows that each u_i is transcendental.*

§3.2 Simple Extension

Definition 3.5. *Let L/K be an extension field and $u \in L$ algebraic over K. The monic minimal polynomial $m_u(X)$ is called the* ***irreducible (or minimal or minimum) polynomial*** *of u.*

Theorem 3.6. *If L is an extension field of K and $u \in L$ is algebraic over K, then*

1. $K(u) = K[u]$
2. $K(u) \cong K[x]/(m_u)$
3. $\{1, u, u^2, \ldots, u^{n-1}\}$ *is a K-basis of $K(u)$, where $n = \deg m_u$*

Corollary 3.7 (Adjoining a root)**.** *Let K be a field and $f \in K[x]$ be a irreducible polynomial. Then there exists a simple extension field $L = K(u)$ such that:*

1. *$u \in L$ is a root of f*
2. *$[L : K] = n$, where $n = \deg f$.;*
3. *L is unique up to an K-isomorphism*

Theorem 3.8. *If $u \in F$ is transcendental over K, then*

1. *K-isomorphism of fields $K(u) \cong K(x)$.*
2. *K-algebra isomorphism $K[u] \cong K[x]$.*

Theorem 3.9 (Uniqueness of simple extension)**.** *Let $\sigma : K_1 \to K_2$ be an isomorphism of fields, u an element of some extension field of K_1 and v an element of some extension field of K_2. Assume either*

- *u is transcendental over K_1 and v is transcendental over K_2 ; or*
- *u is a root of an minimal polynomial $f \in K_1[x]$ and v is a root of $\sigma f \in K_2[x]$.*

Then σ extends to an isomorphism of fields $K_1(u) \cong K_2(v)$ which maps u onto v .

§3.3 n-extension

Theorem 3.10. *If $u_1, \ldots, u_n \in F$ then the field $K(u_1, \ldots, u_n)$ is isomorphic to the quotient field of the ring $K[u_1, \ldots, u_n]$.*

Proof. By first homomorphism theorem, we have

$$K[X_1, \ldots, X_n]/I \cong K(u_1, \ldots, u_n)$$

where I denotes the ideal $\{f(u_1, \ldots, u_n) = 0 : f \in K[X_1, \ldots, X_n]\}$ □

Theorem 3.11. *Let F be a extension of K.*

1. *If each u_i is algebraic over K, then $K(u_1, \ldots, u_n) = K[u_1, \ldots, u_n]$.*
2. *If v_i are algebraically independent then $K(v_1, \ldots, v_n) \cong K(x_1, \ldots, x_n)$.*

§4 Algebraic Extension

In this section, we always assume that all extension L_i/K encountered in a problem are contained in a fixed overfield Ω and $K \subset L_i \subset \Omega$ as before.

Theorem 4.1. *Let F be an extension of K if and only if for every intermediate field E every monomorphism $\sigma : E \to E$ which is the identity on K is in fact an automorphism of E.*

Proof. Suppose F/K is an algebraic extension and E be a intermediate field, thus E/K is also an algebraic extension. For every monomorphism $\sigma : E \to E$ which is the identity on K, if $\sigma(E) \neq E$, there is a element $\alpha \in E - \sigma(E)$.

Let f be the minimal polynomial of α in $K[x]$, and $\alpha_1, \alpha_2, \ldots, \alpha_s$ be all roots of f in E. We have

$$0 = \sigma f(\alpha_k) = \sigma(f)(\sigma\alpha_k) = f(\sigma\alpha_k)$$

It follows from that f is injective, that $\sigma\alpha_k$ is a permutation of $\{\alpha_k\}$. It contradicts the assumption. □

Theorem 4.2. *Let K be a field.*

1. *If L/K is finite, then L is algebraic over K.*
2. *If $\{L_i/K\}_{i\in I}$ be algebraic extensions, then the composition field L is also algebraic over K.*
3. *If L/F and F/K are algebraic extensions, then so is L/K.*

Theorem 4.3. *Let L/K be a field extension and E the set of all elements of L which are algebraic over K. Then E is a subfield of L called* ***maximal algebraic extension of*** *K/L.*

Proof. If $u, v \in E$, then $K(u, v)$ is an algebraic extension field of K. Therefore, since $u - v$ and $uv^{-1} (v \neq 0)$ are in $K(u, v)$, $u - v$ and $uv^{-1} \in E$. This implies that E is a field. □

Theorem 4.4. *The following conditions on a field K are equivalent.*

1. *Every nonconstant polynomial $f \in K[x]$ has a root in K.*
2. *every nonconstant polynomial $f \in K[x]$ splits over K.*
3. *every minimal polynomial in $K[x]$ has degree one.*
4. *there is no algebraic extension field of K except K itself.*
5. *there exists a subfield K of F such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.*

A field K that satisfies the equivalent conditions is said to be ***algebraically closed****.*

Definition 4.5. *Let L/K be a field extension, then the following conditions are equivalent.*

1. *L is algebraic over K and L is algebraically closed.*

2. *L is a splitting field of $K[x]$ over K.*

*The field L that satisfies the equivalent conditions is called an **algebraic closure of** K.*

Theorem 4.6. *Let K be a field. Then the algebraic closure of K exists and is unique up to an isomorphism in* **Field**$/K$.

Proof. Let $\mathcal{F} := \{L : L/K \text{ is finite }\}$ be a collection of extensions (assume that all L is contained in a fixed overfield by theorem 1.3) with partial order defined by $L_1 \leq L_2 \Leftrightarrow L_1 \subset L_2$. Then $\mathcal{F}$ is a directed system in **Field**$/K$. Thus the direct limit

$$\varinjlim L = \bigcup_{L \in \mathcal{F}} L$$

exists (be a field containing all L and K) and is algebraic over K by theorem 4.2 and algebraically closed by corollary 3.7 . ☐

Corollary 4.7. *If L_i/K is algebraic extensions for each i, then there is a algebraic closure $\overline{K}$ of K containing all L_i.*

§4.1 Splitting Fields

Definition 4.8. *Let K be a field and $f \in K[x]$ a polynomial of polynomials of positive. An extension field $L \supset K$ is said to be a **splitting field** over K of the polynomial f if*

(i) f splits in $L[x]$

(ii) $L = K(u_1, \ldots, u_n)$ where $u_1, \ldots, u_n$ are the roots of f in L.

*Let $\mathcal{S}$ be a set of polynomials of positive degree in $K[x]$. An extension field L of K is said to be a **splitting field over** K **of the set** $\mathcal{S}$ if*

(i) every polynomial in $\mathcal{S}$ splits in $L[x]$.

(ii) L is generated over K by the roots of all the polynomials in $\mathcal{S}$.

Remark. *L is a splitting field over K of a finite set $\{f_1, \ldots, f_n\} \subset K[x]$ if and only if L is a splitting field over K of the single polynomial $f = f_1 f_2 \cdots f_n$.*

If F is a splitting field of $\mathcal{S}$ over K, then F is also a splitting field over K of the set $\mathcal{T}$ of all irreducible factors of polynomials in $\mathcal{S}$.

Theorem 4.9 (Existence of splitting field)**.** *If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field L of f with $[L : K] \leq n!$*

Theorem 4.10. *Let $\sigma : K \to K'$ be an isomorphism of fields, $\mathcal{S} = \{f_i\} \subset K[x]$, and $\mathcal{S}' = \{f' = \sigma f_i\}$. If L is a splitting field of $\mathcal{S}$ over K and L' is a splitting field of $\mathcal{S}'$ over K', then σ is extendible to an isomorphism $L \cong L'$.*

Proof. Step 1. Suppose first that $\mathcal{S}$ consists of a single polynomial $f \in K[x]$ and proceed by induction on $n = [L : K]$. If $n = 1$, then $L = K$ and f splits over K. This implies that σf splits over K' and hence that $L' = K'$. Thus σ itself is the desired isomorphism $L = K \xrightarrow{\sigma} K' = L'$.

If $[L : K] => 1$, then f must have an irreducible factor g of degree greater than 1. Let u be a root of g in L. Then verify that σg is irreducible in $K'[x]$. If $v =$ is a root of σg in L', then σ extends to an isomorphism $\tau : K(u) \cong K'(v)$ with $\tau(u) = v$. Since $[K(u) : K] = \deg g > 1$, we must have $[L : K(u)] < n$. Since L is a splitting field of f over $K(u)$ and L' is a splitting field of σf over $K'(v)$, the induction hypothesis implies that τ extends to an isomorphism $L \cong L'$.

Step 2. If $\mathcal{S}$ is arbitrary, let S consist of all triples (E, E', τ), where E is an intermediate field of F and K, E' is an intermediate field of F' and K', and $\tau : E \to E'$ is an isomorphism that extends σ.

Define $(E_1, E_1', \tau_1) \leq (E_2, E_2', \tau_2)$ if $E_1 \subset E_2, E_1' \subset E_2'$ and $\tau_2 \mid E_1 = \tau_1$. Verify that S is a nonempty partially ordered set in which every chain has an upper bound in $\mathcal{S}$. By Zorn's Lemma there is a maximal element (E_0, E_0', τ_0) of $\mathcal{S}$. We claim that $E_0 = F$ and $E_0' = F'$, so that $\tau_0 : F \cong F'$ is the desired extension of σ by the maximality and Step 1. □

Corollary 4.11 (Uniqueness of splitting field)**.** *Let K be a field and $\mathcal{S} \subset K[x]$. Then any two splitting fields of $\mathcal{S}$ are K-isomorphic. In particular, any two algebraic closures of K are K-isomorphic.*

§4.2 Normal Extension

Definition 4.12. *An algebraic extension field L/K is said* ***normal*** *if every irreducible polynomial in $K[x]$ that has a root in L actually splits in $L[x]$.*

Theorem 4.13. *Let L/K be an algebraic extension and $\overline{K}$ be a algebraic closure of K containing L, then the following statements are equivalent.*

1. *L is normal over K.*

2. *L is a splitting field over K of some set $\mathcal{S} \subset K[x]$.*

3. *$\sigma(L) = L$ for all $\sigma \in \mathrm{Hom}_K\left(L, \overline{K}\right)$, that is $\mathrm{Hom}_K\left(L, \overline{K}\right) = \mathrm{Aut}_K L$*

Proof. (1) ⇒ (2). Let $\{u_i \mid i \in I\}$ be a basis of vector space L over K and for each $i \in I$ let $f_i \in K[x]$ be the minimal polynomial of u_i. Since L/K is normal, each f_i splits in $L[x]$. Therefore L is a splitting field over K of $S = \{f_i \mid i \in I\}$.

(2) ⇒ (3). Let u be a root of some polynomial in $\mathcal{S}$. Since L is a splitting field of $\mathcal{S}$ over K, we have $u \in L$. For any $\sigma \in \mathrm{Hom}_K\left(L, \overline{K}\right)$, $\sigma(u)$ is also a root of the same polynomial. Thus $\sigma(u) \in L$. Since L is generated over K by the roots of all polynomials in $\mathcal{S}$, we have σ maps each generator of L into L. It follows that $\sigma(L) \subset L$. Since σ is injective, we have $\sigma(L) = L$.

(3) ⇒ (1). Let $f \in K[x]$ be an irreducible polynomial with a root $u \in L$. If v is any root of f in $\overline{K}$, then there is a $\sigma \in \mathrm{Hom}_K\left(K(u), \overline{K}\right)$ such that $\sigma(u) = v$. Since L/K is algebraic, by

extending σ, we have $\sigma \in \operatorname{Hom}_K\left(L, \overline{K}\right)$. By assumption, we have $\sigma(L) = L$, thus $v = \sigma(u) \in L$. Therefore, $\{\sigma(u)\}$ runs over all roots of f and f splits in $L[x]$. $\square$

Proposition 4.14. *Let k be a field. The following statements hold:*

1. *If $F \supset L \supset k$ and F is normal over k, then F is normal over L.*
2. *If L_1, L_2 are normal over k, then L_1L_2 is normal over k, and so is $L_1 \cap L_2$.*

Definition 4.15. *Let L/K be a algebraic extension, the* ***normal closure*** *of L over K is the smallest normal extension of K containing L, that is, an extension field $\tilde{L}$ of L such that*

(i) *$\tilde{L}$ is normal over K.*

(ii) *no proper subfield of $\tilde{L}$ containing L is normal over K.*

Remark. *The normal closure of L over K exists ($\overline{K}$ is normal over K and contains L) and is unique up to a K-isomorphism.*

$$\bigcap_{\substack{L \subset F \subset \overline{K} \\ F \text{ normal over } K}} F$$

§4.3 Separable Extension

Definition 4.16. *Let L/K be a algebraic extension.*

1. *The polynomial $f \in K[x]$ is said to be* ***separable*** *if every root of f is a simple root in some splitting field of f over K.*
2. *Let $u \in L$ be algebraic over K, then u is said to be* ***separable*** *over K provided its minimal polynomial is separable. It is equivalent that $\gcd(m_u, m_u') = 1$.*
3. *If every element of F is separable over K, then F is said to be a* ***separable extension*** *of K. (thus algebraic extension)*

Remark. *Thus separable polynomial has distinct roots in its splitting field. If $\operatorname{char} K = 0$, every irreducible polynomial in $K[x]$ is separable and every algebraic extension L/K is separable.*

Proposition 4.17. *Let L/K be an algebraic extension. If L is generated by a set of separable elements over K, then L is a separable extension of K.*

Definition 4.18. *Let L/K be an algebraic extension, the* ***separable closure*** *of L over K is the largest separable extension of K contained in L, that is, an extension field L_{sep} of K such that*

(i) *L_{sep} is separable over K.*

(ii) *any proper extension field of L_{sep} contained in L is not separable over K.*

The separable degree of L over K is defined as $[L_{sep} : K]$, denoted by $[L : K]_s$.

Remark. *That is,*

$$L_{sep} = \{u \in L : u \text{ is separable over } K\}$$

§4.4 Purely Inseparable Extension (char p)

Definition 4.19. *Let L/K be an algebraic extension(of characteristic p) and a element $\alpha \in L$ with minimal polynomial $m_\alpha \in K[x]$.*

1. *The **separable degree** of a polynomial $f \in K[x]$ is defined as the number of distinct roots of f in its splitting field over K, denoted by $\deg_s(f)$. And the **separable part** of f is defined as $f_{sep}(x) := \prod(x - \alpha_i)$*

2. *the **inseparable degree** of f is defined as $\deg_i(f) := \deg f / \deg_s(f)$.*

3. *The **separable degree of** α **over** K is*

$$\deg_s \alpha := \textit{number of distinct roots of } m_\alpha \textit{ in its splitting field over } K$$

4. *A element $u \in L$ is **purely inseparable** over K if its minimal polynomial f in $K[x]$ factors in $L[x]$ as $f = (x - u)^m$ (or equivalently $X^{p^n} - a$ for some $a \in K$ and $n \in \mathbb{Z}_{\geq 1}$).*

5. *L is a **purely inseparable extension** of K if every element of L is purely inseparable over K.*

Theorem 4.20. *Let L/K be an algebraic extension(of characteristic p), then the following statements are equivalent:*

1. *L is purely inseparable over K ;*

2. *the minimal polynomial of any $u \in L$ is of the form $x^{p^n} - a \in K[x]$;*

3. *if $u \in L$, then $u^{p^n} \in K$ for some $n \geq 0$;*

4. *the only elements of L which are separable over K are the elements of K itself;*

5. *L is generated over K by a set of purely inseparable elements.*

$\mathrm{Hom}_K(L, L)$

Theorem 4.21 (Decomposition of algebraic extension)**.** *Let L/K be an algebraic extension, then there exists a unique intermediate field M (actually L_{sep}) such that L_{sep}/K is separable and L/L_{sep} is purely inseparable.*

Proof. If $\operatorname{char} K = 0$, then let $M = L$. In the case $\operatorname{char} K = p \neq 0$, let $u \in L$ and m_u be the minimal polynomial of u over K. We can write $m_u(x) = f\left(x^{p^n}\right)$ for some irreducible separable polynomial $f \in K[x]$ and integer $n \geq 0$. Thus f is the minimal polynomial of u^{p^n} over K and $u^{p^n} \in L_{sep}$ is separable over K. Then u is purely inseparable over L_{sep} since its minimal polynomial in $L_{sep}[x]$ divides $X^{p^n} - u^{p^n} = (X - u)^{p^n}$. □

§4.5 Separable degree

Theorem 4.22 (Primitive element theorem)**.** *Let L/K be a finite extension, then the following statements are equivalent.*

1. *there exists an element $u \in L$ such that $L = K(u)$.*

2. *there exists only a finite number of intermediate field such that $K \subset F \subset L$*

Especially, if L/K is finite separable, then $L = K(u)$ for some $u \in L$.

Corollary 4.23. *Let L/K be an algebraic extension and $\overline{K}$ be an algebraic closure of K containing L, then the **separable degree***

$$[L : K]_s := [L_{sep} : K] = \#\operatorname{Hom}_K\left(L, \overline{K}\right)$$

(if finite)

Definition 4.24. *Let L/K be an algebraic extension*

§4.6

Theorem 4.25. *Let L/K be an algebraic extension, then the following statements are equivalent.*

1. *L/K is Galois.*

2. *L is a splitting field over K of and L/K is separable.*

3. *L is a splitting field over K of a set $\mathcal{S}$ of separable polynomials in $K[x]$.*

Proof. (1) $\Rightarrow$ (2). Suppose $u \in F$ has minimal polynomial $f \in K[x]$, then f splits in $F[x]$ into a product of distinct linear factors. Hence u is separable over K. Let $\{v_i \mid i \in I\}$ be a basis of vector space F over K and for each $i \in I$ let $f_i \in K[x]$ be the minimal polynomial of v_i. The preceding remarks show that each f_i is separable and splits in $F[x]$. Therefore F is a splitting field over K of $S = \{f_i \mid i \in I\}$.

(2) $\Rightarrow$ (3) Let set T consists of all irreducible monic factor of polynomial in S. Let $f \in T$, f must be the minimal polynomial of some $u \in F$. Since F is separable over K, f is necessarily separable. It follows that F is a splitting field over K of the set T of separable polynomials consisting of all monic irreducible factors in $K[x]$.

(3) $\Rightarrow$ (1) F is algebraic over K since any splitting field over K is an algebraic extension. If $u \in F - K$, then $u \in K\left(v_1, \ldots, v_n\right)$ with each v_i a root of some $f_i \in T$. $\square$

Chapter X

Galois Theory

Contents

§1 Basic Definition

Definition 1.1. *Let E and F be extension fields of a field K.*

1. *A nonzero map $\sigma : E \to F$ which is both a field homomorphism and a K-module homomorphism is called a* ***K-homomorphism****.*

2. *Similarly if a field automorphism $\sigma \in \operatorname{Aut} F$ is a K-homomorphism, then σ is called a* ***K-automorphism*** *of F.*

3. *The group of all K-automorphisms of F is called the* ***Galois group of*** *F* ***over*** *K and is denoted $\operatorname{Aut}_K F$ or $\operatorname{Gal}(F/K)$.*

Definition 1.2. *Let L/K be an extension.*

1. *If* $H < \operatorname{Aut}_K F$*, then*

$$H' = L^H := \{v \in F : \sigma(v) = v \text{ for all } \sigma \in H\}$$

is an intermediate field of the extension called the ***fixed field of*** H ***in*** F.

2. *If* E *an intermediate field, then*

$$E' = \operatorname{Aut}_E F = \{\sigma \in \operatorname{Aut}_K F : \sigma(u) = u \text{ for all } u \in E\}$$

is a subgroup of $\operatorname{Aut}_K F$.

Definition 1.3. *Let* L/K *be a algebraic extension such that* $K = L^{\operatorname{Aut}_K(L)}$. *Then* L *is said to be a* ***Galois extension of*** K *or to be Galois over* K.

Let X *be an intermediate field or subgroup of the Galois group.* X *will be called* ***closed*** *provided* $X = X''$.

§2

Proposition 2.1. *Let* L/K *be an algebraic extension and* $\overline{K}$ *be an algebraic closure of* K *containing* L*, then*

$$[L : K]_{sep} = \#\operatorname{Hom}_K\left(L, \overline{K}\right)$$

if finite. Thus we have

$$|\operatorname{Aut}_K L| \cdot t = [L : K]_s$$

where $t = \#\left\{\sigma(L) : \sigma \in \operatorname{Hom}_K\left(L, \overline{K}\right)\right\}$ *is the number of distinct* K*-embeddings image of* L*, is also the number of distinct conjugates of* L *in* $\overline{K}$.

Corollary 2.2. *Let* L/K *be an algebraic extension and intermediate field* $E \subset F$*, then*

$$[\operatorname{Aut}_E L : \operatorname{Aut}_F L] \cdot \frac{t_E}{t_F} = [F : E]_{sep}$$

Corollary 2.3. *If* L/K *is a finite extension, then*

$$|\operatorname{Aut}_K L| \leq [L : K]$$

The equality holds if and only if L/K *is finite separable and normal.*

Proposition 2.4. *Let* L *be a field,* $H < \operatorname{Aut}(L)$ *and if* L/L^H *is algebraic, then* L/L^H *is Galois.*

Proof. In any case H is a subgroup of $\operatorname{Aut}_{L^H} L$. If $u \in L - L^H$, then there must be a $\sigma \in H$ such that $\sigma(u) \neq u$. Therefore, the fixed field of $\operatorname{Aut}_{L^H} L$ is L^H, whence L is Galois over L^H. □

§3 Fundamental Theorem

Proposition 3.1. *Let L/K be an extension field.*

1. *Suppose that $E \subset F$ are intermediate fields, then σ_1 and $\sigma_2 \in \operatorname{Aut}_E L$ are in the same left coset of F' if and only if*
$$\sigma_1|_F = \sigma_2|_F$$
thus $[\operatorname{Aut}_E F : \operatorname{Aut}_F F] = \#\{\sigma|_F : \sigma \in \operatorname{Aut}_E L\}$.

2. *Suppose that H, J are subgroups of $\operatorname{Aut}_K L$ with $H < J$ and $\tau_1, \tau_2 \in J$ are in the same left coset of H, then*
$$\tau_1|_{L^H} = \tau_2|_{L^H}$$
thus $[J : H] \geq \#\{\tau|_{L^H} : \tau \in J\}$.

Lemma 3.2. *Let L/K be an extension field and $E \subset F$ are intermediate fields, then σ_1 and $\sigma_2 \in \operatorname{Aut}_E L$ are in the same left coset of F' if and only if*

$$\sigma_1|_F = \sigma_2|_F$$

thus $[\operatorname{Aut}_E F : \operatorname{Aut}_F F] = \#\{\sigma|_F : \sigma \in \operatorname{Aut}_E L\}$.

Theorem 3.3. *Let L/K be an algebraic extension and $E \subset F$ intermediate fields with $[F : E] < \infty$.*

$$[\operatorname{Aut}_E L : \operatorname{Aut}_F L] \leq [F : E]$$

Lemma 3.4. *Suppose that H, J are subgroups of $\operatorname{Aut}_K L$ with $H < J$ and $\tau_1, \tau_2 \in J$ are in the same left coset of H, then*

$$\tau_1|_{L^H} = \tau_2|_{L^H}$$

thus $[J : H] \geq \#\{\tau|_{L^H} : \tau \in J\}$.

Theorem 3.5. *Let χ_i be distinct characters of a group G with degree n_i, then*

Theorem 3.6. *Let L be a field, G be a finite subgroup of $\operatorname{Aut}(L)$ and $K = L^G$, then*

$$[L : K] = |G|$$

Proof. □

Corollary 3.7. *Let L/K be an algebraic extension and H, J be subgroups of $\operatorname{Aut}_K L$ with $[J : H] < \infty$, then*

$$\left[L^H : L^J\right] \leq [J : H]$$

Lemma 3.8. *Let F/K and X, Y be two intermediate fields or two subgroups of the Galois group $\operatorname{Aut}_K F$. Then:*

1. $X \subset Y \Rightarrow Y' \subset X'$

2. $X' = X'''$

Lemma 3.9. *Let L/K, then there is a one-to-one correspondence between the closed intermediate fields and the closed subgroups, given by*

$$E \mapsto E'$$
$$H \mapsto H'$$

Corollary 3.10. *Let F be an extension field of K, L and M intermediate fields with $L \subset M$, and H, J subgroups of $\operatorname{Aut}_K F$ with $H < J$.*

1. *If L is closed and $[M : L]$ finite, then M is closed and $[L' : M'] = [M : L]$*

2. *If H is closed and $[J : H]$ finite, then J is closed and $[H' : J'] = [J : H]$*

3. *If F is a finite dimensional Galois extension of K, then all intermediate fields and all subgroups of the Galois group are closed.*

Proof. (2) Applying successively the facts that $J \subset J''$ and $H = H''$ and Lemmas 2.8 and 2.9 yields

$$[J : H] \leq [J'' : H] = [J'' : H''] \leq [H' : J'] \leq [J : H];$$

this implies that $J = J''$ and $[H' : J'] = [J : H]$. (1) is proved similarly. □

§3.1 Stable Intermediate Fields

Definition 3.11. *Let E be an intermediate field of the extension L/K*

1. *The intermediate field E is said to be* ***stable relative to*** *K* ***and*** *L if every K-automorphism $\sigma \in \operatorname{Aut}_K F$ maps E into itself.*

   Remark. *If E is stable and $\sigma^{-1} \in \operatorname{Aut}_K F$ is the inverse automorphism, thus σ^{-1} also maps E into itself. This implies that $\sigma\,|_E$ is in fact a K-automorphism of E (that is, $\sigma|_E \in \operatorname{Aut}_K E$) with inverse $\sigma^{-1}|_E$.*

2. *A K-automorphism $\tau \in \operatorname{Aut}_K E$ is said to be* ***extendible*** *to F if there exists $\sigma \in \operatorname{Aut}_K F$ such that $\sigma|_E = \tau$.*

   It is easy to see that the extendible K-automorphisms form a subgroup of $\operatorname{Aut}_K E$.

Theorem 3.12. *Let L/K be an extension and E be an intermediate field.*

1. *If E is a stable intermediate field, then*

$$E' = \operatorname{Aut}_E L \lhd \operatorname{Aut}_K L$$

and the quotient group

$$G/E' \cong \{\sigma \in \operatorname{Aut}_K E : \sigma \textit{ is extendible to } F\}$$

2. *If $H \lhd \operatorname{Aut}_K F$, then H' is a stable intermediate field.*

Proof. (1) If $u \in E$ and $\sigma \in \operatorname{Aut}_K F$, then $\sigma(u) \in E$ by stability and hence $\tau\sigma(u) = \sigma(u)$ for any $\tau \in E' = \operatorname{Aut}_E F$. Therefore, for any $\sigma \in \operatorname{Aut}_K F, \tau \in E'$ and $u \in E$, $\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\sigma(u) = u$. Consequently, $\sigma^{-1}\tau\sigma \in E'$ and hence E' is normal in $\operatorname{Aut}_K F$.

Since E is stable, the assignment

$$\sigma \mapsto \sigma|_E$$

defines a group homomorphism $\operatorname{Aut}_K F \to \operatorname{Aut}_K E$ whose image is clearly the subgroup of all K-automorphisms of E that are extendible to F. Observe that the kernel is $E' = \operatorname{Aut}_E F$ and apply the first homomorphism theorem.

(2) If $\sigma \in \operatorname{Aut}_K F$ and $\tau \in H$, then $\sigma^{-1}\tau\sigma \in H'$ by normality. Therefore, for any $u \in H', \sigma^{-1}\tau\sigma(u) = u$, which implies that $\tau\sigma(u) = \sigma(u)$ for all $\tau \in H$. Thus $\sigma(u) \in H'$ for any $u \in H'$, which means that H' is stable. □

Proposition 3.13. *If E is an intermediate field of the extension F/K such that F/E and E/K are both Galois. Then F is Galois over K if and only if every $\sigma \in \operatorname{Aut}_K E$ is extendible to F*

Proof. Sufficiency. We have

$$\operatorname{Aut}_K F/\operatorname{Aut}_E F \cong \{\sigma \in \operatorname{Aut}_K E : \sigma \text{ is extendible to } F\} = \operatorname{Aut}_K E$$

then

$$|\operatorname{Aut}_K F| = |\operatorname{Aut}_E F|\,|\operatorname{Aut}_K E| = [F:E]\,[E:K] = [F:K]$$

It follows from E' is closed and $[K:E'] < \infty$ that K is closed, whence F/K is Galois.

Necessity. Conversely, we have

$$\#\{\sigma \in \operatorname{Aut}_K E : \sigma \text{ is extendible to } F\} = [F:K]\,/\,[F:E] = [E:K] = |\operatorname{Aut}_K E|$$

thus $\{\sigma \in \operatorname{Aut}_K E : \sigma \text{ is extendible to } F\} = \operatorname{Aut}_K E$, that is, every $\sigma \in \operatorname{Aut}_K E$ is extendible to F. □

§3.2 Finite Galois correspondence

Theorem 3.14. *Let L/K be a finite extension. The following statements are equivalent:*

1. *L/K is Galois.*

2. $|\operatorname{Aut}_K L| = [L:K]$.

3. *L/K is normal and separable.*

Theorem 3.15. *Let L/K be a finite Galois extension, then there is a one-to-one correspondence between the set of all intermediate fields and the set of all subgroups of* $\mathrm{Aut}_K L$ *given by*

$$X \leftrightarrow X'$$

such that:

1. *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups*
$$\begin{array}{ccccccc} K & \subset & E_1 & \subset & E_2 & \subset & L \\ G & \supset & \mathrm{Aut}_{E_1} L & \supset & \mathrm{Aut}_{E_2} L & \supset & 1 \end{array}$$
then
$$[E_2 : E_1] = [\mathrm{Aut}_{E_1} L : \mathrm{Aut}_{E_2} L]$$

2. *L is Galois over every intermediate field E, $E'' = E$*

3. *E is Galois over K $\Leftrightarrow$ $E' \lhd \mathrm{Aut}_K F$ $\Leftrightarrow$ $\{\sigma \in \mathrm{Aut}_K E : \sigma \text{ is extendible to } F\} = \mathrm{Aut}_K E$; in this case*
$$K'/E' \cong \{\sigma \in \mathrm{Aut}_K E : \sigma \text{ is extendible to } F\} = \mathrm{Aut}_K E$$

Theorem 3.16 (Artin)**.** *Let F be a field, G a group of automorphisms of F and K the fixed field of G in F. Then F is Galois over K. If G is finite, then F is a finite dimensional Galois extension of K with Galois group G.*

Proof. In any case G is a subgroup of $\mathrm{Aut}_K F$. If $u \in F - K$, then there must be a $\sigma \in G$ such that $\sigma(u) \neq u$. Therefore, the fixed field of $\mathrm{Aut}_K F$ is K, whence F is Galois over K.

If G is finite, $[F : K] = [1' : G'] \leq [G : 1] = |G|$. Consequently, F is finite dimensional over K, whence $G = G''$ by Lemma 2.10(iii). Since $G' = K$ (and hence $G'' = K'$) by hypothesis, we have $\mathrm{Aut}_K F = K' = G'' = G$. □

§3.3

§3.4 Question

Lemma 3.17. *Let K be a field and a element f/g in $K(x)$ with $f/g \notin K$ and f, g relatively prime in $K[x]$*

Proposition 3.18 ($K(x)/K$)**.** *Let $f/g \in K(x)$ with $f/g \notin K$ and f, g relatively prime in $K[x]$ and consider the extension of K by $K(x)$.*

1. *x is algebraic over $K(f/g)$ and $[K(x) : K(f/g)] = \max(\deg f, \deg g)$.*

2. *If $E \neq K$ is an intermediate field, then $[K(x) : E]$ is finite.*

3. *The assignment* $x \mapsto f/g$ *induces a* K*-homomorphism* $\sigma : K(x) \to K(x)$ *such that* $\varphi(x)/\psi(x) \mapsto \varphi(f/g)/\psi(f/g)$. σ *is a* K *automorphism of* $K(x)$ *if and only if* $\max(\deg f, \deg g) = 1$.

4. *Thus* $\operatorname{Aut}_K K(x)$ *consists of all those automorphisms induced by the assignment*

$$x \mapsto (ax+b)/(cx+d)$$

where $a, b, c, d \in K$ *and* $ad - bc \neq 0$.

5. *If* K *is an infinite field, then* $K(x)$ *is Galois over* K. *If* K *is finite, then* $K(x)$ *is not Galois over* K.

Proof. (1) x is a root of the nonzero polynomial $\varphi(y) = (f/g)g(y) - f(y) \in K(f/g)[y]$; show that $\deg \varphi = \max\{\deg f, \deg g\}$ and φ is irreducible in $K(f/g)[y]$

Since f/g is transcendental over K, we may for convenience replace $K(f/g)$ by $K(z)$ (z an indeterminate) and consider $\varphi = zg(y) - f(y) \in K(z)[y]$.

Indeed, φ is irreducible in $K(z)[y]$ provided it is irreducible in $K[z][y]$ by Gauss lemma. The truth of this latter condition follows from the fact that φ is linear in z and f, g are relatively prime.

(3) Assume that $\deg g = \max\{\deg f, \deg g\} > 1$. For any $\varphi/\psi \in K(x)$ such that $\varphi, \psi \in K[x]$,$\gcd(\varphi, \psi) = 1$ and $\deg \varphi = m, \deg \psi = n$ ($m > n$), there exist $u, v \in K[x]$ such that

$$u(x)\varphi(x) + v(x)\psi(x) = 1_K$$

and u Then the image of φ/ψ

$$\varphi(f/g)/\psi(f/g) = \frac{g^k \varphi(f/g)}{g^k \psi(f/g)}$$

where k is sufficiently large that $k > \max\{\deg u + \deg \varphi, \deg v + \deg \psi\}$. Then we have

$$g^k u(f/g)\varphi(f/g) + g^k v(f/g)\psi(f/g) = g^k$$

thus $\gcd(g^m \varphi(f/g), g^m \psi(f/g)) = \gcd(g^m \varphi(f/g), g^{m-n} g^n \psi(f/g))$ is a power of g Therefore, we have

$$\gcd(g^m \varphi(f/g), g^m \psi(f/g)) = 1$$

If we rewrite

$$\varphi(f/g)/\psi(f/g) = F/G$$

where $F, G \in K[x]$, then $\deg F/G = \max\{\deg F, \deg G\} > 1$, the homomorphism is not surjective.

(5) If K is infinite and $K(x)$ is not Galois over K, then $K(x)$ is finite dimensional over the fixed field E of $\operatorname{Aut}_K K(x)$ by (2). But $\operatorname{Aut}_E K(x) = \operatorname{Aut}_K K(x)$ is infinite (4), which contradicts $[E' : 1] \leq [K(x), E]$.

If K is finite and $K(x)$ is Galois over K, then $\operatorname{Aut}_K K(x)$ would be infinite by Lemma 2.9. But $\operatorname{Aut}_K K(x)$ is finite by (4) □

§4 Galois Groups

§4.1

Definition 4.1. *Let K be a field. The **Galois group** of $f \in K[x]$ is the group $\operatorname{Aut}_K F$, where F is a splitting field of f over K.*

Theorem 4.2. *Let K be a field and $f \in K[x]$ an irreducible polynomial of degree n with Galois group $\operatorname{Aut}_K F$. Then*

1. *n divides $|\operatorname{Aut}_K F|$*
2. *$\operatorname{Aut}_K F$ is isomorphic to a transitive subgroup of S_n.*

Proof. (1) If $u_1, \ldots, u_n$ are the distinct roots of f in some splitting field $F(1 \leq n \leq \deg f)$, then every $\sigma \in \operatorname{Aut}_K F$ induces a unique permutation of $\{u_1, \ldots, u_n\}$. Consider S_n as the group of all permutations of $\{u_1, \ldots, u_n\}$ and verify that the assignment of $\sigma \in \operatorname{Aut}_K F$ to the permutation it induces defines a monomorphism $\operatorname{Aut}_K F \rightarrow S_n$ by

$$\sigma \mapsto \begin{pmatrix} u_1 & u_2 & \cdots & u_n \\ u_{\sigma(1)} & u_{\sigma(2)} & \cdots & u_{\sigma(n)} \end{pmatrix}$$

As for (2), F is Galois over K and $[K(u_1) : K] = n = \deg f$. Therefore, G has a subgroup $K(u_1)' = \operatorname{Aut}_{K(u_1)} F$ of index n by the Fundamental Theorem ($[\operatorname{Aut}_K F : K(u_1)'] = [K(u_1) : K]$), whence n divide $|G|$. For any $i \neq j$ there is a K-isomorphism $\sigma : K(u_i) \cong K(u_j)$ such that $\sigma(u_i) = u_j$. Then σ extends to a K-automorphism of F by Theorem 3.8, whence G is isomorphic to a transitive subgroup of S_n. □

Definition 4.3. *Let K be a field with $\operatorname{char} K \neq 2$ and $f \in K[x]$ a polynomial of degree n with n distinct roots $u_1, \ldots, u_n$ in some splitting field F of f over K. Let*

$$\Delta = \prod_{i<j} (u_i - u_j) = (u_1 - u_2)(u_1 - u_3) \cdots (u_{n-1} - u_n) \in F$$

*the **discriminant** of f is the element $D = \Delta^2$.*

Proposition 4.4. *Let K, f, F and Δ be as in Definition .*

(1) The discriminant Δ^2 of f actually lies in K.

(2) For each $\sigma \in \operatorname{Aut}_K F < S_n$, σ is an even [resp. odd] permutation if and only if $\sigma(\Delta) = \Delta$[resp .$\sigma(\Delta) = -\Delta$].

§5 Finite Fields

Theorem 5.1. *Let F be a field and*

(1) let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If char $F = p$ *(prime), then* P $\cong \mathbb{Z}_p$. *If char $F = 0$, then $P \cong \mathbb{Q}$, the field of rational numbers. The field P is called the* ***prime subfield*** *of F.*

(2) If F is a finite field, then char $F = p \neq 0$ *for some prime p and $|F| = p^n$ with $n = [F : P] \geq 1$, we have $\mathbb{Z}_p$-module isomorphism*

$$F \cong (\mathbb{Z}_p)^n$$

Theorem 5.2. *If F is a field and G is a finite subgroup of $F^\times$, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.*

Proof. If $G(\neq 1)$ is a finite abelian group, $G \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_k}$ where $m_1 > 1$ and $m_1 \, |m_2| \cdots \mid m_k \mid p^n - 1$.

Since $m_k \left(\sum Z_{m_i}\right) = 0$, it follows that every $u \in G$ is a root of the polynomial $x^{m_k} - 1_{F'} \in F[x]$ (G is a multiplicative group). Since this polynomial has at most m_k distinct roots in F, we must have $k = 1$ and $G \cong Z_{m_k}$. □

Corollary 5.3. *If F is a finite field with* char $F = p$. *Then*

(1) $F = \mathbb{Z}_p(u)$ where u is a generator of $F^\times$

(2)

Lemma 5.4. *If F is a field of characteristic p and $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by*

$$u \mapsto u^{p^r}$$

is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Theorem 5.5. *Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

Proof. It is clear that

$$u^{p^n} - u = 0$$

for all $u \in F$ and all distinct roots of $x^{p^n} - x$ are F, thus F is a splitting field of $x^{p^n} - x$.

If F is a splitting field of $f = x^{p^n} - x$ over $\mathbb{Z}_p$, then since char $F =$ char $\mathbb{Z}_p = p$, $f' = -1$ and f is relatively prime to f'. Therefore f has p^n distinct roots in F. Let $\varphi : u \mapsto u^{p^n}$ be the monomorphism, it is easy to see that $u \in F$ is a root of f if and only if $\varphi(u) = u$. Use this fact to verify that the set E

$$E = \{t \in F : f(t) = 0\} = \langle\varphi\rangle'$$

is a subfield (fixed field of $\langle\varphi\rangle$) of F of order p^n (f splits and has distinct p^n roots), which necessarily contains the prime subfield $\mathbb{Z}_p$. Since F is a splitting field, it is generated over $\mathbb{Z}_p$ by the roots of f (that is, the elements of E). Therefore, $F = \mathbb{Z}_p(E) = E$. □

Corollary 5.6 (Existence and uniqueness of finite fields)**.** *If p is a prime and $n \geq 1$ an integer, then there exists a field with p^n elements. Any two finite fields with the same number of elements are isomorphic.*

Given p and n, a splitting field F of $x^{p^n} - x$ over $\mathbb{Z}_p$ exists by Theorem 3.2 and has order p^n by Proposition 5.6. Since every finite field of order p^n is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ by Proposition 5.6, any two such are isomorphic by Corollary 3.9.

§5.1 Extension over finite fields

Theorem 5.7. *If K is a finite field, then*

(1) For any $n \in \mathbb{Z}_{>1}$ there exists a simple extension field $F = K(u)$ such that $[F : K] = n$.

(2) Any two n-dimensional extension fields of K are K-isomorphic.

(3) For any $n \geq 1$ an integer, there exists an minimal polynomial of degree n in $K[x]$.

Proof. (1) Given K of order p^r let F be a splitting field of

$$f = x^{p^{rn}} - x$$

over K. By Proposition 5.6 every $u \in K$ satisfies $u^{p^r} = u$ and it follows inductively that $u^{p^{rn}} = u$ for all $u \in K$. Therefore, F is actually a splitting field of f over $\mathbb{Z}_p$. Since F consists of precisely the p^{nr} distinct roots of f, we have

$$p^{nr} = |F| = |K|^{[F:K]} = (p^r)^{[F:K]}$$

whence $[F : K] = n$. Corollary 5.4 implies that F is a simple extension of $\mathbb{Z}_p$, hence of K.

(2) Uniqueness. If F_1 is another extension field of K with $[F_1 : K] = n$, then $[F_1 : \mathbb{Z}_p] = n\,[K : \mathbb{Z}_p] = nr$, whence $|F_1| = p^{nr}$. By Proposition 5.6 F_1 is a splitting field of $x^{p^{nr}} - x$ over $\mathbb{Z}_p$ and hence over K. Consequently, F and F_1 are K-isomorphic, hence are isomorphic. □

Theorem 5.8. *If F is a finite dimensional extension field of a finite field K (It equivalent that $\mathbb{Z}_p \subset K \subset F$ are finite extension with $[F : \mathbb{Z}_p] = n, [K : \mathbb{Z}_p] = r$), then*

(1) $r \mid n$

(2) F is Galois over K.

(3) The Galois group $\mathrm{Aut}_K F = \langle \varphi^r \rangle$ is cyclic.

Proof. (1) Consider

$$[F : K]\,[K : \mathbb{Z}_p] = [F : \mathbb{Z}_p]$$

that is, $[F : K]\,r = n$

(2) F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. It follows from all roots of $x^{p^n} - x$ are distinct that F is Galois over $\mathbb{Z}_p$, hence over K.

(3) The map $\varphi : F \to F$ given by $u \mapsto u^p$ is a $\mathbb{Z}_p$-automorphism of F with order n. Since $\left|\mathrm{Aut}_{\mathbb{Z}_p} F\right| = [F : \mathbb{Z}_p] = n$ by the Fundamental Theorem, $\mathrm{Aut}_{\mathbb{Z}_p} F$ must be the cyclic group generated by φ.

Since $\mathrm{Aut}_K F$ is a subgroup of $\mathrm{Aut}_{\mathbb{Z}_p} F$, $\mathrm{Aut}_K F$ is also cyclic of order $[F : K] = n/r$. On the other hand, $\varphi^r : u \mapsto u^{p^r}$, automorphism of F, fix K and φ^r is of order n/r. Therefore, we have

$$\mathrm{Aut}_K F = \langle \varphi^r \rangle$$

□