CHAPTER 1

Groups

1.1. Definitions and Easy Facts

Definition 1.1. A *group* is a nonempty set G equipped with a binary operation $\cdot$ satisfying the following axioms.

(i) (associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;

(ii) (existence of identity) there exists $e \in G$ such that $ea = ae = a$ for all $a \in G$;

(iii) (existence of inverse) for each $a \in G$ there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

If $ab = ba$ for all $a, b \in G$, G is called *abelian*. (Note. It is more appropriate to treat abelian groups as $\mathbb{Z}$-modules.)

Facts. Let G be a group.

(i) The identity e and the inverse of $a \in G$ are unique. (Let e' be another identity of G and b another inverse of a. Then $e' = e'e = e$ and $b = be = b(aa^{-1}) = (ba)a^{-1} = a^{-1}$.)

(ii) (Cancelation) Let $a, b, c \in G$. Then $ab = ac \Rightarrow b = c$; $ba = ca \Rightarrow b = c$; $ab = e \Rightarrow a = b^{-1}$.

(iii) If $a_1, \dots, a_n \in G$, parentheses are not needed to define $a_1 \cdots a_n$ because of the associativity. Moreover, $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

Examples. *Abelian groups*: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{R}^\times = \mathbb{R} \setminus \{0\})$, $(\mathbb{C}^\times, \cdot)$, $\mathbb{Z}_n$ (integers modulo n).

Automorphism groups (groups of bijections which preserve a certain structure): S_X = the group of all permutations of a set X; $\mathrm{GL}(V)$ = the group of all invertible linear transformations of a vector space V; $\mathrm{GL}(n, F)$ = the group of $n \times n$ invertible matrices over a field F, $\mathrm{GL}(n, F) \cong \mathrm{GL}(F^n)$; the group of isometries of a metric space; groups of automorphisms of groups, rings, modules, fields, graphs, etc.

Groups as invariants: the fundamental group and homology groups of a topological space.

The law of exponents. Let G be a group, $a \in G$, $m, n \in \mathbb{Z}$. Then $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$. (Note. $a^0 := e$; $a^{-n} := (a^{-1})^n$ for $n \in \mathbb{Z}^+$.)

Additive notation (usually for abelian groups). We write $a + b$ for ab, 0 for e, $-a$ for a^{-1} and na for a^n.

Cartesian product. If G and H are groups, the $G \times H$ is a group with operation defined component wise.

Homomorphism. Let G and H be groups. A map $f : G \to H$ is called a *homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in G$. It follows that $f(e_G) = e_H$ and

$f(a^{-1}) = f(a)^{-1}$ for $a \in G$. $\ker f := f^{-1}(e_H) = \{a \in G : f(a) = e_H\}$. f is 1-1 $\Leftrightarrow \ker f = \{e_G\}$. If $f : G \to H$ is a homomorphism and a bijection, f is called an *isomorphism.* It follows that $f^{-1} : H \to G$ is also an isomorphism. If there exists an isomorphism $f : G \to H$, G and H are called isomorphic ($G \cong H$). Isomorphic groups have the same structure.

$\mathrm{Aut}(G) :=$ the set of all *automorphisms* of G (isomorphisms from G to G).

$(\mathrm{Aut}(G), \circ)$ is the *automorphism group* of G.

Example. $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\times$, $A \mapsto \det A$, is a homomorphism.

Example. $G =$ the set of all fractional linear transformations of $\mathbb{C}$ (functions of the form $f(z) = \dfrac{az+b}{cz+d}$, where $ad - bc \neq 0$). $(G, \circ)$ is a group.

$$\begin{aligned} \phi : \quad \mathrm{GL}(2, \mathbb{C}) &\longrightarrow G \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} &\longmapsto f, \end{aligned}$$

where $f(z) = \dfrac{az+b}{cz+d}$, is a homomorphism with $\ker \phi = \{aI_2 : a \in \mathbb{C}^\times\}$.

Subgroups. Let $(G, \cdot)$ be a group. $H \subset G$ is called a *subgroup* of G, denoted as $H < G$, if $(H, \cdot)$ is a group. If $X \subset G$,

$$\langle X \rangle := \bigcap_{X \subset H < G} H$$

is the smallest subgroup of G containing X; it is called the subgroup of G generated by X.

$$\langle X \rangle = \{a_1^{e_1} \cdots a_n^{e_n} : n \geq 0,\ a_1, \dots, a_n \in G,\ e_1, \dots, e_n \in \mathbb{Z}\}.$$

If $G = \langle a \rangle$, G is called *cyclic.*

Example. Let F be a field and $X \subset \mathrm{GL}(n, F)$ the set of all elementary matrices. Then $\langle X \rangle = \mathrm{GL}(n, F)$.

Proposition 1.2. *Let G be a group and $\emptyset \neq H \subset G$.*

(i) *$H < G \Leftrightarrow ab^{-1} \in H$ for all $a, b \in H$.*

(ii) *If $|H| < \infty$, then $H < G \Leftrightarrow H$ is closed under multiplication.*

Proof. (ii) ($\Leftarrow$) Only have to show that H contains e and is closed under inversion. Let $a \in H$. The map $x \mapsto ax$ from H to H is 1-1 hence is onto. So, there exists $x \in H$ such that $ax = x$. Thus $e = x \in H$. Also, there exists $y \in H$ such that $ay = e$, so $a^{-1} = y \in H$. □

Cosets. Let $H < G$ be groups and $a \in G$. $aH = \{ah : h \in H\}$ is called a *left coset* of H in G with representative a. Ha is a right coset of H in G. $G/H := \{aH : a \in G\}$, $H\backslash\backslash G := \{Ha : a \in G\}$. $aH = bH \Leftrightarrow b^{-1}a \in H$; $Ha = Hb \Leftrightarrow ab^{-1} \in H$. Cosets in G/H ($H\backslash\backslash G$) form a partition of G

Proposition 1.3.

(i) $|G/H| = |H\backslash\backslash G|$. *($|G/H|$ is called the* index *of H in G, denoted by $[G : H]$.)*

(ii) $|G| = |G/H|\,|H|$.

PROOF. (i) $\alpha : G/H \to H\backslash\backslash G$, $aH \mapsto (aH)^{-1} = Ha^{-1}$, is a bijection.

(ii) $f : G \to G/H$, $a \mapsto aH$, is onto. For each $aH \in G/H$, $f^{-1}(aH) = aH$; hence $|f^{-1}(aH)| = |aH| = |H|$. So $|G| = |G/H|\,|H|$. □

COROLLARY 1.4 (Lagrange's theorem). *If* $H < G$ *and* $|G| < \infty$*, then* $|H| \bigm| |G|$.

For $a \in G$, the *order* of a is

$$o(a) := |\langle a \rangle| = \begin{cases} \min\{n \in \mathbb{Z}^+ : a^n = e\} & \text{if there is } n \in \mathbb{Z}^+ \text{ such that } a^n = e, \\ \infty & \text{otherwise.} \end{cases}$$

FACT. Let $|G| < \infty$ and $a \in G$. Then $o(a) \bigm| |G|$ and $a^{|G|} = e$.

EXAMPLE (Euler's theorem). For $n \in \mathbb{Z}^+$, $\phi(n) := |\{x \in \mathbb{Z} : 0 < x \le n,\ (x, n) = 1\}|$. We have

$$x^{\phi(n)} \equiv 1 \pmod{n} \quad \text{for all } x \in \mathbb{Z} \text{ and } n \in \mathbb{Z}^+ \text{ with } (x, n) = 1.$$

PROOF. Let $G = \{x \in \mathbb{Z}_n : (x, n) = 1\}$. $(G, \cdot)$ is a group of order $\phi(n)$. So $x^{\phi(n)} = 1$ in G. □

FACT. Let $H, K < G$ be groups. Then $|H||K| = |HK||H \cap K|$. If H and K are finite, $|HK| = |H||K|/|H \cap K|$.

PROOF. Define $f : H \times K \to HK$, $(h, k) \mapsto hk$. For $hk \in HK$, $f^{-1}(hk) = \{(ha, a^{-1}k) : a \in H \cap K\}$; hence $|f^{-1}(hk)| = |H \cap K|$. So, $|H \times K| = |HK||H \cap K|$. □

1.2. Normal Subgroups and Quotient Groups

DEFINITION 1.5. Let $H < G$ be groups. H is called a *normal* subgroup of G, denoted as $H \lhd G$, if $aH = Ha$ for all $a \in G$. If $H \lhd G$,

$$\begin{array}{ccc} (G/H) \times (G/H) & \longrightarrow & G/H \\ (aH,\ bH) & \longmapsto & abH \end{array}$$

is a well defined binary operation on G/H which makes G/H a group (the *quotient* or *factor* group of G by H).

THE CANONICAL HOMOMORPHISM. Let $H \lhd G$. Then

$$\begin{array}{rccc} \pi : & G & \longrightarrow & G/H \\ & a & \longmapsto & aH \end{array}$$

is an onto homomorphism with $\ker \pi = H$.

EASY FACT. Let $f : G \to H$ be a homomorphism and $K < H$. Then $f(G) < H$ and $f^{-1}(K) < G$. If $K \lhd H$, $f^{-1}(K) \lhd G$.

EASY FACTS. Let G be a group.

(i) $H \lhd G \Leftrightarrow H = \ker f$ for some homomorphism $f : G \to K$.

(ii) $Z(G) := \{a \in G : ax = xa\ \forall x \in G\}$ (the *center* of G) is a normal subgroup of G. If $H < Z(G)$, $H \lhd G$.

(iii) If $[G : H] = 2$, $H \lhd G$.

PROOF. (iii) Let $a \in G$. If $a \in H$, $aH = H = Ha$. If $a \notin H$, $aH = G\setminus H = Ha$ since $G = H \mathbin{\dot\cup} aH = H \mathbin{\dot\cup} Ha$. □

Easy facts.

(i) If $H < G$ and $K < G$, then $HK < G \Leftrightarrow HK = KH$.
(ii) If $H < G$ and $K \lhd G$, then $HK < G$.
(iii) If $H \lhd G$ and $K \lhd G$, then $HK \lhd G$.

Theorem 1.6 (The correspondence theorem). *Let $N \lhd G$ and let $\mathcal{A} = \{K < G : N \subset K\}$, $\mathcal{B} =$ the set of all subgroups of G/N. Then*

$$\begin{array}{rccc} f: & \mathcal{A} & \longrightarrow & \mathcal{B} \\ & K & \longmapsto & K/N \end{array}$$

is a bijection. Moreover, $K/N \lhd G/N \Leftrightarrow K \lhd G$.

Universal mapping property of the quotient group. Let $N \lhd G$ and $f : G \to H$ a group homomorphism such that $\ker f \supset N$. Then $\exists!$ homomorphism $\bar{f} : G/N \to H$ such that the following diagram commutes.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Proof. Let $\bar{f}(aN) = f(a)$. □

Three isomorphism theorems.

First isomorphism theorem. *Let $f : G \to H$ be a homomorphism. Then $G/\ker f \cong f(G)$.*

Proof. By the universal mapping property, $f : G \to H$ induces a homomorphism $\bar{f} : G/\ker f \to f(G)$. $\bar{f}$ is onto and $\ker \bar{f} = \{\ker f\}$. Hence $\bar{f}$ is an isomorphism. □

Second isomorphism theorem. *Let $H < G$ and $N \lhd G$. Then $HN/N \cong H/(N \cap H)$.*

Proof. $f : H \to HN/N$, $h \mapsto hN$, is an onto homomorphism with $\ker f = N \cap H$. □

Third isomorphism theorem. *Let $N \lhd G$, $H \lhd G$ and $N \subset H$. Then $(G/N)\big/(H/N) \cong G/H$.*

Proof. $f : G/N \to G/H$, $aN \mapsto aH$, is a well-defined onto homomorphism with $\ker f = H/N$. □

Example. If G is a cyclic group, then $G \cong \mathbb{Z}$ or $\mathbb{Z}_n$.

Proof. Let $G = \langle a \rangle$. Then $f : \mathbb{Z} \to G$, $n \mapsto a^n$, is an onto homomorphism. If $\ker f = \{0\}$, $G \cong \mathbb{Z}$. If $\ker f \neq \{0\}$, let n be the smallest positive integer in $\ker f$. Then $\ker f = n\mathbb{Z}$. So $G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. □

Fact. If $(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Fact. If $H, K \lhd G$, $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof. For all $h \in H$, $k \in K$, we have $hkh^{-1}k^{-1} \in H \cap K$; hence $hkh^{-1}k^{-1} = e$, i.e., $hk = kh$. Define $f : H \times K \to HK$, $(h,k) \mapsto hk$. Then f is an isomorphism. □

Conjugation. For $a \in G$,

$$\begin{array}{cccc} \phi_a : & G & \longrightarrow & G \\ & x & \longmapsto & axa^{-1} \end{array}$$

is an automorphism of G (conjugation by a). A subgroup $H < G$ is normal iff $\phi_a(H) = H$ for all $a \in G$. H is called a *characteristic* subgroup of G if $f(H) = H$ for all $f \in \text{Aut}(G)$. "Characteristic" ⇒ "normal"; the converse is false, e.g., $\mathbb{Z}_2 \times \{0\}$ is a normal but not characteristic subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$\text{Inn}(G) := \{\phi_a : a \in G\}$ is a normal subgroup of $\text{Aut}(G)$ and is called the *inner automorphism group* of G. (In fact, if $f \in \text{Aut}(G)$, $f\phi_a f^{-1} = \phi_{f(a)}$.) Moreover, $\text{Inn}(G) \cong G/Z(G)$. (Proof. $g : G \to \text{Inn}(G)$, $a \mapsto \phi_a$, is an onto homomorphism with $\ker g = Z(G)$.)

Example. Let G be a group with $|G| > 2$. Then $|\text{Aut}(G)| > 1$.

Proof. If G is nonabelian, $|\text{Inn}(G)| = |G/Z(G)| > 1$. So, assume that G is abelian. If $a^2 \neq e$ for some $a \in G$, $x \mapsto x^{-1}$ is a nontrivial automorphism of G. If $a^2 = e$ for all $a \in G$, G is a vector space over $\mathbb{Z}_2$ of dimension > 1. In this case, $\text{Aut}(G) = \text{GL}(G)$. Let E be a basis of G and choose $\epsilon_1, \epsilon_2 \in E$ distinct. Then $\exists f \in \text{GL}(G)$ such that $f(\epsilon_1) = \epsilon_2$. □

The commutator subgroup and abelianization. An element of the form $x^{-1}y^{-1}xy$ $(x, y \in G)$, denoted by $[x,y]$, is called a *commutator* of G. $G' = \langle\{x^{-1}y^{-1}xy : x, y \in G\}\rangle$ is the *commutator subgroup* of G.

Proposition 1.7.

(i) *G' is a characteristic subgroup of G and G/G' is abelian.*

(ii) *Let $H < G$. Then $H \lhd G$ with G/H abelian ⇔ $H \supset G'$.*

Note. G' is the smallest normal subgroup H of G such that G/H is abelian. G/G' is called the abelianization *of G.*

Proof. (i) $\{x^{-1}y^{-1}xy : x, y \in G\}$ is invariant under any automorphism of G.

(ii) (⇒) $\forall x, y \in G$, since G/H is abelian, $(xH)(yH) = (yH)(xH)$; so $x^{-1}y^{-1}xy \in H$.

(⇐) $H/G' \lhd G/G' \Rightarrow H \lhd G$. $G/H \cong (G/G')/(H/G')$ is abelian. □

Normal subgroups at top and bottom. Let $H < G$. If $H \subset Z(G)$ or $H \supset G'$, then $H \lhd G$.

If G is abelian, every subgroup of G is normal. The converse is false, as shown by the next example.

Example. (The *quaternion* group) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. The multiplication in Q_8 is defined by rules $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ik = -j$, $kj = -i$, $ji = -k$; see Figure 1.1. $Z(Q_8) = \{\pm 1\}$. Every subgroup of Q_8 is normal, yet Q_8 is nonabelian. $Q_8 = \langle\{i,j\}\rangle$. Let $A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right]$, $C = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right] \in \text{GL}(2, \mathbb{C})$. Then $G = \{\pm I, \pm A, \pm B, \pm C\} < \text{GL}(2, \mathbb{C})$ and $Q_8 \cong G$. (The isomorphism is given by $i \mapsto A$, $j \mapsto B$.)

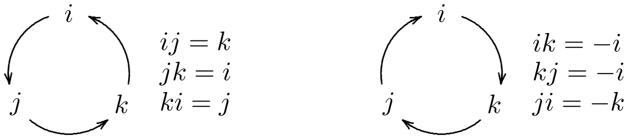


FIGURE 1.1. Multiplication in Q_8

Advanced Reading

HAMILTONIAN GROUPS. A nonabelian group G is called *Hamiltonian* if all its subgroups are normal.

THEOREM 1.8 (Dedekind, Baer). *G is Hamiltonian $\Leftrightarrow$*

$$G \cong Q_8 \times A \times B,$$

where A is an elementary abelian 2-group and B is an abelian group whose elements all have odd order.

LEMMA 1.9. *Let G be a group and $x, y \in G$ such that $[x, y]$ commutes with x and y. Then*

(i) $[x^i, y^j] = [x, y]^{ij}$, *$i, j \in \mathbb{Z}$;*
(ii) $(xy)^i = x^i y^i [y, x]^{\binom{i}{2}}$, *$i \in \mathbb{N}$.*

PROOF. (i) First assume $i, j \geq 0$. We have $[x, y]^2 = (x^{-1}y^{-1}xy)x^{-1}y^{-1}xy = x^{-1}(x^{-1}y^{-1}xy)y^{-1}xy = [x^2, y]$. Induction shows that $[x, y]^i = [x^i, y]$. In the same way, $[x^i, y]^j = [x^i, y^j]$.

If $i < 0$, note that $[x^{-1}, y] = [x, y]^{-1}$.

(ii) Induction on i.

$$\begin{aligned}(xy)^{i+1} &= x^i y^i [y, x]^{\binom{i}{2}} xy = x^i y^i xy [y, x]^{\binom{i}{2}} = x^i x y^i [y^i, x] y [y, x]^{\binom{i}{2}} \\ &= x^{i+1} y^{i+1} [y, x]^{i + \binom{i}{2}} = x^{i+1} y^{i+1} [y, x]^{\binom{i+1}{2}}.\end{aligned}$$

□

PROOF OF THEOREM 1.8. ($\Leftarrow$) Let $H < G$. Then $H = (H \cap (Q_8 \times A)) \times (H \cap B)$. (Here we abuse the notation by treating $(Q_8 \times A) \times B$ as an internal direct product.) It suffices to show that $H_1 := H \cap (Q_8 \times A) \lhd Q_8 \times A$. If H_1 contains an element of order 4, then $H_1 \supset \{h^2 : h \in H_1\} = Z(Q) = G'$. So $H \lhd G$. If H_1 contains no element of order 4, then $H_1 \subset Z(G)$. Also, $H_1 \lhd G$.

($\Rightarrow$) 1° Let $x, y \in G$ such that $c := [x, y] \neq 1$. Since $\langle x \rangle$, $\langle y \rangle \lhd G \Leftrightarrow c \in \langle x \rangle \cap \langle y \rangle$. So, $x^i = c = y^j$ for some $i, j \in \mathbb{Z}^+$. Put $Q = \langle x, y \rangle$. Then $Q' = \langle c \rangle \subset Z(Q)$. By Lemma 1.9 (i), $c^i = [x^i, y] = [c, y] = 1$. Hence $o(x)$, $o(y) < \infty$.

2° In 1°, assume $o(x) + o(y)$ is minimal. Let p be a prime factor of $o(x)$. The minimality of $o(x) + o(y)$ implies $1 = [x^p, y] = c^p$. So $o(c) = p$. Also, $o(x)$ cannot have prime factors different from p. So $o(x)$ (and $o(y)$) are powers of p. Write $x^{\alpha p^r} = c = y^{\beta p^s}$, $\alpha, \beta \in \mathbb{Z}^+$, $r, s \in \mathbb{N}$, $p \nmid \alpha, \beta$. Then $o(x) = p^{r+1}$, $o(y) = p^{s+1}$. Let $\alpha', \beta' \in \mathbb{Z}$ such that $\alpha'\alpha \equiv 1 \equiv \beta'\beta \pmod{p}$. Then

$$x^{\beta' p^r} = x^{\beta'\alpha'\alpha p^r} = c^{\alpha'\beta'} = y^{\alpha'\beta'\beta p^s} = y^{\alpha' p^s},$$

where $c^{\alpha'\beta'} = [x^{\beta'}, y^{\alpha'}]$. Replacing x, y, c by $x^{\beta'}, y^{\alpha'}, c^{\alpha'\beta'}$ respectively, we may assume $x^{p^r} = c = y^{p^s}$. Note that $r, s > 0$ since otherwise $[x, y] = 1$.

3° In 2°, assume $r \geq s$. Since $x^{-p^{r-s}}y$ does not commute with x, by the minimality of $o(x) + o(y)$, $o(x^{-p^{r-s}}y) \geq o(y) = p^{s+1}$. By Lemma 1.9 (ii),

$$1 \neq (x^{-p^{r-s}}y)^{p^s} = x^{-p^r}y^{p^s}[y, x^{-p^{r-s}}]^{\binom{p^s}{2}} = [y,x]^{-p^{r-s}\binom{p^s}{2}} = c^{-\frac{1}{2}p^r(p^s-1)}.$$

So, $p \nmid \frac{1}{2}p^r(p^s-1) \Rightarrow p = 2$ and $r = 1$. So, $o(x) = 4$, $x^2 = y^2$, $yxy^{-1} = x^{-1} \Rightarrow Q$ is a homomorphic image of Q_8. Q is nonabelian $\Rightarrow Q = Q_8$.

4° $G = QC$ where $C = C_G(Q)$. (Let $g \in G$. Then $gxg^{-1} = x^{\pm 1} = x^{(-1)^a}$, $gyg^{-1} = y^{\pm 1} = y^{(-1)^b}$, $a, b \in \{0, 1\}$. Then $y^a x^b g$ commutes with x and y, i.e. $y^a x^b g \in C$.

5° C has no element of order 4. (Assume $g \in C$ with $o(g) = 4$. Then $g \notin Q$, so $o(gx) = 2$ or 4. Since $[gx, y] \neq 1$, $ygxy^{-1} = (gx)^{-1}$, i.e. $g = g^{-1}$. Contradiction.)

6° C is abelian. (Otherwise, C would be a Hamiltonian group without element of order 4, which contradicts 3°.) For every $g \in G$, gx does not commute with y. By 1°, $o(gx) < \infty \Rightarrow o(g) < \infty$. So, C is torsion $\Rightarrow C = A \times B$, where A is an elementary abelian 2-group and every element of B has odd order. Then $G = QC \cong QA \times B$. Since A is a vector space over $\mathbb{Z}_2$, $A = (Q \cap A) \times A'$ for some $A' < A$. It's easy to see that $QA = Q \times A'$. □

End Advanced Reading

1.3. The Symmetric Group

The *symmetric group* of a set X, denoted by S_X, is the group of all permutations of X. If $|X| = n$, (may assume $X = \{1, \dots, n\}$), write $S_X = S_n$. $|S_n| = n!$.

Cayley's theorem. Every group G is isomorphic to a subgroup of S_G. If $|G| = n$, G is embedded in S_n.

Proof. Define

$$\begin{array}{cccc} f: & G & \to & S_G \\ & a & \mapsto & f(a) \end{array} \quad \text{where} \quad \begin{array}{cccc} f(a): & G & \to & G \\ & x & \mapsto & ax. \end{array}$$

f is a homomorphism with $\ker f = \{e\}$. □

Notation. $\sigma \in S_n$ is denoted by

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Let $i_1, \dots, i_k \in \{1, \dots, n\}$ be distinct. $(i_1, \dots, i_k) \in S_n$ is the permutation which maps i_1 to i_2, i_2 to i_3, ..., i_{k-1} to i_k, i_k to i_1 and leaves other elements unchanged; it is a called a *k-cycle*. A *transposition* is a 2-cycle. A 1-cycle is the identity of S_n.

Facts.

(i) Disjoint cycles commute.
(ii) $(i_1, \dots, i_k) = (i_2, \dots, i_k, i_1) = \cdots$.
(iii) $(i_1, \dots, i_k)^{-1} = (i_k, \dots, i_1)$.
(iv) $\sigma \cdot (i_1, \dots, i_k) \cdot \sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_k))$.

Theorem 1.10. *Every $\sigma \in S_n$ is a product of disjoint cycles. The cycles are unique except for the order in which they appear in the product.*

PROOF. *Existence.* Induction on n. In the sequence $1, \sigma(1), \sigma^2(1), \dots$, let i be th smallest positive integer such that $\sigma^i(1) = 1$. Then $\tau := (1, \sigma(1), \dots, \sigma^{i-1}(1))^{-1}\sigma$ fixes $1, \sigma(1), \dots, \sigma^{i-1}(1)$; hence $\tau \in S_{\{1,\dots,n\}\setminus\{\sigma(1),\dots,\sigma^{i-1}(1)\}}$. By the induction hypothesis, τ is a product of disjoint cycles involving $\{1, \dots, n\} \setminus \{\sigma(1), \dots, \sigma^{i-1}(1)\}$. So, $\sigma = (1, \sigma(1), \dots, \sigma^{i-1}(1))\tau$ is a product of disjoint cycles.

Uniqueness. Assume $\sigma = (1, i_2, \dots, i_k)\alpha = (1, j_2, \dots, j_l)\beta$, where α (β) is a product of disjoint cycles involving $\{1, \dots, n\} \setminus \{1, i_1, \dots, i_k\}$ ($\{1, \dots, n\} \setminus \{1, j_1, \dots, j_l\}$). Then for $2 \le s \le \min\{k, l\}$, $i_s = \sigma^s(1) = j_s$. Claim that $k = l$. (If $k < l$, then $1 = \sigma(i_k) = \sigma(j_k) = j_{k+1}$, which is a contradiction.) So $\alpha = \beta$. By induction, the disjoint cycles in α and β are the same. □

EASY FACT. If the disjoint cycles in $\sigma \in S_n$ are of lengths $l_1, \dots, l_k$, then $o(\sigma) = \text{lcm}(l_1, \dots, l_k)$.

FACT. S_n is generated by each of the following subsets.

(i) $\{(1, 2), (1, 3), \dots, (1, n)\}$.
(ii) $\{(1, 2), (2, 3), \dots, (n - 1, n)\}$.
(iii) $\{(1, 2), (1, 2, \dots, n)\}$.

PROOF. (i) $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$; $(i, j) = (1, i)(1, j)(1, i)$.
(ii) $(1, j) = (j - 1, j)(1, j - 1)(j - 1, j)$, $2 \le j \le n$.
(iii) $(i, i + 1) = (1, 2, \dots, n)(i - 1, i)(1, 2, \dots, n)^{-1}$. □

THE SIGN OF A PERMUTATION. Let $f(x_1, \dots, x_n)$ be a polynomial in $x_1, \dots, x_n$ with coefficients in $\mathbb{Z}$ and let $\sigma \in S_n$. Define $\sigma(f) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

$$\sigma\Big(\prod_{1\le i<j\le n}(x_i - x_j)\Big) = \prod_{1\le i<j\le n}(x_{\sigma(i)} - x_{\sigma(j)}) = \pm \prod_{1\le i<j\le n}(x_i - x_j).$$

(Note. $\big\{\{\sigma(i), \sigma(j)\} : 1 \le i < j \le m\big\}$ is the set of all 2-element subsets of $\{1, \dots, n\}$.) Write

$$\sigma\Big(\prod_{1\le i<j\le n}(x_i - x_j)\Big) = \text{sign}(\sigma) \prod_{1\le i<j\le n}(x_i - x_j),$$

where $\text{sign}(\sigma) \in \{\pm 1\}$. Then $\text{sign} : S_n \to (\{\pm 1\}, \cdot)$ is a homomorphism (onto when $n \ge 2$). $\text{sign}(1, 2) = -1$; hence $\text{sign}(i, j) = -1$ since (i, j) is conjugate to $(1, 2)$. $A_n := \ker \text{sign}$ is the *alternating group* of degree n.

FACTS.

(i) Each $\sigma \in S_n$ is a product of either an even number of transpositions (not necessarily disjoint) or an odd number of transpositions, but not both; σ is called *even* or *odd* accordingly. A_n is the set of even permutations.
(ii) $|A_n| = \frac{1}{2}n!$ for $n \ge 2$.
(iii) $\text{sign}(i_1, \dots, i_k) = (-1)^{k-1}$.

PROPOSITION 1.11. *A_n is generated by 3-cycles.*

PROOF. Only have to show that $(i, j)(k, l)$ ($i \ne j$, $k \ne l$) is generated by 3-cycles. If $\{i, j\} = \{k, l\}$, then $(i, j)(k, l) = \text{id}$. If $|\{i, j\} \cap \{k, l\}| = 1$, may assume $\{i, j\} = \{1, 2\}$, $\{k, l\} = \{1, 3\}$. Then $(1, 2)(1, 3) = (3, 2, 1)$. If $\{i, j\} \cap \{k, l\} = \emptyset$, then $(i, j)(k, l) = ((i, j)(j, k))((j, k)(k, l))$ where $|\{i, j\} \cap \{j, k\}| = 1 = |\{j, k\} \cap \{k, l\}|$. □

The dihedral group D_n. D_n is the subgroup of S_n generated by $\alpha = (1,\dots,n)$ and $\beta = (2,n)(3,n-1)\cdots(\lceil\frac{n}{2}\rceil, \lfloor\frac{n}{2}\rfloor + 2)$.

Facts about D_n.

(i) $o(\alpha) = n$, $o(\beta) = 2$, $\beta\alpha\beta^{-1} = \alpha^{-1}$.

(ii) For $n \ge 3$, $|D_n| = 2n$. $D_n = \{\alpha^i\beta^j : 0 \le i \le n-1,\ 0 \le j \le 1\}$.

(iii)

$$Z(D_n) = \begin{cases} \{\mathrm{id},\ \alpha^{n/2}\} & \text{if } n \text{ is even,} \\ \{\mathrm{id}\} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. (i) $\beta\alpha\beta^{-1} = \beta(\dots, n-1, n, 1, 2, 3, \dots)\beta^{-1} = (\dots, 3, 2, 1, n, n-1, \dots) = \alpha^{-1}$.

(ii) By (i), $\{\alpha^i\beta^j : 0 \le i \le n-1,\ 0 \le j \le 1\}$ is closed under multiplication. So $D_n = \{\alpha^i\beta^j : 0 \le i \le n-1,\ 0 \le j \le 1\}$. $\alpha^i\beta^j$, $0 \le i \le n-1$, $0 \le j \le 1$, are all distinct. (Assume $\alpha^{i_1}\beta^{j_1} = \alpha^{i_2}\beta^{j_2}$, $0 \le i_1, i_2 \le n-1$, $0 \le j_1, j_2 \le 1$. Then $\alpha^{i_1-i_2} = \beta^{j_2-j_1}$, $1 = \beta^{j_2-j_1}(1) = \alpha^{i_1-i_2}(1) \equiv 1 + i_1 - i_2 \pmod{n}$. So, $i_1 = i_2$; hence $j_1 = j_2$.) □

Let X_n be a regular n-gon in $\mathbb{R}^2$ with vertices labeled by $1, 2, \dots, n$ (Figure 1.2). A symmetry of X is a rigid motion in $\mathbb{R}^3$ which permutes the vertices of X_n. A symmetry of X can be treated as a permutation of the vertices of X.

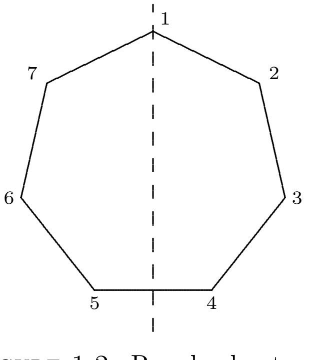


Figure 1.2. Regular heptagon

Fact. $D_n =$ the group of symmetry of X_n.

Proof. Let $\sigma \in S_n$ be a symmetry of X_n with $\sigma(1) = i$. Then $\alpha^{-i}\sigma$ is a symmetry of X_n which fixes 1. Thus $\alpha^{-i}\sigma$ is either the identity or the reflection β, i.e. $\alpha^{-i}\sigma = \beta^j$, $j = 0$ or 1. So, $\sigma = \alpha^i\beta^j \in D_n$. □

Definition 1.12. A group $G \ne \{e\}$ is called *simple* if the only normal subgroups of G are $\{e\}$ and G.

Fact. A finite abelian group G is simple $\Leftrightarrow$ $G \cong \mathbb{Z}_p$ where p is a prime.

Simplicity of A_n $(n \ge 5)$. If $n \ge 5$, A_n is simple.

Proof. 1° If $n \ge 5$, all 3-cycles in A_n are conjugate in A_n.

Let $i_1, \dots, i_5 \in \{1, \dots, n\}$ be distinct (arbitrary). Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i_1 & i_2 & i_3 & i_4 & i_5 & \cdots \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i_1 & i_2 & i_3 & i_5 & i_4 & \cdots \end{pmatrix}$$

such that $\alpha \in A_n$. Then $\alpha(1,2,3)\alpha^{-1} = (i_1, i_2, i_3)$.

2° Let $\{\text{id}\} \neq N \lhd A_n$. To show $N = A_n$, it suffices to show that N contains a 3-cycle. (By the normality of N and 1°, N contains all 3-cycles. By Proposition 1.11, $N = A_n$.) Let $\text{id} \neq \sigma \in N$, written as a product of disjoint cycles.

Case 1. σ has a cycle of length $r \geq 4$, say $\sigma = (1, \dots, r) \cdot \alpha$. Let $\delta = (1,2,3) \in A_n$. Then $N \ni \sigma^{-1}(\delta\sigma\delta^{-1}) = (r, \dots, 2, 1)(2, 3, 1, 4, \dots, r) = (1, 3, r)$.

Case 2. σ has two 3-cycles, say, $\sigma = (1,2,3)(4,5,6) \cdot \alpha$. Let $\delta = (1,2,4) \in A_n$. Then, $N \ni \sigma^{-1}(\delta\sigma\delta^{-1}) = (3,2,1)(6,5,4)(2,4,3)(1,5,6) = (1,4,2,6,3)$. We are in case 1.

Case 3. One cycle of σ has length 3; all others have length ≤ 2. Then σ^2 is a 3-cycle.

Case 4. All cycles of σ have length ≤ 2. Say, $\sigma = (1,2)(3,4)\alpha$. Let $\delta = (1,2,3) \in A_n$. Then $N \ni \sigma(\delta\sigma\delta^{-1}) = (1,2)(3,4)(2,3)(1,4) = (1,3)(2,4) := \tau$. Let $\epsilon = (1,3,5)$. Then $N \ni \tau(\epsilon\tau\epsilon^{-1}) = (1,3)(2,4)(3,5)(2,4) = (1,3,5)$. □

Note. A_1, A_2, A_3 are simple. A_4 is not simple. $K = \{\text{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd A_4$.

1.4. Group Actions

S_X and ${}_XS$. Let X be a set and σ a permutation of X. When applying σ to $x \in X$, we can write σ to the left or right of x, i.e. $\sigma(x)$ or $(x)\sigma$. In the first notation, the rule of composition is $(\tau\sigma)(x) = \tau(\sigma(x))$; the symmetric group on X is denoted by S_X. In the second notation, the rule of composition is $(x)(\tau\sigma) = ((x)\tau)\sigma$; the symmetric group on X is denoted by ${}_XS$. (Note. $\sigma \mapsto \sigma$ ($\sigma \mapsto \sigma^{-1}$) is an anti isomorphism (isomorphism) between S_X and ${}_XS$.)

Definition 1.13. Let G be a group and X a set. A left (right) *action* of G on X is a homomorphism $\phi : G \to S_X$ (${}_XS$). Usually, for $g \in G$, the image $\phi(g)$ is still denoted by g. So, for a left (right) action, $gx = \phi(g)(x)$ ($xg = (x)\phi(g)$). Equivalently, a left action on G on X is a map

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & gx \end{array}$$

such that $ex = x$ and $g_1(g_2x) = (g_1g_2)x$ for all $x \in X$ and $g_1, g_2 \in G$. A right action of g on X is a map $X \times G \to X$ with similar properties.

Example. Let V be a vector space over F and $\text{Hom}_F(V, F)$ the dual of V.

$$\begin{array}{ccc} \text{GL}(V) \times V & \longrightarrow & V \\ (f, x) & \longmapsto & f(x) \end{array}$$

is a left action on $\text{GL}(V)$ on V.

$$\begin{array}{ccc} \text{Hom}_F(V, F) \times \text{GL}(V) & \longrightarrow & \text{Hom}_F(V, F) \\ (l, f) & \longmapsto & l \circ f \end{array}$$

is a right action of $\text{GL}(V)$ on $\text{Hom}_F(V, F)$.

Definition 1.14. Let G act on X (left action). For $x \in X$, $[x] := \{gx : g \in G\}$ is the G-*orbit* of x, $G_x := \{g \in G : gx = x\} < G$ is the *stabilizer* of x. The G-orbits form a partition of X. If X has only one G-orbit, we say that G acts transitively on X.

Easy facts. Let G act on X.

(i) For $x \in X$, $[G : G_x] = |[x]|$.
(ii) For $g \in G$ and $x \in X$, $G_{gx} = gG_xg^{-1}$.

Proof. (i) Define

$$\begin{array}{rccc} f: & G/G_x & \longrightarrow & [x] \\ & gG_x & \longmapsto & gx. \end{array}$$

Then f is a well defined bijection. □

Conjugation and the class equation. G acts on G by conjugation: $G \times G \to G$, $(a, x) \mapsto axa^{-1}$. $[x]$ is the *conjugacy class* of x in G. $G_x = \{a \in G : axa^{-1} = x\} =: C_G(x)$ is the *centralizer* of x in G. Note that $|[x]| = 1$ iff $x \in Z(G)$. Let $\{x_i : i \in I\}$ be a set of representatives of the conjugacy classes of G not contained in $Z(G)$. Then $[x]$, $x \in Z(G)$, and $[x_i]$, $i \in I$, are all the conjugacy classes of G. Hence

$$|G| = \sum_{x \in Z(G)} |[x]| + \sum_{i \in I} |[x_i]| = |Z(G)| + \sum_{i \in I} [G : C_G(x_i)]. \tag{1.1}$$

(1.1) is called the *class equation* of G.

Normalizer. Let G be a group and $\mathcal{S}(G)$ the set of all subgroups of G. G acts on $\mathcal{S}(G)$ by conjugation: $G \times \mathcal{S}(G) \to \mathcal{S}(G)$, $(a, H) \mapsto aHa^{-1}$. For $H < G$, $G_H = \{a \in G : aHa^{-1} = H\} =: N_G(H)$ is the *normalizer* of H in G. ($N_G(H)$ is the largest subgroup K of G such that $H \lhd K$.) $[G : N_G(H)]$ is the number of conjugates of H in G.

p-group actions. Let p be a prime. A group G is called a p-*group* if and only if for each $a \in G$, $o(a)$ is a power of p. A finite group G is a p-group $\Leftrightarrow$ $|G|$ is a power of p. (This follows from Sylow's theorem.)

Lemma 1.15. *Let G be a finite p-group acting on a finite set X. Let $X_0 = \{x \in X : gx = x \ \forall g \in G\}$. Then $|X| \equiv |X_0| \pmod{p}$.*

Proof. For $x \in X$, $[x] = \{x\} \Leftrightarrow x \in X_0$. Let $[x_1], \dots, [x_n]$ be all the distinct G-orbits such that $\{x_1, \dots, x_k\} = X_0$. Then

$$|X| = \sum_{i=1}^{n} |[x_i]| = k + |[x_{k+1}]| + \cdots + |[x_n]| \equiv k \pmod{p}.$$

□

Proposition 1.16 (Facts about finite p-groups). *Let p be a prime and G a nontrivial finite p-group.*

(i) *$Z(G) \neq \{e\}$.*
(ii) *If $H < G$ with $[G : H] = p$, then $H \lhd G$.*
(iii) *If $|G| = p^2$, then G is abelian.*

TABLE 1.1. Examples of Lemma 1.15

G	X	action	X_0	conclusion	in particular
G	N $\{e\} \neq N \lhd G$	conjugation	$N \cap Z(G)$	$\lvert N \cap Z(G)\rvert \equiv 0 \pmod{p}$	$\lvert N \cap Z(G)\rvert > 1$
H	G/H $H < G$	left multiplication	$N_G(H)/H$	$[N_G(H) : H] \equiv [G : H]$ $\pmod{p}$	if $p \mid [G : H]$, $N_G(H) \neq H$

PROOF. (i) and (ii) are special cases of Table 1.1.

(iii) 1° Let G be any group. If $G/Z(G)$ is cyclic, G is abelian.

2° If $|G| = p^2$, $|Z(G)| = p$ or p^2. However, $|Z(G)| \neq p$. (Otherwise, $G/Z(G)$ is cyclic $\Rightarrow$ G is abelian $\Rightarrow$ $|Z(G)| = p^2$.) □

PROPOSITION 1.17. *Let G be a group. If there exists $H < G$ such that $[G : H] = n < \infty$, then there exists $N \lhd G$ such that $N \subset H$ and $[G : N] \mid n!$.*

PROOF. G acts on G/H: $(a, gH) \mapsto agH$. Let N be the kernel of this action. Then $N \lhd G$, $N \subset H$ and $G/N \hookrightarrow S_{G/H} = S_n$. □

EXAMPLE. Let G be a simple group with $|G| > 2$. If $\exists\, H < G$ such that $[G : H] = n > 1$, then $G \hookrightarrow A_n$.

PROOF. In the proof of Proposition 1.17, $N = \{e\}$ and $G = G/N \hookrightarrow S_{G/H} = S_n$. Assume $G \subset S_n$. We claim that $G \subset A_n$. (If $G \not\subset A_n$, then $[G : G \cap A_n] = 2$. So, $G \cap A_n \lhd G, \rightarrow\leftarrow$.) □

THEOREM 1.18 (Burnside's lemma). *Let G be a finite group acting on a finite set X. Then the number of G-orbits in X is*

$$n = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

where $\mathrm{Fix}(g) = |\{x \in X : gx = x\}|$.

PROOF. Let $\mathcal{X} = \{(g, x) : g \in G,\ x \in X,\ gx = x\}$. Counting $(g, x) \in \mathcal{X}$ in the order of g, x, we have $|\mathcal{X}| = \sum_{g \in G} \mathrm{Fix}(g)$. Counting $(g, x) \in \mathcal{X}$ in the order of x, g, we also have $|\mathcal{X}| = \sum_{x \in X} |G_x|$. Let $[x_1], \dots, [x_n]$ be the G-orbits in X. Then

$$\sum_{x \in X} |G_x| = \sum_{i=1}^{n} \sum_{x \in [x_i]} |G_x| = \sum_{i=1}^{n} \sum_{x \in [x_i]} \frac{|G|}{|[x]|} = \sum_{i=1}^{n} \sum_{x \in [x_i]} \frac{|G|}{|[x_i]|} = \sum_{i=1}^{n} |G| = n|G|.$$

So, $n|G| = \sum_{g \in G} \mathrm{Fix}(g)$. Hence the theorem. □

1.5. Sylow's Theorem

THEOREM 1.19 (Sylow). *Let G be a finite group with $|G| = p^e m$, where p is a prime, $e > 0$, and $p \nmid m$.*

(i) *Every p-subgroup (including $\{e\}$) of G is contained in a subgroup of order p^e. (A subgroup of G of order p^e is called a* Sylow p-subgroup.*)*

(ii) *All Sylow p-subgroups are conjugate in G.*

(iii) *Let n_p denote the number of Sylow p-subgroups of G. Then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.*

Proof. 1° Let $\mathcal{X} = \{X \subset G : |X| = p^e\}$. Then $|\mathcal{X}| = \binom{p^e m}{p^e} \equiv m \not\equiv 0 \pmod{p}$. G acts on $\mathcal{X}$: $G \times \mathcal{X} \to \mathcal{X}$, $(g, X) \mapsto gX$. There exists $X \in \mathcal{X}$ such that $|[X]| \not\equiv 0 \pmod{p}$, i.e. $|G|/|G_X| \not\equiv 0 \pmod{p}$. So, $p^e \bigm| |G_X|$. Choose $x_0 \in X$. Then $|G_X| = |G_X x_0| \le |G_X X| = |X| = p^e$. So, $P := G_X$ is a Sylow p-subgroup of G.

2° Let $\mathcal{P} = \{gPg^{-1} : g \in G\}$. P acts on $\mathcal{P}$ by conjugation. $\{P\}$ is the only orbit with one element. (If $P_1 \in \mathcal{P}$ such that $P_1 \ne P$ and $\{P_1\}$ is an orbit, then PP_1 is a p-subgroup of G with $|PP_1| > p^e$, which is a contraction.) So, $|\mathcal{P}| \equiv 1 \pmod{p}$ by Lemma 1.15. Since $|\mathcal{P}| \bigm| |G|$, we must have $|\mathcal{P}| \bigm| m$.

3° Let P_1 be a p-subgroup of G. P_1 acts on $\mathcal{P}$ by conjugation. Since $|\mathcal{P}| \equiv 1 \pmod{p}$, there exists $P_2 \in \mathcal{P}$ such that $\{P_2\}$ is a P_1-orbit. Then $P_1 \subset P_2$. (Otherwise, P_1P_2 is a p-subgroup of G with $|P_1P_2| > p^e$.) This also shows that $\mathcal{P}$ is the set of all Sylow p-subgroups of G, i.e. $n_p = |\mathcal{P}|$. □

Proposition 1.20. *Let P be a Sylow p-subgroup of G. Then $N_G(N_G(P)) = N_G(P)$.*

Proof. Let $x \in N_G(N_G(P))$. Then $xPx^{-1} \subset xN_G(P)x^{-1} = N_G(P)$. Since both xPx^{-1} and P are Sylow p-subgroups of $N_G(P)$, by Sylow's theorem, there exists $y \in N_G(P)$ such that $xPx^{-1} = yPy^{-1} = P$. So, $x \in N_G(P)$. □

Proposition 1.21. *Let $H \lhd G$, $|H| < \infty$ and P a Sylow p-subgroup of H. Then $G = H\,N_G(P)$.*

Proof. Let $x \in G$. Then P and xPx^{-1} are conjugate in H, i.e. $xPx^{-1} = yPy^{-1}$ for some $y \in H$. So, $y^{-1}x \in N_G(P)$ and $x = y(y^{-1}x) \in HN_G(P)$. □

Note. The method in the above two proofs is called the *Frattini argument.*

Semidirect product. Let N and H be groups and $\theta : H \to \mathrm{Aut}(N)$ a homomorphism. The semidirect product $N \rtimes_\theta H$ is a group where $N \rtimes_\theta H = N \times H$ as a set and

$$(n_1, h_1)(n_2, h_2) = \big(n_1[\theta(h_1)(n_2)],\, h_1h_2\big).$$

$N' := N \times \{e_H\} \lhd N \rtimes_\theta H$, $H' := \{e_G\} \times H < N \rtimes_\theta H$; $N' \cong N$, $H' \cong H$; $N \rtimes_\theta H = N'H'$, $N' \cap H' = \{e\}$; $H \cong (N \rtimes_\theta H)/N'$.

$G \cong N \rtimes_\theta H$ for some $\theta \Leftrightarrow G = N'G'$ where $G \rhd N' \cong N$, $G > H' \cong H$ and $N' \cap H' = \{e\}$.

Proposition 1.22. *Let $|G| = pq$ where $p < q$ are primes.*

(i) *If $p \nmid q - 1$, $G \cong \mathbb{Z}_{pq}$.*
(ii) *If $p \mid q-1$, then $G \cong \mathbb{Z}_{pq}$ or $G \cong \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$, where $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ $(\cong \mathbb{Z}_q^\times)$ is any 1-1 homomorphism.*

Proof. (ii) Assume G is nonabelian. Let Q be a Sylow q-subgroup and P a Sylow p-subgroup of G. Then $Q \lhd G$; hence $G = QP$. Write $Q = \langle a \rangle$, $P = \langle b \rangle$. Then $bab^{-1} = a^k$, where $k \in \mathbb{Z}_q^\times$ has multiplicative order p. Let $[\theta(1)](1) = l \in \mathbb{Z}_q$. Then $[\theta(1)](x) = lx\,\forall x \in \mathbb{Z}_q$. Since $\theta(1) \in \mathrm{Aut}(\mathbb{Z}_q)$, $l \in \mathbb{Z}_q^\times$. Since $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ is 1-1, $o(\theta(1)) = o(1)$ (in $\mathbb{Z}_p$) $= p$. So the multiplicative order of l in $\mathbb{Z}^\times$ is p. We use the fact that $\mathbb{Z}_q^\times$ is cyclic (Proposition 3.40). Since $k, l \in \mathbb{Z}_q^\times$ are both of order p, we can write $l = k^s$, $p \nmid s$. (Cf. Exercise 1.3 (iv).) Let $c = b^s$. Then $P = \langle c \rangle$ and

$cac^{-1} = a^l$. Then

$$\begin{array}{rccc} \phi: & \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p & \longrightarrow & G \\ & (i,j) & \longmapsto & a^i c^j \end{array}$$

is an isomorphism. In fact,

$$\begin{aligned} \phi\big((i_1, j_1)(i_2, j_2)\big) &= \phi(i_1 + [\theta(j_1)](i_2),\, j_1 + j_2) \\ &= \phi\big(i_1 + [\theta(1)^{j_1}](i_2),\, j_1 + j_2\big) \\ &= \phi(i_1 + l^{j_1} i_2,\, j_1 + j_2) \\ &= a^{i_1 + l^{j_1} i_2} c^{j_1 + j_2} \\ &= a^{i_1} (c^{j_1} a c^{-j_1})^{i_2} c^{j_1 + j_2} \quad (\because\ c^{j_1} a c^{-j_1} = a^{l^{j_1}}) \\ &= a^{i_1} c^{j_1} a^{i_2} c^{-j_1} c^{j_1 + j_2} \\ &= a^{i_1} c^{j_1} a^{i_2} c^{j_2} \\ &= \phi(i_1, j_1)\phi(i_2, j_2). \end{aligned}$$

□

Example. Let $|G| = pqr$, where $p < q < r$ are primes. Then the Sylow r-subgroup of G is normal.

Proof. Let $Q < G$, $R < G$ such that $|Q| = q$, $|R| = r$. Assume to the contrary that $R \ntriangleleft G$. Then $n_r = pq$, i.e. $N_G(R) = R$. If $Q \lhd G$, then $R \lhd QR$, $N_G(R) \supset QR$, which is a contradiction. If $Q \ntriangleleft G$, $n_q = r$ or pr. Then G has $pq(r-1)$ elements of order r and at least $r(q-1)$ elements of order q. Note that $pq(r-1) + r(q-1) > pqr$, contradiction. □

Example. If G is a simple group of order 60, then $G \cong A_5$.

Proof. 1° Let $\mathcal{P}$ be the set of all Sylow 5-subgroups of G. Then $|\mathcal{P}| = 6$. Let G act on $\mathcal{P}$ by conjugation. Then $G \hookrightarrow S_{\mathcal{P}} = S_6$. Thus $G \hookrightarrow A_6$. (Otherwise, $[G : G \cap A_6] = 2 \Rightarrow G \cap A_6 \lhd G$.) So, we assume $G \subset A_6$.

2° We claim that $\exists\, \theta \in \mathrm{Aut}(A_6)$ such that $\theta(G) = \{\sigma \in A_6 : \sigma(1) = 1\} \cong A_5$. Define

$$\begin{array}{rccc} \phi: & A_6 & \longrightarrow & S_{A_6/G} \\ & \sigma & \longmapsto & \phi(\sigma), \end{array}$$

where

$$\begin{array}{rccc} \phi(\sigma): & A_6/G & \longrightarrow & A_6/G \\ & \alpha G & \longmapsto & \sigma\alpha G. \end{array}$$

Then ϕ is a homomorphism with $\ker\phi \subset G$. Hence $\ker\phi = \{\mathrm{id}\}$ and $\phi : A_6 \hookrightarrow S_{A_6/G}$. Since A_6 is simple, $\phi : A_6 \xrightarrow{\cong} A_{A_6/G}$. Write $A_6/G = \{G_1, \dots, G_6\}$, where $G_1 = G$. Let $f : \{1, \dots, 6\} \to A_6/G$, $i \mapsto G_i$. Define

$$\begin{array}{rccc} \theta: & A_6 & \longrightarrow & A_6 \\ & \sigma & \longmapsto & f^{-1}\phi(\sigma)f. \end{array}$$

Then $\theta \in \mathrm{Aut}(A_6)$. If $\sigma \in G$, $[\theta(\sigma)](1) = [f^{-1}\phi(\sigma)f](1) = [f^{-1}\phi(\sigma)](G) = f^{-1}(G) = 1$. □

1.6. Finitely Generated Abelian Groups

If A and B are abelian groups, $A \times B$ is also denoted by $A \oplus B$.

THEOREM 1.23 (Structure of finitely generated abelian groups). *Every finitely generated abelian group G is isomorphic to*

$$\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{e_s}} \oplus \mathbb{Z}^r,$$

where $p_1, \dots, p_s$ are primes (not necessarily distinct), $e_i > 0$, $r \geq 0$. The numbers $p_1^{e_1}, \dots, p_s^{e_s}$ (the elementary divisors of G) and r (the rank of G) are uniquely determined by G.

PROOF. This is a special case of Theorem 2.57, the structure theorem of finitely generated modules over a PID. □

FACTS.

(i) The number of nonisomorphic abelian groups of order $p_1^{e_1} \cdots p_s^{e_s}$ is $P(e_1) \cdots P(e_s)$, where $P(e)$ is the number of partitions of e.

(ii) Assume A, B, C are finitely generated abelian groups. Then $A \oplus A \cong B \oplus B \Rightarrow A \cong B$; $A \oplus C \cong B \oplus C \Rightarrow A \cong B$. (Use the structure theorem.) These are false if A, B, C are not finitely generated. Let $A = \mathbb{Z}^{\aleph_0}$ and $B = \mathbb{Z}$. Then $A \oplus A \cong B \oplus A$ but $A \ncong B$. Corner's theorem (next) shows that there is an abelian group A such that $A \oplus A \oplus A \cong A$ but $A \oplus A \ncong A$. Let $B = A \oplus A$. Then $B \oplus B \cong A \oplus A$ but $B \ncong A$.

Advanced Reading

THEOREM 1.24 (Corner [**4**]). *Let $r \in \mathbb{Z}^+$. There exists a countable reduced torsion-free abelian group G such that for $m, n \in \mathbb{Z}^+$, $G^m \cong G^n \Leftrightarrow m \equiv n \pmod{r}$. (An abelian group is called* reduced *if its only divisible subgroup is $\{0\}$.)*

LEMMA 1.25 (Corner [**3**]). *Let A be a ring such that $(A, +)$ is countable, reduced, and torsion-free. Then $A \cong \operatorname{End}(G)$ for some countable, reduced, torsion-free abelian group G.*

LEMMA 1.26. *Let G be an abelian group and ω_1, ω_2 two idempotents in $\operatorname{End}(G)$. Then $\omega_1 G \cong \omega_2 G \Leftrightarrow$ there exist $x, y \in \operatorname{End}(G)$ such that $\omega_1 = xy$ and $\omega_2 = yx$.*

PROOF. ($\Leftarrow$) Let $y^* : \omega_1 G \to \omega_2 G$, $\omega_1 a \mapsto y\omega_1 a$ and $x^* : \omega_2 G \to \omega_1 G$, $\omega_2 a \mapsto x\omega_2 a$. Then x^* and y^* are inverses of each other.

($\Rightarrow$) Let $\alpha : \omega_1 G \to \omega_2 G$ and $\beta : \omega_2 G \to \omega_1 G$ be inverse isomorphisms. Let $y = \alpha\omega_1$ and $x = \beta\omega_2$. □

PROOF OF THEOREM 1.24. Only have to consider $r > 1$. Let A be the ring freely generated by x_i, y_i, $0 \leq i \leq r$, subject to the relation

$$y_i x_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases} \qquad \sum_{i=0}^{r} x_i y_i = 1.$$

1° $(A, +)$ is free abelian of countable rank.

We have $A \cong B/C$, where B is the ring freely generated by x_i, y_i, $0 \leq i \leq r$, subject to the relations

$$y_i x_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j \end{cases}$$

and C is the ideal of B generated by $1-\sum_{i=0}^{r} x_i y_i$.

We claim that B is free abelian with a basis

$$x_{i_1}\cdots x_{i_m} y_{j_n}\cdots y_{j_1},\quad n,m\ge 0,\ 0\le i_k, j_k\le r. \tag{1.2}$$

Let $\mathcal{A}$ be the set of elements in (1.2), $\mathcal{B}$ the set of products of elements of $\{x_1,\dots,x_r,\ y_1,\dots,y_r\}$ containing at least one string $y_i x_j$ $(i\ne j)$ but no string $y_i x_i$, and $\mathcal{C}$ the set of products of elements in $\{x_1,\dots,x_r,y_1,\dots,y_r\}\cup\{y_i x_i-1: 1\le i\le r\}$ containing at least one $y_i x_i-1$ but no string $y_i x_i$. Then $\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ is a $\mathbb{Z}$-basis of the free ring generated by $\{x_1,\dots,x_r,y_1,\dots,y_r\}$. To see this, it suffices to show that $\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ is linearly independent over $\mathbb{Z}$. Assume

$$\alpha_1 a_1+\cdots+\alpha_s a_s+\beta_1 b_1+\cdots+\beta_t b_t+\gamma_1 c_1+\cdots+\gamma_u c_u=0, \tag{1.3}$$

where $a_i\in\mathcal{A}$, $b_j\in\mathcal{B}$, $c_k\in\mathcal{C}$, $\alpha_i,\beta_j,\gamma_k\in\mathbb{Z}$. Assume that c_1 has the largest number of elements in $\{x_1,\dots,x_r,y_1,\dots,y_r\}$ (counted with multiplicity). In (1.3), expand each c_k as a product of elements in $\{x_1,\dots,x_r,y_1,\dots,y_r\}$. Let c_1' be obtained from c_1 by replacing each $y_i x_i-1$ with $y_i x_i$. Then in the LHS of (1.3), $\gamma_1 c_1'$ is the only term of involving c_1'. Therefore, $\gamma_1=0$. In the same way, $\gamma_1=\cdots=\gamma_u=0$. It follows immediately that $\alpha_1=\cdots=\alpha_s=\beta_1=\cdots=\beta_t=0$.

Since B is the free ring on $\{x_1,\dots,x_r,y_1,\dots,y_r\}$ modulo the ideal generated by $\mathcal{B}\cup\mathcal{C}$, B is free abelian with a basis $\mathcal{A}$.

C is generated by

$$x_{i_1}\cdots x_{i_m}\Bigl(1-\sum_{i=0}^{r} x_i y_i\Bigr) y_{j_n}\cdots y_{j_1},\quad n,m\ge 0,\ 0\le i_k,j_k\le r.$$

It can be seen that $B=C\oplus D$, where

$$D:=\langle x_{i_1}\cdots x_{i_m} y_{j_n}\cdots y_{j_1},\quad n,m\ge 0,\ 0\le i_k,j_k\le r,\ (i_m,j_n)\ne(r,r)\rangle.$$

Thus $B/C\cong D$.

2° By Lemma 1.25, $A=\operatorname{End}(G)$ for some countable, reduced, torsion-free abelian group G. Let $\omega_i=x_i y_i$, $0\le i\le r$. Then $1=\omega_0+\cdots+\omega_r$ is a decomposition of 1 into orthogonal idempotents. So,

$$G=\sum_{i=0}^{r}\omega_i G.$$

Since $\omega_i=x_i y_i$ and $1=y_i x_i$, by Lemma 1.26, $G\cong\omega_i G$. Thus $G\cong G^{r+1}$; hence $G^m\cong G^n$ if $m\equiv n \pmod r$.

3° There exists $\mathbb{Z}$-linear map $T:A\to\mathbb{Z}_r$ such that

(i) $T(xy)=T(yx)$, $x,y\in A$;
(ii) $T(\omega_i)=1$, $0\le i\le r$.

We only have to construct a $\mathbb{Z}$-linear map $T^*:B\to\mathbb{Z}_r$ satisfying the analogies of (i) and (ii) and $T^*|_C=0$. Define

$$T^*(x_{i_1}\cdots x_{i_m} y_{j_n}\cdots y_{j_1})=\begin{cases}1 & \text{if } m=n \text{ and } i_k=j_k,\ 1\le k\le m,\\ 0 & \text{otherwise}\end{cases}$$

and extend T^* to B by linearity.

4° $G^m\not\cong G^n$ if $m\not\equiv n \pmod r$.

Assume $G^m \cong G^n$ for some $1 \le m, n \le r$. Then

$$\Big(\sum_{i=0}^{m-1} \omega_i\Big)G = \sum_{i=0}^{m-1} \omega_i G \cong \sum_{i=0}^{n-1} \omega_i G = \Big(\sum_{i=0}^{n-1} \omega_i\Big)G.$$

By Lemma 1.26, there exist $x, y \in A$ such that $\sum_{i=0}^{m-1} \omega_i = xy$, $\sum_{i=0}^{n-1} \omega_i = yx$. Then in $\mathbb{Z}_r$,

$$m = T\Big(\sum_{i=0}^{m-1} \omega_i\Big) = T(xy) = T(yx) = T\Big(\sum_{i=0}^{n-1} \omega_i\Big) = n.$$

□

End Advanced Reading

1.7. Free Groups

F_X, THE FREE GROUP ON X. Let X be a set and

$$\mathcal{W} = \big\{x_1^{e_1} \cdots x_s^{e_s} : s \ge 0,\ x_i \in X,\ e_i \in \{\pm 1\}\big\}.$$

(Here, $x_1^{e_1} \cdots x_s^{e_s}$ is a formal product and is called a *word* in X.) For $u, v \in \mathcal{W}$, say $u \sim v$ if v can be obtained form u by deleting and inserting strings of the form xx^{-1} or $x^{-1}x$, $x \in X$. $\sim$ is an equivalence relation on $\mathcal{W}$; the equivalence class of $u \in \mathcal{W}$ is denoted by $[u]$. Put $F_X = \mathcal{W}/\sim$ and for $[u], [v] \in \mathcal{W}/\sim$, define $[u][v] = [uv]$, where uv is the concatenation of u and v. This gives a well defined operation on F_X; F_X with this operation is a group, called the *free group* on X; $\operatorname{rank} F_X := |X|$.

Let G be any group and $f : X \to G$. Then there is a unique homomorphism $\bar{f} : F_X \to G$ such that

$$\begin{tikzcd} F \arrow[dr, "\bar{f}"] & \\ X \arrow[u, "\iota"] \arrow[r, "f"'] & G \end{tikzcd}$$

commutes, where $\iota(x) = [x]$, $x \in X$.

Every group is a homomorphic image of a free group.

A word $w \in \mathcal{W}$ is called reduced if it contains no strings xx^{-1} or $x^{-1}x$, $x \in X$.

FACT. Every class in $\mathcal{W}/\sim$ contains a unique reduced word.

PROOF. (Uniqueness) Let $\mathcal{R}$ be the set of all reduced words in $\mathcal{W}$. Define

$$\begin{array}{rccc} f: & X & \longrightarrow & S_{\mathcal{R}} \\ & x & \longmapsto & f(x) \end{array}$$

where

$$\begin{array}{rccl} f(x): & \mathcal{R} & \longrightarrow & \mathcal{R} \\ & x_1^{e_1} \cdots x_s^{e_s} & \longmapsto & \begin{cases} x x_1^{e_1} \cdots x_s^{e_s} & \text{if } x_1^{e_1} \ne x^{-1}, \\ x_2^{e_2} \cdots x_s^{e_s} & \text{if } x_1^{e_1} = x^{-1}. \end{cases} \end{array}$$

Note that for $x \in X$, we have

$$\begin{array}{cccl} f(x)^{-1}: & \mathcal{R} & \longrightarrow & \mathcal{R} \\ & x_1^{e_1}\cdots x_s^{e_s} & \longmapsto & \begin{cases} x^{-1}x_1^{e_1}\cdots x_s^{e_s} & \text{if } x_1^{e_1} \neq x, \\ x_2^{e_2}\cdots x_s^{e_s} & \text{if } x_1^{e_1} = x. \end{cases} \end{array}$$

There exists homomorphism $\bar{f} : F_X \to S_{\mathcal{R}}$ such that $\bar{f}([x]) = f(x)$ for all $x \in X$. Assume $x_1^{e_1}\cdots x_s^{e_s}, y_1^{f_1}\cdots y_t^{f_t} \in \mathcal{R}$ such that $[x_1^{e_1}\cdots x_s^{e_s}] = [y_1^{f_1}\cdots y_t^{f_t}]$. Then $x_1^{e_1}\cdots x_s^{e_s} = \big(f(x_1)^{e_1}\cdots f(x_s)^{e_s}\big)(1) = \bar{f}([x_1^{e_1}\cdots x_s^{e_s}])(1) = \bar{f}([y_1^{f_1}\cdots y_t^{f_t}])(1) = \big(f(y_1)^{f_1}\cdots f(y_t)^{f_t}\big)(1) = y_1^{f_1}\cdots y_t^{f_t}$. □

So, $\iota : X \to F_X$ is an injection and X can be regarded as a subset of F_X.

Presentation. Let X be a set and R a set of words in X. Define

$$\langle X \mid R\rangle = F_X/N,$$

where N is the *normal closure* of $\{[r] : r \in R\}$ in F_X, i.e., the smallest subgroup of F_X containing $\{[r] : r \in R\}$. If $G \cong \langle X \mid R\rangle$, $\langle X \mid R\rangle$ is called a *presentation* of G; elements in X are called *generators*; elements in R are called *relations*.

Theorem 1.27 (Van Dyck). *Let G be a group generated by $X \subset G$. Let R be a set of words in X such that for every $r \in R$, $r = 1$ in G, i.e., the relation $r = 1$ is satisfied in G. Then $\exists!$ onto homomorphism $\langle X \mid R\rangle \to G$ such that $[x] \mapsto x$ for all $x \in X$.*

Proof. Let N be the normal closure of $\{[r] : r \in R\}$ in F_X. The map $f : X \to G$, $x \mapsto x$, induces a homomorphism $\bar{f} : F_X \to G$ such that $[x] \mapsto x$. Since $G = \langle X\rangle$, $\bar{f}$ is onto. By assumption, $\{[r] : r \in R\} \subset \ker \bar{f}$. So $N \subset \ker \bar{f}$. Thus, $\bar{f}$ induces an onto homomorphism from $F_X/N = \langle X \mid R\rangle$ to G.

The uniqueness is obvious since $\langle X \mid R\rangle$ is generated by $\{[x]N : x \in X\}$. □

Abuse of notation. In a presentation $\langle X \mid R\rangle = F_X/N$, an element $[u]N$, where u is word in X, is usually denoted by u.

Examples.

- $D_n = \langle \alpha, \beta \mid \alpha^n = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{-1}\rangle$.
- The *infinite dihedral group*
$$D_\infty = \langle \alpha, \beta \mid \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{-1}\rangle.$$
- The quaternion group
$$Q_8 = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ yxy^{-1} = x^{-1}\rangle.$$

Proof. $Q_8 = \langle i, j\rangle$, where i, j satisfies relations $i^4 = 1$, $j^2 = i^2$, $jij^{-1} = i^{-1}$. By Van Dyck's theorem, $\exists$ onto homomorphism

$$G := \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ yxy^{-1} = x^{-1}\rangle \longrightarrow Q_8 \tag{1.4}$$

such that $x \mapsto i$, $y \mapsto j$. Every element in G can be written as x^iy^j, $0 \le i \le 3$, $0 \le j \le 1$. So, $|G| \le 8$. Hence the homomorphism in (1.4) is an isomorphiam. □

- The *generalized quaternion group*
$$Q_{4n} = \langle x, y \mid x^{2n} = 1,\ y^2 = x^n,\ yxy^{-1} = x^{-1} \rangle.$$
Let $\xi = e^{2\pi i/2n}$, $A = \begin{bmatrix} \xi & \\ & \xi^{-1} \end{bmatrix}$, $B = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$. Then $\exists$ an isomorphism $Q_{4n} \xrightarrow{\cong} \langle A, B \rangle \subset \mathrm{GL}(2, \mathbb{C})$ such that $x \mapsto A$, $y \mapsto B$. $|Q_{4n}| = 4n$.

The braid group on n strings.

$B_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ 1 \le i \le n-2;\ \sigma_i\sigma_j = \sigma_j\sigma_i,\ |i-j| > 1 \rangle$.

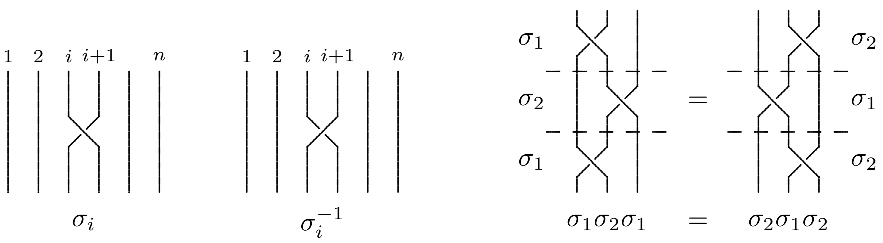


Figure 1.3. The braid group

Fact. Let $X = A \mathbin{\dot\cup} B$, H the subgroup of F_X generated by A and N the normal closure of B in F_X. Then $F_X = HN$ and $H \cap N = \{1\}$. In particular, $F/N \cong H$ is free on A.

Proof. Only have to show $H \cap N = \{1\}$. Define
$$\begin{array}{rccl} \phi: & X & \longrightarrow & F_A \\ & x & \longmapsto & \begin{cases} x & \text{if } x \in A, \\ 1 & \text{if } x \in B. \end{cases} \end{array}$$
ϕ induces a homomorphism $\bar\phi : F_X \to F_A$ such that $N \subset \ker\bar\phi$ and $\bar\phi|_H : H \to F_A$ is an isomorphism. If $w \in H \cap N$, then $\bar\phi|_H(w) = \bar\phi(w) = 1$, hence $w = 1$. □

Fact. $F_{X_1} \cong F_{X_2} \Leftrightarrow |X_1| = |X_2|$.

Proof. ($\Rightarrow$) $F_{X_i}/(F_{X_i})'$ is free abelian of rank $|X_i|$. □

Theorem 1.28 (The Nielson-Schreier theorem). *Let F be a free group on X and $G < F$. Then G is a free group. If $[F : G] = m < \infty$, then* $\operatorname{rank} G = m|X| + 1 - m$. *($|X|$ may be infinite.)*

Advanced Reading

Proof. (Based on Weir [**23**]; see Rotman [**19**] and Robinson [**18**] for more details.)

1° Let τ be a (right) transversal (function) of G in F, i.e., τ is a function from $G\backslash\backslash F$ to F such that $\pi \circ \tau = \mathrm{id}_{G\backslash\backslash F}$, where $\pi : F \to G\backslash\backslash F$ is the canonical map. Always assume that $\tau(G) = 1$. Define
$$\begin{array}{rccl} \alpha: & F \times (G\backslash\backslash F) & \longrightarrow & G \\ & (u, C) & \longmapsto & \tau(C)u\tau(Cu)^{-1}. \end{array}$$

Let $\tilde{F}$ be the free group on $X \times (G\backslash\backslash F)$. $\phi := \alpha|_{X\times(G\backslash\backslash F)}$ induces a homomorphism $\bar{\phi} : \tilde{F} \to G$.

2° We construct a map $\psi : F \times (G\backslash\backslash F) \to \tilde{F}$ such that the following diagram commutes.

$$\begin{tikzcd}
\tilde{F} \arrow[drr, "\bar{\phi}"] & & \\
& F \times (G\backslash\backslash F) \arrow[ul, "\psi"'] \arrow[r, "\alpha"] & G \\
X \times (G\backslash\backslash F) \arrow[uu] \arrow[ur] \arrow[urr, "\phi=\alpha|_{X\times(G\backslash\backslash F)}"'] & &
\end{tikzcd}$$

Define

$$\begin{array}{rccc} \psi : & F \times (G\backslash\backslash F) & \longrightarrow & \tilde{F} \\ & (u, C) & \longmapsto & u^C \end{array}$$

where u^C is defined inductively on the length of u:

$$u^C = \begin{cases} 1 & \text{if } u = 1, \\ (x, C) & \text{if } u = x \in X, \\ (x, Cx^{-1})^{-1} & \text{if } u = x^{-1}, x \in X, \\ v^C y^{Cv} & \text{if } u = vy \text{ is reduced and } y \in X \cup X^{-1}. \end{cases}$$

Then for all $u, v \in F$ and $C \in G\backslash\backslash F$, $(uv)^C = u^C v^{Cu}$, $(u^{-1})^C = (u^{Cu^{-1}})^{-1}$ and

$$\bar{\phi}(u^C) = \tau(C)\, u\, \tau(Cu)^{-1}.$$

3° Let

$$\begin{array}{rccc} \beta : & G & \longrightarrow & \tilde{F} \\ & u & \longmapsto & u^G \end{array}$$

β is a homomorphism and $\bar{\phi} \circ \beta = \mathrm{id}_G$. So, $\bar{\phi}$ is onto, β is 1-1, and

$$G \cong \tilde{F} / \ker \bar{\phi}.$$

4° Let N be the normal closure of $\{\tau(C)^G : C \in G\backslash\backslash F\}$ in $\tilde{F}$. We claim that $\ker \bar{\phi} = N$.

$\bar{\phi}(\tau(C)^G) = \tau(G)\tau(C)\tau(C)^{-1} = 1$. So, $N \subset \ker \bar{\phi}$. To show that $\ker \bar{\phi} \subset N$, note that $\ker \bar{\phi} = \ker \gamma$, where $\gamma = \beta \circ \bar{\phi}$. It suffices to show that $\gamma(x^C) \equiv x^C \pmod{N}$ for $(x, C) \in X \times (G\backslash\backslash F)$. We have $\gamma(x^C) = \big[\tau(C)\, x\, \tau(Cx)^{-1}\big]^G = \tau(C)^G x^C \big(\tau(Cx)^{-1}\big)^{G\tau(C)x} = \tau(C)^G x^C \big(\tau(Cx)^G\big)^{-1} \equiv x^C \pmod{N}$.

5° There exists a (right) transversal τ of G in F ($\tau(G) = 1$) such that if a reduced word $uy \in \mathrm{im}(\tau)$, $y \in X \cup X^{-1}$, then $u \in \mathrm{im}(\tau)$. $\mathrm{im}(\tau)$ is said to have the Schreier property and τ is called a Schreier transversal. (For each $C \in G\backslash\backslash F$, the length of C, denoted by $|C|$, is defined to be the minimum length of words in C. Define $\tau(C)$ inductively on $|C|$. $\tau(G) = 1$. Assume that $\tau(D)$ have been defined for all $D \in G\backslash\backslash F$ with $|D| < |C|$. Let $uy \in C$ ($y \in X \cup X^{-1}$) be of minimum length. Define $\tau(C) = \tau(Gu)y$.)

6° Let τ be a Schreier transversal of G in F. For each $G \neq C \in G\backslash\backslash F$, $\tau(C) = ux^e$ (reduced), $x \in X$, $e \in \{\pm 1\}$. So, $\tau(C)^G = u^G (x^e)^{Gu}$, where

$$(x^e)^{Gu} = \left\{ \begin{array}{ll} x^{Gu} & \text{if } e = 1 \\ (x^{Gux^{-1}})^{-1} & \text{if } e = -1 \end{array} \right\} = (x^D)^e \quad \text{for some } D \in G\backslash\backslash F.$$

Since $\text{im}(\tau)$ has the Schreier property, $u \in \text{im}(\tau)$, so $u^G \in N$, hence $x^D \in N$. Applying the same argument to u and use induction on the length of u, we see that $\tau(C)^G$ is a product of certain elements in N of the form x^D ($x \in X$, $D \in G\backslash\backslash F$) and their inverses. So N is the normal closure of $N \cap \big(X \times (G\backslash\backslash F)\big)$. Then

$$\begin{aligned} G &\cong \tilde{F}/N \qquad \text{(by 3°, 4°)} \\ &\cong \text{the free group on } X \times (G\backslash\backslash F)\big) \setminus N. \end{aligned}$$

7° Assume $[F : G] = m < \infty$. To show that $\operatorname{rank} G = m|X| + 1 - m$, it suffices to show that

$$\big|N \cap \big(X \times (G\backslash\backslash F)\big)\big| = m - 1.$$

Note that for $x^C \in X \times (G\backslash\backslash F)$, $x \in N$ ($= \ker \bar{\phi}$) $\Leftrightarrow \tau(C)\, x\, \tau(Cx)^{-1} = 1$. Define

$$\begin{array}{rccc} \theta : & (G\backslash\backslash F) \setminus \{G\} & \longrightarrow & N \cap \big(X \times (G\backslash\backslash F)\big) \\ & C & \longmapsto & \theta(C) \end{array}$$

where

$$\theta(C) = \begin{cases} x^{Gu} & \text{if } \tau(C) = ux \text{ (reduced) } x \in X, \\ x^C & \text{if } \tau(C) = ux^{-1} \text{ (reduced) } x \in X. \end{cases}$$

By the argument in 6°, $\theta(C) \in N$. θ is 1-1. (Assume $\theta(C_1) = \theta(C_2)$. If $\tau(C_1) = u_1 x_1$ and $\tau(C_2) = u_2 x_2^{-1}$, where $x_1, x_2 \in X$ and $u_1 x_1$ and $u_2 x_2^{-1}$ are reduced, then $(x_1, Gu_1) = \theta(C_1) = \theta(C_2) = (x_2, Gu_2 x_2^{-1})$. So $x_1 = x_2$ and $u_1 = u_2 x_2^{-1}$. But then $u_1 x_1$ is not reduced, $\rightarrow\leftarrow$. So we may assume $\tau(C_1) = u_1 x_1$, $\tau(C_2) = u_2 x_2$ or $\tau(C_1) = u_1 x_1^{-1}$, $\tau(C_2) = u_2 x_2^{-1}$. Then it follows that $C_1 = C_2$.) Given $x^C \in N$ ($x \in X$),

$$x^C = \begin{cases} \theta(C) & \text{if } \tau(C) \text{ (reduced) ends with } x^{-1}, \\ \theta(Cx) & \text{otherwise.} \end{cases}$$

So θ is also onto. □

End Advanced Reading

1.8. Nonabelian Groups of Order ≤ 30

Order pq, $p \mid q - 1$. Orders 6, 10, 14, 21, 22, 26 are covered by Proposition 1.22.

Order 8. $G \cong Q_8$ or D_4.

Proof. G has no element of order 8. G has an element of order 4. (Otherwise, $x^2 = e\ \forall x \in G$. Then G is abelian.) Let $a \in G$ such that $o(a) = 4$. Choose $b \in G \setminus \langle a \rangle$. Then $G = \langle a, b \rangle$. Since $|G/\langle a \rangle| = 2$, $b^2 \in \langle a \rangle$; hence $b^2 = a^2$ or e since $o(b^2) = 1$ or 2. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$; hence $bab^{-1} = a^{-1}$.

Case 1. $b^2 = a^2$. Then $G \cong Q_8$.

Case 2. $b^2 = e$. Then $G \cong D_4$. □

Table 1.2. Nonabelain groups of order ≤ 30

$\lvert G\rvert$	G	#
6	S_3	1
8	$D_4,\ Q_8$	2
10	D_5	1
12	$A_4,\ D_6,\ \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$	3
14	D_7	1
16	$D_8,\ Q_{16},\ D_4 \times \mathbb{Z}_2,\ Q_8 \times \mathbb{Z}_2,\ \mathbb{Z}_8 \rtimes_{\beta_1} \mathbb{Z}_2,\ \mathbb{Z}_8 \rtimes_{\beta_2} \mathbb{Z}_2,$ $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\beta_3} \mathbb{Z}_2,\ (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\beta_4} \mathbb{Z}_2,\ \mathbb{Z}_4 \rtimes_{\beta_5} \mathbb{Z}_4$	9
18	$D_9,\ S_3 \times \mathbb{Z}_3,\ (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	3
20	$D_{10},\ \mathbb{Z}_5 \rtimes_{\gamma_1} \mathbb{Z}_4,\ \mathbb{Z}_5 \rtimes_{\gamma_2} \mathbb{Z}_4$	3
21	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	1
22	D_{11}	1
24	$D_4 \times \mathbb{Z}_3,\ Q_8 \times \mathbb{Z}_3,\ \mathbb{Z}_3 \rtimes_{\delta_1} \mathbb{Z}_8,\ \mathbb{Z}_3 \rtimes_{\delta_2} (\mathbb{Z}_4 \times \mathbb{Z}_2),$ $\mathbb{Z}_3 \rtimes_{\delta_3} (\mathbb{Z}_4 \times \mathbb{Z}_2),\ \mathbb{Z}_2 \times D_6,\ \mathbb{Z}_3 \rtimes_{\delta_4} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2),$ $Q_8 \rtimes_{\delta_5} \mathbb{Z}_3,\ \mathbb{Z}_3 \rtimes_{\delta_6} Q_8,\ \mathbb{Z}_3 \rtimes_{\delta_7} D_4,\ \mathbb{Z}_3 \rtimes_{\delta_8} D_4,\ S_4$	12
26	D_{13}	1
27	$\mathbb{Z}_9 \rtimes \mathbb{Z}_3,\ (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$	3
28	$D_{14},\ \mathbb{Z}_7 \rtimes \mathbb{Z}_4$	2
30	$D_{15},\ D_5 \times \mathbb{Z}_3,\ S_3 \times \mathbb{Z}_5$	3

Order 12. $G \cong A_4$ or D_6 or $\mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$, where $\alpha : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\alpha(1)](1) = -1$.

Proof. Let P be a Sylow 3-subgroup of G and Q a Sylow 2-subgroup of G. G acts on G/P by left multiplication which gives a homomorphism $f : G \to S_{G/P}$ with $\ker f \subset P$. If $\ker f = \{e\}$, then $G \hookrightarrow S_4$, so $G \cong A_4$. If $\ker f = P$, then $P \lhd G$ hence $G = P \rtimes Q$. In this case it is easy to show that $G \cong D_6$ if $Q \cong \mathbb{Z}_2 \times Z_2$ and $G \cong \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$ if $Q \cong \mathbb{Z}_4$. □

We have

$$\langle x, y \mid x^3 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle \xrightarrow{\cong} \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4 \qquad (x \mapsto (1,0),\ y \mapsto (0,1)).$$

Let $a = ((1,2,3),2)$, $b = ((1,2),1) \in S_3 \times \mathbb{Z}_4$ and $T = \langle a, b \rangle < S_3 \times \mathbb{Z}_4$. Then $|T| = 12$ and

$$T = \langle a, b \mid a^6 = 1,\ a^3 = b^2,\ bab^{-1} = a^{-1} \rangle.$$

Also

$$\langle x, y \mid x^3 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle \xrightarrow{\cong} T \qquad (x \mapsto a^2,\ y \mapsto b).$$

Order 16. Table 1.3. (Cf. [**2**, §118].)

Order 20. $G \cong D_{10}$ or $\mathbb{Z}_5 \rtimes_{\gamma_1} \mathbb{Z}_4$ or $\mathbb{Z}_5 \rtimes_{\gamma_2} \mathbb{Z}_4$, where $\gamma_1, \gamma_2 : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_5)$, $[\gamma_1(1)](1) = 2$, $[\gamma_2(1)](1) = -1$.

Table 1.3. Nonabelian groups of order 16

group	presentation
D_8	$\langle x, y \mid x^8 = y^2 = 1,\ yxy^{-1} = x^{-1}\rangle$
Q_{16}	$\langle x, y \mid x^8 = 1,\ y^2 = x^4,\ yxy^{-1} = x^{-1}\rangle$
$D_4 \times \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ y^{-1}xy = x^{-1},$ $xz = zx,\ yz = zy\rangle$
$Q_8 \times \mathbb{Z}_2$	$\langle x, y, z \mid x^4 = z^2 = 1,\ y^2 = x^2,$ $y^{-1}xy = x^{-1},\ xz = zx,\ yz = zy\rangle$
$\mathbb{Z}_8 \rtimes_{\beta_1} \mathbb{Z}_2,$ $\beta_1 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_8),\ [\beta_1(1)](1) = 5.$	$\langle x, y \mid x^8 = y^2 = 1,\ y^{-1}xy = x^5\rangle$
$\mathbb{Z}_8 \rtimes_{\beta_2} \mathbb{Z}_2$ $\beta_1 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_8),\ [\beta_1(1)](1) = -1.$	$\langle x, y \mid x^8 = y^2 = 1,\ y^{-1}xy = x^{-1}\rangle$
$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\beta_3} \mathbb{Z}_2,$ $\beta_3 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2),$ $\beta_3(1) : \begin{cases} (1,0) \mapsto (1,0), \\ (0,1) \mapsto (2,1). \end{cases}$	$\langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ xy = yx,$ $z^{-1}xz = x,\ z^{-1}yz = x^2y\rangle$
$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\beta_4} \mathbb{Z}_2,$ $\beta_4 : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2),$ $\beta_4(1) : \begin{cases} (1,0) \mapsto (1,1), \\ (0,1) \mapsto (0,1). \end{cases}$	$\langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ xy = yx,$ $z^{-1}xz = xy,\ z^{-1}yz = y\rangle$
$\mathbb{Z}_4 \rtimes_{\beta_5} \mathbb{Z}_4$ $\beta_5 : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_4),\ [\beta_1(1)](1) = -1.$	$\langle x, y \mid x^4 = y^4 = 1,\ y^{-1}xy = x^{-1}\rangle$

Proof. Let $\langle a\rangle \lhd G$ be the Sylow 5-subgroup and P a Sylow 2-subgroup. If $P = \langle b\rangle\langle c\rangle$, where $o(b) = o(c) = 2$, we may assume $bab^{-1} = a$. (If $bab^{-1} = a^{-1}$ and $cac^{-1} = a^{-1}$, then $(bc)a(bc)^{-1} = a$.) Then $G = \langle ab\rangle\langle c\rangle$, where $\mathbb{Z}_{10} \cong \langle ab\rangle \lhd G$. Thus $G \cong \mathbb{Z}_{10} \rtimes \mathbb{Z}_2 \cong D_{10}$. If $P = \langle b\rangle \cong \mathbb{Z}_4$, then $G \cong \mathbb{Z}_5 \rtimes_\gamma \mathbb{Z}_4$, where $\gamma : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_5)$ is a homomorphism such that $[\gamma(1)](1) \neq 1$. If $[\gamma(1)](1) = 2$ or 3, $G \cong \mathbb{Z}_5 \rtimes_{\gamma_1} \mathbb{Z}_4$. If $[\gamma(1)](1) = -1$, $G \cong \mathbb{Z}_5 \rtimes_{\gamma_2} \mathbb{Z}_4$.

$\mathbb{Z}_5 \rtimes_{\gamma_1} \mathbb{Z}_4 \not\cong \mathbb{Z}_5 \rtimes_{\gamma_2} \mathbb{Z}_4$ since $Z(\mathbb{Z}_5 \rtimes_{\gamma_1} \mathbb{Z}_4) = \{(0,0)\}$ but $Z(\mathbb{Z}_5 \rtimes_{\gamma_2} \mathbb{Z}_4) = \langle(0,2)\rangle$ □

Order 24. Table 1.4. (Cf. [**2**, §126].)

Order 27. $\mathbb{Z}_9 \rtimes_{\epsilon_1} \mathbb{Z}_3$, $\epsilon_1 : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_9)$, $[\epsilon_1(1)](1) = 4$; $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\epsilon_2} \mathbb{Z}_3$,

$$\epsilon_2 : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3), \quad \epsilon_2(1) : \begin{cases} (1,0) \mapsto (1,0), \\ (0,1) \mapsto (1,1). \end{cases}$$

Order 28. $G \cong D_{14}$ or $\mathbb{Z}_7 \rtimes \mathbb{Z}_4$.

Table 1.4. Nonabelian groups of order 24

group	presentation
$D_4 \times \mathbb{Z}_3$	
$Q_8 \times \mathbb{Z}_3$	
$\mathbb{Z}_3 \rtimes_{\delta_1} \mathbb{Z}_8$, $\delta_1 : \mathbb{Z}_8 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_1(1)](1) = -1$	$\langle a, b \mid a^8 = b^3 = 1,\ a^{-1}ba = b^{-1} \rangle$
$\mathbb{Z}_3 \rtimes_{\delta_2} (\mathbb{Z}_4 \times \mathbb{Z}_2)$, $\delta_2 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_2(1,0)](1) = 1$, $[\delta_2(0,1)](1) = -1$	$\langle a, b, c \mid a^3 = b^4 = c^2 = 1,\ bc = cb,$ $b^{-1}ab = a,\ cac = a^{-1} \rangle$
$\mathbb{Z}_3 \rtimes_{\delta_3} (\mathbb{Z}_4 \times \mathbb{Z}_2)$, $\delta_3 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_3(1,0)](1) = -1$, $[\delta_3(0,1)](1) = 1$	$\langle a, b, c \mid a^3 = b^4 = c^2 = 1,\ bc = cb,$ $b^{-1}ab = a^{-1},\ cac = a \rangle$
$\mathbb{Z}_2 \times D_6$	
$\mathbb{Z}_3 \rtimes_{\delta_4} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ $\delta_4 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_4(1,0,0)](1) = -1$, $[\delta_4(0,1,0)](1) = 1$, $[\delta_4(0,0,1)](1) = 1$	$\langle a, b, c, d \mid a^3 = b^2 = c^2 = d^2 = 1,$ $bc = cb,\ cd = dc,\ db = bd,$ $bab = a^{-1},\ cac = a,\ dad = a \rangle$
$Q_8 \rtimes_{\delta_5} \mathbb{Z}_3$, $\delta_5 : \mathbb{Z}_3 \to \mathrm{Aut}(Q_8)$, $\delta_5(1) : \begin{cases} i \mapsto j \\ j \mapsto k \end{cases}$	$\langle a, b, c \mid a^4 = c^3 = 1,\ a^2 = b^2,$ $b^{-1}ab = a^{-1},\ c^{-1}ac = b,\ c^{-1}bc = ab \rangle$
$\mathbb{Z}_3 \rtimes_{\delta_6} Q_8$, $\delta_6 : Q_8 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_6(i)](1) = 1$, $[\delta_6(j)](1) = -1$	$\langle a, b, c \mid a^3 = b^4 = 1,\ b^2 = c^2,$ $c^{-1}bc = b^{-1},\ b^{-1}ab = a,\ c^{-1}ac = a^{-1} \rangle$
$\mathbb{Z}_3 \rtimes_{\delta_7} D_4$, $\delta_7 : D_4 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_7(\alpha)](1) = 1$, $[\delta_7(\beta)](1) = -1$	$\langle a, b, c \mid a^3 = b^4 = c^2 = 1,\ cbc = b^{-1},$ $b^{-1}ab = a,\ cac = a^{-1} \rangle$
$\mathbb{Z}_3 \rtimes_{\delta_8} D_4$, $\delta_8 : D_4 \to \mathrm{Aut}(\mathbb{Z}_3)$, $[\delta_8(\alpha)](1) = -1$, $[\delta_8(\beta)](1) = 1$	$\langle a, b, c \mid a^3 = b^4 = c^2 = 1,\ cbc = b^{-1},$ $b^{-1}ab = a^{-1},\ cac = a \rangle$
S_4	$\langle a, b \mid a^4 = b^3 = (ab)^2 = 1 \rangle$

Proof. Let P be the Sylow 7-subgroup of G and Q a Sylow 2-subgroup of G. Then $P \cong \mathbb{Z}_7$ and $G \cong P \rtimes Q$. If $Q \cong \mathbb{Z}_4$, $G \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_4$. If $Q \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $G \cong D_{14}$. □

Order 30. $G \cong D_{15}$ or $D_5 \times \mathbb{Z}_3$ or $S_3 \times \mathbb{Z}_5$.

Proof. Let P be the Sylow 5-subgroup of G and Q a Sylow 3-subgroup of G. Since $P \lhd G$, $PQ < G$ and $PQ \cong \mathbb{Z}_5 \times \mathbb{Z}_3$. So, $G \cong (\mathbb{Z}_5 \times \mathbb{Z}_3) \rtimes_\theta \mathbb{Z}_2$, where

$\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_3)$,

$$\theta(1) : \quad \begin{cases} (1,0) \mapsto (-1,0), \\ (0,1) \mapsto (0,1), \end{cases} \quad \text{or} \quad \begin{cases} (1,0) \mapsto (1,0), \\ (0,1) \mapsto (0,-1), \end{cases} \quad \text{or} \quad \begin{cases} (1,0) \mapsto (-1,0), \\ (0,1) \mapsto (0,1). \end{cases}$$

In the three cases, $G \cong D_5 \times \mathbb{Z}_3$, $S_3 \times \mathbb{Z}_5$ and D_{15} respectively. □

Advanced Reading

1.9. Group Extensions

If $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ is an exact sequence of groups, G is called an *extension* of K by Q. If there is a homomorphism $j : Q \to G$ such that $p \circ j = \mathrm{id}_Q$, the exact sequence (or the extension) is called *split*. Given K, G, Q there exists split sequence $1 \to K \xrightarrow{i} G \underset{j}{\overset{p}{\rightleftarrows}} Q \to 1$ iff $G \cong K \rtimes Q$.

Q-MODULES INDUCED BY EXTENSIONS. Let $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ be an extension, where K is *abelian* and G is written additively. There exists a homomorphism $\phi : Q \to \mathrm{Aut}(K)$. Let $j : Q \to G$ be any lifting. Then for $x \in Q$,

$$\begin{array}{rccc} \phi(x) : & K & \longrightarrow & K \\ & a & \longmapsto & i^{-1}\big(j(x) + i(a) - j(x)\big). \end{array}$$

ϕ is independent of j. ϕ defines an action of Q on K; hence K is a (left) Q-module. To recap, an extension $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ with abelian K induces a Q-module K.

Given a Q-module K, an extension $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ is said to realize the Q-module K if the Q-module K coincides with the one induced by the extension.

Let K be a Q-module and $f : Q \times Q \to K$ a function. Define a binary operation $+$ on $K \times Q$:

$$(a, x) + (b, y) = \big(a + xb + f(x, y), xy\big).$$

The $(K \times Q, +)$ is a group $\Leftrightarrow$

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0 \quad \forall x, y, z \in Q. \tag{1.5}$$

f is called a 2-cocycle if (1.5) holds. $(K \times Q, +)$ is denoted by $G(K, Q, f)$ if f is a 2-cocycle.

NOTE.

(i) (1.5) $\Leftrightarrow$ the associativity of $+$.

(ii) (1.5) implies that $f(1, y) = f(1, 1)$, $f(x, 1) = xf(1, 1)$ $\forall x, y \in Q$. (1.5) also implies the existence of identity and the inverse in $G(K, Q, f)$. ($0_{G(K,Q,f)} = (-f(1, 1), 1)$, $-(a, x) = (-x^{-1}a - f(1, 1) - f(x^{-1}, x),\ x^{-1})$.)

(iii) If f is a 2-cocycle, then there exists an exact sequence

$$0 \longrightarrow K \xrightarrow{\ i\ } G(K, Q, f) \xrightarrow{\ p\ } Q \longrightarrow 1 \tag{1.6}$$

where

$$\begin{array}{rccc} i : & K & \longrightarrow & G(K, Q, f) \\ & a & \longmapsto & (a - f(1, 1),\ 1), \end{array} \tag{1.7}$$

$$\begin{array}{rccc} p : & G(K, Q, f) & \longrightarrow & Q \\ & (a, x) & \longmapsto & x. \end{array} \tag{1.8}$$

Moreover, extension (1.6) realizes the Q-module K.

Let $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ be an extension making K a Q-module. Let $j : Q \to G$ be a lifting. Then

$$j^*(x,y) := i^{-1}\big(j(x) + j(y) - j(xy)\big) \tag{1.9}$$

is a 2-cocycle. Moreover,

$$\begin{array}{rccc} \phi: & G(K,Q,j^*) & \longrightarrow & G \\ & (a,x) & \longmapsto & i(a)+j(x) \end{array}$$

is an isomorphism and the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "i'"] \arrow[d, "\mathrm{id}"] & G(K,Q,j^*) \arrow[r, "p'"] \arrow[d, "\phi"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\ 0 \arrow[r] & K \arrow[r, "i"] & G \arrow[r, "p"] & Q \arrow[r] & 1 \end{tikzcd}$$

commutes, where i' and p' are defined by (1.7) and (1.8). If $j' : Q \to G$ is another lifting. Then $j'(x) - j(x) = h(x)$ for some function $h : Q \to K$. Moreover,

$$j'^*(x,y) - j^*(x,y) = xh(y) - h(xy) + h(x).$$

The second cohomology group. Let K be a Q-module. $Z^2(Q,K) :=$ the abelian group of all 2-cocycles $f : Q \times Q \to K$. A function $f : Q \times Q \to K$ is called a 2-coboundary if $f(x,y) = xh(y) - h(xy) + h(x)$ for some $h : Q \to K$. $B^2(Q,K) :=$ the set of all 2-*coboundaries*. Then $B^2(Q,K) < Z^2(Q,K)$. $H^2(Q,K) := Z^2(Q,K)/B^2(Q,K)$ is the 2nd *cohomology group* of Q with coefficients in K.

Equivalence of extensions. Let K be a Q-module and let

$$0 \longrightarrow K \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1 \tag{1.10}$$

$$0 \longrightarrow K \xrightarrow{i'} G' \xrightarrow{p'} Q \longrightarrow 1 \tag{1.11}$$

be two extensions realizing the Q-module K. The two extensions are called equivalent if there exists an isomorphism $\phi : G \to G'$ such that the following diagram commutes.

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "i"] \arrow[d, "\mathrm{id}"] & G \arrow[r, "p"] \arrow[d, "\phi"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\ 0 \arrow[r] & K \arrow[r, "i'"] & G' \arrow[r, "p'"] & Q \arrow[r] & 1 \end{tikzcd}$$

Theorem 1.29 (The meaning of $H^2(Q,K)$). *Let K be a Q-module. Let $\mathcal{E}(Q,K)$ be the family of all equivalence classes of extensions of K by Q realizing the Q-module K. There is a bijection $\alpha : H^2(Q,K) \to \mathcal{E}(Q,K)$; $\alpha(0) =$ the class of split extensions.*

Proof. $\alpha : f + B^2(Q,K) \mapsto [G(K,Q,f)]$, $f \in Z^2(Q,K)$; $\alpha^{-1} : [G] \mapsto j^* + B^2(Q,K)$, where $j : Q \to G$ is a lifting and $j^* \in Z^2(Q,K)$ is given by (1.9). □

Corollary 1.30. *Let K be a Q-module. If $H^2(Q,K) = 0$, then every extension of K by Q realizing the Q-module K is a semidirect product $K \rtimes Q$.*

Proposition 1.31. *Let K be a Q-module where $|K| = m$, $|Q| = n$ and $(m,n) = 1$. Then $H^2(Q,K) = 0$.*

Proof. Let $f \in Z^2(Q, K)$. Then

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0 \quad \forall x, y, z \in Q.$$

Sum over $z \in Q \Rightarrow$

$$xh(y) - h(xy) + h(x) = nf(x,y),$$

where $h(x) = \sum_{z \in Q} f(x,z)$. So, $nf \in B^2(Q, K)$. Since $(m,n) = 1$, $f \in B^2(Q, K)$. □

Complement. Two subgroups H, K of G are called *complements* of each other if $G = HK$ and $H \cap K = \{0\}$.

Corollary 1.32. *If $|G| = mn$, $(m,n) = 1$ and G has an abelian normal subgroup K of order m. Then K has a complement.*

Theorem 1.33 (The Schur-Zassenhaus theorem). *If $|G| = mn$, $(m,n) = 1$ and G has a normal subgroup K of order m, then K has a complement.*

Proof. Induction on m. If K has a nontrivial subgroup N such that $N \lhd G$, K/N has a complement H/N in G/N. Since $N \lhd H$, $|H| = |N|n$, $(|N|, n) = 1$ and $|N| < m$, H has a subgroup of order n.

So, we may assume that K is a minimal normal subgroup of G. Let $P \neq 1$ be a Sylow subgroup of K. Since $G = K\,N_G(P)$ (Frattini argument), $G/K = K\,N_G(P)/K \cong N_G(P)/K \cap N_G(P) = N_G(P)/N_K(P)$. If $N_G(P) \neq G$, then $|N_K(P)| < |K| = m$. The induction hypothesis applied to $N_K(P) \lhd N_G(P)$ implies that $N_G(P)$ has a subgroup of order n.

So, assume $N_G(P) = G$, i.e. $P \lhd G$. Then $1 \neq Z(P) \lhd G$. Since $Z(P) \subset K$, the minimality of $K \Rightarrow K = Z(P)$, which is abelian. Corollary 1.32 applies. □

End Advanced Reading

1.10. Normal and Subnormal Series

Definition 1.34. Let G be a group.

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{e\} \tag{1.12}$$

is called a *subnormal series* of G. G_i/G_{i+1}, $0 \le i \le m-1$, are the factor groups of the series. The length of (1.12) is $|\{0 \le i \le m-1 : G_i \neq G_{i+1}\}|$. If $G_i \lhd G$, $1 \le i \le m$, (1.12) is called a *normal series.* If G_i/G_{i+1} is simple for all $0 \le i \le m-1$, (1.12) is called a *composition series.* If G_i/G_{i+1} is abelian for all $0 \le i \le m-1$, (1.12) is called a *solvable series.*

A (sub)normal series

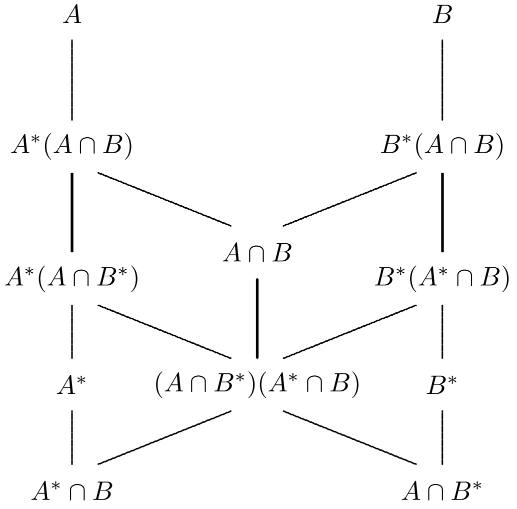
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{e\} \tag{1.13}$$

is called a refinement of (1.12) if $\{G_0, \dots, G_m\} \subset \{H_0, \dots, H_n\}$. Two subnormal series $\mathcal{S} : G = G_0 \rhd \cdots \rhd G_m = \{e\}$ and $\mathcal{T} : G = H_0 \rhd \cdots \rhd H_n = \{e\}$ are called equivalent if there is a bijection between the nontrivial factors of $\mathcal{S}$ and those of $\mathcal{T}$ such that the corresponding factors are isomorphic.

Theorem 1.35 (The Schreier refinement theorem). *Any two (sub)normal series of G have equivalent refinements.*

LEMMA 1.36 (Zassenhaus). *Let A^*, A, B^*, B be subgroups of G such that $A^* \lhd A$ and $B^* \lhd B$. Then $A^*(A \cap B^*) \lhd A^*(A \cap B)$, $B^*(A^* \cap B) \lhd B^*(A \cap B)$ and*

$$\frac{A^*(A \cap B)}{A^*(A \cap B^*)} \cong \frac{B^*(A \cap B)}{B^*(A^* \cap B)}.$$



PROOF. Let $D = (A^* \cap B)(A \cap B^*)$. We claim that $D \lhd A \cap B$. Since $A^* \lhd A$, we have $A^* \cap B \lhd A \cap B$; since $B^* \lhd B$, we have $A \cap B^* \lhd A \cap B$. So, $D = (A^* \cap B)(A \cap B^*) \lhd A \cap B$.

It suffices to show

$$\frac{A^*(A \cap B)}{A^*(A \cap B^*)} \cong \frac{A \cap B}{D}.$$

(By symmetry, we have $\frac{B^*(A \cap B)}{B^*(A^* \cap B)} \cong \frac{A \cap B}{D}$.) Define

$$\begin{array}{rccl} \phi : & A^*(A \cap B) & \longrightarrow & \dfrac{A \cap B}{D} \\ & ax & \longmapsto & Dx, \quad a \in A^*,\ x \in A \cap B. \end{array}$$

1° ϕ is well defined. If $ax = a'x'$, where $a, a' \in A^*$ and $x, x' \in A \cap B$, then $x'x^{-1} = (a')^{-1}a \in A^* \cap (A \cap B) = A^* \cap B \subset D$. So, $Dx = Dx'$.

2° ϕ is onto. Obvious.

3° ϕ is a homomorphism. $\forall\, ax, a'x' \in A^*(A \cap B)$, we have $\phi(axa'x') = \phi(axa'x^{-1}xx') = Dxx' = \phi(ax)\phi(a'x')$ since $xa'x^{-1} \in A^*$.

4° $\ker \phi = A^*D = A^*(A^* \cap B)(A \cap B^*) = A^*(A \cap B^*)$.

By the 1st isomorphism theorem, $\frac{A^*(A \cap B)}{A^*(A \cap B^*)} \cong \frac{A \cap B}{D}$. □

PROOF OF THEOREM 1.35. Let $\mathcal{S} : G = G_0 \rhd \cdots \rhd G_m = \{e\}$ and $\mathcal{T} : G = H_0 \rhd \cdots \rhd H_n = \{e\}$ be two (sub)normal series. Let

$$G_{ij} = G_{i+1}(G_i \cap H_j), \quad H_{ij} = H_{j+1}(G_i \cap H_j), \quad 0 \le i \le m,\ 0 \le j \le n.$$

$(G_{m+1} := \{e\},\ H_{n+1} := \{e\}.)$ Then

$$\begin{aligned} G_{i-1,n} &= G_{i,0} = G_i, && 1 \le i \le m-1,\\ H_{m,j-1} &= H_{0,j} = H_j, && 1 \le j \le n-1,\\ G_{m-1,n-1} &= H_{m-1,n-1} = G_{m-1} \cap H_{n-1}. \end{aligned}$$

We have a refinement $\mathcal{S}'$ for $\mathcal{S}$

$$\mathcal{S}' : \quad \begin{array}{ccccccccccccc} G & = & G_{00} & \rhd & G_{01} & \rhd & \cdots & \rhd & G_{0,n-1} & \rhd & & \\ & & G_{10} & \rhd & G_{11} & \rhd & \cdots & \rhd & G_{1,n-1} & \rhd & & \\ & & \vdots & & \vdots & & & & \vdots & & & \\ & & G_{m-1,0} & \rhd & G_{m-1,1} & \rhd & \cdots & \rhd & G_{m-1,n-1} & \rhd & \{e\} \end{array}$$

and a refinement $\mathcal{T}'$ for $\mathcal{T}$

$$\mathcal{T}' : \quad \begin{array}{cccc} G & & & \\ \shortparallel & & & \\ H_{00} & H_{01} & \cdots & H_{0,n-1} \\ \triangledown & \triangledown & & \triangledown \\ H_{10} & H_{11} & \cdots & H_{1,n-1} \\ \triangledown & \triangledown & & \triangledown \\ \vdots & \vdots & & \vdots \\ \triangledown & \triangledown & & \triangledown \\ H_{m-1,0} & H_{m-1,1} & \cdots & H_{m-1,n-1} \\ \triangledown & \triangledown & & \triangledown \\ & & & \{e\} \end{array}$$

We claim that $\mathcal{S}'$ and $\mathcal{T}'$ are equivalent. It suffices to show $G_{ij}/G_{i,j+1} \cong H_{ij}/H_{i+1,j}$, $0 \le i \le m-1$, $0 \le j \le n-1$. By the Zassenhaus lemma,

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

□

Fact. Every finite group has a composition series.

Theorem 1.37 (Jordan-Hölder). *Any two composition series of a group G are equivalent.*

Proof. Let $\mathcal{S}$ and $\mathcal{T}$ be two composition series of G. By Theorem 1.35, $\mathcal{S}$ and $\mathcal{T}$ have refinements $\mathcal{S}'$ and $\mathcal{T}'$ such that $\mathcal{S}'$ and $\mathcal{T}'$ are equivalent. But $\mathcal{S}' = \mathcal{S}$ and $\mathcal{T}' = \mathcal{T}$. □

Examples of composition series. $S_n \rhd A_n \rhd \{\text{id}\}$, where $n \ge 5$. $S_4 \rhd A_4 \rhd K \rhd \langle (1,2)(3,4) \rangle \rhd \{\text{id}\}$.

Derived groups and solvable groups. Let G be a group. $G^{(0)} := G$, $G^{(i+1)} := (G^{(i)})'$. $G^{(i)}$ is called the ith *derived group* of G. If $G^{(n)} = \{e\}$ for some $n \in \mathbb{Z}^+$, G is called *solvable*.

Example.

$$S_n' = \begin{cases} A_n & \text{if } n \geq 3, \\ \{\text{id}\} & \text{if } n \leq 2, \end{cases} \qquad A_n' = \begin{cases} A_n & \text{if } n \geq 5, \\ K & \text{if } n = 4, \\ \{\text{id}\} & \text{if } n \leq 3. \end{cases}$$

Proof. Assume $n \geq 3$. Since S_n/A_n is abelian, $S_n' \subset A_n$. Since $(i,j,k) = (i,j)(i,k)(i,j)^{-1}(i,k)^{-1} \in S_n'$ for all distinct $i,j,k \in \{1,\dots,n\}$, we have $A_n \subset S_n'$.

If $n \geq 5$, $\{\text{id}\} \neq A_n' \lhd A_n$ and A_n is simple. So $A_n' = A_n$. A_4/K is abelian, so $A_4' \subset K$. Since $A_4' \lhd S_4$ and $A_4' \neq \{\text{id}\}$, we have $A_4' = K$. □

Proposition 1.38. *G is solvable $\Leftrightarrow$ G has a solvable series.*

Proof. ($\Rightarrow$) $G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} = \{e\}$ is a solvable series.

($\Leftarrow$) Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$ be a solvable series. Then $G_i \supset G_{i-1}'$, $1 \leq i \leq n$. So, $\{e\} = G_n \supset G_{n-1}' \supset G_{n-2}'' \supset \cdots \supset G_0^{(n)} = G^{(n)}$. □

Fact. Let $N \lhd G$. Then G is solvable $\Leftrightarrow$ N and G/N are both solvable.

Proof. ($\Rightarrow$) Assume $G^{(n)} = \{e\}$. Then $N^{(n)} = \{e\}$ and $(G/N)^{(n)} = \{N\}$.

($\Leftarrow$) A solvable series of G/N and a solvable series of N give rise to a solvable series of G. □

Examples. Finite p-groups are solvable. S_n ($n \geq 5$) is not solvable.

Theorem 1.39 (The Burnside p-q theorem). *If $|G| = p^a q^b$, where p, q are primes, then G is solvable.*

The proof needs representation theory.

Theorem 1.40 (The Feit-Thompson theorem). *Every finite group of odd order is solvable.*

The proof is over 250 pages [**7**].

Central series and nilpotent groups.

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

such that $G_{i+1}/G_i \subset Z(G/G_i)$ is called a *central series* of G. A central series is an ascending series. If G has a central series, G is called *nilpotent*.

Easy fact. Let G be a group. $Z_0(G) := \{e\}$. $Z_{i+1}(G)$ is defined by $Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$. Then G is nilpotent $\Leftrightarrow$ $Z_n(G) = G$ for some $n \in \mathbb{Z}^+$.

Proof. ($\Rightarrow$) Let $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a central series. Use induction to show $G_i \subset Z_i(G)$. Assume $G_{i-1} \subset Z_{i-1}(G)$. Since $f : G/G_{i-1} \to G/Z_{i-1}(G)$, $gG_{i-1} \mapsto gZ_{i-1}(G)$, is an onto homomorphism and since $G_i/G_{i-1} \subset Z(G/G_{i-1})$, we have $G_iZ_{i-1}(G)/Z_{i-1}(G) = f(G_i/G_{i-1}) \subset Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G)$. So $G_i \subset Z_i(G)$. □

Easy fact. G nilpotent $\Rightarrow$ G solvable.

Example. Let $3 \leq n = 2^t m$, $2 \nmid m$. Consider the dihedral group

$$D_n = \langle \alpha, \beta \mid \alpha^n = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{-1} \rangle.$$

First assume $m \geq 3$. We claim that

$$Z_i(D_n) = \begin{cases} \langle \alpha^{n/2^i} \rangle & \text{if } 0 \leq i \leq t, \\ \langle \alpha^m \rangle & \text{if } i > t. \end{cases} \tag{1.14}$$

To see (1.14), use induction on i. Assume that $i < t$ and $Z_i(D_n) = \langle \alpha^{n/2^i} \rangle$. Then $D_n/Z_i(D_n) = \langle \bar{\alpha}, \bar{\beta} \rangle \cong D_{n/2^i}$, where $\bar{\alpha} = \alpha Z_i(D_n)$, $\bar{\beta} = \beta Z_i(D_n)$, $o(\bar{\alpha}) = n/2^i$, $o(\bar{\beta}) = 2$, $\bar{\beta}\bar{\alpha}\bar{\beta}^{-1} = \bar{\alpha}^{-1}$. Hence, $Z(D_n/Z_i(D_n)) = \langle \bar{\alpha}^{n/2^{i+1}} \rangle = \langle \alpha^{n/2^{i+1}} \rangle / Z_i(D_n)$. So $Z_{i+1}(D_n) = \langle \alpha^{n/2^{i+1}} \rangle$. Since $D_n/Z_t(D_n) = D_n/\langle \alpha^m \rangle \cong D_m$, $Z(D_n/Z_t(D_n)) = Z_t(D_n)/Z_t(D_n)$, so $Z_{t+1}(D_n) = Z_t(D_n)$. In the same way, $Z_i(D_n) = Z_t(D_n)$ for all $i > t$.

Now assume $m = 1$, i.e., $n = 2^t$. The same argument shows that

$$Z_i(D_n) = \begin{cases} \langle \alpha^{n/2^i} \rangle & \text{if } 0 \leq i < t, \\ D_n & \text{if } i \geq t. \end{cases}$$

So, D_n is nilpotent iff n is a power of 2. (Note. D_n is always solvable.)

Fact 1.41. If G is nilpotent and $H \subsetneqq G$, then $H \neq N_G(H)$.

Proof. Let $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a central series. Choose i such that $G_i \subset H$ but $G_{i+1} \not\subset H$. Since $G_{i+1}/G_i \subset Z(G/G_i)$. $G_{i+1}/G_i \subset N_{G/G_i}(H/G_i) \Rightarrow G_{i+1} \subset N_G(H)$. □

Fact. Finite p-groups are nilpotent.

Proof. Let $|G| = p^k$. If $Z_i(G) \neq G$, then $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ is nontrivial. So $Z_i(G) \subsetneq Z_{i+1}(G)$. Thus $Z_n(G) = G$ for some $n > 0$. □

Proposition 1.42. *Let G be a finite group. Then G is nilpotent $\Leftrightarrow$ $G \cong$ the direct product of its Sylow subgroups.*

Proof. ($\Rightarrow$) Only have to show that every Sylow subgroup P of G is normal. By Proposition 1.20, $N_G(N_G(P)) = N_G(P)$. If $N_G(P) \neq G$, by Fact 1.41, $N_G(N_G(P)) \neq N_G(P)$, which is a contradiction. So, $N_G(P) = G$, i.e. $P \lhd G$.

($\Leftarrow$) $H \times K$ is nilpotent $\Leftrightarrow$ H and K are both nilpotent. □

1.11. Examples of Automorphism Groups

Automorphism groups of S_n and A_n.

Lemma 1.43. *If $f \in \mathrm{Aut}(A_n)$ maps a 3-cycle to a 3-cycle, then $\exists \alpha \in S_n$ such that $f(\sigma) = \alpha\sigma\alpha^{-1}$ $\forall \sigma \in A_n$.*

Proof. When $n \leq 3$, the claim is obviously true. So assume $n \geq 4$.

First note that f maps all 3-cycles to 3-cycles. When $n = 4$, every 3-cycle is conjugate to $(1,2,3)$ or $(1,2,3)^{-1}$ in A_4. When $n \geq 5$, all 3-cycles are conjugate in A_n.

Let $f\big((1,2,3)\big) = (a_1,a_2,a_3)$. Since $(a_1,a_2,a_3)f\big((1,2,4)\big) = f\big((1,2,3)(1,2,4)\big)$ $= f\big((1,3)(2,4)\big)$ has order 2, after a cyclic shift of (a_1,a_2,a_3), we have $f\big((1,2,4)\big) = (a_1,a_2,a_4)$. For $i \geq 5$, since $(a_1,a_2,a_3)f\big((1,2,i)\big) = f\big((1,3)(2,i)\big)$ has order 2, we must have $f\big((1,2,i)\big) = (a_1,a_2,a_i)$ or (a_2,a_3,c) or (a_3,a_1,d), where $a_i \notin$

$\{a_1,\dots,a_4\}$ and $c,d\notin\{a_1,a_2,a_3\}$. In the last two cases, $o\big[f\big((1,2,4)\big)f\big((1,2,i)\big)\big]\neq 2$, which is a contradiction. So, we must have $f\big((1,2,i)\big)=(a_1,a_2,a_i)$. Therefore,

$$f\big((1,2,i)\big)=(a_1,a_2,a_i)=\alpha(1,2,i)\alpha^{-1},\qquad i\geq 3,$$

where $\alpha(i)=a_i$, $1\leq i\leq n$. Since A_n is generated by $(1,2,i)$, $3\leq i\leq n$, we have $f(\sigma)=\alpha\sigma\alpha^{-1}$ $\forall\sigma\in A_n$. □

LEMMA 1.44. *Let $G<S_n$ with $[S_n:G]=n$. Then $\exists\theta\in\mathrm{Aut}(S_n)$ such that $\theta(G)=\{\sigma\in S_n:\sigma(1)=1\}\cong S_{n-1}$.*

PROOF. Let $\phi:S_n\to S_{S_n/G}$ be the action of S_n on S_n/G by left multiplication. Then $\ker\phi\subset G$. Since the only normal subgroup of S_n with an order dividing $(n-1)!$ is $\{\mathrm{id}\}$, we have $\ker\phi=\{\mathrm{id}\}$. So ϕ is an isomorphism. Write $S_n/G=\{G_1,\dots,G_n\}$, where $G_1=G$. Let $f:\{1,\dots,n\}\to S_n/G$, $i\mapsto G_i$. Define

$$\begin{array}{cccc}\theta: & S_n & \longrightarrow & S_n\\ & \sigma & \longmapsto & f^{-1}\phi(\sigma)f.\end{array}$$

Then $\theta\in\mathrm{Aut}(S_n)$. If $\sigma\in G$, $\big[\theta(\sigma)\big](1)=\big[f^{-1}\phi(\sigma)f\big](1)=\big[f^{-1}\phi(\sigma)\big](G)=1$. □

THEOREM 1.45. (i) *For $n\geq 4$, $\rho:\mathrm{Aut}(S_n)\to\mathrm{Aut}(A_n)$, $f\mapsto f|_{A_n}$, is an isomorphism.*

(ii) *Assume $n\neq 6$. Then*

$$\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)\cong\begin{cases}1 & \text{if } n\leq 2,\\ S_n & \text{if } n\geq 3,\ n\neq 6,\end{cases}$$

$$\mathrm{Aut}(A_n)\cong\begin{cases}1 & \text{if } n\leq 2,\\ \mathbb{Z}_2 & \text{if } n=3,\\ S_n & \text{if } n\geq 4,\ n\neq 6.\end{cases}$$

(iii) *$\mathrm{Aut}(S_6)=\mathrm{Aut}(A_6)$ and $[\mathrm{Aut}(S_6):\mathrm{Inn}(S_6)]=2$.*

PROOF. 1° For $n\geq 4$, ρ is 1-1. (Thus we may write $\mathrm{Aut}(S_n)\subset\mathrm{Aut}(A_n)$.)

Assume $f\in\mathrm{Aut}(S_n)$ such that $f|_{A_n}=\mathrm{id}_{A_n}$. To prove $f=\mathrm{id}$, it suffices to show that $f\big((1,2)\big)=(1,2)$. Assume to the contrary that $f\big((1,2)\big)\neq(1,2)$. $f\big((1,2)\big)$ is a product of k disjoint transpositions. Thus

$$2(n-2)!=\big|C_{S_n}\big((1,2)\big)\big|=\big|C_{S_n}\big[f\big((1,2)\big)\big]\big|=2^k k!(n-2k)!,$$

which implies that $k=1$ or $n=6$ and $k=3$. In either cases, we have $C_{A_n}\big((1,2)\big)\neq C_{A_n}\big[f\big((1,2)\big)\big]$, which is a contradiction.

2° For $n\geq 4$, $n\neq 6$, $\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)$ and $\rho:\mathrm{Aut}(S_n)\to\mathrm{Aut}(A_n)$ is an isomorphism.

Let $g\in\mathrm{Aut}(A_n)$ and let $\sigma\in A_n$ be a 3-cycle. The $f(\sigma)$ is a product of k disjoint 3-cycles. We have

$$\frac{1}{2}\,3(n-3)!=|C_{A_n}(\sigma)|=\big|C_{A_n}\big(g(\sigma)\big)\big|=\frac{1}{2}\,3^k k!(n-3k)!. \tag{1.15}$$

The integer solutions of (1.15) are $(n,k)=(n,1)$ and $(n,k)=(6,2)$. Since $n\neq 6$, we have $k=1$. By Lemma 1.43, $g=\rho(f)$ for some $f\in\mathrm{Inn}(S_n)$. Therefore, $\rho\big|_{\mathrm{Inn}(S_n)}:\mathrm{Inn}(S_n)\to\mathrm{Aut}(A_n)$ is onto. By 1°, $\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)$ and $\rho:\mathrm{Aut}(S_n)\to\mathrm{Aut}(A_n)$ is an isomorphism.

3° $[\text{Aut}(A_6) : \text{Inn}(S_6)] \le 2$.

Let $f, g \in \text{Aut}(A_6)$. If f maps a 3-cycle to a 3-cycle, by Lemma 1.43, $f \in \text{Inn}(S_6)$. Assume that both f and g maps every 3-cycle to a product of two disjoint 3-cycles. Then f maps every product of two disjoint 3-cycles to a 3-cycle. (Note that in A_6, the number of 3-cycles equals the number of products of two disjoint 3-cycles.) Hence fg maps all 3-cycles to 3-cycles. By Lemma 1.43, $fg \in \text{Inn}(S_6)$. So, $[\text{Aut}(A_6) : \text{Inn}(S_6)] \le 2$.

4° $\text{Aut}(S_6) \ne \text{Inn}(S_6)$.

Let $\mathcal{P}$ be the set of 6 Sylow 5-subgroups of S_5. Let $\phi : S_5 \to S_{\mathcal{P}}$ $(= S_6)$ be the action of S_5 on $\mathcal{P}$ by conjugation. Then $\ker\phi = \{\text{id}\}$. (Since S_5 acts transitively on $\mathcal{P}$, $6 \bigm| |S_5/\ker\phi|$. Since A_5 is only one nontrivial normal subgroup of S_5, we have $\ker\phi = \{\text{id}\}$.) Thus $\phi(S_5)$ is a subgroup of $S_{\mathcal{P}}$ of index 6. By Lemma 1.44, $\exists f \in \text{Aut}(S_{\mathcal{P}})$ such that $f\bigl(\phi(S_5)\bigr)$ is the stabilizer of some $P \in \mathcal{P}$. Since $\phi(S_5)$ acts transitively on $\mathcal{P}$, we must have $f \notin \text{Inn}(S_{\mathcal{P}})$. (If $f = \alpha(\ )\alpha^{-1}$ for some $\alpha \in S_{\mathcal{P}}$, then $\phi(S_5)$ stabilizes $\alpha^{-1}(P)$, $\rightarrow\leftarrow$.)

5° By 1° , 3° and 4°, we have

$$\text{Inn}(S_6) \subsetneq \text{Aut}(S_6) \subset \text{Aut}(A_6)$$

and $[\text{Aut}(A_6) : \text{Inn}(S_6)] \le 2$. So, $\text{Aut}(S_6) = \text{Aut}(A_6)$ and $[\text{Aut}(S_6) : \text{Inn}(S_6)] = 2$.

6° The remaining claims in (ii) about $\text{Aut}(S_n)$ and $\text{Aut}(A_n)$ for $n \le 3$ are obvious. (To see that $\text{Aut}(S_3) = \text{Inn}(S_3)$, note that $\forall f \in \text{Aut}(S_3)$, $f\bigl((1,2)\bigr)$ is a 2-cycle and $f\bigl((1,2,3)\bigr)$ is a 3-cycle; hence $|\text{Aut}(S_3)| \le 3 \cdot 2 = |\text{Inn}(S_3)|$.) □

Note.

(i) Assume $f \in \text{Aut}(S_6) \setminus \text{Inn}(S_6)$. By Lemma 1.43, f maps every 3-cycle to a product of two disjoint 3-cycles and vice versa. By a similar argument, f maps every transposition to a product of 3 disjoint transpositions and vice versa.

(ii) By Lemma 1.44 and Theorem 1.45, if $n \ne 6$, every subgroup $G < S_n$ with $|G| = (n-1)!$ must fix one of $1, \dots, n$. This is false for $n = 6$.

The Automorphism group of $\text{GL}(n, F)$.

Let F be a field and $n \ge 2$. For each $P \in \text{GL}(n, F)$, $\sigma \in \text{Aut}(F)$ and representation $\chi : \text{GL}(n, F) \to F^{\times}$, define

$$\begin{array}{rccc} g_{P,\sigma,\chi} : & \text{GL}(n,F) & \longrightarrow & \text{GL}(n,F) \\ & A & \longmapsto & \chi(A)PA^{\sigma}P^{-1}. \end{array}$$

Then $g_{P,\sigma,\chi} \in \text{Aut}\bigl(\text{GL}(n, F)\bigr)$ and

$$G = \{g_{P,\sigma,\chi} : P \in \text{GL}(n,F),\ \sigma \in \text{Aut}(F),\ \chi : \text{GL}(n,F) \to F^{\times} \text{ is a representation}\}$$

is a subgroup of $\text{Aut}\bigl(\text{GL}(n, F)\bigr)$. The automorphism

$$\begin{array}{rccc} \tau : & \text{GL}(n,F) & \longrightarrow & \text{GL}(n,F) \\ & A & \longmapsto & (A^{-1})^T \end{array}$$

is an involution. $\tau \notin G$ unless $n = 2$; see Exercise 1.17. $\text{Aut}\bigl(\text{GL}(n, F)\bigr)$ is generated by G and τ; see [**5**].

Exercises

1.1. Let $f : G \to H$ be a homomorphism of groups and $X \subset G$. Prove that $f(\langle X\rangle) = \langle f(X)\rangle$.

1.2. (Double cosets) Let H and K be subgroups of G. For $a \in G$, $HaK := \{hak : h \in H,\ k \in K\}$ is called an (H, K)-*double coset* in G.
   (i) Prove that the set of all (H, K)-cosets form a partition of G.
   (ii) Assume H and K are finite. Prove that $|HaK| = \frac{|H||K|}{|H\cap aKa^{-1}|}$.

1.3. (Cyclic groups)
   (i) Prove that every subgroup of a cyclic group is cyclic.
   (ii) Prove that every quotient group of a cyclic group is cyclic.
   (iii) Let G be an infinite group. Prove that $G \cong \mathbb{Z} \Leftrightarrow G$ is isomorphic to every nontrivial subgroup of G.
   (iv) If G is a cyclic group of order n. Then for every $m \mid n$, G has a unique subgroup of order m. (If $G = \langle a\rangle$, then $\langle a^{\frac{n}{m}}\rangle$ is the unique subgroup of order m.)

1.4. (Diagram chasing) A sequence of groups and homomorphisms

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

is called *exact* at G_i if $\operatorname{im} f_{i-1} = \ker f_i$; the sequence is called exact if it is exact at G_i for all i. An exact sequence $1 \to K \xrightarrow{f} G \xrightarrow{h} Q \to 1$ is called a *short exact sequence*. Let

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & A' \arrow[r, "f'"] \arrow[d, "\alpha'"'] & B' \arrow[r, "g'"] \arrow[d, "\beta'"] & C' \arrow[r] \arrow[d, "\gamma'"] & 1 \\
1 \arrow[r] & A'' \arrow[r, "f''"] \arrow[d] & B'' \arrow[r, "g''"] \arrow[d] & C'' \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

be a commutative diagram of groups such that all columns are exact and the 2nd and 3rd rows are exact. Prove that the 1st row is also exact.

1.5. Determine all subgroups of S_4 and identify the ones that are normal.

1.6. (The converse of Lagrange's theorem is false.) Prove that A_n does not have a subgroup of index 2.

1.7. Assume $H < S_n$ such that $[S_n : H] = 2$. Prove that $H = A_n$.

1.8. (Application of Burnside's lemma) Each vertex of a regular n-gon is to be colored with any of c colors. Two colored regular n-gons are considered the same if one can be obtained from the other through a rotation or a reflection. Find the total number of different ways to color the regular n-gon. (Let $\mathcal{X}$

be the set of all colored regular n-gons. Then D_n acts on $\mathcal{X}$ and the number to be found is the number of D_n-orbits in $\mathcal{X}$.)

1.9. Prove that there are no simple groups of order 120 and 300.

1.10. (Groups of order $2pq$) Let G be a nonabelian group of order $2pq$, where $2 < p < q$ are primes.

(i) Assume $q \not\equiv 1 \pmod{p}$. Then

$$G \cong (\mathbb{Z}_q \times \mathbb{Z}_p) \rtimes_{\alpha_i} \mathbb{Z}_2$$

for some $i = 1, 2, 3$, where $\alpha_i : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_q \times \mathbb{Z}_p)$,

$$\alpha_1(1) : \begin{cases} (1,0) \mapsto (-1,0), \\ (0,1) \mapsto (0,1); \end{cases} \quad \alpha_2(1) : \begin{cases} (1,0) \mapsto (1,0), \\ (0,1) \mapsto (0,-1); \end{cases} \quad \alpha_3(1) : \begin{cases} (1,0) \mapsto (-1,0), \\ (0,1) \mapsto (0,-1). \end{cases}$$

Moreover, $(\mathbb{Z}_q \times \mathbb{Z}_p) \rtimes_{\alpha_i} \mathbb{Z}_2$, $i = 1, 2, 3$, are pairwise nonisomorphic.

(ii) Assume $q \equiv 1 \pmod{p}$. In addition to the three groups in (i), there is a fourth group

$$(\mathbb{Z}_q \rtimes \mathbb{Z}_p) \rtimes_\beta \mathbb{Z}_2,$$

where $\mathbb{Z}_q \rtimes \mathbb{Z}_p = \langle a, b \mid a^q = b^p = 1,\ bab^{-1} = a^k \rangle$, $o(k) = p$ in $\mathbb{Z}_p^\times$, and $\beta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_q \rtimes \mathbb{Z}_p)$,

$$\beta(1) : \begin{cases} a \mapsto a^{-1}, \\ b \mapsto b. \end{cases}$$

Note that

$$(\mathbb{Z}_q \rtimes \mathbb{Z}_p) \rtimes_\beta \mathbb{Z}_2 = \langle a, b, c \mid a^q = b^p = c^2 = 1,\ bab^{-1} = a^k,\ cac^{-1} = a^{-1},\ cbc^{-1} = b \rangle.$$

1.11. (Generalized quaternion groups) Let $n \ge 1$ and $Q_{4n} = \langle x, y \mid x^{2n} = 1,\ x^n = y^2,\ yxy^{-1} = x^{-1} \rangle$. Also let

$$A = \begin{bmatrix} \xi & \\ & \xi^{-1} \end{bmatrix}, \quad A = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \in \mathrm{GL}(2, \mathbb{C}),$$

where $\xi = e^{2\pi i/2n}$, and let $G = \langle A, B \rangle < \mathrm{GL}(2, \mathbb{C})$.

(i) Prove that $\exists$ an onto homomorphism $f : Q_{4n} \to G$ such that $f(x) = A$ and $f(y) = B$.

(ii) Prove that $|Q_{4n}| \le 4n$ and $|G| \ge 4n$. Thus, $|Q_{4n}| = |G| = 4n$ and $f : Q_{4n} \to G$ is an isomorphism.

1.12. Prove that $S_4 \cong \langle a, b \mid a^4 = b^3 = (ab)^2 = 1 \rangle$.

1.13. Prove that Q_8 cannot be embedded in S_7.

1.14. Prove that if n is odd, $D_{2n} \cong D_n \times \mathbb{Z}_2$.

1.15. Let $|X| = \infty$. Prove that $\mathrm{Aut}(S_X) \ne \mathrm{Inn}(S_X)$.

1.16. Let $n \ge 4$, $\alpha = (1, 2, \dots, n)$, $\beta = (1, 4)(2, 3) \in S_n$. Then

$$\langle \alpha, \beta \rangle = \begin{cases} D_n & \text{if } n = 4, 5, \\ S_n & \text{if } n \ge 6 \text{ and } n \text{ is even}, \\ A_n & \text{if } n \ge 6 \text{ and } n \text{ is odd}. \end{cases}$$

1.17. Let F be a field and $n \geq 3$. Then there do not exist $P \in \mathrm{GL}(n, F)$, $\sigma \in \mathrm{Aut}(F)$ and a representation $\chi : \mathrm{GL}(n, F) \to F^{\times}$ such that

$$(A^{-1})^T = \chi(A) P A^{\sigma} P^{-1} \qquad \text{for all } A \in \mathrm{GL}(n, F). \tag{1.16}$$

Note. If $n = 2$, then

$$(A^{-1})^T = \frac{1}{\det A} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} A \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{-1} \qquad \text{for all } A \in \mathrm{GL}(2, F).$$

1.18. Let F be a field and $f : \mathrm{GL}(n, F) \to F^{\times}$ a homomorphism. Prove that $\exists!$ a homomorphism $g : F^{\times} \to F^{\times}$ such that $f = g \circ \det$.

1.19. Let $G = \langle \{A, B\} \rangle < \mathrm{GL}(2, \mathbb{Q})$, where

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Let $U = \{\left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right] : a \in \mathbb{Q}\} < \mathrm{GL}(2, \mathbb{Q})\}$. Prove that $G \cap U$ is not finitely generated.

1.20. (Dixon [**6**, Problem 6.39]) Let G be a finite p-group such that $Z(G')$ is cyclic. Prove that G' is abelian.

1.21. Let H and K be normal subgroups of G such that G/H and G/K are both solvable. Prove that $G/H \cap K$ is solvable. (Hint. Consider $H/H \cap K$ and $(G/H \cap K)/(H/H \cap K)$. Use the 2nd and 3rd isomorphism theorems.)

1.22. Let G be group. A normal subgroup $N \lhd G$ is called minimal if $N \neq \{e\}$ and $\nexists\, K \lhd G$ such that $\{e\} \neq K \subsetneq N$. Assume that G is a finite solvable group and N a minimal normal subgroup of G. Prove that N is an elementary abelian p-group, i.e., $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ for some prime p.

CHAPTER 2

Rings and Modules

2.1. Rings, Basic Definitions

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

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

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

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

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

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

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

Basic properties of rings.

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

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

Types of rings.

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

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

Field. Commutative division ring.

Examples.

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

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

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

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

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

Proof. We have

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

where

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

If I and J are ideals of R, define

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

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

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

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

is an onto homomorphism (canonical homomorphism).

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

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

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

Isomorphism theorems.

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

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

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

(i) $R \times R \to R$, $(x, y) \mapsto x + y$;
(ii) $R \to R$, $x \mapsto -x$;
(iii) $R \times R \to R$, $(x, y) \mapsto xy$.

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

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

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

2.2. Prime Ideals and Maximal Ideals

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

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

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

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

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

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

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

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

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

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

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

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

(i)

$$e_ie_j = \begin{cases} e_i & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

($e_1, \dots, e_n$ are called orthogonal idempotents*.)*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note.

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

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

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

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

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

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

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

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

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

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

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

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

PID $\Rightarrow$ UFD.

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

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

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

$$\mathbb{Z}[\sqrt{d}], \qquad d = -2,\ -1,\ 2,\ 3,\ 6,\ 7,\ 11,\ 19,$$

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

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

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

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

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

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

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

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

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

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

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

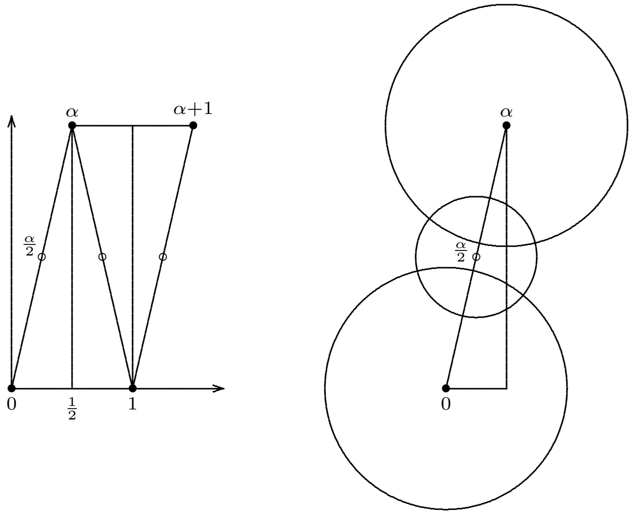


Figure 2.1. Example 2.14

3° $\mathbb{Z}[\alpha]$ is a PID.

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

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

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

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

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

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

(iii) a, b both odd. We have

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4. Fractions and Localization

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

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

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

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

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

(i) *The map*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5. Polynomial Rings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

Facts.

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

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

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

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

The Hasse derivative. Let R be a commutative ring. For $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ and $k \geq 0$, define

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1° Existence of factorization.

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

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

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

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

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

2° Uniqueness of factorization.

Suppose

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

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

In $F[x]$,

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

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

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

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

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

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

2.6. Modules, Definitions and Basic Facts

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Isomorphism Theorems.

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

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

is an isomorphism.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For each $x \in X$, $\exists$ a finite subset $\{y_1, \dots, y_n\} \subset Y$ such that $x = r_1 y_1 + \cdots + r_n y_n$, $r_i \in R$. Define $f(x) = \{y_1, \dots, y_n\}$. We claim that $\bigcup_{x\in X} f(x) = Y$. (Otherwise, X is spanned by $Y_1 := \bigcup_{x\in X} f(x) \subsetneq Y$; hence Y is spanned by Y_1, $\rightarrow\leftarrow$.) Now,

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

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

Facts. Let D be a division ring.

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

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

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

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

(ii) Define a D-map

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

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

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

□

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

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

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

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

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

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

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

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

2.7. Projective and Injective Modules

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

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

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

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

commutes.

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

(i) *$\exists$ an R-map $h : C \to B$ such that $g \circ h = \mathrm{id}_C$.*

(ii) *$\exists$ an R-map $k : B \to A$ such that $k \circ f = \mathrm{id}_A$.*

(iii) *$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is isomorphic to $0 \to A \xrightarrow{\iota_1} A \oplus C \xrightarrow{\pi_2} C \to 0$.*

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

Proof. (i) ⇒ (iii).

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

commutes, where

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

is an isomorphism by the five lemma (next).

(ii) ⇒ (iii).

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

commutes, where

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

is an isomorphism by the five lemma.

(iii) ⇒ (i) and (ii).

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

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

Lemma 2.34 (The five lemma). *Let*

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

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

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

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

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

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

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

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

commutes.

Free modules are projective.

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

(i) *P is projective.*

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

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

Proof. (i) ⇒ (ii).

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

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

(iii) ⇒ (i).

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

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

Pull back. Let

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

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

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

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

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

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

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

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

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

Proof. Let X be a basis of F. Let

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

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

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

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

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

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

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

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

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

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

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

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

Projective modules over a local ring.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Write

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

By (2.5) and (2.6), we have

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

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

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

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

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

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

commutes.

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

Proof. ($\Rightarrow$)

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

($\Leftarrow$)

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

$$h(b) = (h_i(b))_{i\in I}.$$

□

Push out. Let

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

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

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

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

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

(i) *E is injective.*

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

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

Proof. (i) $\Rightarrow$ (ii).

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

(ii) $\Rightarrow$ (i). Use a push out

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

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

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

(iii) $\Rightarrow$ (ii). Obvious. □

NOTE. Theorem 2.45 also provides a quick proof of (iii) $\Rightarrow$ (i).

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

PROOF. ($\Leftarrow$) Given

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

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

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

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

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

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

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

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

FACTS.

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

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

(iii) D injective $\Rightarrow$ D divisible.

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

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

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

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

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

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

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

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

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

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

where

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

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

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

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

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

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

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

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

2.8. Chain Conditions

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

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

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

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

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

Proofs of Theorems 2.47 and 2.48 are the same as the proofs in the group case; see Theorem 1.35 and 1.37.

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

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

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

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

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

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

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

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

(ii) *A has DCC $\Leftrightarrow$ every nonempty family of submodules of A contains a minimal element.*

PROOF. (i) *Every submodule of A is finitely generated $\Rightarrow$ A has ACC.*

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

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

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

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

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

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

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

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

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

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

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

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

Put

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

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

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

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

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

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

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

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

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

By the five lemma, $B_k = B_{n+k}$. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.9. Finitely Generated Modules over a PID

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

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

where

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

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

Proof. *Existence of decomposition* (2.8).

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

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

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

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

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

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

Then

$$\begin{bmatrix} f_1' \\ \vdots \\ f_m' \end{bmatrix} = \begin{bmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ & 0 & & 0 \end{bmatrix} \begin{bmatrix} e_1' \\ \vdots \\ e_n' \end{bmatrix}.$$

So, $K = (f_1', \dots, f_m') = (d_1 e_1', \dots, d_r e_r')$. Since

$$\begin{aligned} R^n &= Re_1' \oplus \cdots \oplus Re_n', \\ K &= Rd_1e_1' \oplus \cdots \oplus Rd_ne_n' \quad (d_i = 0 \text{ for } i > r), \end{aligned}$$

we have

$$\begin{aligned} A = R^n/K &\cong Re_1'/Rd_1e_1' \oplus \cdots \oplus Re_n'/Rd_ne_n' \\ &\cong R/(d_1) \oplus \cdots \oplus R/(d_n) \\ &\cong R/(d_{a+1}) \oplus \cdots \oplus R/(d_n). \end{aligned}$$

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

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

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

Assume that

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

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

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

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

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

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

$$Rd_i z_{i+1} \oplus \cdots \oplus Rd_i z_s \supset Rd_i w_i' \oplus \cdots \oplus Rd_i w_s'.$$

So,

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

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

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

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

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

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

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

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

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

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

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

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

Example. Let

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

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

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

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

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

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

Existence of the decomposition of A.

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

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

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

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

Then

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

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

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

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

Uniqueness of the decomposition of A. Let

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

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

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

□

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

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

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

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

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

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

Then ϕ is an $F[x]$-map with

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

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

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

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

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

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

where

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

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

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

Then by the proof of Theorem 2.57,

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

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

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

where

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

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

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

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

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

Exercises

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

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

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

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

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

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

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

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

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

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

2.9. (i) Let

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

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

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

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

(iii) Let

$$\begin{tikzcd}
 & 0 \arrow[rr] & & A_3 \arrow[rr, "f_3"] \arrow[dd, dashed, "\alpha_4^3"] & & B_3 \arrow[rr, "g_3"] \arrow[dd, "\beta_4^3"] & & C_3 \arrow[dd, "\gamma_4^3"] \\
0 \arrow[rr] & & A_1 \arrow[ur, dashed, "\alpha_3^1"] \arrow[rr, "f_1"] \arrow[dd, dashed, "\alpha_2^1"'] & & B_1 \arrow[ur, "\beta_3^1"] \arrow[rr, "g_1"] \arrow[dd, "\beta_2^1"'] & & C_1 \arrow[ur, "\gamma_3^1"] \arrow[dd, "\gamma_2^1"'] & \\
 & 0 \arrow[rr] & & A_4 \arrow[rr, "f_4"] & & B_4 \arrow[rr, "g_4"] & & C_4 \\
0 \arrow[rr] & & A_2 \arrow[ur, dashed, "\alpha_4^2"'] \arrow[rr, "f_2"'] & & B_2 \arrow[ur, "\beta_4^2"'] \arrow[rr, "g_2"'] & & C_2 \arrow[ur, "\gamma_4^2"'] &
\end{tikzcd}$$

be a commutative diagram with exact rows. Then $\exists!$ R-maps $\alpha_2^1, \alpha_3^1, \alpha_4^2, \alpha_4^3$ such that the resulting diagram commutes. (Of course, there is a 3-D version of (ii).)

Bibliography

[1] H. Bass, *Big projective modules are free*, Illinois J. Math. **7** (1963), 24 – 31.

[2] W. Burnside, *Theory of Groups of Finite Order*, Dover, New York, 1955.

[3] A. L. S. Corner, *Every countable reduced torsion-free ring is an endomorphism ring*, Proc. London Math. Soc. **13** (1963), 687 – 710.

[4] A. L. S. Corner, *On a conjecture of Pierce concerning direct decompositions of Abelian groups*, 1964 Proc. Colloq. Abelian Groups (Tihany, 1963), 43 – 48, Akadémiai Kiadó, Budapest.

[5] J. Dieudonné, *On the Automorphisms of the Classical Groups, with a Supplement by Loo-Keng Hua*, Mem. Amer. Math. Soc., 1951.

[6] J. D. Dixon, *Problems in Group Theory*, Blaisdell Publishing Co., Waltham, MA, 1967

[7] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775 – 1029.

[8] I. N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. **75** (1953), 864 – 871.

[9] I. N. Herstein, *Noncommutative Rings*, The Carus Mathematical Monographs, No. 15, The Mathematical Association of America, distributed by John Wiley & Sons, Inc., New York 1968.

[10] X. Hou, *On the analytic solution of the Cauchy problem*, Proc. Amer. Math. Soc. **137** (2009), 597 – 606.

[11] T. W. Hungerford, *Algebra*, Springer-Verlag, New York-Berlin, 1980.

[12] N. Jacobson, *Basic algebra I*, W. H. Freeman and Company, New York, 1985.

[13] I. Kaplansky, *Projective modules*, Ann. of Math **68** (1958), 372 – 377.

[14] T. Y. Lam, *Serre's Problem on Projective Modules*, Springer-Verlag, Berlin, 2006.

[15] G. Malle, B. H. Matzat, *Inverse Galois theory*, Springer-Verlag, Berlin, 1999.

[16] D. Quillen, *Projective modules over polynomial rings*, Invent. Math. **36** (1976), 167 – 171.

[17] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[18] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1996.

[19] J. J. Rotman, *Advanced Modern Algebra*, Prentice Hall, Inc., Upper Saddle River, NJ, 2002.

[20] I. R. Safarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 525 – 578 (Russian) [English translation: Amer. Math. Soc. Transl. II **4** (1956), 185 – 237].

[21] A. A. Suslin, *Projective modules over polynomial rings are free*, (in Russian) Dokl. Akad. Nauk SSSR **229** (1976), 1063 – 1066. English translation: Soviet Math. Dokl. **17** (1976), 1160 – 1164.

[22] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1997.

[23] A. J. Weir, *The Reidemeister-Schreier and Kuroš subgroup theorems*, Mathematika **3** (1956), 47 – 55.