CHAPTER II

GROUPS

§2.1 Formalities on groups

(2.1.1) Let G be a set with a "law of composition"

$$G \times G \longrightarrow G$$

sending (x, y) to xy which satisfies the following properties

(i) $x(yz) = (xy)z$ for all x, y, z in G,

(ii) there is an element $e \in G$ such that $ex = x = xe$ for all $x \in G$.

We say then that G is a *monoid*. A monoid G is a *group* if the law of composition satisfies

(iii) for every $x \in G$, there is a $y \in G$ such that $xy = yx = e$;

such a y must be uniquely determined and we denote it by x^{-1} called the *inverse* of x. A group G is said to be *commutative* (or *abelian*) if

(iv) $xy = yx$ for all x, y in G.

A subset H of a group G is said to be a *subgroup* of G if H is again a group. A nonempty subset H of a group G is a subgroup if and only if $x^{-1}y \in H$ for all x, y in H.

(2.1.2) Let G and G' be groups. A map $f\colon G \to G'$ is a *group homomorphism* if for any $x, y \in G$ we have

$$f(xy) = f(x)f(y).$$

The *kernel* of a group homomorphism f is defined to be

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e\},$$

which is a subgroup of G. A group homomorphism f is injective if and only if $\mathrm{Ker}(f)$ is trivial. A bijective homomorphism of G into itself is called an *automorphism.* A set of all automorphism of a group G, written $\mathrm{Aut}(G)$, is again a group under the composition of automorphisms.

Let $f_i\colon G_i \to G_{i+1} (i = 1, 2, \ldots, n)$ be group homomorphisms so that we have a sequence,

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \cdots \xrightarrow{f_n} G_{n+1}.$$

We will say that the above sequence is *exact* if $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ for $i = 1, 2, \ldots, n$. An exact sequence of the type

$$(*) \qquad (e) \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow (e)$$

is called a *short exact sequence.*[†]

(2.1.3) Let G be a group and H be a subgroup of G. A *left coset* of H in G is a subset of the type

$$aH = \{ah \mid h \in H\}.$$

A subset of the type Ha is called a *right coset.* The set of all left (resp. right) cosets is denoted by G/H (resp. $G\backslash H$). Any two left cosets are either identical or disjoint and the union of all left cosets is the whole group G.

Let G be a finite group. The number of left cosets of H in G is denoted by $[G\colon H]$ and is called the *index* of H in G. The index of the trivial group is called the *order* of G (i.e., the number of elements of G). We will denote the order of G by $o(G)$. If $g \in G$ then the order $o(g)$ of g is defined to be the order of the cyclic subgroup generated by g. If $K \subset H$ are subgroups of G then one proves the formula

$$[G\colon H][H\colon K] = [G\colon K].$$

Even if G is an infinite group, this formula is valid if the indices appearing in the formula are finite. In particular, *if H is a subgroup of G then $o(H)|o(G)$.*

[†]Some authors say this is an extension of G_1 by G_3 and the others say this is an extension of G_3 by G_1. We will try not to use these terminologies.

(2.1.4) (Group action) Let G be group and X be a set. We say that G *acts on* X (on the left) if there is a map

$$G \times X \longrightarrow X$$

sending (g, x) to gx satisfying the properties

(i) $(g_1 g_2)x = g_1(g_2 x)$,

(ii) $ex = x$.

For example, if H is a subgroup of G, then G acts on G/H *via* $g(xH) = gxH$ for $g \in G$ and $xH \in G/H$. Similarly G also acts on $G\backslash H$. The symmetric group on n letters $\mathfrak{S}_n$ acts on the set $\{1, 2, \ldots, n\}$ in an obvious way.

Let G act on a set X. Then we define an equivalence relation $\sim$ on X by $x \sim y$ if and only if $y = gx$ for some $g \in G$. For $x \in X$, the *orbit* of x is the equivalence class;

$$Gx = \{gx \mid g \in G\}.$$

We have $X = \cup Gx$, where the union is disjoint if we take one representative from each equivalence class.

The *isotropy group* (or *stabilizer*) of $x \in X$ is defined by

$$I_x = \{g \in G \mid gx = x\}.$$

Now the map $G \to Gx$ sending g to gx induces a bijection

$$G/I_x \longrightarrow Gx.$$

Hence if X is finite then we have,

$$[G\colon I_x] = |Gx| \quad \text{and} \quad |X| = \sum [G\colon I_x] \tag{1}$$

where $|\cdot|$ denotes the cardinality and the sum runs over all inequivalent x's.

We let a group G acts on itself *via* conjugation, namely send (g, x) to gxg^{-1}. Let

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

be the *center* of the group G. Then $x \in Z(G)$ if and only if the isotropy group I_x of x is G, i.e., $[G : I_x] = 1$.

Suppose G is a finite group. Collecting all those terms whose isotropy group is G in the first sum and the others in the second, we have the *class formula*,

$$o(G) = o(Z(G)) + \sum [G\colon I_x] \tag{2}$$

where the second sum runs over all representatives of inequivalent classes whose isotropy groups are distinct from G. As an illustration of the class formula, we see that *if the order of a group is a power of a prime then its center is nontrivial.* In fact, if the center is trivial then $o(Z(G)) = 1$. Reading the equation (2) modulo p we have $0 \equiv 1$ which is a contradiction.

We say that a group action is *transitive* if for any x and x' in X there is $g \in G$ such that $x' = gx$.

(2.1.5) A subgroup N of a group G is *normal* if $gN = Ng$ for all $g \in G$. (We often denote a normal subgroup by $N \lhd G$.) In this case, the set of all left cosets, G/N of N becomes a group under the law of composition

$$(gN)(g'N) = gg'N.$$

The group G/N is called the *quotient group* of G by N. We have the canonical map

$$f\colon G \longrightarrow G/N$$

given by $f(x) = xN$ which is surjective of course. We sometimes denote xN by $\bar{x}$. We have an exact sequence

$$(e) \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow (e).$$

Let S be a subset of G. Define the *normalizer* of S in G by

$$N(S) = \{g \in G \mid gS = Sg\}.$$

Hence if we let G act on the subsets of G *via* conjugation then $N(S)$ is the isotropy group of S. If H is a subgroup of G then $N(H)$ is the largest subgroup of G in which H is normal.

(2.1.6) (Semidirect product) Let H be a subgroup of a group G, and N be a normal subgroup. Then the set

$$NH = \{nh \mid n \in N, h \in H\}$$

becomes a subgroup of G. And we have $HN = NH$. We say that G is a *semidirect product* of N and H if N is normal in G, H is a subgroup, $N \cap H = (e)$ and $NH = G$.

If G is a semidirect product of N and H then we can define a homomorphism

$$\phi\colon H \longrightarrow \mathrm{Aut}(N)$$

by $\phi(h)(n) = hnh^{-1}$, which we sometimes denote by n^h. We define a law of composition on the set $N \times H$ by

$$(n, h)(m, k) = (nm^h, hk) = (n\phi(h)m, hk).$$

Then $N \times H$ becomes a group with the identity (e, e) and the inverse of (n, h) is given by $(\phi(h^{-1})n^{-1}, h^{-1})$. We denote the resulting group by $N \times_\phi H$. If G is a semidirect product of N and H then we have a map

$$N \times_\phi H \longrightarrow G$$

sending (n, h) to nh. Then one easily proves that this map is an isomorphism.

More generally, suppose N and H be any two groups, and $\phi\colon H \to \mathrm{Aut}(N)$ be a group homomorphism. We can form the *semidirect product* $N \times_\phi H$ as before. Then we can identify N and H as subgroups of $N \times_\phi H$ in an obvious way. Further N is normal, $NH = N \times_\phi H$ and $N \cap H = (e)$.

In any case, we have a short exact sequence

$$(e) \longrightarrow N \xrightarrow{i} N \times_\phi H \xrightarrow{\pi} H \longrightarrow (e).$$

An extension arising as a semidirect product is called a *split extension* – π has a right inverse which is a group homomorphism. Note the map $(n, h) \mapsto n$ which is a left inverse of i is not a group homomorphism in general.

(2.1.7) (Direct product of groups) Let $\{G_i\}_{i\in I}$ be a family of groups. Let $G = \prod_{i\in I} G_i$ be the (set theoretic) product of G_i's. The elements of G consists of all sequences $(x_i)_{i\in I}$. with $x_i \in G_i$. We define the group structure on G by componentwise multiplication namely if $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ are two elements of G then their product is defined to be $(x_i y_i)_{i\in I}$. We have the projection

$$\pi_i \colon G \longrightarrow G_i$$

sending $(x_i)_{i\in I}$ to x_i. *Then the group G together with the family of homomorphisms $\{\pi_i\}$ is the product of the groups $\{G_i\}_{i\in I}$* in the sense of (1.2.3). In fact, if $f_i \colon G' \to G_i$ is a family of group homomorphisms, then the map defined by $f(x')_i = f_i(x')$ satisfies the required property.

We denote the product of the two groups G_1 and G_2 by $G_1 \times G_2$. Note that in (2.1.6), if ϕ is trivial then the semidirect product becomes the product.

Let $\bigoplus_{i\in I} G_i$ be the subgroup of $\prod_{i\in I} G_i$ consisting of all $(x_i)_{i\in I}$ such that $x_i = e$ except only finitely many i's. The group $\bigoplus_{i\in I} G_i$ is called the *direct sum* of the family $\{G_i\}$.

If the index set I is finite, say $I = \{1, 2, \ldots, n\}$ then the product $G_1 \times \cdots \times G_n$ is the same as $G_1 \oplus \cdots \oplus G_n$ and we will not distinguish these two groups.

(2.1.8)(Coproduct) We will sketch the construction of the coproduct of a family $\{G_i\}$ of groups. Assume that the groups G_i are arranged so that any two of the groups intersect only in the identity $\{e\}$. (Show that this is always possible set theoretically.) Let X be the union $\bigcup_{i\in I} G_i$. Consider the sequence of the elements of X,

$$a_1 a_2 \cdots a_n, \quad a_i \in X$$

such that

(i) no a_i is the identity,

(ii) a_i and a_{i+1} are not in the same group.

On the set of all such sequences together with the identity element e, we define a law of composition;

$$(a_1 \cdots a_n)(b_1 \cdots b_m) = \begin{cases} a_1 \cdots a_{n-1}(a_n b_1) b_2 \cdots b_m & (\text{if } a_n \text{ and } b_1 \text{ are in the same group} \\ & \quad \text{then multiply them}) \\ a_1 \cdots a_n b_1 b_2 \cdots b_m & (\text{otherwise}) \ . \end{cases}$$

Under this law of composition it becomes a group with the identity e. We denote the resulting group by $\coprod_{i \in I} G_i$. Now there are natural monomorphisms

$$j_k \colon G_k \to \coprod_{i \in I} G_i .$$

Then the group $\coprod_{i \in I} G_i$ *together with the monomorphisms* j_k *form a coproduct (or free product) of the family* $\{G_i\}_{i \in I}$. In fact, if G is a group and $f_k \colon G_k \to G$ are group homomorphisms then there is an obvious homomorphism

$$f \colon \coprod_{i \in I} G_i \longrightarrow G$$

making the diagram

$$\begin{array}{ccc} G_k & \xrightarrow{j_k} & \coprod_{i \in I} G_i \\ & {\scriptstyle f_k} \searrow \quad \swarrow {\scriptstyle f} & \\ & G & \end{array}$$

commutative. Clearly such f is uniquely determined.

In the category of abelian groups the coproduct of a family $\{A_i\}$ becomes the direct sum $\oplus A_i$ (Ex.7).

(2.1.9) (Free group) Let X be a nonempty set. Consider the set of the following type of symbols, called the *words*

(i) 1,

(ii) $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ where $x_i \in X$ and i_k is either +1 or -1, and x and x^{-1} are not adjacent.

To multiply these symbols, we juxtapose two such words and reduce it by canceling the expression xx^{-1}. The symbol 1 plays the role of the identity. In this way we get a group denoted by $F(X)$, and is called the *free group on X. The group $F(X)$ is the free object on the set X in the category of groups.* To see this let G be a group and $f\colon X \to G$ be a map (of sets). Now there is a unique group homomorphism $f'\colon F(X) \to G$ so that $i \circ f' = f$ where $i\colon X \to F(X)$ is the inclusion.

(2.1.10) (Group presentation) Let G be a group and X be a subset of G. Let $\langle X\rangle$ be the subgroup of G generated by X i.e., $\langle X\rangle$ is the smallest subgroup of G containing X. Let $F(X)$ be the free group on X where X is a generating set of G. Then we have a surjective group homomorphism $\phi\colon F(X) \to G$. The kernel N of ϕ is a normal subgroup of $F(X)$ and we have $F(X)/N \cong G$. *Hence every group is a quotient of a free group.*

Now suppose G is *finitely generated* i.e., there is a finite subset $X = \{x_1, \ldots, x_n\}$ such that $\langle X\rangle = G$. If G is finitely generated and if $N = \mathrm{Ker}(\phi)$ is also finitely generated, say $N = \langle r_1, \ldots, r_m\rangle$ then we say that G is *finitely presented.* We may say then that G is generated by $x_1, \ldots, x_n$ with the relations $r_1, \ldots, r_m$ or the group G has the presentation;

$$G = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_m\rangle.$$

For example, the cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n has a presentation

$$\langle x \mid x^n = e\rangle,$$

and the *dihedral group* D_n of degree n has the presentation

$$D_n = \langle x, y \mid x^n = e,\ y^2 = e,\ yx = x^{-1}y\rangle.$$

with its order $2n$. The *quaternion group* Q (of order 8) has a presentation (Cf. Ex.15)

$$Q = \langle x, y \mid x^4 = e,\ y^2 = x^2,\ yxy^{-1} = x^{-1} \rangle.$$

(2.1.11) (Amalgamated sum) Let $\lambda_i \colon H \to G_i (i = 1, 2)$ be group homomorphisms. The *amalgamated sum of* G_1 *and* G_2 *over* H which is denoted by $G_1 \coprod_H G_2$, is the quotient $(G_1 \coprod G_2)/N$ where N is the normal subgroup of $G_1 \coprod G_2$ generated by

$$\{\lambda_1(h)\lambda_2(h^{-1}) \mid h \in H\}.$$

Let α_i be the composition of the maps

$$\alpha_i : G_i \to G_1 \coprod G_2 \to G_1 \coprod_H G_2.$$

Then

is a *push-out diagram* i.e., for any $f_i \colon G_i \to K\, (i = 1, 2)$ such that $f_1 \circ \lambda_1 = f_2 \circ \lambda_2$ there is a unique group homomorphism $f \colon G_1 \coprod_H G_2 \to K$ such that $f \circ \alpha_i = f_i (i = 1, 2)$. Note that if H is trivial then $G_1 \coprod_H G_2 = G_1 \coprod G_2$.

(2.1.12) (Direct limit) Let I be a set of indices with a partial ordering $\leq$. Suppose $\{A_i\}_{i \in I}$ is a family of abelian groups and suppose, whenever $i \leq j$, there are homomorphisms of abelian groups

$$f_j^i \colon A_i \longrightarrow A_j$$

with compatibility conditions

$$f_k^j \circ f_j^i = f_k^i \ (i \le j \le k) \ \text{ and } \ f_i^i = \mathrm{id}.$$

We call such a family $\{A_i, f_j^i\}$ an *inductive* (*direct*) system. Let M be the subgroup of $\underset{i\in I}{\oplus} A_i$ which is generated by

$$\{a_i - f_j^i(a_i) \mid a_i \in A_i, i \le j\}.$$

The abelian group $(\oplus A_i)/M$ is called the *direct* (*inductive*) *limit* of $\{A_i\}_{i\in I}$ and is denoted by $\varinjlim_{i\in I} A_i$. The natural maps

$$f_i \colon A_i \longrightarrow \varinjlim_{i\in I} A_i$$

obtained by composing the maps $A_i \to \oplus A_i \to \oplus A_i/M$ satisfy

$$f_j \circ f_j^i = f_i.$$

The direct limit has the following universal property: Let B be an abelian group and $g_i \colon A_i \to B$ be homomorphisms such that

$$g_j \circ f_j^i = g_i \text{ whenever } i \le j.$$

Then there exists a unique map $g \colon \varinjlim_{i\in I} A_i \to B$ such that $g \circ f_i = g_i$.

Further this universal property characterizes the direct limit $\varinjlim A_i$.

Note that for $a_i \in A_i$, and $a_j \in A_j$ we have $f_i(a_i) = f_j(a_j)$ if and only if there is $k \in I$ such that $k \ge i, k \ge j$ and $f_k^i(a_i) = f_k^j(a_j)$ in A_k.

Let $\{B_i, g_j^i\}$ be another inductive system. Suppose $\{\phi_i : A_i \to B_i\}$ be a morphism of inductive systems i.e., $g_j^i \circ \phi_i = \phi_j \circ f_j^i$. Then the family $\{\phi_i\}$ induces a group homomorphism

$$\varinjlim_{i\in I}\phi_i : \varinjlim_{i\in I} A_i \longrightarrow \varinjlim_{i\in I} B_i.$$

For example, if $\{A_i\}(i = 1, 2, \ldots.)$ are increasing sequence of subgroups of an abelian group A then $\varinjlim A_i = \cup A_i$. And if I has the largest member m then we have $\varinjlim A_i = A_m$.

For another example, let $\mathcal{U}$ be the set of all open sets of $\mathbb{C}$ containing 0 and define a partial ordering on $\mathcal{U}$ by $U \leq V$ if and only if $V \subseteq U$. For $U \in \mathcal{U}$ let $\mathcal{O}_U$ be the set of all analytic functions on U. Then an element of $\mathcal{O} = \varinjlim_{U\in\mathcal{U}} \mathcal{O}_U$ is represented by $f \in \mathcal{O}_U$ for some $U \in \mathcal{U}$ and, any two $f \in \mathcal{O}_U$ and $g \in \mathcal{O}_V$ are identified if and only if there is $W \in \mathcal{U}$ such that $W \subseteq U \cap V$ and $f|_W = g|_W$. The ring $\mathcal{O}$ becomes a "discrete valuation ring" which we call the *germs of analytic functions* at 0. (See (3.4.8).)

(2.1.13) (Inverse limit) Inverse limit is dual to the notion of direct limit. Let I be a set of indices with a partial ordering $\leq$. Suppose $\{A_i\}_{i\in I}$ is a family of abelian groups and suppose, whenever $i \leq j$, there are homomorphisms of abelian groups

$$f_i^j : A_j \longrightarrow A_i$$

with compatibility conditions

$$f_k^i \circ f_i^j = f_k^j \ (i \leq j \leq k) \quad \text{and} \quad f_i^i = \mathrm{id}.$$

Such a family $\{A_i, f_i^j\}$ is called an *inverse* (*projective*) system. The *inverse* (*projective*) *limit* of the family $\{A_i\}_{i\in I}$ is defined to be

$$\varprojlim_{i\in I} A_i = \{(x_i)_{i\in I} \in \prod_{i\in I} A_i \mid f_i^j(x_j) = x_i \text{ for all } \ i \leq j\}.$$

The maps

$$f_j : \varprojlim A_i \longrightarrow A_j$$

induced by the k-th projection satisfy,

$$f_i^j \circ f_j = f_i \text{ whenever } i \leq j.$$

As in the direct case the inverse limit can be characterized by the following universal property: Let B be an abelian group and $g_i \colon B \to A_i$ be homomorphisms such that

$$f_i^j \circ g_j = g_i \text{ whenever } i \leq j.$$

Then there exists a unique map $g \colon B \longrightarrow \varprojlim_{i \in I} A_i$ such that $f_i \circ g = g_i$.

Let $\{B_i, g_j^i\}$ be another inverse system. Suppose $\{\phi_i : A_i \to B_i\}$ be a morphism of inverse systems i.e., $g_i^j \circ \phi_j = \phi_i \circ f_i^j$. Then the family $\{\phi_i\}$ induces a group homomorphism

$$\varprojlim_{i \in I} \phi_i : \varprojlim_{i \in I} A_i \longrightarrow \varprojlim_{i \in I} B_i.$$

Consider a rather special case. Let R be a commutative ring and I be an ideal. We have the natural maps

$$R/I \xleftarrow{\phi_1} R/I^2 \xleftarrow{\phi_2} R/I^3 \xleftarrow{\phi_3} \cdots$$

Then

$$\varprojlim_n R/I^n = \{(x_1, x_2, \dots) \in \textstyle\prod_{n \geq 1} R/I^n \mid x_{n-1} = \phi_n(x_n) \text{ for all } n > 1\}.$$

We sometimes call $\varprojlim_n R/I^n$ the *completion* of R with respect to the ideal I.

When $R = \mathbb{Z},\ I = (p)$ where p is a prime, then $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is denoted by $\hat{\mathbb{Z}}_p$ and is called the ring of *p-adic integers.*[†] It turns out that $\hat{\mathbb{Z}}_p$ is a "complete local" ring with a unique nonzero prime (principal) ideal generated by $\phi(p)$.

If $\{A_i\}$ is a family of subgroups of an abelian group then $\varprojlim A_i = \cap A_i$. For more about limits see Appendix.

Exercises 2.1

1. Let H and K be two subgroups of G.
   (i) If H, K are finite then we have
   $$|HK| = o(H)o(K)/o(H \cap K).$$
   (ii) The subset HK is a subgroup if and only if $HK = KH$.
   (iii) The subset of the form HgK is called a *double coset.* Show that G is a disjoint union of double cosets. The set of all double cosets is denoted by $H\backslash G/K$.
2. Let G be a finite group and H be a proper subgroup. Then $\underset{g\in G}{\cup} gHg^{-1} \neq G$. (Hint : The number of elements of $\cup gHg^{-1} < o(G)$.)
3. Prove the following statements.
   (i) In (2.1.2)(*) show that $G_3 \cong G_2/\mathrm{Im}(f_1)$.
   (ii) If H, N are subgroups of G and N is normal then we have an exact sequence
   $$(e) \longrightarrow H \cap N \longrightarrow H \longrightarrow NH/N \longrightarrow (e)$$
   so that we have an isomorphism $H/N \cap H \cong NH/N$.
   (iii) If $N_1 \subseteq N_2$ are normal subgroups of G then
   $$(e) \longrightarrow N_2/N_1 \longrightarrow G/N_1 \longrightarrow G/N_2 \longrightarrow (e)$$
   is an exact sequence so that we have an isomorphism $G/N_2 \cong (G/N_1)/(N_2/N_1)$.

[†]Usual notation for the ring of p-adic integers is $\mathbb{Z}_p$ but we reserve it for a localization (3.2.4).

4. Show that D_4 and $\mathfrak{S}_3$ are semidirect products of their proper subgroups.
5. The group of invertible upper triangular matrix (under multiplication) of size n is a semidirect product of the group of diagonal matrices and the group of upper triangular matrices with 1's on the diagonal.
6. A group G is a direct product of N and H if and only if an extension

$$(e) \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \to (e)$$

has a *retraction* $r\colon G \to N$ (i.e., r is a group homomorphism such that $r \circ \iota = \mathrm{id}_N$).
7. In the category of abelian groups show that the coproduct of a family $\{A_i\}$ becomes the direct sum $\oplus A_i$.
8. Prove the following statements.
   (i) There is a surjection $G_1 \coprod G_2 \to G_1 \times G_2$.
   (ii) $G_1 \coprod G_2 \cong G_2 \coprod G_1$.
   (iii) If N is a normal subgroup of $G_1 \coprod G_2$ generated by G_1 then $(G_1 \coprod G_2)/N \cong G_2$.
   (iv) If $f_i\colon G_i \to H_i$ $(i = 1, 2)$ are group homomorphisms then there is a group homomorphism

$$f_1 \coprod f_2\colon G_1 \coprod G_2 \longrightarrow H_1 \coprod H_2.$$

   (v) Prove $\mathbb{Z}/2 \coprod \mathbb{Z}/3 = \langle a, b \mid a^2 = b^3 = e\rangle$. Also show that this group is isomorphic to $\mathrm{SL}(2, \mathbb{Z})/(\pm I)$. (Hint: Let $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and send a to S and b to ST.)
9. Let $G = G_1 \coprod_H G_2$.
   (i) Show G is finitely generated if G_1 and G_2 are finitely generated.
   (ii) If G_1, G_2 are finitely generated then G is finitely presented if and only if H is finitely presented.
10. Prove:
    (i) Show that a finite group is finitely presented.
    (ii) Construct a subgroup of the free group on two generators which is not finitely generated.
11. Let G be free a group on a set X.

(i) If G is also free on a set Y then X and Y has the same cardinality. The common cardinality is called the *rank*.

(ii) The free group on one generator is isomorphic to the infinite cyclic group $\mathbb{Z}$.

(iii) If G is a free group is of rank ≥ 2 then G has a free subgroup of any finite rank.

12. Prove that a group G is free if and only if for every short exact sequence

$$(e) \longrightarrow H \longrightarrow E \longrightarrow G \longrightarrow (e)$$

there is a section $s : G \to E$.

13. Prove:

(i) The group $\langle x, y \,|\, x^2 = y^3 = (xy)^2 = e\rangle$ is isomorphic to $\mathfrak{S}_3$.

(ii) The group $\langle x, y \,|\, x^3 = y^2 = (xy)^3 = e\rangle$ is isomorphic to A_4.

14. The quaternion group Q (2.1.12) is isomorphic to the group $\{\pm 1, \pm i, \pm j, \pm k\}$ with the relations $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$. What is the center of Q ? Every subgroup of Q is normal. The quaternion group Q is not isomorphic to D_4.

15. Let $G_{m,n,r,s}$ be the group defined by the presentation

$$G_{m,n,r,s} = \langle x, y \,|\, x^m = e,\ y^n = x^r,\ yxy^{-1} = x^s\rangle$$

where m, n are nonnegative integers and r, s are arbitrary integers such that $m, r(s-1)$ and $s^n - 1$ are not all zero. Let $d = \gcd\{m,\ |r(s-1)|,\ |s^n - 1|\}$. Then the order of $G_{m,n,r,s}$ is dn. Also show that the subgroup N generated by x is normal and find $o(N)$.

16. With the notations of (1.2.5), show that the pullback is given by

$$A \times_C B = \{(a, b) \mid f(a) = g(a)\}$$

in the category of groups. In the category of abelian groups the push out is given by

$$X = A \times B/\{(f(a), -g(a)) \mid a \in A\}.$$

17. Prove:

(i) There is a natural injection $\phi\colon \mathbb{Z} \to \hat{\mathbb{Z}}_p$.

(ii) $(x_0, x_1, \dots) \in \hat{\mathbb{Z}}_p$ is a unit if and only if $x_0 \neq 0$.

(iii) $\hat{\mathbb{Z}}_p$ is a local ring with a unique nonzero prime (principal) ideal generated by $\phi(p)$.

18. Prove that $\varprojlim_n R[X]/(X^n) \cong R[[X]]$.
19. If $\{A_i\}$ is a family of subgroups of an abelian group then $\varprojlim A_i = \cap A_i$.
20. Let $\hat{\mathbb{Q}}_p$ be the quotient field of $\hat{\mathbb{Z}}_p$. Prove that $\varinjlim \mathbb{Z}/p^n\mathbb{Z} \cong \hat{\mathbb{Q}}_p/\hat{\mathbb{Z}}_p$.
21. Prove $\varprojlim\{\mathbb{Z}/n\mathbb{Z} : \text{ all positive integer } n\} \cong \prod_{\text{all prime } p} \hat{\mathbb{Z}}_p$

2.2 Structure of groups

(2.2.1) (Free abelian groups) An abelian group G is said to be *free* (resp. *finitely generated free* if G is isomorphic to a direct sum (resp. finite direct sum) of copies of $\mathbb{Z}$. We will deal with the finitely generated case for clarity even though sometimes the arguments goes through for the infinite case also.

Let G be the additive group $\mathbb{Z}^n$ (the n-copies of $\mathbb{Z}$). Suppose G is also isomorphic to $\mathbb{Z}^m$ for some m, say $\phi\colon \mathbb{Z}^n \to \mathbb{Z}^m$ is an isomorphism. Reduce the isomorphism ϕ modulo a prime p to get the isomorphism $\bar{\phi}\colon (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^m$ of vector spaces over the finite field $\mathbb{Z}/p$. From the linear algebra we see that $n = m$. The uniquely determined integer n is called the *rank* of the free abelian group G.

The group $\mathbb{Z}^n$ is generated by $e_i = (0, \ldots, 1, \ldots, 0)$ $(i = 1, 2, \ldots, n)$ where 1 is in the i-th place and 0 elsewhere. These are linearly independent over $\mathbb{Z}$ i.e., if $\sum n_i e_i = 0$ with $n_i \in \mathbb{Z}$ then we have $n_i = 0$ for all i. A linearly independent set of an abelian group which generates G is called a *basis* of G. Hence we showed that $\mathbb{Z}^n$ has a basis $\{e_1, \ldots, e_n\}$. Conversely if $X = \{x_1, \ldots, x_n\}$ is a basis of an abelian group G then G is isomorphic to $\mathbb{Z}^n$, an isomorphism being given by sending x_i to e_i. Hence an abelian group is free if and only if it has a basis. Since the cardinality of a basis is uniquely determined, a free abelian group is uniquely determined by its rank up to an isomorphism.

A free abelian group G is a free object on its basis $X = \{x_1, \ldots, x_n\}$ in the sense of (1.2.4). In fact, let H be an abelian group and $f\colon X \to H$ be a map (of sets) such that $f(x_i) = h_i$.

$$\begin{array}{ccc} X = \{x_1, \ldots, x_n\} & \to & G \\ & f \searrow \quad \swarrow \bar{f} & \\ & H & \end{array}$$

Then we define $\bar{f}\colon G \to H$ by $\bar{f}(x_i) = h_i$ and extend it by using $\mathbb{Z}$-linearity.

(2.2.2) Let G be an (additive) abelian group with the identity element 0. An element $g \in G$ is said to be *torsion* if there is an integer n such that $ng = 0$. We say that G is a *torsion group* if every element of G is torsion; G is *torsion free* if every non-zero element of G is not a torsion. Define

$$G_\tau = \{g \in G \mid g \text{ is torsion}\}.$$

Then G_τ is a torsion group, and G/G_τ is torsion free. We have an exact sequence

$$(0) \longrightarrow G_\tau \longrightarrow G \longrightarrow G/G_\tau \longrightarrow (0)$$

where G_τ is a torsion group and G/G_τ is torsion free.

(2.2.3) *Let G, G_1 and G_2 be abelian groups. Then the following conditions are equivalent.*

(i) $G \cong G_1 \oplus G_2$.

(ii) *We have an exact sequence*

$$(*) \qquad (0) \longrightarrow G_1 \xrightarrow{\iota} G \xrightarrow{\pi} G_2 \longrightarrow (0)$$

and there is a group homomorphism $s\colon G_2 \to G$ (called a *section*) *such that $\pi \circ s = \mathrm{id}$*, i.e., *the above exact sequence splits.*

(iii) *We have an exact sequence* (*) *of* (ii) *and a group homomorphism $r\colon G \to G_1$* (called a *retraction*) *such that $r \circ \iota = \mathrm{id}$.*

(iv) *There are endomorphisms $\phi_i\colon G \to G$ $(i = 1, 2)$ such that*

$$\mathrm{Im}(\phi_i) = G_i, \phi_1 + \phi_2 = \mathrm{id}_G \quad \text{and} \quad \phi_i \circ \phi_j = \delta_{ij}\phi_j$$

where δ_{ij} is the Kronecker delta.

Furthermore, if G_2 is a free abelian group in (*) *of* (ii) *then the exact sequence splits.*

(See Ex. 1 for further equivalent conditions.)

Proof. (i) $\Rightarrow$ (ii) By identifying G with $G_1 \oplus G_2$ we choose ι to be the inclusion of G_1 into G and π be the projection to the second factor. Now define $s(x) = (0, x)$.

(ii) $\Rightarrow$ (iii) Let $x \in G$. Then $x - s \circ \pi(x)$ is in the kernel of π which is the same as the image of ι. Since ι is injective, there is a unique $y \in G_1$ such that $\iota(y) = x - s \circ \pi(x)$. Now define $r(x) = y$. Now one checks that $r \circ \iota = \mathrm{id}$.

(iii) $\Rightarrow$ (i) Define a map $G \to G_1 \oplus G_2$ by sending an element x of G to $(r(x), \pi(x))$. For the inverse of this map let $(a, b) \in G_1 \oplus G_2$ and let $b' \in G$ be such that $\pi(b') = b$. Now map (a, b) to $\iota(a) + b' - \iota \circ r(b')$. One checks that these maps are inverses to each other.

(i) $\Rightarrow$ (iv) Let ϕ_i be the composition $G \overset{proj.}{\longrightarrow} G_i \overset{incl.}{\longrightarrow} G$. Now it is easy to check (iv).

(iv)$\Rightarrow$ (i) Exercise.

For the last part, let $\{z_i\}$ be a free basis of G_2 and x_i be a lift of z_i in G. Then there must be a torsion free element in the coset $x_i + G_1$ in G, say $\bar{x}_i$ (otherwise $\pi(x_i) = z_i$ must be a torsion). Hence we can define the map s by requiring $s(z_i) = \bar{x}_i$.

We remark here that if the groups are non-abelian then the results above are false. For example, consider a semidirect product $N \times_\phi H$. We have an exact sequence

$$(e) \longrightarrow N \overset{\iota}{\longrightarrow} N \times_\phi H \overset{\pi}{\longrightarrow} H \longrightarrow (e).$$

There is a section $s\colon H \to N \times_\phi H$ defined by $s(h) = (0, h)$. However, $N \times_\phi H$ is not isomorphic to the direct sum $N \oplus H$ unless ϕ is trivial. Cf. Ex.2.1.6.

(2.2.4) *A subgroup H of a free abelian group G of rank n is free of rank $\leq n$. A finitely generated torsion free abelian group is free.*

Proof. We induct on n. The result for $n = 1$ is well known. (A subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer n and it is isomorphic to $\mathbb{Z}$.) Let $G = \overset{n}{\underset{i=1}{\oplus}} \mathbb{Z}x_i$ $(n > 1)$. Consider

the projection $f : G \to \mathbb{Z}x_1$ sending $\sum n_i x_i$ to $n_1 x_1$. Let H_1 be the kernel of $f\,|_H$. Then H_1 is a subgroup of $\mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n$. By induction on rank, H_1 is free of rank $\leq n-1$. Now $f(H)$ is either 0 or infinite cyclic. We have an exact sequence,

$$(0) \longrightarrow H_1 \longrightarrow H \longrightarrow f(H) \longrightarrow (0),$$

with $f(H)$ free of rank 1 or 0. Hence $H \cong H_1 \oplus f(H)$ (2.2.3). Hence H is free of rank $\leq n$.

For the second statement, let $S = \{x_1, \ldots, x_n\}$ be a maximal $\mathbb{Z}$-linear independent subset of G. Let H be the subgroup of G generated by S. Then H is free (exercise). If $y \in G$, then $\{y, x_1, \ldots, x_n\}$ is linearly dependent. Hence there are integers m's not all zero such that

$$my + m_1 x_1 + \cdots + m_n x_n = 0.$$

Hence my lies in H. Since this is true for a finite set of generators of G, there is a nonzero integer k such that $kG \subseteq H$. Since the map sending x to kx is a monomorphism, we see that G is isomorphic to $kG = \{kg \mid g \in G\}$. The group kG, being a subgroup of H, is free. Since the multiplication-by-k map is an isomorphism between G and kG we conclude that G is free.

(2.2.5) *Throughout this subsection G is a finite abelian group.* Let G be a finite abelian group of order n, and let $n = rs$ where r and s are relatively prime. Then there are integers a and b such that $ra + sb = 1$. Therefore, $G = raG + sbG \subseteq rG + sG \subseteq G$. Hence we have equalities everywhere. On the other hand, if $g \in rG \cap sG$ then $sg = rg = 0$. Hence $g = rag + sbg = 0$. And therefore $G = rG \oplus sG$.

For a nonnegative integer k let

$$G_k = \{g \in G \mid kg = 0\}.$$

Then since $rsG = nG = 0$, we have $sG \subseteq G_r$. Conversely, if $g \in G_r$ then $g = rag + sbg = sbg$. Therefore $sG = G_r$. Similarly we have $rG = G_s$. Hence $G = G_r \oplus G_s$, by Ex.1

Summing up we have proved that *if G is an abelian group of order $n = rs$ where r and s are relatively prime, then*

$$G = G_r \oplus G_s. \tag{1}$$

Hence if G is an abelian group of order $p_1^{r_1} \cdots p_t^{r_t}$ then

$$G = G_{p_1^{r_1}} \oplus \cdots \oplus G_{p_t^{r_t}}. \tag{1'}$$

In particular, $\mathbb{Z}/mn \cong \mathbb{Z}/n \oplus \mathbb{Z}/m$ for relatively prime integers m and n.

Let p be a prime and define

$$G(p) = \{g \in G \mid p^n g = 0 \text{ for some } n\}$$

which we call the *p-primary* part of G. If G is finite then $G(p)$ is of prime power order i.e., a *p-group*. Now it is easy to show that $G(p_i) = G_{p_i^{r_i}}$. Therefore *if G is an abelian group of order $n = p_1^{r_1} \cdots p_t^{r_t}$ then G is isomorphic to the direct sum of its primary parts*

$$G \cong G(p_1) \oplus \cdots \oplus G(p_t) \tag{2}$$

with each $G(p_i)$ a p_i-group.

(2.2.6) *A finite abelian p-group G is isomorphic to a product of cyclic p-groups* i.e., *G is isomorphic to*

$$\mathbb{Z}/p^{r_1} \oplus \cdots \oplus \mathbb{Z}/p^{r_n},$$

where $r_1 \geq r_2 \geq \cdots \geq r_n$, and the sequence of integers $(r_1, \ldots, r_n)$ is uniquely determined.

Proof. Let $x_1 \in G$ be an element of maximal order, say p^{r_1}. Let G_1 be the cyclic subgroup of G generated by x_1. Then, by induction, we see that

$$G/G_1 \cong \bar{G}_2 \oplus \cdots \oplus \bar{G}_n \tag{*}$$

where $\bar{G}_i$ are cyclic of order p^{r_i} generated by $\bar{x}_i$ and $r_2 \geq \cdots \geq r_n$. Now there is an element $x_i \in G$ which represents $\bar{x}_i$ and is of order p^{r_i}. To see this we may assume $n = 2$ by induction. Let x_2' be a lift of $\bar{x}_2$ in G. Then $p^{r_2} x_2' \in G_1$ and $p^{r_1} x_2' = 0$ by maximality of (p-power) p^{r_1}. Since G_1 is cyclic of order p^{r_1} with $r_1 \geq r_2$, we see $p^{r_2} x_2' \in \mathrm{Ker}(G_1 \xrightarrow{p^{r_1 - r_2}} G_1)$ $= \mathrm{Im}(G_1 \xrightarrow{p^{r_2}} G_1)$. Hence there is $z \in G_1$ such that $p^{r_2} x_2' = p^{r_2} z$. Then $x_2 = x_2' - z$ will represent $\bar{x}_2$ with precise order p^{r_2}.

Let G_i be the cyclic subgroup of G generated by x_i. Now we will show that $G \cong G_1 \oplus \cdots \oplus G_n$ by using Ex.1. In fact, if $x \in G$ then $\bar{x} = m_2\bar{x}_2 + \cdots + m_n\bar{x}_n$ for some integers $m_2, \ldots, m_n$. Hence $x - m_2x_2 - \cdots - m_nx_n$ is in G_1. Therefore we can find m_1 such that $x = m_1x_1 + \cdots + m_nx_n$; G is generated by $x_1, \ldots, x_n$. Now we need to show that $(G_1 + \cdots + G_i) \cap G_{i+1} = (0)$. Let $x \in (G_1 + \cdots + G_i) \cap G_{i+1}$. Then we can write

$$x = m_1x_1 + \cdots + m_ix_i = -m_{i+1}x_{i+1}$$

with $m_j < p^{r_j}$ $(j = 1, 2, \ldots, i+1)$. Taking bar, we see that $m_2 = \cdots = m_{i+1} = 0$ by (*). This in turn implies that $m_1 = 0$ also. Hence all m_j's are zero.

We leave the proof of uniqueness of $(r_1, \ldots, r_n)$ as an exercise.

(2.2.7) Let G be a finite abelian group. Then by (2.2.6) above, we have

$$G \cong G(p_1) \oplus \cdots \oplus G(p_n), \quad \text{where} \quad G(p_i) \cong \mathbb{Z}/p_i^{e_{i_1}} \oplus \cdots \oplus \mathbb{Z}/p_i^{e_{i_s}}, \tag{1}$$

where p's are primes and e's are positive integers such that $e_{i_1} \geq \cdots \geq e_{i_s}$.

Now using the fact that $\mathbb{Z}/mn \cong \mathbb{Z}/n \oplus \mathbb{Z}/m$ for relatively prime integers m and n, we see that (by collecting the terms of different primes) G is isomorphic to a direct sum of the cyclic group of the type $\mathbb{Z}/p_1^{e_1} \cdots p_n^{e_n}$. For example,

$$\mathbb{Z}/2^3 \times \mathbb{Z}/2^2 \times \mathbb{Z}/2 \times \mathbb{Z}/3^5 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \cong \mathbb{Z}/2^2 3^5 5 \times \mathbb{Z}/2^2 3 \times \mathbb{Z}/2.$$

Here the first factor on the right hand side is the product of the terms of the highest prime power from each prime and the second factor is the product of the factors of the next highest prime power orders etc.

Hence we conclude that *if G is a finite abelian group then there is a unique sequence of integers $(m_1, \ldots, m_r)$ such that*

$$G \cong \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r \tag{2}$$

with $m_r \mid m_{r-1} \mid \cdots \mid m_1$. The sequence $(m_1, \ldots, m_r)$ is called the *invariants* of the finite abelian group G.

As an exercise find all isomorphism classes of abelian group of order $2^3 3^3 5^2$.

(2.2.8) (Jordan-Hölder Theorem) Let G be a group. A (finite) sequence of subgroups

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = (e)$$

is called a *composition series* if G_{i+1} is normal in G_i and G_i/G_{i+1} is *simple* (i.e., it has no nontrivial normal subgroup). A group may or may not have a composition series; for example $\mathbb{Z}$ has no composition series for any nonzero subgroup of $\mathbb{Z}$ contains an infinite descending chain of subgroups.

Let

$$G = H_1 \supseteq H_2 \cdots \supseteq H_m = (e)$$

be another composition series of G. We say that they are *equivalent* if $m = n$ and $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$ for some permutation σ of $\{1, 2, \ldots, n\}$. Jordan-Hö1der theorem asserts that *if a group G has a composition series then any two of the composition series are equivalent.* For a proof we refer to any algebra text. As an exercise find two composition series of the group $\mathbb{Z}/3^2 5^3$ and show that they are equivalent.

(2.2.9) *Let G be a finite group.*

(i) *If p is a prime number dividing the order of G then G has a subgroup of order p.*

(ii) (Sylow Theorem) *Let p^n be the highest power of p dividing the order of G. Then there is a subgroup of order p^n in G* which we call a *p-Sylow subgroup.*

Proof. (i) Recall the class formula (2.1.4)(2)

$$o(G) = o(Z(G)) + \sum [G, I_x].$$

If $p | o(Z(G))$ then we can find a subgroup of $Z(G)$ of order p by the classification of finite abelian groups (2.2.7). Now suppose $p \nmid o(Z(G))$. Since $p | o(G)$ we must have $p \nmid [G : I_x]$ for some x by the class formula (2.1.4). Hence $p | o(I_x)$ and $o(I_x) < o(G)$. By induction I_x has a subgroup of order p which completes the proof.

(ii) If $o(G) = p$, then there is nothing to prove. If there is a subgroup H whose index is prime to p, then $p^n | o(H)$. Hence, by induction, H (hence G) has a subgroup of order p^n.

Therefore we may assume that every subgroup has an index divisible by p. From the class formula we have $p | o(Z(G))$ since $p | [G, I_x]$. Let a be an element of $Z(G)$ whose order is p (2.2.7), and let H be the subgroup generated by a. Then H is normal in G, since H is contained in the center. Let $f : G \to G/H$ be the canonical map. Then $p^{n-1} | o(G/H)$. By induction there is a subgroup K of G/H of order p^{n-1}. Now the subgroup $f^{-1}(K)$ of G has order p^n.

(2.2.10) (Sylow Theorems) *Let G be a finite group.*

(i) *If H is a p-group then H is contained in a p-Sylow subgroup.*

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

(iii) *The number of p-Sylow subgroups is congruent to 1 modulo p and divides the order of G.*

Proof. (i) Let $\mathcal{S}$ be the set of all p-Sylow subgroups of G and $P \in \mathcal{S}$. We let G act on $\mathcal{S}$ *via* conjugation (note that a conjugation of a p-Sylow subgroup is again a p-Sylow)

$$G \times \mathcal{S} \longrightarrow \mathcal{S}.$$
$$(g, Q) \mapsto gQg^{-1}$$

Then the isotropy group I_P contains P. Let $\mathcal{S}_0$ be the orbit of P. Then by the maximality (of p-power) of P the cardinality of $\mathcal{S}_0$ is prime to p (since $|\mathcal{S}_0| = [G : I_P]$ and $P \subseteq I_P$). We let H act on $\mathcal{S}_0$ *via* conjugation;

$$H \times \mathcal{S}_0 \to \mathcal{S}_0.$$

Since $\mathcal{S}_0$ is a disjoint union of H-orbits, and since the index of a proper subgroup of H is divisible by p, at least one of H-orbit contains exactly one element, say P'. Hence $H \subseteq N(P')$.

Now we contend that $H \subseteq P'$. In fact, since P' is normal in $N(P'), HP'$ is a subgroup (of $N(P')$) and P' is normal in HP'. We have an isomorphism (Ex.(2.1.3)),

$$HP'/P' \xrightarrow{\cong} H/H \cap P'.$$

Hence the order of HP' is a power of p. Now the maximality of P' implies that $P' = HP'$. Therefore $H \subseteq P'$.

(ii) In the proof of (i), we let H be one of p-Sylow subgroups. Then $H \subseteq P'$ which belongs to the orbit $\mathcal{S}_0$ of P. Since both are maximal p-subgroups, we have $H = P'$. Hence they are conjugate.

(iii) In the proof of (i), we let $H = P$. Then exactly one H-orbit of $\mathcal{S}_0$ contains single element, namely P. In fact, obviously the orbit of $P \in \mathcal{S}_0$ is $\{P\}$. On the other hand, if $Q \in \mathcal{S}_0$ has a single orbit then as in the proof of (i) above we see $P \subseteq Q$. Thus $P = Q$ by the maximality of p-power order.

Hence we conclude that the number of conjugates of P is congruent to 1 modulo p. Finally, since the number of conjugates is $|\mathcal{S}_0| = [G : I_P]$, it divides the order of G.

(2.2.11) (Groups of order *pq*) *Let G be a group of order pq where p, q are primes with $p > q$.*

(i) *If $q \nmid (p-1)$ then G is isomorphic to $\mathbb{Z}/pq$.*

(ii) *If $q|(p-1)$ then G is isomorphic to either $\mathbb{Z}/pq$ or*

$$\langle a, b \mid a^p = e, b^q = e, ba = a^s b \rangle$$

where $s \not\equiv 1 (\bmod p)$ and $s^q \equiv 1 (\bmod p)$.

Proof. Let A, B be subgroups of order p and q respectively. Then A and B are isomorphic to $\mathbb{Z}/p$ and $\mathbb{Z}/q$. Further, A is normal subgroup of G (Ex.18). One checks that $A \cap B = (e)$ and $AB = G$. Hence G is a semidirect product $A \times_\phi B$ for some $\phi\colon B \to \mathrm{Aut}(A)$ (2.1.6). The group $\mathrm{Aut}(A)$ is isomorphic to the group of units $(\mathbb{Z}/p)^*$ of $(\mathbb{Z}/p)$ which is cyclic of order $(p-1)$.

(i) If $q \nmid (p-1)$ then there is no nontrivial group homomorphism ϕ since B is cyclic of prime order ϕ must be injective unless ϕ is trivial. Hence we have

$$G \cong A \oplus B \cong \mathbb{Z}/p \oplus \mathbb{Z}/q \cong \mathbb{Z}/pq.$$

(ii) Now suppose $q|(p-1)$. If ϕ is a trivial homomorphism then G is isomorphic to $\mathbb{Z}/pq$ as in (i) above.

If ϕ is nontrivial then ϕ is determined by $\phi(1) = s$ in $(\mathbb{Z}/p)^*$. Since ϕ is nontrivial and since $\phi(q)$ must be the identity we have

$$s \not\equiv 1(\bmod p) \quad \text{and} \quad s^q \equiv 1(\bmod p).$$

Now G is generated by $a = (1,0)$ and $b = (0,1)$ and their orders are p and q respectively i.e., $a^p = e$ and $b^q = e$. Denoting the group operation in $A \times_\phi B$ by $\circ$, we compute,

$$b \circ a = (0,1) \circ (1,0) = (0 + 1^{\phi(1)}, 1) = (s,0) \circ (0,1) = a^s \circ b.$$

(2.2.12) Let G be a group, and H_1 and H_2 be two subgroups of G. We define $[H_1, H_2]$ be the subgroup of G generated by the elements of the form

$$h_1 h_2 h_1^{-1} h_2^{-1} \quad \text{where} \quad h_1 \in H_1 \quad \text{and} \quad h_2 \in H_2.$$

We define the subgroups $D^i(G)$ and $C^i(G)$ as follows;

$$D^1(G) = C^1(G) = [G, G]\,;$$
$$D^i(G) = [D^{i-1}(G), D^{i-1}(G)] \quad \text{and} \quad C^i(G) = [G, C^{i-1}(G)].$$

Both $D^i(G)$ and $C^i(G)$ are normal subgroups of G (Ex.14). We have the descending chain of subgroups,

$$D^1(G) \supseteq D^2(G) \supseteq D^3(G) \supseteq \cdots,$$
$$C^1(G) \supseteq C^2(G) \supseteq C^3(G) \supseteq \cdots,$$

which are called the *derived series* and the *lower central series* respectively. Let H be a subgroup of G and $N \triangleright G$ and let $\pi : G \to G/N$ be the projection. Then we have

$$D^i(H) \subseteq D^i(G),\ C^i(H) \subseteq C^i(G) \text{ and}$$
$$\pi(D^i(G)) = D^i(G/N),\ \pi(C^i(G)) = C^i(G/N).$$

Note that $C^i(G)/C^{i+1}(G)$ is in the center of $G/C^{i+1}(G)$ (Ex.19). A group G is said to be *solvable* (resp. *nilpotent*) if $D^{k+1}(G)$ (resp. $C^{k+1}(G)$) is trivial for some integer k; the smallest such k is called the *solvability* (resp. *nilpotency*) *class* of G. Since $D^i(G) \subseteq C^i(G)$ we see that a nilpotent group is solvable. Trivially an abelian group is nilpotent. A subgroup and a quotient of a solvable (resp. nilpotent) group are solvable (resp. nilpotent).

(2.2.13) *The following conditions are equivalent.*

(i) *G is nilpotent with nilpotency class $\leq n$.*

(ii) *There is a sequence of subgroups*

$$G = G^1 \supseteq G^2 \supseteq \cdots \supseteq G^{n+1} = (e)$$

such that $[G, G^k] \subseteq G^{k+1} (1 \leq k \leq n)$. (Note G^k is necessarily normal in G.)

(iii) *There is a subgroup A in $Z(G)$ such that G/A is nilpotent with nilpotency class $\leq (n-1)$.*

Proof. (i) $\Rightarrow$ (ii) Take $G^k = C^k(G)$.

(ii) $\Rightarrow$ (i) By induction one shows that $C^k(G) \subseteq G^{k+1}$.

(iii) $\Rightarrow$ (i) Let $f\colon G \to G/A$ be the canonical homomorphism. Then $f(C^n(G)) = C^n(G/A) = (e)$ and hence $C^n(G) \subseteq A$. Therefore, $C^{n+1}(G) = (e)$.

(i) $\Rightarrow$ (iii) Take $A = C^n(G)$. Cf. Ex.12.

(2.2.14) *The following conditions are equivalent.*

(i) *G is solvable with solvability class $\leq n$.*

(ii) *There is a sequence of normal subgroups of* G

$$G = G^1 \supseteq G^2 \supseteq \cdots \supseteq G^{n+1} = (e),$$

such that G^{k+1} *is normal in* G^k *and* G^k/G^{k+1} *is commutative.*

(iii) *There is a normal commutative subgroup* A *of* G *such that* G/A *is solvable.*

Proof. (i) $\Rightarrow$ (ii) Take $G^k = D^k(G)$.

(ii) $\Rightarrow$ (iii) Take $A = G^n$.

(iii) $\Rightarrow$ (i) Exercise.

(2.2.15) *Let* G *be a finite group. The following conditions are equivalent.*

(i) G *is nilpotent.*

(ii) *For any prime* p*, there is a (unique) normal* p*-Sylow subgroup of* G*.*

(iii) G *is a product of* p*-groups* (for various p's).

Proof. (i) $\Rightarrow$ (ii) Let P be a p-Sylow subgroup. First we claim $N(P) = NN(P)$. For this let $g \in NN(P)$ and write $N = N(P)$; $gNg^{-1} \subseteq N$. Then gPg^{-1} and P are p-Sylow subgroups of N. Hence there is $h \in N$ such that $gPg^{-1} = hPh^{-1}$. Thus $h^{-1}g \in N$; $g \in hN = N$. Obviously $N(P) \subseteq NN(P)$ by definition.

This in turn implies $N(P)(= N) = G$. In fact, assume the contrary i.e., $N \neq G$. Let G^k be as in (2.2.13)(ii) and $N^k = N \cdot G^k$. Then we have a chain $G = N^1 \supseteq N^2 \supseteq \cdots \supseteq N$. First we claim N^{k+1} is normal in N^k. For this let $h \in N$ then $hN^{k+1}h^{-1} = hN \cdot G^{k+1}h^{-1} = hNh^{-1}G^{k+1} = N \cdot G^{k+1} = N^{k+1}$ since N and G^{k+1} are normal in G. On the other hand if $s \in G^k$ and $h \in N$ then $shs^{-1} = shs^{-1}h^{-1}h \in [G, G^k] \cdot N \subseteq G^{k+1}N = N^{k+1}$. Hence N and G^k normalize N^{k+1}; N^{k+1} is normal in N^k as claimed. Finally since we assumed $G \neq N$ we can choose the largest integer k such that $N^k \supsetneq N$ then we see that the normalizer of N is strictly bigger than N which contradicts to our previous assertion.

(ii) $\Rightarrow$ (iii) Let I be the set of primes dividing the order of G and for each $p \in I$ let P_p be the p-Sylow subgroup of G. Let ϕ be the canonical map $\prod_{p \in I} P_p \to G$ which maps $(g_p)_{p \in I}$ to $\prod_{p \in I} g_p$. We claim that ϕ is an isomorphism. In fact, if $g \in P_p$ and $h \in P_q$ for

distinct primes p, q then $ghg^{-1}h^{-1} \in P_p \cap P_q = (e)$. Hence $gh = hg$. This implies that ϕ is a group homomorphism. To see ϕ is onto first note that $\mathrm{Im}(\phi)$ contains all P_p's since $\phi|_{P_p}$ is the inclusion. Hence the order of $\mathrm{Im}(\phi)$ is divisible by the highest power of primes which divides $o(G)$. Hence $G =$Im(ϕ). Since the orders of the groups $\prod_{p\in I} P_p$ and G are the same, ϕ is an isomorphism.

(iii) $\Rightarrow$ (i) A p-group is nilpotent. In fact, we know that the center is nontrivial by the class formula. By induction, $G/Z(G)$ is nilpotent. Now G is nilpotent by (2.2.13)(iii). To finish the proof use the fact that a product of nilpotent groups are nilpotent Ex.12 (ii).

(2.2.16) Early 1980's, people succeeded in classifying all finite simple groups. For a brief historical survey article of this matter see the article by *Ron Solomon* "On finite simple groups and their classification", AMS, *Notice*, Vol. 42, No. 2 (1995).

Exercises 2.2

1. Let G be an abelian group, $G_1, \ldots, G_n$ be subgroups of G. Then the following conditions are equivalent.
   (i) $G \cong G_1 \oplus \cdots \oplus G_n$.
   (ii) Every element of $x \in G$ can be written uniquely as $x = x_1 + \cdots + x_n$ where x_i is an element of G_i $(i = 1, \ldots, n)$.
   (iii) $G_1 + \cdots + G_n = G$ and $(G_1 + \cdots + G_i) \cap G_{i+1} = (0)$ for each i.
2. Answer the following questions.
   (i) List all nonisomorphic abelian groups of order $2^3 3^3 5^2$.
   (ii) List all groups of order 8 (abelian or not). Show your list is complete.
3. Express $(\mathbb{Z}/n)^*$, the group of units of $\mathbb{Z}/n$ as a direct product of cyclic groups of the form (2.2.7) (2).
4. The group of rational numbers $\mathbb{Q}$ is not finitely generated; it is not free either.

5. An abelian group is a free object in the category of abelian groups if and only if it is isomorphic to a direct sum of copies (finite or not) of $\mathbb{Z}$'s.
6. Let p be a prime number.
   (i) A group of order p^2 is abelian.
   (ii) Construct a non abelian group of order p^3 .
7. Show that a countable product of $\mathbb{Z}$ is not free. (Hint: Write A for the product of countable copies of $\mathbb{Z}$. If A is free then its rank must be $\aleph_1$. Let p be a prime. If A were free then A/pA is a $\mathbb{Z}/p\mathbb{Z}$-vector space whose dimension is $\aleph_1$. For a nonzero integer k, let $v_p(k)$ be the maximal power of p which divides k and let $v_p(0) = \infty$. Let S be the subgroup of A defined by

$$S = \{(a_1, a_2, \dots) \in A \mid v_p(a_i) \to \infty \text{ as } i \to \infty\}$$

   and let $x = (p, p^2, p^3, \dots) \in A$. Then multiplication-by-x map is an isomorphism from A to S. Hence if A were free of dimension $\aleph_1$ then S/pS is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension $\aleph_1$. But S/pS is generated, as a $\mathbb{Z}/p\mathbb{Z}$-vector space, by the family $\{e_i\}_{i=1}^{\infty}$ whose i-th coordinate is 1 and zero elsewhere.)
8. Every finite group has a composition series.
9. Let G be a finite group and p be a prime. If every subgroup of G has an index divisible by p then G is a p-group.
10. Let G be a group order $p^n m$ where $(m, p) = 1$.
    (i) There is a subgroup of G of order $p^i (1 \le i \le n)$.
    (ii) A subgroup of order p^i is normal in some subgroup of order p^{i+1}.
11. Answer the following questions.
    (i) Find all 2-Sylow subgroups of in $\mathfrak{S}_4$. To which groups are they isomorphic?
    (ii) Find 2-Sylow subgroups of $\mathfrak{S}_5$. Show one of them is isomorphic to D_4. What is the center of D_4 ?
12. Prove:
    (i) If there is an exact sequence

$$(0) \longrightarrow A \longrightarrow G \longrightarrow H \longrightarrow (e)$$

where A is abelian and H is nilpotent, then G is nilpotent.

(ii) A product of nilpotent groups is nilpotent.

13. Show that $\mathfrak{S}_3$ is solvable but not nilpotent.

14. A subgroup H of G is called *characteristic* if $\sigma(H) \subseteq H$ for all $\sigma \in \mathrm{Aut}(G)$. Show that a characteristic subgroup is normal. Show that $D^i(G)$ and $C^i(G)$ are characteristic subgroups.

15. If G is a finite nilpotent group of order n and $m|n$ then G has a subgroup of order m.

16. If N and H are normal nilpotent subgroup of G then HN is also normal nilpotent.

17. The dihedral group D_n is nilpotent if and only if n is a power of 2.

18. Let H be a subgroup of a finite group G. If $[G : H]$ is the smallest prime p dividing the order of G, then H is normal in G. (Hint: Let G act on G/H by left translation to get a map $f\colon G \to \mathfrak{S}_p$ (= the permutation group on the left cosets of H). Show that $\mathrm{Ker}(f) = H$.)

19. Prove the following statements.

(i) The quotient $G/[G, G]$ is abelian and if N is a normal subgroup of G such that G/N is normal then $[G, G] \subseteq N$. That is $G/[G, G]$ is the largest abelian quotient of G.

(ii) Let G be a group and H be a subgroup of G and N be a normal subgroup of G. Let $f\colon G \to G/N$ be the canonical map. Then $f(H)$ is contained in the center of G/N if and only if $[G, H]$ is contained in N.

20. The *Frattini group* $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups. If G is finite then $\Phi(G)$ is nilpotent.

21. Let F be a field.

(i) The group G consisting of all matrices of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \qquad a, b, c \in F,$$

is a nilpotent group. Can you generalize this fact ?

(ii) Let G be the group of all the matrices of the form

$$\begin{bmatrix} a & c \\ 0 & b \end{bmatrix}, \qquad a, b, c \in F,\ ab \neq 0,$$

is a solvable group. Can you generalize this? Is this nilpotent?

22. For $n \geq 5$, $\mathfrak{S}_n$ is not solvable.
23. The dihedral group D_n is solvable.
24. Let S and T be solvable subgroups of G. If S is normal in G then ST is a solvable subgroup of G.
25. Any group of order p^2q where p, q are primes is solvable.
26. If G is nonabelian group of order p^3 (p is a prime) then $Z(G) = [G\colon G]$.
27. Any group of order ≤ 60 is of prime order or has a nontrivial normal subgroup.
28. A finite group G is called *supersolvable* if there is a composition series

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = (e)$$

consisting of normal subgroups of G such that G_i/G_{i+1} is cyclic.

(i) Every subgroup, every quotient and a finite product of supersolvable group is supersolvable.

(ii) Show: nilpotent $\Rightarrow$ supersolvable $\Rightarrow$ solvable.

(iii) The alternating group A_4 is solvable but not supersolvable. Find an example which is supersolvable but not nilpotent.

(iv) If G is supersolvable the $[G, G]$ is nilpotent.

(v) If G has a cyclic subgroups A, B such that $G = A \cdot B = B \cdot A$ then G is supersolvable.