CHAPTER 5

Further Topics on Groups

5.1. Direct Products of Groups

Consider the cartesian product $G_1 \times \ldots \times G_k$, where $G_1, \ldots, G_k$ are groups.

For $(g_1, \ldots, g_k), (h_1, \ldots, h_k) \in G_1 \times \ldots \times G_k$, define

$$(g_1, \ldots, g_k) * (h_1, \ldots, h_k) = (g_1 h_1, \ldots, g_k h_k). \tag{5.1}$$

Note that we have used multiplicative notation for $G_1, \ldots, G_k$.

We leave it as an exercise to check the following three results.

Theorem 5.1. *$G_1 \times \ldots \times G_k$, together with the operation $*$ defined by* (5.1)*, forms a group.*

Definition. The group in Theorem 5.1 is called the direct product of the groups $G_1, \ldots, G_k$.

Proposition 5.2. *The direct product $G_1 \times \ldots \times G_k$ is abelian if and only if the groups $G_1, \ldots, G_k$ are all abelian.*

Proposition 5.3. *Suppose that the groups $G_1, \ldots, G_k$ are all finite. Then*

(i) $|G_1 \times \ldots \times G_k| = |G_1| \ldots |G_k|$*;*
(ii) *the order of $(g_1, \ldots, g_k) \in G_1 \times \ldots \times G_k$ is the least common multiple of the orders of $g_1, \ldots, g_k$ in $G_1, \ldots, G_k$ respectively; and*
(iii) *$G_1 \times \ldots \times G_k$ is cyclic if and only if $G_1, \ldots, G_k$ are all cyclic and the orders $|G_1|, \ldots, |G_k|$ are pairwise coprime.*

So far we have been "building up" groups from smaller groups. However, the really interesting task is to "factor" a given group into a direct product of smaller groups.

Theorem 5.4. *A group G is isomorphic to a direct product $H' \times K'$ if and only if G has two subgroups H and K such that*

(i) $H \cap K = \{e\}$*;*
(ii) *$hk = kh$ for every $h \in H$ and $k \in K$; and*
(iii) $G = \{hk : h \in H,\ k \in K\}$*.*

The proof of Theorem 5.4 is rather hard. However, the following result follows easily, and is left as an exercise.

Corollary 5.5. *Suppose that G is an abelian group of order n. Then G is isomorphic to a direct product $H' \times K'$ if and only if G has two subgroups H and K such that $H \cap K = \{e\}$ and $|H||K| = n$.*

Definition. We say that a group G is indecomposable if the following condition is satisfied: If H and K are groups and G is isomorphic to the direct product $H \times K$, then either $H = \{e\}$ or $K = \{e\}$.

For every $m \in \mathbb{N}$ and $m \geqslant 2$, we shall denote by $\mathbb{Z}_m$ the group $(\mathbb{Z}_m, +)$.

Proposition 5.6. *For every prime p and every $a \in \mathbb{N}$, the group $\mathbb{Z}_{p^a}$ is indecomposable.*

PROOF. Suppose that $\mathbb{Z}_{p^a}$ is isomorphic to the direct product $H \times K$, where $H \neq \{e\}$ and $K \neq \{e\}$. Since $|H||K| = |\mathbb{Z}_{p^a}| = p^a$, there exist $b, c \in \mathbb{N}$ such that $|H| = p^b$ and $|K| = p^c$. It follows that $|H|$ and $|K|$ are not coprime, so that $H \times K$ is not cyclic in view of Proposition 5.3(iii). This is a contradiction, since $\mathbb{Z}_{p^a}$ is cyclic. ◯

PROPOSITION 5.7. *Suppose that $m = p_1^{a_1} \ldots p_k^{a_k}$, where $p_1, \ldots, p_k$ are distinct primes and where $a_1, \ldots, a_k \in \mathbb{N}$. Then $\mathbb{Z}_m$ is isomorphic to the direct product $\mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$.*

PROOF. Note that the numbers $p_1^{a_1}, \ldots, p_k^{a_k}$ are pairwise coprime. It follows from Propositions 5.3(iii) and 5.3(i) that $\mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$ is cyclic and of order $p_1^{a_1} \ldots p_k^{a_k}$. Hence $\mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$ is isomorphic to $\mathbb{Z}_m$. ◯

We state without proof the following important result, usually known as the fundamental theorem of finite abelian groups.

THEOREM 5.8. *Suppose that G is a finite abelian group of order at least 2. Then there exist primes $p_1, \ldots, p_k$, not necessarily distinct, and $a_1, \ldots, a_k \in \mathbb{N}$ such that G is isomorphic to the direct product $\mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$. Furthermore, the numbers $p_1^{a_1}, \ldots, p_k^{a_k}$ are unique up to their order.*

EXAMPLE. Are $\mathbb{Z}_{48} \times \mathbb{Z}_{72}$ and $\mathbb{Z}_{24} \times \mathbb{Z}_{144}$ isomorphic? To answer this question, let us first factorize each of these groups using Theorem 5.8. Consider first of all $\mathbb{Z}_{48}$. Then since $48 = 2^4 3$, $\mathbb{Z}_{48}$ is isomorphic to precisely one of the following:

$$\begin{aligned}
&\mathbb{Z}_3 \times \mathbb{Z}_{16}, \\
&\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_8, \\
&\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4, \\
&\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \\
&\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

All except the first of these are non-cyclic in view of Proposition 5.3(iii). It follows that $\mathbb{Z}_{48}$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{16}$. Similarly, $\mathbb{Z}_{72}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_9$. On the other hand, $\mathbb{Z}_{24}$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_8$ and $\mathbb{Z}_{144}$ is isomorphic to $\mathbb{Z}_9 \times \mathbb{Z}_{16}$. It follows that the two groups in question are isomorphic.

5.2. Geometric Interpretation of Matrix Groups

The purpose of this section is to give a geometric interpretation of the multiplicative group $\mathcal{M}^*_{2,2}(\mathbb{R})$ of invertible 2×2 matrices with entries in $\mathbb{R}$.

Consider the vector space $\mathbb{R}^2$. Let $L : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear transformation. In other words, for all vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$ and for all scalars $\lambda \in \mathbb{R}$, we have $(\mathbf{x} + \mathbf{y})L = \mathbf{x}L + \mathbf{y}L$ and $(\lambda\mathbf{x})L = \lambda(\mathbf{x}L)$.

Suppose further that the linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ is invertible. Then $L : \mathbb{R}^2 \to \mathbb{R}^2$ can be described in terms of an element of $\mathcal{M}^*_{2,2}(\mathbb{R})$. In fact, an alternative notation for $\mathcal{M}^*_{2,2}(\mathbb{R})$ is $\mathrm{GL}(2, \mathbb{R})$; this is known as a general linear group.

Recall the following facts about linear transformations $L : \mathbb{R}^2 \to \mathbb{R}^2$ and 2×2 matrices with entries in $\mathbb{R}$.

(i) If $L : \mathbb{R}^2 \to \mathbb{R}^2$ is a linear transformation, then there is a 2×2 matrix A with entries in $\mathbb{R}$ such that for every $\mathbf{x} \in \mathbb{R}^2$, we have $\mathbf{x}L = \mathbf{x}A$. Furthermore,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $(a, b) = (1, 0)L$ and $(c, d) = (0, 1)L$ are the images under L of the basis elements $(1, 0)$ and $(0, 1)$ respectively.

(ii) Note that the image under $L : \mathbb{R}^2 \to \mathbb{R}^2$ of a square with vertices $(0, 0), (1, 0), (1, 1), (0, 1)$ is a parallelogram with vertices $(0, 0), (a, b), (a + c, b + d), (c, d)$. The orientation is preserved if $\det A = ad - bc > 0$, and reversed if $\det A = ad - bc < 0$. It can also be shown that the area of the parallelogram is $|\det A| = |ad - bc|$. Furthermore, if $\det A = ad - bc = 0$, then the parallelogram has zero area.

(iii) The linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ is invertible if and only if the matrix A is invertible, *i.e.* if and only if $\det A \neq 0$, *i.e.* if and only if $A \in \mathrm{GL}(2, \mathbb{R})$.

It follows from (ii) that for the linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ to preserve area and orientation, the matrix $A \in \mathrm{GL}(2,\mathbb{R})$ must satisfy $\det A = 1$. This leads to the set

$$\mathrm{SL}(2,\mathbb{R}) = \{A \in \mathrm{GL}(2,\mathbb{R}) : \det A = 1\}.$$

THEOREM 5.9. $\mathrm{SL}(2,\mathbb{R})$ *is a normal subgroup of* $\mathrm{GL}(2,\mathbb{R})$.

PROOF. Clearly the identity matrix $I \in \mathrm{SL}(2,\mathbb{R})$. On the other hand, if $A, B \in \mathrm{SL}(2,\mathbb{R})$, then clearly $\det(AB) = (\det A)(\det B) = 1$, so that $AB \in \mathrm{SL}(2,\mathbb{R})$; also, $\det(A^{-1}) = 1/(\det A) = 1$, so that $A^{-1} \in \mathrm{SL}(2,\mathbb{R})$. It follows from Theorem 1.4 that $\mathrm{SL}(2,\mathbb{R})$ is a subgroup of $\mathrm{GL}(2,\mathbb{R})$. On the other hand, for every $C \in \mathrm{GL}(2,\mathbb{R})$ and every $A \in \mathrm{SL}(2,\mathbb{R})$,

$$\det(C^{-1}AC) = (\det C^{-1})(\det A)(\det C) = (\det C^{-1})(\det C) = 1,$$

so that $C^{-1}AC \in \mathrm{SL}(2,\mathbb{R})$. It follows that $\mathrm{SL}(2,\mathbb{R})$ is a normal subgroup of $\mathrm{GL}(2,\mathbb{R})$. ○

DEFINITION. The group $\mathrm{SL}(2,\mathbb{R})$ is called a special linear group or a unimodular group.

Rotations about the origin in $\mathbb{R}^2$ can also be described by matrices in $\mathrm{GL}(2,\mathbb{R})$. In fact, an anti-clockwise rotation by angle θ about the origin can be described by the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Let

$$\mathcal{R}(2) = \{R_\theta : 0 \leqslant \theta < 2\pi\}.$$

PROPOSITION 5.10. $\mathcal{R}(2)$ *is a subgroup of* $\mathrm{SL}(2,\mathbb{R})$.

PROOF. Clearly $\det R_\theta = 1$ for every $\theta \in [0, 2\pi)$, and that $I = R_0$. On the other hand, if $\theta, \phi \in [0, 2\pi)$, then let

$$\psi = \theta + \phi - 2\pi \left[\frac{\theta + \phi}{2\pi}\right].$$

It is clear that $\psi \in [0, 2\pi)$ and $R_\theta R_\phi = R_\psi$. Finally, if $\theta \in (0, 2\pi)$, then $2\pi - \theta \in (0, 2\pi)$. Clearly $R_\theta R_{2\pi-\theta} = I$. The result now follows from Theorem 1.4. ○

The dihedral group D_4 can also be described by matrices in $\mathrm{GL}(2,\mathbb{R})$. Suppose that the four vertices of the square are $(\pm 1, \pm 1)$. Then an anti-clockwise rotation of $90°$ can be described by the matrix $R_{\pi/2}$, while a reflection across the vertical axis can be described by the matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We can therefore conclude that D_4 is isomorphic to a subgroup of $\mathrm{GL}(2,\mathbb{R})$.

Problems for Chapter 5

1. For each of the following groups G, find the order of G, determine whether G is abelian and whether G is cyclic, and determine the order of the elements of G:

    (i) $G = (\mathbb{Z}_4, +) \times (\mathbb{Z}_7, +)$
    (ii) $G = S_3 \times (\mathbb{Z}_2, +)$
    (iii) $G = A_3 \times (\mathbb{Z}_7^*, \cdot)$

2. Show that the three groups below are pairwise non-isomorphic:

    (i) $(\mathbb{Z}_{16}, +)$
    (ii) $(\mathbb{Z}_4, +) \times (\mathbb{Z}_4, +)$
    (iii) $(\mathbb{Z}_4, +) \times (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$

3. Show that S_3 is indecomposable.

4. Show that $(\mathbb{Z}_7^*, \cdot)$ is isomorphic to $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$.

5. Show that every abelian group of order 105 is isomorphic to $(\mathbb{Z}_{105}, +)$.

6. Determine the number of non-isomorphic abelian groups of order 45.

7. Determine the number of non-isomorphic abelian groups of order 144.

8. Determine the number of non-isomorphic groups of order 6 by following the steps below, where G denotes a group of order 6:

    (i) Determine the number of non-isomorphic abelian groups G of order 6.
    (ii) Suppose that G is non-abelian. Show that the order of the elements of G cannot exceed 3.
    (iii) Suppose that G is non-abelian. Show that G must have an element of order 3.
    (iv) Let $x \in G$ be of order 3, and write $G = \{e, x, x^2, y, z, u\}$. Suppose further that $y^2 = e$, to be justified later in (vii). Justify that we may assume that $xy = z$.
    (v) Continuing from (iv), show that we cannot have $yx = z$.
    (vi) Continuing from (iv) and assuming that $yx = u$, complete the group table for G and show that G is isomorphic to S_3.
    (vii) Show by contradiction that if G is non-abelian, then G must have an element of order 2.
    (viii) Determine the answer.