Chapter 3

Group Theory from a Mathematical Viewpoint

Takao Satoh

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.72131

Abstract

In this chapter, for the reader who does not major in mathematics but chemistry, we discuss general group theory from a mathematical viewpoint without proofs. The main purpose of the chapter is to reduce reader's difficulties for the abstract group theory and to get used to dealing with it. In order to do this, we exposit definitions and theorems of the field without rigorous and difficult arguments on the one hand and give lots of basic and fundamental examples for easy to understand on the other hand. Our final goal is to obtain well understandings about conjugacy classes, irreducible representations, and characters of groups with easy examples of finite groups. In particular, we give several character tables of finite groups of small order, including cyclic groups, dihedral groups, symmetric groups, and their direct product groups. In Section 8, we deal with directed graphs and their automorphism groups. It seems that some of ideas and techniques in this section are useful to consider the symmetries of molecules in chemistry.

Keywords: group theory, finite groups, conjugacy classes, representation theory, character tables, directed graphs, automorphisms of graphs

1. Introduction

To make a long story short, a group is a set equipped with certain binary operation, for example, the set of all integers with the addition and the set of all nth power roots of unity with the multiplication. One of the origins of the group theory goes back to the study of the solvability of algebraic equations by Galois in the nineteenth century. He focused on the permutations of the solutions of an equation and gave rise to a concept of permutation groups. On the other hand, in 1872 Felix Klein proposed that every geometry is characterized by its underlying transformation groups. Here the transformation group means the group that comes from certain symmetries of the space. By using group theory, he classified Euclidean geometry and non-Euclidean geometry. As is shown earlier, groups have been established as important research objects on the study of permutations and symmetries of a given object. The

group theory has achieved a good progress in modern mathematics and has various deep and sophisticated theories itself.

Today, the group theory has multiple facets and widespread applications in a broad range of science, including not only mathematics and physics but also chemistry. In chemistry, group theory is used to study the symmetries and the crystal structures of molecules. For each molecule, a certain group, which is called the point group, is defined by the symmetries on the molecule. The structure of this group reflects many physical and chemical properties, including the chirality and the spectroscopic property of the molecule. The group theory has become a standard and a powerful tool to study various properties of the molecule from a viewpoint of the molecular orbital theory, for example, the orbital hybridizations, the chemical bonding, the molecular vibration, and so on. In general, although each of modern mathematical theories is quite abstract and sophisticated to apply to the other sciences, the group theory has succeeded to achieve a good application by many authors, including Hans Bethe, Eugene Wigner, László Tisza, and Robert Mulliken. It seems that such expansions of mathematics to the other sciences are quite blessed facts for mathematicians.

Here we organize the contents of this chapter. First, we give mathematical notation and conventions which we use in this chapter. The reader is assumed to be familiar with elemental linear algebra and set theory. In Section 3, we review the definitions and some fundamental and important properties of groups. In particular, we show several methods to make new groups from known groups by considering subgroups and quotient groups. Then, we consider to classify known groups by using the concept of group isomorphism. In Section 4, we discuss and give many examples of finite groups, including symmetric groups, alternating groups, and dihedral groups. Then we give the classification theorem for finite abelian groups, which we can regard as an expansion of the Chinese remainder theorem. In Section 5, we consider to classify elements of groups by the conjugation and discuss the decomposition of a group into its conjugacy classes. In Section 6, we explain basic facts in representation theory of finite groups. In particular, we review representations of groups, irreducible representations, and characters. Finally, we give several examples of character tables of well-known finite groups. In Section 8, we consider finite-oriented graphs and their automorphisms. The automorphism group of a graph strongly reflects the symmetries of the graph. We remark that the reader can read this section without the knowledge of the facts in Sections 5 and 6.

2. Notation and conventions

In this section, we fix some notation and conventions and review some definitions in the set theory and the linear algebra:

$$\mathbf{N} := \text{the set of natural numbers} = \{1, 2, 3, \ldots\}$$

$$\mathbf{Z} := \text{the set of integers} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

$$\mathbf{Q} := \text{the set of rational numbers}$$

$$\mathbf{R} := \text{the set of real numbers}$$

$$\mathbf{C} := \text{the set of complex numbers} = \left\{ a + b\sqrt{-1} \,|\, a, b \in \mathbf{R} \right\}$$

- For any $a, b \in \mathbf{Z} \setminus \{0\}$, the greatest common divisor of a and b is denoted by $\gcd(a, b)$.
- For a set X, the cardinality of X is denoted by $|X|$. If X is a finite set, $|X|$ means the number of elements of X.
- For sets X and Y, the difference of sets X and Y is denoted by $X \setminus Y := \{x \mid x \in X, x \notin Y\}$.
- A map $f : X \to Y$ is surjective if for any $y \in Y$; there exists some $x \in X$ such that $f(x) = y$.
- A map $f : X \to Y$ is injective if $f(x) = f(x')$ for $x, x' \in X$; then $x = x'$.
- A map $f : X \to Y$ is bijective if f is surjective and injective. In other words, the bijective map is one-to-one correspondence between X and Y.
- Let K be $\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$. For K-vector spaces V and W, a map $f : V \to W$ is K-linear if f satisfies

$$f(\boldsymbol{x} + \boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y}),$$
$$f(k\boldsymbol{x}) = kf(\boldsymbol{x})$$

for any $\boldsymbol{x}, \boldsymbol{y} \in V$ and $k \in K$.

- A linear map $f : V \to V$ is called a linear transformation on V.

3. General group theory

In this section, we review elemental and fundamental topics in group theory, based on the authors' book [1]. There are hundreds of textbooks for the group theory. Venture to say, if the reader wants to learn more from a viewpoint of symmetries, it seems to be better to see [2]. For high motivated readers, see [3, 4] for mathematical details.

3.1. Groups

Let G be a set. For any $\sigma, \tau \in G$, if there exists the unique element $\sigma \cdot \tau \in G$, which is called the **product** of σ and τ, such that the product satisfies the following three conditions, then the set G is called a **group**:

- **(Associativity)** For any $\sigma, \tau, \rho \in G$, $(\sigma \cdot \tau) \cdot \rho = \sigma \cdot (\tau \cdot \rho)$.
- **(Unit)** There exists some element $e \in G$ such that for any $\sigma \in G$,

$$e \cdot \sigma = \sigma \cdot e = \sigma.$$

We call the element e the **unit** of G. According to the mathematical convention, we write 1_G or simply 1, for the unit.

- **(Inverse element)** For any $\sigma \in G$, there exists some element $\sigma' \in G$ such that

$$\sigma \cdot \sigma' = \sigma' \cdot \sigma = e.$$

We call σ' the **inverse** element of σ and write σ^{-1}.

If the definition of the product is clear from the content, we often omit the symbol $\cdot$ and write $\sigma\tau$ instead of $\sigma \cdot \tau$ for simplicity. The product is a binary operator on G and is also called the **multiplication** of G.

Here we consider the following examples:

(E1) Each of the sets **Z**, **Q**, **R**, and **C** is a group with the usual addition. For the case **Z**, we see that the unit is 0 and for any $n \in \mathbf{Z}$, the inverse of n is $-n$. In general, if the product of a group G is additive, then G is called an **additive group**. We remark that **N** is not a group with the usual addition since any element does not have its inverse.

(E2) The set $\mathbf{R}^{\times} := \mathbf{R} \setminus \{0\}$ with the usual multiplication of real numbers forms a group. We see that the unit is 1 and for any $r \in \mathbf{R}^{\times}$, the inverse of r is $1/r$. We remark that **R** with the usual multiplication is not a group since 0 does not have its inverse. In general, if the product of a group G is multiplicative, then G is called a **multiplicative group**. Similarly, $\mathbf{Q}^{\times} := \mathbf{Q} \setminus \{0\}$ and $\mathbf{C}^{\times} := \mathbf{C} \setminus \{0\}$ are multiplicative groups.

(E3) For any $n \in \mathbf{N}$ $(n \geq 1)$, let $\mathcal{U}_n$ be the set of nth power roots of unity:

$$\mathcal{U}_n := \left\{ \exp\left(\frac{2k\pi\sqrt{-1}}{n}\right) \in \mathbf{C} \,\middle|\, 0 \leq k \leq n-1 \right\},$$

where

$$\exp\left(\frac{2k\pi\sqrt{-1}}{n}\right) := \cos\left(\frac{2k\pi}{n}\right) + \sqrt{-1}\sin\left(\frac{2k\pi}{n}\right).$$

Then $\mathcal{U}_n$ with the usual multiplication of **C** forms a group. Geometrically, $\mathcal{U}_n$ is the set of vertices of the regular n-gon on the unit circle in the complex plane **C**. For example, $\mathcal{U}_6$ consists of the following points for $\zeta = \exp\left(\frac{2\pi\sqrt{-1}}{6}\right)$ in **Figure 1**.

In general, for a group G, if G consists of finitely many elements, then G is called a **finite group**. The number of elements of a finite group G is called the **order** of G, denoted by $|G|$. If G is not a finite group, then G is called an **infinite group**. The group $\mathcal{U}_n$ is a finite group of order n, and the groups discussed in (E1) and (E2) are infinite groups.

(E4) Let K be **Q**, **R**, or **C**. We denote by $\mathrm{M}(2, K)$ the set of 2×2 matrices with all entries in K:

$$\mathrm{M}(2, K) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a, b, c, d \in K \right\}.$$

Furthermore, we denote by $\mathrm{GL}(2, K)$ the set of elements of $\mathrm{M}(2, K)$ whose determinant is not equal to zero:

$$\mathrm{GL}(2, K) := \{A \in \mathrm{M}(2, K) \mid \det A \neq 0\}.$$

Then $\mathrm{M}(2, K)$ with the usual addition of matrices forms an additive group. The unit of $\mathrm{M}(2, K)$ is zero matrix, and for any $A = (a_{ij}) \in \mathrm{M}(2, K)$, its inverse is $-A := (-a_{ij})$. Since $\mathrm{GL}(2, K)$ does not

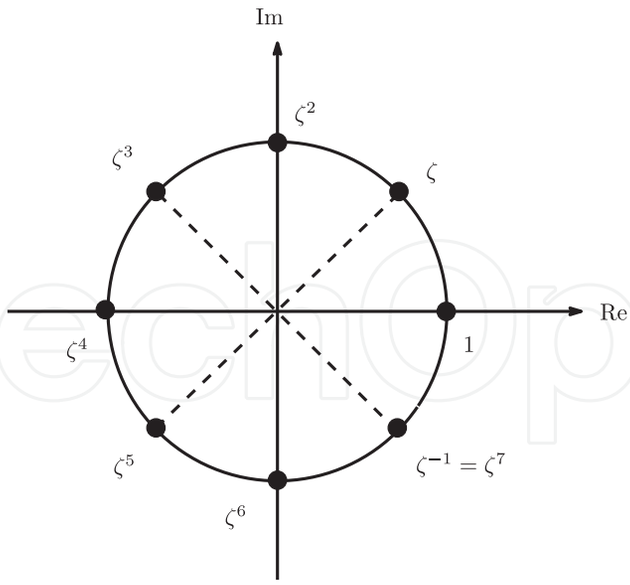

Figure 1. The sixth roots of unity.

have the zero matrix, the set $\mathrm{GL}(2,K)$ is not an additive group. On the other hand, the set $\mathrm{GL}(2,K)$ with the usual multiplication of matrices forms a multiplicative group. The unit of $\mathrm{GL}(2,K)$ is the unit matrix E_2, and for any $A = (a_{ij}) \in \mathrm{GL}(2,K)$, its inverse is the inverse matrix A^{-1} as follows:

$$E_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^{-1} = \frac{1}{\det A} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

The group $\mathrm{GL}(2,K)$ is called the **general linear group** of degree 2. Similarly, we can consider the general linear group $\mathrm{GL}(n,K)$ of degree n for any $n \in \mathbf{N}$.

Both $\mathrm{M}(2,K)$ and $\mathrm{GL}(2,K)$ are infinite groups. But the most significant difference between them is the commutativity of the products. Although we see $A + B = B + A$ in $\mathrm{M}(2,K)$ for any $A, B \in \mathrm{M}(2,K)$, the equation $AB = BA$ does not hold in $\mathrm{GL}(2,K)$ in general. For example, if $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, then we see

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

For a group G, if $\sigma\tau = \tau\sigma$ holds for any $\sigma, \tau \in G$, then G is called an **abelian group**. The group $\mathrm{GL}(2,K)$ is a non-abelian group, and all the groups as mentioned before except for $\mathrm{GL}(2,K)$ are abelian groups.

3.2. Subgroups

Since group theory is an abstract itself, it had better for beginners to have sufficiently enough examples to understand it. In order to make further examples, we consider several methods to make new groups from known groups. The first one is a subgroup.

Let G be a group. If a nonempty subset H of G satisfies the following two conditions, then H is called a **subgroup** of G:

- For any $\sigma, \tau \in H$, $\sigma\tau \in H$.
- For any $\sigma \in H$, $\sigma^{-1} \in H$.

We can consider H itself is a group by restricting the product of G to H. For any group G, the one point subset $\{1_G\}$ is a subgroup of G. We call this subgroup the **trivial subgroup** of G. Let us consider some other examples:

(E5) The additive group $\mathbf{Z}$ is a subgroup of $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{Z}$. For any $n \in \mathbf{Z}$, the subset

$$n\mathbf{Z} := \{0, \pm n, \pm 2n, \ldots\} \subset \mathbf{Z}$$

of $\mathbf{Z}$ consisting of multiples of n is a subgroup of $\mathbf{Z}$. Since $0\mathbf{Z} = \{0\}$ is the trivial subgroup, and since $n\mathbf{Z} = (-n)\mathbf{Z}$, we usually consider the case $n \in \mathbf{N}$.

(E6) Consider the group $\mathcal{U}_6$ consisting of 6th power roots of unity. Then we can consider $\mathcal{U}_2$ and $\mathcal{U}_3$ are subgroups of $\mathcal{U}_6$.

(E7) Let K be $\mathbf{Q}$, $\mathbf{R}$, or $\mathbf{C}$. The subset

$$\mathrm{SL}(2, K) := \{A \in \mathrm{GL}(2, K) \mid \det A = 1\} \subset \mathrm{GL}(2, K)$$

of $\mathrm{GL}(2, K)$ consisting of matrices whose determinants are equal to one is a subgroup of $\mathrm{GL}(2, K)$. We call $\mathrm{SL}(2, K)$ the **special linear group** of degree 2.

In general, we can construct a subgroup from a subset of a group. Let S be a subset of a group G. Then the subset

$$\langle S \rangle := \left\{ s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m} \mid m \in \mathbf{Z}_{\geq 0}, s_i \in S, e_i = \pm 1 \right\}$$

of G consisting of elements which are written as a product of some elements in S, and their inverses are a subgroup of G. Remark that if $m = 0$, the product $s_1^{e_1} \cdots s_m^{e_m}$ means 1_G and that for any $\sigma = s_1^{e_1} s_2^{e_2} \cdots s_m^{e_m} \in \langle S \rangle$, its inverse is given by $\sigma^{-1} = s_m^{-e_m} s_{m-1}^{-e_{m-1}} \cdots s_1^{-e_1}$. We call $\langle S \rangle$ the subgroup of G **generated by** S. The elements of S are called **generators** of the subgroup $\langle S \rangle$. Here we give some examples:

(E8) The additive group $\mathbf{Z}$ is generated by 1. For any $n \geq 1$, the group $\mathcal{U}_n$ of nth power roots of unity is generated by $\zeta = \exp\left(2\pi\sqrt{-1}/n\right)$. In general, a group generated by a single element is called a **cyclic group**. Thus, $\mathbf{Z}$ is an infinite cyclic group, and $\mathcal{U}_n$ is a finite cyclic group. Remark that -1 and $\zeta^{-1} = \exp\left(-2\pi\sqrt{-1}/n\right)$ are also generators of $\mathbf{Z}$ and $\mathcal{U}_n$, respectively.

(E9) It is known that the additive groups $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ and the multiplicative groups $\mathrm{GL}(2, K)$ and $\mathrm{SL}(2, K)$ for $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ are not finitely generated group.

Next, we consider a relation between the orders of a finite group and its subgroup. Let G be a group and H a subgroup of G. For any $\sigma \in G$, the subset

$$\sigma H := \{\sigma\tau \in G \mid \tau \in H\}$$

is called a left coset of H in G. We can see that $\sigma H = \tau H$ if and only if there exists some $h \in H$ such that $\sigma = \tau h$.

(E10) In the additive group $\mathbf{Z}$, for any $n \in \mathbf{N}$, consider the subgroup $n\mathbf{Z}$. Then, since the product of $\mathbf{Z}$ is written additively, a left coset of $n\mathbf{Z}$ is given by

$$\sigma + n\mathbf{Z} = \{\sigma + n\tau \mid \tau \in \mathbf{Z}\}$$

for an element $\sigma \in \mathbf{Z}$. On the other hand, if we take the remainder r of the division of σ by n, then we see $\sigma + n\mathbf{Z} = r + n\mathbf{Z}$. Hence all left cosets of $n\mathbf{Z}$ in $\mathbf{Z}$ are given by

$$n\mathbf{Z},\ 1 + n\mathbf{Z},\quad (n-1) + n\mathbf{Z}.$$

For simplicity, we write $[r]_n$ for $r + n\mathbf{Z}$.

(E11) Consider the finite cyclic group $\mathcal{U}_6$ and its subgroup $\mathcal{U}_2 = \{\pm 1\}$ of order 2. Set $\zeta := \exp\left(2\pi\sqrt{-1}/6\right)$. Then we can see that

$$\zeta\mathcal{U}_2 = \{\pm\zeta\} = \left\{\zeta, \zeta^4\right\} = \zeta^4\mathcal{U}_2, \quad \zeta^2\mathcal{U}_2 = \zeta^5\mathcal{U}_2, \quad \zeta^3\mathcal{U}_2 = \mathcal{U}_2.$$

Hence there exist three left cosets of $\mathcal{U}_2$.

In example (E11), we can see that the order of $\mathcal{U}_2$ times the number of left cosets of $\mathcal{U}_2$ is equal to six, which is the order of $\mathcal{U}_6$. This is no coincidence. In general, for a finite group G and a subgroup H of G, the number of left cosets of H is called the **index** of H in G and is denoted by $[G : H]$. Then we have the following:

Theorem 3.1 (Lagrange). *As the above notation C, we have* $|G| = |H|[G : H]$. *Namely, the order of any subgroup of a finite group G is a divisor of* $|G|$.

As a corollary, we obtain the following:

Corollary 3.2. *If G is a finite group of prime order, then G is a cyclic group.*

3.3. Quotient groups

For a group G and its subgroup H, the set of left cosets of H is denoted by

$$G/H := \{\sigma H \mid \sigma \in G\}.$$

In general, this set does not have a natural group structure. Here we consider a condition to make it a group.

Let N be a subgroup of G. If $\sigma n \sigma^{-1} \in N$ for any $n \in N$ and any $\sigma \in G$, then N is called a **normal subgroup** of G. If G is abelian group, any subgroup of G is a normal subgroup. For a normal

subgroup N of G, we define the product on G/N by using that on G. Namely, for any $\sigma N, \tau N \in G/N$, define

$$\sigma N \cdot \tau N := (\sigma\tau)N.$$

Then this definition is well defined, and G/N with this product forms a group. The unit is $1_G N = N$, and for any $\sigma N \in G/N$, its inverse is given by $(\sigma N)^{-1} = \sigma^{-1}N$. We call G/N the **quotient group** of G by N.

(E12) The most important example for quotient groups is

$$\mathbf{Z}/n\mathbf{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

for $n \in \mathbf{N}$. For any $a, b \in \mathbf{Z}$, we have

$$[a]_n + [b]_n = [a+b]_n, \quad -[a]_n = [-a]_n.$$

For example, in the group $\mathbf{Z}/6\mathbf{Z}$, we have

$$[1]_6 + [3]_6 = [4]_6, \quad [2]_6 + [7]_6 = [9]_6 = [3]_6, \quad -[4]_6 = [-4]_6 = [2]_6.$$

For any $0 \leq r \leq n-1$, since we see

$$[r]_n = [1]_n + [1]_n + \cdots + [1]_n \in \mathbf{Z}/n\mathbf{Z},$$

the group $\mathbf{Z}/n\mathbf{Z}$ is a cyclic group of order n generated by $[1]_n$.

3.4. Homomorphisms and isomorphisms

As mentioned above, we have many examples of groups. Here, we consider relations between groups and examine which ones are essentially of the same type of groups. To say more technically, we classify groups by using isomorphisms.

Let G and H be groups. If a map $f : G \to H$ satisfies

$$f(\sigma\tau) = f(\sigma)f(\tau) \quad \text{for any } \sigma, \tau \in G,$$

then f is called a **homomorphism**. A bijective homomorphism $f : G \to H$ is called an **isomorphism**. Namely, an isomorphism is a map such that it is one-to-one correspondence between the groups and that it preserves the products of the groups. If G and H are isomorphic, we write $G \cong H$.

(E13) Set

$$\mathbf{R}_{>0} := \{x \in \mathbf{R} \mid x > 0\},$$

and consider it as a multiplicative subgroup of $\mathbf{R}^\times$. The exponent map $\exp : \mathbf{R} \to \mathbf{R}_{>0}$ is an isomorphism from the additive group $\mathbf{R}$ to $\mathbf{R}_{>0}$.

(E14) Let K be $\mathbf{Q}$, $\mathbf{R}$, or $\mathbf{C}$. Then the determinant map $\det \mathrm{GL}(2,K) \to K^\times$ is a homomorphism. It is, however, not an isomorphism since f is not injective. For example, $\det E_2 = \det(-E_2) = 1$.

On the other hand, $\mathrm{SL}(2,K)$ is a normal subgroup of $\mathrm{GL}(2,K)$. For any $\sigma, \tau \in \mathrm{GL}(2,K)$, we can see that

$$\sigma\mathrm{SL}(2,K) = \tau\mathrm{SL}(2,K) \Leftrightarrow \det\sigma = \det\tau.$$

Define the map $f : \mathrm{GL}(2,K)/\mathrm{SL}(2,K) \to K^\times$ by

$$\sigma\mathrm{SL}(2,K) \mapsto \det\sigma.$$

Then f is an isomorphism. Indeed f is injective. For any $x \in K^\times$, if we consider the element $\sigma := \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,K)$, we have $f(\sigma\mathrm{SL}(2,K)) = x$. Hence f is surjective. Moreover, we have

$$\begin{aligned} f((\sigma\mathrm{SL}(2,K))(\tau\mathrm{SL}(2,K))) &= f((\sigma\tau)\mathrm{SL}(2,K)) = \det(\sigma\tau) \\ &= (\det\sigma)(\det\tau) = f(\sigma\mathrm{SL}(2,K))f(\tau\mathrm{SL}(2,K)). \end{aligned}$$

(E15) For any $n \in \mathbf{N}$, define the map $f : \mathbf{Z}/n\mathbf{Z} \to \mathcal{U}_n$ by $[k]_n \mapsto \exp\left(2k\pi\sqrt{-1}/n\right)$. Then f is an isomorphism since f is bijective, and

$$\begin{aligned} f\left([k]_n + [l]_n\right) &= f\left([k+l]_n\right) = \exp\left(2(k+l)\pi\sqrt{-1}/n\right) \\ &= \exp\left(2k\pi\sqrt{-1}/n\right)\exp\left(2l\pi\sqrt{-1}/n\right) = f\left([k]_n\right)f\left([l]_n\right). \end{aligned}$$

Let G and H be isomorphic groups. Then, even if G and H are different as a set, they have the same structure as a group. This means that if one is abelian, finite or finitely generated, then so is the other, respectively. In other words, for example, an abelian group is never isomorphic to a non-abelian group and so on.

4. Finite groups

In this section, we give some examples of important finite groups.

4.1. Symmetric groups

For any $n \in \mathbf{N}$, set $X := \{1, 2, \ldots, n\}$. A bijective map $\sigma : X \to X$ is called a permutation on X. A permutation σ is denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Remark that this is not a matrix. We can omit a letter i $(1 \le i \le n)$ if the letter i is fixed. For example, for $n = 4$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}$$

We call the permutation

$$\varepsilon := \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

the **identity permutation**.

Let $\mathfrak{S}_n$ be the set of permutations on X. For any $\sigma, \tau \in \mathfrak{S}_n$, define the product of σ and τ to be the composition $\sigma \circ \tau$ as a map. Then the set $\mathfrak{S}_n$ with this product forms a group. We call it the **symmetric group** of degree n. The unit is the identity permutation, and for any $\sigma \in \mathfrak{S}_n$, its inverse is given by

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

The symmetric group $\mathfrak{S}_n$ is a finite group of order $n!$.

Since $\mathfrak{S}_1$ is the trivial group, and

$$\mathfrak{S}_2 = \left\{ \varepsilon, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$

we see that $\mathfrak{S}_n$ is abelian if $n \leq 2$. For $n = 3$, we have

$$\mathfrak{S}_3 = \left\{ \varepsilon, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

and

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Hence, $\mathfrak{S}_3$ is non-abelian. Similarly, for any $n \geq 3$, $\mathfrak{S}_n$ is non-abelian.

Here we consider another description of permutations. For distinct letters $a_1, \ldots, a_m \in X$, the permutation

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{m-1} & a_m \\ a_2 & a_3 & \cdots & a_m & a_1 \end{pmatrix}$$

is denoted by $(a_1, a_2, \cdots, a_m)$ and is called a **cyclic permutation** of length m. We call a cyclic permutation of length 2 a **transposition**. Namely, any transposition is of type

$$(i, j) = \begin{pmatrix} i & j \\ j & i \end{pmatrix}.$$

A cyclic permutation of length 1 is nothing but the identity permutation:

$$(1) = (2) = \cdots = (n) = \varepsilon.$$

In general, a permutation cannot be written as a single cyclic permutation but a product of some cyclic permutations which do not have a common letter. For example, consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Then we see

$$\sigma : 1 \mapsto 3 \mapsto 4 \mapsto 1, \quad 2 \mapsto 5 \mapsto 2,$$

and hence

$$\sigma = (1,3,4)(2,5) = (2,5)(1,3,4).$$

Remark that two cyclic permutations which do not have a common letter are commutative. For any cyclic permutation $(a_1, a_2, \cdots, a_m)$, we have

$$(a_1, a_2, \cdots, a_m) = (a_1, a_2)(a_2, a_3)\cdots(a_{m-1}, a_m).$$

By using the above facts, we see

Theorem 4.1. *Every permutation can be written as a product of transpositions.*

An expression of a permutation as a product of transpositions is not unique. For example,

$$(1,3,2) = (1,2)(1,3) = (1,3)(2,3).$$

However, we have

Theorem 4.2. *For any permutation σ, consider expressions of σ as a product of transpositions. Then the parity of the number of transpositions is invariant.*

For a permutation σ, if σ is written as a product of even (resp. odd) numbers of transpositions, then σ is called **even permutation** (resp. **odd permutation**). For example, the cyclic permutation $(a_1, a_2, \cdots, a_m)$ is even (resp. odd) permutation if m is odd (resp. even).

4.2. Alternating groups

In this subsection, we consider important normal subgroups of the symmetric groups. Let $\mathfrak{A}_n$ be the set of even permutations of $\mathfrak{S}_n$. For any $\sigma \in \mathfrak{A}_n$, if we write σ as a product of transpositions, $\sigma = \tau_1 \cdots \tau_k$, then we see

$$\sigma^{-1} = \tau_k \tau_{k-1} \cdots \tau_1 \in \mathfrak{A}_n.$$

Clearly, if $\sigma, \tau \in \mathfrak{A}_n$, then $\sigma\tau \in \mathfrak{A}_n$. Thus, the subset $\mathfrak{A}_n$ is a subgroup of $\mathfrak{S}_n$. We call $\mathfrak{A}_n$ the **alternating group** of degree n. It is easily seen that $\mathfrak{A}_n$ is a normal subgroup of $\mathfrak{S}_n$. For example, for $n = 3$ and 4, we have

$$\mathfrak{A}_3 = \{\varepsilon, (1,2,3), (1,3,2)\},$$
$$\mathfrak{A}_4 = \{\varepsilon, (1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

For any $\sigma \in \mathfrak{S}_n$, we have

$$\sigma\mathfrak{A}_n = \begin{cases} (1,2)\mathfrak{A}_n, & \text{if } \sigma \text{ is odd permutation,} \\ \mathfrak{A}_n, & \text{if } \sigma \text{ is even permutation.} \end{cases}$$

Hence $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$. Therefore, from Lagrange's theorem, we see that $\mathfrak{A}_n$ is a finite group of order $n!/2$.

4.3. Dihedral groups

For any $n \in \mathbf{N}$ $(n \geq 3)$, consider a regular polygon V_n with n sides, and fix it. A map $\sigma : V_n \to V_n$ is called a congruent transformation on V_n if σ preserves the distance between any two points in V_n. Namely, σ is considered as a symmetry on V_n. Set

$$D_n := \{\sigma : V_n \to V_n \mid \sigma \text{ is a congruent transformation}\}.$$

For any $\sigma, \tau \in D_n$, define the product of σ and τ to be the composition $\sigma \circ \tau$ as a map. Then the set D_n with this product forms a group. We call it the **dihedral group** of degree n. The unit is the identity transformation.

Each congruent transformation on V_n is determined by the correspondence between vertices of V_n. Indeed, attach the number $1, 2, \ldots, n$ to vertices of V_n in counterclockwise direction. For any $\sigma \in D_n$, if $\sigma(1) = i$, then the vertices $2, 3, \ldots, n$ are mapped to $i+1, i+2, \ldots, n, 1, 2, \ldots i-1$, respectively, Cor mapped to $i-1, i-2, \ldots, 1, n, n-1, \ldots, i+1$, respectively. If we express this by using the notation for permutations, we have

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i & i+1 & \cdots & i-2 & i-1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i & i-1 & \cdots & i+2 & i+1 \end{pmatrix}.$$

The former case is a rotation, and the latter case is the composition of a rotation and a reflection. For $n = 3$, see **Figure 2**. Thus the dihedral group D_n is a finite group of order $2n$ and is naturally considered as a subgroup of $\mathfrak{S}_n$. For $n = 3$, since D_3 is a subgroup of $\mathfrak{S}_3$, and since both groups are of order 6, we see that $D_3 = \mathfrak{S}_3$.

Let $\sigma \in D_n$ be the rotation of V_n with angle $\frac{2\pi}{n}$ in the counterclockwise direction and $\tau \in D_n$ be the reflection of V_n which fixes the vertex 1. Namely,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & n & \cdots & 3 & 2 \end{pmatrix}.$$

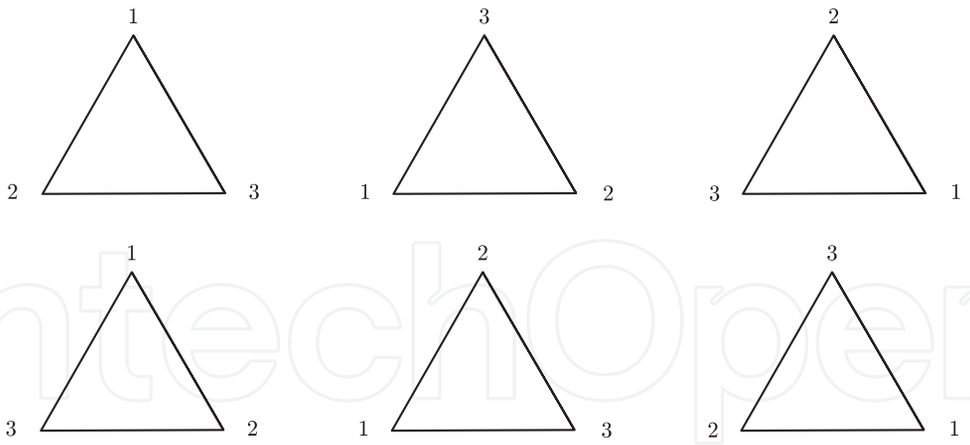

Figure 2. The transformations of the regular triangle.

Then the reflection of V_n which fixes the vertex i is written as $\sigma^{i-1}\tau\sigma^{-(i-1)}$. Hence D_n is generated by σ and τ. Moreover, we have

$$D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}.$$

4.4. The structure theorem for finite abelian groups

In this subsection, we give a complete classification of finite abelian groups up to isomorphism. To begin with, we review the direct product of groups.

Let G and H be groups. Consider the direct product set

$$G \times H := \{(g,h) \mid g \in G,\ h \in H\},$$

and define the product of elements $(g,h), (g',h') \in G \times H$ to be

$$(g,h) \cdot (g',h') := (gg', hh').$$

Then $G \times H$ with this product forms a group. The unit is $(1_G, 1_H)$, and for any $(g,h) \in G \times H$, its inverse is given by $(g^{-1}, h^{-1}) \in G \times H$. We call the group $G \times H$ the **direct product group** of G and H. Similarly, for finitely many groups $G_1, G_2, \ldots, G_n$, we can define its direct product group $G_1 \times \cdots \times G_n$. For each $1 \leq i \leq n$, if G_i is a finite group of order m_i, then $G_1 \times \cdots \times G_n$ is a finite group of order $m_1 m_2 \cdots m_n$. The following theorem is famous in elementary number theory.

Theorem 4.3 (Chinese remainder theorem). *For any $m, n \in \mathbf{N}$ such that $\gcd(m,n) = 1$. Then we have*

$$\mathbf{Z}/mn\mathbf{Z} \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

An isomorphism $f : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ is given by

$$[x]_{mn} \mapsto \left([x]_m, [x]_n\right).$$

(E16) Consider the case $m = 2$ and $n = 3$. Each element $[x]_6$ of $\mathbf{Z}/6\mathbf{Z}$ is mapped to the following element by the above isomorphism f:

$$[1]_6 \mapsto ([1]_2, [1]_3), \quad [2]_6 \mapsto ([2]_2, [2]_3) = ([0]_2, [2]_3), \quad [3]_6 \mapsto ([3]_2, [3]_3) = ([1]_2, [0]_3),$$
$$[4]_6, \mapsto ([4]_2, \ [4]_3) \ = ([0]_2, [1]_3), \quad [5]_6 \mapsto ([5]_2, [5]_3) = ([1]_2, [2]_3), \quad [0]_6 \mapsto ([0]_2, [0]_3).$$

(E17) If $\gcd(m, n) \neq 1$, the theorem does not hold. For example, consider the case of $m = n = 2$. Any element $x \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ satisfies that $x + x$ is equal to zero. On the other hand, for the element $y := [1]_4 \in \mathbf{Z}/4\mathbf{Z}$, $y + y$ is not equal to zero. Hence the group structures of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$ are different.

Now, we show one of the most important theorems in finite group theory.

Theorem 4.4 (structure theorem for finite abelian groups). *Let G be a nontrivial finite abelian group. Then G is isomorphic to a direct product of finite cyclic groups of prime power order*:

$$G \cong \mathbf{Z}/p_1^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{e_r}\mathbf{Z}.$$

The tuple $\left(p_1^{e_1}, p_2^{e_2}, \ldots, p_r^{e_r}\right)$ is uniquely determined by G, up to the order of the factors.

(E18) The list of finite abelian groups of order 72 up to isomorphism is given by

$$\mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}, \quad \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z},$$
$$\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}, \quad \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z},$$
$$\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

5. Conjugacy classes

In this section, we consider the classification of elements of a group by using the conjugation. The results of this section are used in Section 6.

Let G a group. For elements $x, y \in G$, if there exists some $g \in G$ such that $x = gyg^{-1}$; then we say that x is **conjugate** to y and write $x \sim y$. This is an equivalence relation on G. Namely, for any $x \in G$, we have $x \sim x$ by observing $x = 1_G x 1_G^{-1}$. If $x \sim y$, then $x = gyg^{-1}$ for some $g \in G$. Thus $y = g^{-1}x\left(g^{-1}\right)^{-1}$, and hence $y \sim x$. If $x \sim y$ and $y \sim z$, then $x = gyg^{-1}$ and $y = hzh^{-1}$ for some $g, h \in G$. Thus $x = (gh)z(gh)^{-1}$, and hence $x \sim z$. For any $x \in G$, the set

$$C(x) := \{y \in G \mid y \sim x\}$$

is called the **conjugacy class** of x in G. If G is abelian group, for any $x \in G$, there exists no element conjugate to x except for x, and hence $C(x) = \{x\}$. Here we give a few examples.

(E19) (Dihedral groups) For $n \geq 3$, the conjugacy classes of D_n are as follows:

1. If n is even:

$$\{1\}, \{\sigma, \sigma^{-1}\}, \{\sigma^2, \sigma^{-2}\}, \ldots, \left\{\sigma^{\frac{n-2}{2}}, \sigma^{\frac{2-n}{2}}\right\}, \left\{\sigma^{\frac{n}{2}}\right\},$$
$$\{\tau, \sigma^2\tau, \ldots, \sigma^{n-2}\tau\}, \{\sigma\tau, \sigma^3\tau, \ldots, \sigma^{n-1}\tau\}.$$

2. If n is odd:

$$\{1\}, \{\sigma, \sigma^{-1}\}, \{\sigma^2, \sigma^{-2}\}, \ldots, \left\{\sigma^{\frac{n-1}{2}}, \sigma^{\frac{1-n}{2}}\right\},$$
$$\{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\}.$$

Indeed, for the case where n is even, we can see the above from the following observation. For any $x \in D_n$, since

$$x\sigma^i x^{-1} = \begin{cases} \sigma^j\sigma^i\sigma^{-j} = \sigma^i, & \text{if } x = \sigma^j, \\ \sigma^j\tau\sigma^i\tau\sigma^{-j} = \sigma^{-i}, & \text{if } x = \sigma^j\tau, \end{cases}$$

the conjugates of σ^i are $\sigma^{\pm i}$. On the other hand, for any $x \in D_n$, since

$$x\sigma^i\tau x^{-1} = \begin{cases} \sigma^j\sigma^i\tau\sigma^{-j} = \sigma^{i+2j}\tau, & \text{if } x = \sigma^j, \\ \sigma^j\tau\sigma^i\tau\tau\sigma^{-j} = \sigma^{i+2(j-i)}\tau, & \text{if } x = \sigma^j\tau, \end{cases}$$

the conjugates of $\sigma^i\tau$ are $\sigma^k\tau$ for any k such that $k \equiv i \pmod 2$. These facts induce Part (1).

(E20) (Symmetric groups) For any $\sigma \in \mathfrak{S}_n$, we can write σ as a product of cyclic permutations which do not have a common letter, like

$$\sigma = (a_1 \cdots a_k)(b_1 \cdots b_l) \cdots (c_1 \cdots c_m).$$

Furthermore, we may assume $k \geq l \geq \cdots \geq m$ since the cyclic permutations appeared in the right hand side are commutative. Then we call $(k, l, \ldots, m)$ is the **cycle type** of σ.

Theorem 5.1. *Elements $\sigma, \sigma' \in \mathfrak{S}_n$ are conjugate if and only if the cycle types of σ and σ' are equal.*

For example, conjugacy classes of $\mathfrak{S}_4$ are given by

Cycle type	**Conjugacy class**
$(1,1,1,1)$	$\{1_{\mathfrak{S}_4}\}$
$(2,1,1)$	$\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$
$(2,2)$	$\{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$
$(3,1)$	$\{(1,2,3),(1,2,4),(1,3,2),(1,3,4),(1,4,2),(1,4,3),(2,3,4),(2,4,3)\}$
(4)	$\{(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\}$

In the above examples, we verify that the number of elements of any conjugacy class is a divisor of the order of the group. In general, we have

Theorem 5.2. *Let G be a finite group. For any $x \in G$, $|C(x)|$ is a divisor of $|G|$.*

6. Representation theory of finite groups

In this section, we give a brief introduction to representation theory of finite groups. There are also hundreds of textbooks for the representation theory. One of the most famous and standard textbooks is [5]. For high motivated readers, see [6–8] for mathematical details.

6.1. Representations

In this subsection, we assume that G is a finite group. Let V be a finite-dimensional $\mathbf{C}$-vector space. Consider the following situation. For any $\sigma \in G$ and any $\mathbf{v} \in V$, there exists a unique element $\sigma \cdot \mathbf{v} \in V$ such that

1. $\sigma \cdot (\boldsymbol{v} + \boldsymbol{w}) = \sigma \cdot \boldsymbol{v} + \sigma \cdot \boldsymbol{w}$,
2. $\sigma \cdot (\alpha \boldsymbol{v}) = \alpha(\sigma \cdot \boldsymbol{v})$,
3. $\sigma \cdot (\tau \cdot \boldsymbol{v}) = (\sigma\tau) \cdot \boldsymbol{v}$,
4. $1_G \cdot \boldsymbol{v} = \boldsymbol{v}$

for any $\sigma, \tau \in G$, $\alpha \in \mathbf{C}$ and $\boldsymbol{v}, \boldsymbol{w} \in V$. Then we say that G **acts** on V and V is called a G**-vector space**.

The conditions (1) and (2) mean that for any $\sigma \in G$, the map $\rho(\sigma) : V \to V$ defined by $\mathbf{v} \mapsto \sigma \cdot \mathbf{v}$ is a linear transformation on V. Furthermore, from the conditions (3) and (4), we see that for any $\sigma \in G$, the linear transformation $\rho\left(\sigma^{-1}\right)$ is the inverse linear transformation of $\rho(\sigma)$. Namely, each $\rho(\sigma)$ is a bijective. Set

$$\mathrm{GL}(V) := \{f : V \to V \mid f \text{ is abijective linear transformation}\},$$

and consider it as a group with the product given by the composition of maps. Then we obtain the group homomorphism $\rho : G \to \mathrm{GL}(V)$ by $\sigma \mapsto \rho(\sigma)$. In general, for a finite group G and for a finite-dimensional $\mathbf{C}$-vector space V, a homomorphism $\rho : G \to \mathrm{GL}(V)$ is called a **representation** of G. Then V is a G-vector space by the action of G on V given by

$$\sigma \cdot \boldsymbol{v} := (\rho(\sigma))(\mathbf{v})$$

for any $\sigma \in G$ and $\boldsymbol{v} \in V$. The dimension $\dim_{\mathbf{C}} V$ of V as a $\mathbf{C}$-vector space is called the **degree** of the representation ρ. Observe the following examples:

(E21) For any finite group G, and any $\mathbf{C}$-vector space V, we can consider the trivial action of G on V by $\sigma \cdot \boldsymbol{v} := \boldsymbol{v}$ for any $\sigma \in G$ and $\boldsymbol{v} \in V$. Namely, we can consider the homomorphism $\mathbf{triv} : G \to \mathrm{GL}(V)$ by assigning σ to the identity map on V for any $\sigma \in G$. This is called the **trivial representation** of G.

(E22) For any $n \in \mathbf{N}$, consider the cyclic group $\mathcal{U}_n$ and the action of $\mathcal{U}_n$ on $\mathbf{C}$ given by the usual multiplication $\exp\left(2k\pi\sqrt{-1}/n\right) \cdot z := \exp\left(2k\pi\sqrt{-1}/n\right)z$ of the complex numbers for any $k \in \mathbf{Z}$ and $z \in \mathbf{C}$. The action of $\exp\left(2k\pi\sqrt{-1}/n\right)$ on $\mathbf{C}$ is the rotation on $\mathbf{C}$ in the counterclockwise direction centered at the origin with angle $(2k\pi)/n$. If we take $1 \in \mathbf{C}$ as a basis of the $\mathbf{C}$-vector space $\mathbf{C}$, we can identify $\mathrm{GL}(\mathbf{C})$ with the general linear group $\mathrm{GL}(1, \mathbf{C}) = \mathbf{C}^\times$ by considering the matrix representation. Under this identification, the corresponding representation $\rho : \mathcal{U}_n \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^\times$ is given by the natural inclusion map $\mathcal{U}_n \acute{} \mathbf{C}^\times$.

(E23) Consider the symmetric group $\mathfrak{S}_3$ and the numerical vector space $\mathbf{C}^3$. The group $\mathfrak{S}_3$ naturally acts on $\mathbf{C}^3$ by the permutation of the components given by

$$\sigma \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} := \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ x_{\sigma^{-1}(3)} \end{pmatrix}.$$

If we take the standard basis $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$ as a basis of $\mathbf{C}^3$, we can identify $\mathrm{GL}\left(\mathbf{C}^3\right)$ with the general linear group $\mathrm{GL}(3, \mathbf{C})$ by considering the matrix representation. Under this identification, the corresponding representation $\rho : \mathfrak{S}_3 \to \mathrm{GL}\left(\mathbf{C}^3\right) = \mathrm{GL}(3, \mathbf{C})$ is given by $\sigma \mapsto \left(\boldsymbol{e}_{\sigma(1)}\, \boldsymbol{e}_{\sigma(2)} \boldsymbol{e}_{\sigma(3)}\right)$. Similarly, we can obtain the representation $\rho : \mathfrak{S}_n \to \mathrm{GL}(\mathbf{C}^n) = \mathrm{GL}(n, \mathbf{C})$ that is given by

$$\sigma \mapsto \left(\boldsymbol{e}_{\sigma(1)}\, \boldsymbol{e}_{\sigma(2)} \cdots \boldsymbol{e}_{\sigma(n)}\right).$$

This is called the **permutation representation** of $\mathfrak{S}_n$.

Next we consider subrepresentations of a representation. Let $\rho : G \to \mathrm{GL}(V)$ a representation. If there exists a subspace W of V such that

$$\sigma \cdot \boldsymbol{w} \in W \ (\Leftrightarrow (\rho(\sigma))(\boldsymbol{w}) \in W)$$

for any $\sigma \in G$ and $\boldsymbol{w} \in W$, then W is called a G**-subspace** of V. For any $\sigma \in G$, the restriction $\rho(\sigma)|_W : W \to W$ of $\rho(\sigma)$ is a bijective linear transformation on W, and we obtain the representation $\rho|_W : G \to \mathrm{GL}(W)$ given by $\sigma \mapsto \rho(\sigma)|_W$. It is called a **subrepresentation** of ρ.

(E24) Consider the permutation representation $\rho : \mathfrak{S}_3 \to \mathrm{GL}\left(\mathbf{C}^3\right) = \mathrm{GL}(3, \mathbf{C})$ as in (E23). Let us consider subspaces

$$W_1 := \left\{ \begin{pmatrix} x \\ x \\ x \end{pmatrix} \;\middle|\; x \in \mathbf{C} \right\},\ W_2 := \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \;\middle|\; x, y, z \in \mathbf{C},\ x + y + z = 0 \right\}$$

of $\mathbf{C}^3$. It is easily seen that these are $\mathfrak{S}_3$-subspaces and the subrepresentation $\rho|_{W_1}$ is the trivial representation. Geometrically, W_1 and W_2 in $\mathbf{C}^3$ are drawn in **Figure 3**. In a precise sense, if we naturally consider $\mathbf{R}^3$ as a subset of $\mathbf{C}^3$, then **Figure 3** shows $W_1 \cap \mathbf{R}^3$ and $W_2 \cap \mathbf{R}^3$ in $\mathbf{R}^3$.

For a G-vector space V, if there exist G-subspaces W_1 and W_2 of V such that any element $\mathbf{v} \in V$ can be **uniquely** written as

$$\boldsymbol{v} = \boldsymbol{w}_1 + \boldsymbol{w}_2 \ (\boldsymbol{w}_1 \in W_1, \boldsymbol{w}_2 \in W_2),$$

then V is called the **direct sum** of W_1 and W_2 and is written as $V = W_1 \oplus W_2$. Similarly, we can define the direct sum of G-subspaces $W_1, W_2, \ldots, W_m$ for any $m \geq 3$. Let ρ, $\rho|_{W_1}$, and $\rho|_{W_2}$ be the correspondent representations of G to V, W_1, and W_2, respectively. We also say that the representation ρ is the direct sum of $\rho|_{W_1}$ and $\rho|_{W_2}$.

(E25) As the notation in (E24), V is the direct sum of W_1 and W_2. Indeed, for the standard basis $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$ of V, we see that $\boldsymbol{e}_1 + \boldsymbol{e}_2 + \boldsymbol{e}_3$ and $\boldsymbol{e}_1 - \boldsymbol{e}_2, \boldsymbol{e}_1 - \boldsymbol{e}_3$ are bases of W_1 and W_2, respectively. Thus, for any $\boldsymbol{x} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + x_3\boldsymbol{e}_3 \in \mathbf{C}^3$, we can rewrite

$$\boldsymbol{x} = \frac{x_1 + x_2 + x_3}{3}(\boldsymbol{e}_1 + \boldsymbol{e}_2 + \boldsymbol{e}_3) + \frac{x_1 - 2x_2 + x_3}{3}(\boldsymbol{e}_1 - \boldsymbol{e}_2) + \frac{x_1 + x_2 - 2x_3}{3}(\boldsymbol{e}_1 - \boldsymbol{e}_3).$$

Furthermore, we verify that this expression is unique by direct calculations.

In general, we have

Theorem 6.1 (Maschke). *Let $\rho : G \to \mathrm{GL}(V)$ a representation and W a G-subspace of V. Then there exists a G-subspace W' such that $V = W \oplus W'$.*

6.2. Irreducible representations

In subsection 4.4, we have discussed the classification of finite abelian groups by using the concept of group isomorphisms. Here we consider the classification of finite-dimensional representations of finite groups by using irreducible representations and equivalence relations among representations.

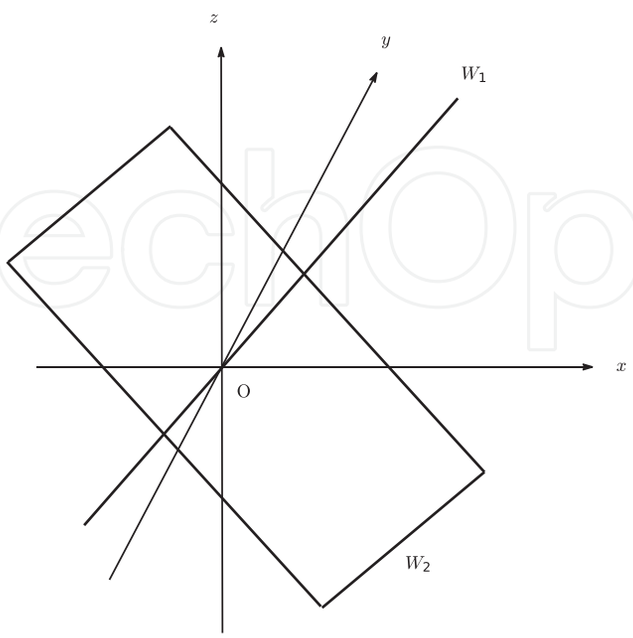

Figure 3. The subspaces W_1 and W_2 in $\mathbf{C}^3$.

Let G be a finite group and $\rho : G \to \mathrm{GL}(V)$ its representation. The trivial subspaces $\{\mathbf{0}\}$ and V are G-subspaces of V. If V has no G subspace other than these, V is called the **irreducible G-space**, and ρ is called the **irreducible representation** of G.

(E26) Any one-dimensional representation is trivial. For example, the representation $\rho : \mathcal{U}_n \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^\times$ in (E23) is irreducible. Let us consider the other example. For any $\sigma \in \mathfrak{S}_n$, set

$$\mathrm{sgn}\,(\sigma) := \begin{cases} 1 & \text{if} \quad \sigma \text{ is even permutation,} \\ -1 & \text{if} \quad \sigma \text{ is odd permutation.} \end{cases}$$

Then we can easily see that the map $\mathrm{sgn} : \mathfrak{S}_n \to \mathbf{C}^\times = \mathrm{GL}(\mathbf{C})$ is a homomorphism and, hence, is a representation of $\mathfrak{S}_n$. This irreducible representation is called the **signature representation** of $\mathfrak{S}_n$.

(E27) As the notation in (E24), $\rho|_{W_1}$ is irreducible since it is one-dimensional. The representation $\rho|_{W_2}$ is also irreducible. Indeed, if W_2 is not irreducible, there exists a one-dimensional G-subspace W in W_2 since W_2 is a 2-dimensional G-vector space. Take $\boldsymbol{w} \in W$ ($\boldsymbol{w} \neq \mathbf{0}$). Then $\boldsymbol{w}$ is an eigenvector of $\rho|_{W_2}(\sigma)$ for any $\sigma \in \mathfrak{S}_3$. However, we can see that there is no such vector in W_2 by direct calculations.

By observing (E25), (E26), and (E27), we see that $\mathbf{C}^3$ is a direct sum of the irreducible G-subspaces W_1 and W_2. In general, by using Maschke's theorem above, we obtain.

Theorem 6.2. *For any representation $\rho : G \to \mathrm{GL}(V)$ of a finite group G, the G-vector space V can be written as a direct sum of some irreducible G-subspaces. Namely, ρ can be written as sum of some irreducible representations of G.*

Remark that the expression of a direct sum of irreducible representations is not unique in general. For example, let $\rho : G \to \mathrm{GL}(\mathbf{C}^2)$ be the trivial representation. Then for the standard basis $\boldsymbol{e}_1, \boldsymbol{e}_2$ of $\mathbf{C}^2$, we have

$$\mathbf{C}^2 = \mathbf{C}\boldsymbol{e}_1 \oplus \mathbf{C}\boldsymbol{e}_2 = \mathbf{C}\boldsymbol{e}_1 \oplus \mathbf{C}(\boldsymbol{e}_1 + \boldsymbol{e}_2) = \mathbf{C}\boldsymbol{e}_1 \oplus \mathbf{C}(\boldsymbol{e}_1 + 2\boldsymbol{e}_2) = \cdots.$$

In order to do the classification of representations, we consider the equivalency of representations. Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be representations of G. If there exists a bijective linear map $\iota : V_1 \to V_2$ such that

$$\iota(\sigma \cdot \boldsymbol{v}) = \sigma \cdot \iota(\boldsymbol{v}), \quad \sigma \in G, \boldsymbol{v} \in V_1,$$

then we say that V_1 is isomorphic to V_2 as a G-vector space and write $V_1 \cong V_2$. We also say that ρ_1 is equivalent to ρ_2 and write $\rho_1 \sim \rho_2$.

(E28) For any group G. let **unit** : $G \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^\times$ be the trivial representation of G. Then any trivial representation $\rho : G \to \mathrm{GL}(V)$ is equivalent to **unit**. The representation **unit** is called the **unit representation** of G.

The following theorem is one of the most important theorems in representation theory of finite groups.

Theorem 6.3. *Let G be a finite group.*

1. *The number of irreducible representations of G up to equivalent is finite. Furthermore, it is equal to the number of the conjugacy classes of G.*
2. *For any representation $\rho : G \to \mathrm{GL}(V)$, ρ is equivalent to a direct sum of some irreducible representations*:

   $V \cong W_1 \oplus W_2 \oplus \cdots \oplus W_m$.

   Furthermore, the tuple of the components is uniquely determined by G, up to the order.

6.3. Characters

In this subsection, for a given representation, we give a method to determine whether it is irreducible or not by using characters. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Take a basis $v_1, \ldots, v_n$ of V, and fix it. By using this basis, we can consider $\rho(\sigma)$ as an $(n \times n)$-matrix $A_\sigma = (a_{ij})$, which is the matrix representation of $\rho(\sigma)$. Then set

$$\chi_\rho(\sigma) := \mathrm{Tr}(A_\sigma) = a_{11} + a_{22} + \cdots + a_{nn} \in \mathbf{C}$$

for any $\sigma \in G$. Remark that this definition is well defined since it does not depend on the choice of a basis of V. Indeed, if $w_1, \ldots, w_n$ is another basis of V, the matrix representation of $\rho(\sigma)$ with respect to this basis is given by $P^{-1}A_\sigma P$ for a some regular matrix P. Hence $\mathrm{Tr}(P^{-1}A_\sigma P) = \mathrm{Tr}(A_\sigma)$. We call the map $\chi_\rho : G \to \mathbf{C}$ the **character** of ρ. Remark that for elements $\sigma, \tau \in G$, if $\sigma \sim \tau$, then $\rho(\sigma) \sim \rho(\tau)$ in $\mathrm{GL}(V)$. Thus, $\chi_\rho(\sigma) = \chi_\rho(\tau)$. Namely, χ_ρ is constant on each of the conjugacy classes of G.

(E29) Consider the example (E25). Let $\rho : \mathfrak{S}_3 \to \mathrm{GL}(\mathbf{C}^3)$ be the permutation representation of $\mathfrak{S}_3$. The conjugacy classes of $\mathfrak{S}_3$ are as follows:

Cycle type	Conjugacy class
$(1,1,1)$	$\{1_{\mathfrak{S}_3}\}$
$(2,1)$	$\{(1,2),(1,3),(2,3)\}$
(3)	$\{(1,2,3),(1,3,2)\}$

Hence, in order to calculate the values of the character χ_ρ of ρ, it suffices to calculate its values on $1_{\mathfrak{S}_3}$, $(1,2)$, and $(1,2,3)$. If we take the standard basis e_1, e_2, e_3 of $\mathbf{C}^3$, we have $\rho(\sigma) = (e_{\sigma(1)}\, e_{\sigma(2)}\, e_{\sigma(3)})$, and hence

$$\chi_\rho(1_{\mathfrak{S}_3}) = 3, \quad \chi_\rho((1,2)) = 1, \quad \chi_\rho((1,2,3)) = 0.$$

In general, as in (E29), for a representation $\rho : G \to \mathrm{GL}(V)$, $\chi_\rho(1_G)$ is the degree of the representation, which is equal to $\dim_{\mathbf{C}}(V)$.

Now, we define the inner product of characters. For complex functions $\varphi, \psi : G \to \mathbf{C}$ on G, set

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \varphi(\sigma)\overline{\psi(\sigma)}$$

where $\overline{z}$ means the complex conjugation of $z \in \mathbf{C}$. We call it the inner product of ϕ and ψ. The following theorems are quite important and useful from the viewpoint to find and to calculate all of the irreducible representations.

Theorem 6.4.

1. (*Orthogonality*) *Let* $\rho_i : G \to \mathrm{GL}(V_i)$ $(i = 1, 2)$ *be irreducible representations. Then*

$$\left\langle \chi_{\rho_1}, \chi_{\rho_2} \right\rangle = \begin{cases} 1 & \text{if} \quad \rho_1 \sim \rho_2, \\ 0 & \text{if} \quad \rho_1 / \sim \rho_2. \end{cases}$$

2. For a representation $\rho : G \to \mathrm{GL}(V)$,

$$\rho \ \textit{is irreducible} \Leftrightarrow \left\langle \chi_\rho, \chi_\rho \right\rangle = 1.$$

σ	$\mathbf{1}_{\mathfrak{S}_3}$	$(\mathbf{1},\mathbf{2})$	$(\mathbf{1},\mathbf{3})$	$(\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{2})$
$\chi_{\mathbf{unit}}(\sigma)$	1	1	1	1	1	1
$\chi_{\mathrm{sgn}}(\sigma)$	1	−1	−1	−1	1	1
$\chi_{\rho\vert_{W_2}}(\sigma)$	2	0	0	0	−1	−1

(E30) We have the three irreducible representations of $\mathfrak{S}_3$. By direct calculations, we obtain the following list:

Hence we see that in each of cases, we have $\left\langle \chi_\rho, \chi_\rho \right\rangle = 1$.

By Theorem 6.3, we see that for any representation $\rho : G \to \mathrm{GL}(V)$, V can be written as

$$V \cong W_1^{\oplus m_1} \oplus W_2^{\oplus m_2} \oplus \cdots \oplus W_k^{\oplus m_k}$$

where each W_i is an irreducible G-vector space and W_i is not isomorphic to W_j as a G-vector space if $i \neq j$. For each $1 \leq i \leq k$, the number m_i is called the **multiplicity** of W_i in V.

Theorem 6.5. *As the notation above, let* ρ_i *be the irreducible representation of* G *correspond to the* G*-vector space* W_i*. Then we have*

1. $\chi_\rho = m_1\chi_{\rho_1} + \cdots + m_k\chi_{\rho_k}$.

2. $\left\langle \chi_\rho, \chi_{\rho_i} \right\rangle = m_i$.

Namely, each of the multiplicity of the irreducible G*-vector spaces in* V *is calculated by the inner product of the characters*

3. $|G| = \sum_{i=1}^{k} \chi_{\rho_i}(1)^2$.

Namely, the sum of the squares of the degrees of the irreducible representations is equal to the order of G.

From the above theorems, we verify that if we want to know all irreducible representations of G, it suffices to calculate its characters. The list of all values of all characters is called the **character table** of G. Finally, we give a few examples of the character tables of finite groups.

(E31) Observe (E30). Since we have

$$\chi_{\mathbf{unit}}(1)^2 + \chi_{\mathrm{sgn}}(1)^2 + \chi_{\rho|_{W_2}}(1)^2 = 4 + 1 + 1 = 6 = |\mathfrak{S}_3|,$$

it turns out that **unit**, sgn, and $\rho|_{W_2}$ are all irreducible representations of $\mathfrak{S}_3$ up to equivalence. Hence the list in (E30) is the character table of $\mathfrak{S}_3$.

(E32) Consider the cyclic group $\mathcal{U}_n$. Since $\mathcal{U}_n$ is abelian, any conjugacy class consists of a single element, and there exist n conjugacy classes. Hence there exist n distinct irreducible representations. Now, for any $0 \leq l \leq n-1$, define the map $\rho_l : \mathcal{U}_n \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^\times$ by

$$\zeta^k \mapsto \zeta^{kl} \quad (0 \leq k \leq n-1)$$

where $\zeta = \exp\left(2\pi\sqrt{-1}/n\right)$. Then we obtain

σ	$\mathbf{1}_{\mathcal{U}_n}$	ζ	ζ^2	...	ζ^{n-1}
$\chi_{\rho_0}(\sigma)$	1	1	1	1	1
$\chi_{\rho_1}(\sigma)$	1	ζ	ζ^2	...	ζ^{n-1}
$\vdots$					$\vdots$
$\chi_{\rho_{n-1}}(\sigma)$	1	ζ^{n-1}	ζ^{n-2}	...	ζ

Hence we see that $\rho_0, \rho_1, \ldots, \rho_{n-1}$ are nonequivalent one-dimensional representations, and hence the above list is the character table of $\mathcal{U}_n$. In general, all irreducible representations of an abelian group are of degree 1.

(E33) (Dihedral groups) For $n \geq 3$, consider the dihedral groups D_n. First, for any $a, b = \pm 1$, there exist the four one-dimensional representations $\varepsilon_{a,b} : D_n \to \mathbf{C}^\times$ defined by

$$\varepsilon_{a,b}(x) = \begin{cases} (-1)^{ak} & \text{if} \quad x = \sigma^k, \\ (-1)^{ak+b} & \text{if} \quad x = \sigma^k\tau. \end{cases}$$

These maps are characterized by the images of σ and τ, which are $(-1)^a$ and $(-1)^b$, respectively. Next, for any $1 \leq l \leq n-1$, we can consider the two-dimensional representations $\rho_l : D_n \to \mathrm{GL}(2, \mathbf{C})$ given by

$$\rho_l(x) = \begin{cases} \begin{pmatrix} \cos 2kl\pi/n & -\sin 2kl\pi/n \\ \sin 2kl\pi/n & \cos 2kl\pi/n \end{pmatrix} & \text{if} \quad x = \sigma^k, \\ \begin{pmatrix} \cos 2kl\pi/n & -\sin 2kl\pi/n \\ \sin 2kl\pi/n & \cos 2kl\pi/n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{if} \quad x = \sigma^k\tau. \end{cases}$$

i. The case where n is even. For any $1 \leq l \leq \frac{n-2}{2}$, since we can see $\left\langle \chi_{\rho_l}, \chi_{\rho_l} \right\rangle = 1$ by direct calculation, ρ_ls are irreducible representations of D_n. Since we have

$$\begin{aligned} \chi_{\varepsilon_{1,1}}(1)^2 + \quad & \chi_{\varepsilon_{1,-1}}(1)^2 + \chi_{\varepsilon_{-1,1}}(1)^2 + \chi_{\varepsilon_{-1,-1}}(1)^2 \\ & + \chi_{\rho_1}(1)^2 + \cdots + \chi_{\rho_{\frac{n-2}{2}}}(1)^2 = 2n = |D_n|, \end{aligned}$$

it turns out that $\varepsilon_{a,b}$ and ρ_l for $a, b = \pm 1$ and $1 \leq l \leq \frac{n-2}{2}$ are all irreducible representations of D_n up to equivalence. The character table of D_4 is give as follows:

x	$\{\mathbf{1}_{D_4}\}$	$\{\sigma, \sigma^3$	$\{\sigma^2\}$	$\{\sigma\tau, \sigma^3\tau\}$	$\{\tau, \sigma^2\tau\}$
$\chi_{\varepsilon_{1,1}}(x)$	1	1	1	1	1
$\chi_{\varepsilon_{1,-1}}(x)$	1	1	1	−1	−1
$\chi_{\varepsilon_{-1,1}}(x)$	1	−1	1	−1	1
$\chi_{\varepsilon_{-1,-1}}(x)$	1	−1	1	1	−1
$\chi_{\rho_1}(\sigma)$	2	0	−2	0	0

ii. The case where n is odd. Similarly, we can see that $\varepsilon_{1,b}$ and ρ_l for $b = \pm 1$ and $1 \leq l \leq \frac{n-1}{2}$ are all irreducible representations of D_n up to equivalence. The character table of D_5 is give as follows:

x	$\{\mathbf{1}_{D_5}\}$	$\{\sigma, \sigma^4\}$	$\{\sigma^2, \sigma^3\}$	$\{\tau, \sigma\tau, \ldots, \sigma^4\tau\}$
$\chi_{\varepsilon_{1,1}}(x)$	1	1	1	1
$\chi_{\varepsilon_{1,-1}}(x)$	1	1	1	−1
$\chi_{\rho_1}(\sigma)$	2	$2\cos 2\pi/5$	$2\cos 4\pi/5$	0
$\chi_{\rho_2}(\sigma)$	2	$2\cos 4\pi/5$	$2\cos 2\pi/5$	0

7. Direct products

In chemistry, groups appear in symmetries of molecules. The structures of some of them are given by direct products of finite groups. Here we consider direct product groups and its irreducible representations.

Let G and H be finite groups. Set

$$G \times H := \{(g,h) \mid g \in G,\ h \in H\},$$

and define the product on $G \times H$ by

$$(g,h) \cdot (g',h') := (gg',hh').$$

Then $G \times H$ with this product forms a group. This is called the **direct product group** of G and H. The unit is $(1_G, 1_H)$, and the inverse of (g,h) is $\left(g^{-1}, h^{-1}\right)$. If G and H are finite groups, then it is clear that $|G \times H| = |G||H|$. For conjugacy classes C and C' of G and H, respectively, the direct product set $C \times C'$ is a conjugacy class of $G \times H$, and any conjugacy class of $G \times H$ is obtained by this way.

In order to construct irreducible representations of $G \times H$, we consider tensor products of vector spaces. For G-vector space V and H-vector space W, let F be the vector space with basis $\{(\boldsymbol{v},\boldsymbol{w}) \mid \boldsymbol{v} \in V,\ \ \boldsymbol{w} \in W\}$ and R the subspace of F generated by

$$\begin{aligned}
&(\boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{w}) - (\boldsymbol{v}_1, \boldsymbol{w}) - (\boldsymbol{v}_2, \boldsymbol{w}),\\
&(\boldsymbol{v}, \boldsymbol{w}_1 + \boldsymbol{w}_2) - (\boldsymbol{v}, \boldsymbol{w}_1) - (\boldsymbol{v}, \boldsymbol{w}_2),\\
&(\alpha\boldsymbol{v}, \boldsymbol{w}) - \alpha(\boldsymbol{v}, \boldsymbol{w}),\ \ (\boldsymbol{v}, \alpha\boldsymbol{w}) - \alpha(\boldsymbol{v}, \boldsymbol{w}),
\end{aligned}$$

for any $\boldsymbol{v}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in V$, $\boldsymbol{w}, \boldsymbol{w}_1, \boldsymbol{w}_2 \in W$, and $\alpha \in \mathbf{C}$. The quotient vector space F/R is called the **tensor product** of V and W and is denoted by $V \otimes W$. The coset class of $(\boldsymbol{v}, \boldsymbol{w})$ is denoted by $\boldsymbol{v} \otimes \boldsymbol{w}$. If $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ and $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ are bases of V and W, respectively, then elements $\boldsymbol{v}_i \otimes \boldsymbol{w}_j$ ($1 \le i \le m$ and $1 \le j \le n$) form a basis of $V \otimes W$. Hence $\dim(V \otimes W) = (\dim V)(\dim W)$.

For any $g \in G$ and $h \in H$, we can define the action of $G \times H$ on $V \otimes W$ by

$$(g,h) \cdot \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}\boldsymbol{v}_i \otimes \boldsymbol{w}_j := \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}(g\boldsymbol{v}_i) \otimes \left(h\boldsymbol{w}_j\right),$$

and hence, $V \otimes W$ is a $G \times H$-vector space. For the representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ corresponding to the G-vector spaces V and W, respectively, we denote by $\rho \otimes \rho' : G \to \mathrm{GL}(V \otimes W)$ the representation corresponding to the $(G \times H)$-vector space $V \otimes W$. Then we have

Theorem 7.1. (*1*) *As the notation above, if* ρ *and* ρ' *are irreducible, so is* $\rho \otimes \rho'$.

(2) If $\rho_1, \ldots, \rho_k$ (*resp.* $\rho'_1, \ldots, \rho'_l$) *are all irreducible representations of* G (*resp.* H) *up to equivalence, then* $\rho_i \otimes \rho_{j'}$ ($1 \le i \le m$ *and* $1 \le j \le n$) *are all irreducible representations of* $G \times H$ *up to equivalence.*

(E34) For $V = \mathbf{C}$ and $W = \mathbf{C}$, the tensor product $V \otimes W$ of V and W is a one-dimensional $\mathbf{C}$-vector space with basis $1 \otimes 1$. Thus, we have a bijective linear map $V \otimes W \to \mathbf{C}$ given by

$$a(1 \otimes 1) \mapsto a.$$

In general, we identify $\mathbf{C} \otimes \mathbf{C}$ with $\mathbf{C}$ through this map.

Let us consider the direct product $\mathcal{U}_2 \times \mathcal{U}_3$. Under the identification $\mathbf{C} \otimes \mathbf{C} = \mathbf{C}$, the character table is given as follows:

σ	$\{(\mathbf{1},\mathbf{1})\}$	$\{(\mathbf{1},\zeta)\}$	$\{(\mathbf{1},\zeta^{\mathbf{2}})\}$	$\{(-\mathbf{1},\mathbf{1})\}$	$\{(-\mathbf{1},\zeta)\}$	$\{(-\mathbf{1},\zeta^{\mathbf{2}})\}$
$\chi_{\rho_0 \otimes \rho_0}(\sigma)$	1	1	1	1	1	1
$\chi_{\rho_0 \otimes \rho_1}(\sigma)$	1	ζ	ζ^2	1	ζ	ζ^2
$\chi_{\rho_0 \otimes \rho_2}(\sigma)$	1	ζ^2	ζ	1	ζ^2	ζ
$\chi_{\rho_1 \otimes \rho_0}(\sigma)$	1	1	1	-1	-1	-1
$\chi_{\rho_1 \otimes \rho_1}(\sigma)$	1	ζ	ζ^2	-1	$-\zeta$	$-\zeta^2$
$\chi_{\rho_1 \otimes \rho_2}(\sigma)$	1	ζ^2	ζ	-1	$-\zeta^2$	$-\zeta$

where $\zeta = \exp 2\pi\sqrt{-1}/3$.

(E35) Consider the direct product $\mathcal{U}_2 \times \mathfrak{S}_3$. Its character table is given as follows:

σ	$\{(\mathbf{1},\mathbf{1}_{\mathfrak{S}_3})\}$	$\{(\mathbf{1},(\boldsymbol{i},\boldsymbol{j}))\}$	$\{(\mathbf{1},(\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}))\}$	$\{(-\mathbf{1},\mathbf{1}_{\mathfrak{S}_3})\}$	$\{(-\mathbf{1},(\boldsymbol{i},\boldsymbol{j}))\}$	$\{(-\mathbf{1},(\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}))\}$
$\chi_{\rho_0 \otimes \mathbf{unit}}(\sigma)$	1	1	1	1	1	1
$\chi_{\rho_0 \otimes \mathrm{sgn}}(\sigma)$	1	-1	1	1	-1	1
$\chi_{\rho_0 \otimes \rho\vert_{W_2}}(\sigma)$	2	0	-1	2	0	-1
$\chi_{\rho_1 \otimes \mathbf{unit}}(\sigma)$	1	1	1	-1	-1	-1
$\chi_{\rho_1 \otimes \mathrm{sgn}}(\sigma)$	1	-1	1	-1	1	-1
$\chi_{\rho_1 \otimes \rho\vert_{W_2}}(\sigma)$	2	0	-1	-2	0	1

8. Graphs and their automorphisms

In this section, we consider directed graphs and their automorphism groups. Here we do not assume for the reader to know the facts in Sections 5 and 6.

8.1. Graphs

According to literatures, there are several different definitions of a graph. Briefly Ca **directed graph** Γ consists of **vertices** and **oriented edges** whose endpoints are vertices. (For details for the definition of graphs, see page 14 of [9].) For an oriented edge e, we denote by $i(e)$ and $t(e)$ the **initial vertex** and the **terminal vertex** of e. Each oriented edge e has the **inverse edge** $\overline{e}$ such that $\overline{e} \neq e$ and $\overline{\overline{e}} = e$. It is clear that $i(\overline{e}) = t(e)$ and $t(\overline{e}) = i(e)$. An oriented edge e such that $i(e) = t(e)$ is called a **loop**. For any $v, w \in V(\Gamma)$, we assume that there may exist more than one oriented edge whose initial vertex is v and terminal vertex w. If this is the case, we say that Γ has multiple oriented edges.

(E36) A directed graph is easy to understand if it is drawn by a picture. See **Figure 4**. The vertices v, w, x, y, z are depicted by small circles. The oriented edges a, b, c, d, e, f, g, h are

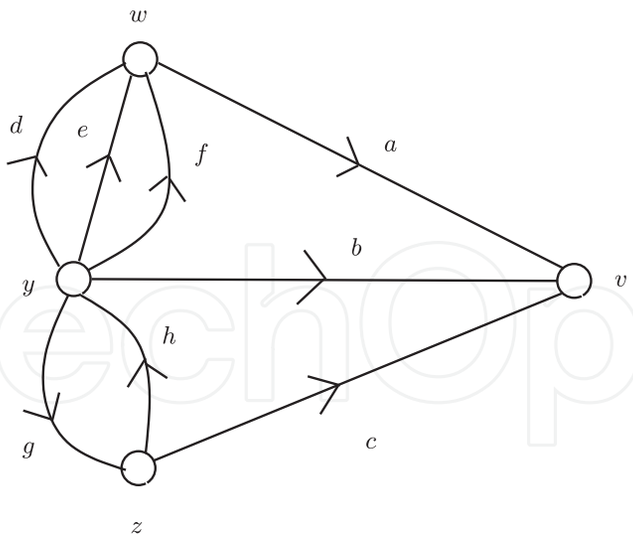

Figure 4. An example of a graph.

depicted by arrows from the initial vertex to the terminal vertex, and their inverse edges are omitted for simplicity.

We denote by $V(\Gamma)$ and $E(\Gamma)$ the sets of the vertices and the oriented edges of Γ, respectively. If both $V(\Gamma)$ and $E(\Gamma)$ are finite set, we call Γ a finite graph. Here, we consider only finite graphs. Remark that $|E(\Gamma)|$ is always even since $E(\Gamma)$ is written as $\{e_1, \overline{e}_1, \ldots, e_m, \overline{e}_m\}$. For any $v, w \in V(\Gamma)$, if there exists a successive sequence of oriented edges such that the initial vertex of the first edge is v and the terminal vertex of the last edge w, then the graph is called a **connected graph**. For example, see **Figure 5**. In the following, we assume that all graphs are connected.

8.2. Automorphisms of graphs

Let Γ and Γ' be graphs. A morphism of directed graphs from Γ to Γ' is a map

$$\sigma : V(\Gamma) \cup E(\Gamma) \to V(\Gamma') \cup E(\Gamma')$$

which maps vertices to vertices and edges to edges, such that

$$\sigma(i(e)) = i(\sigma(e)),\ \sigma(t(e)) = t(\sigma(e)),\ \sigma(\overline{e}) = \overline{\sigma(e)}$$

for any $e \in E(\Gamma)$. Namely, σ maps the initial vertex, the terminal vertex, and the inverse edge of an oriented edge to those of the corresponding oriented edge, respectively. For simplicity, we write $\sigma : \Gamma \to \Gamma'$. If σ is bijective, then it is called an **isomorphism**. An isomorphism from Γ to Γ is called an **automorphism** of Γ. Let $\mathrm{Aut}(\Gamma)$ be the set of all automorphisms of Γ. Then $\mathrm{Aut}(\Gamma)$ with the composition of maps forms a group. We call it the **automorphism group** of Γ. Let us consider a few easy examples of $\mathrm{Aut}(\Gamma)$.

(E37) See **Figure 6**. The graph Γ_1 consists of one vertex v and two oriented edges e and $\overline{e}$. Hence all morphisms from Γ_1 to Γ_1 are automorphisms since if $\sigma : \Gamma \to \Gamma$ is a morphism, then $\sigma(v) = v$, and $\sigma(e) = e$ or $\sigma(e) = \overline{e}$. If $\sigma(e) = e$, then $\sigma(\overline{e}) = \overline{e}$ as a consequence, and hence σ is the identity map on Γ. If $\sigma(e) = \overline{e}$, then $\sigma(\overline{e}) = e$ as a consequence, and hence σ is the

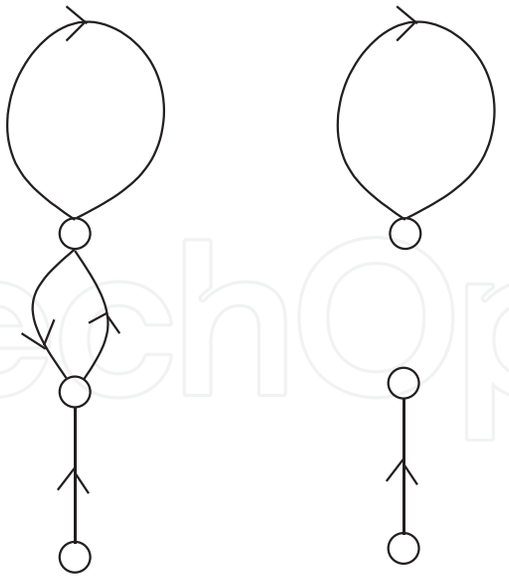

Figure 5. Examples of a connected and a non-connected graph.

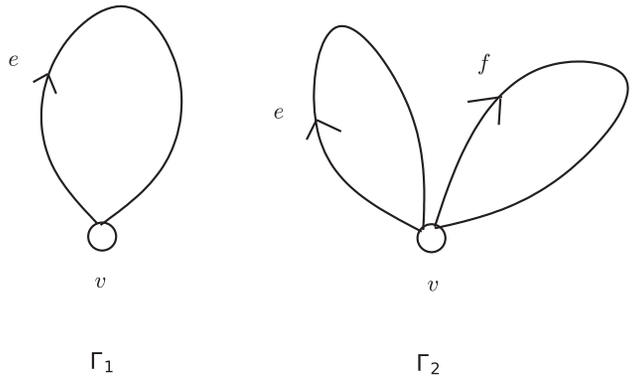

Figure 6. Graphs which have one vertex.

orientation-reversing automorphism on Γ. Thus, $\mathrm{Aut}(\Gamma_1) = \{\sigma_1, \sigma_2\} \cong \mathbf{Z}/2\mathbf{Z}$ where $\sigma_1(e) = e$ and $\sigma_2(e) = \overline{e}$.

On the other hand, the graph Γ_2 consists of one vertex v and four oriented edges $e, \overline{e}, f$, and $\overline{f}$. It is easily seen that there are eight possible automorphisms on Γ_2. Namely, all of them map v to v, and the correspondences of edges are given by

$$\sigma_1 : (e,f) \mapsto (e,f),\ \sigma_2 : (e,f) \mapsto (\overline{e},f),\ \sigma_3 : (e,f) \mapsto \left(e,\overline{f}\right),\ \sigma_4 : (e,f) \mapsto \left(\overline{e},\overline{f}\right),$$
$$\sigma_5 : (e,f) \mapsto (f,e),\ \sigma_6 : (e,f) \mapsto \left(\overline{f},e\right),\ \sigma_7 : (e,f) \mapsto (f,\overline{e}),\ \sigma_8 : (e,f) \mapsto \left(\overline{f},\overline{e}\right).$$

Hence $\mathrm{Aut}(\Gamma_2) = \{\sigma_1, \ldots, \sigma_8\}$. It turns out that σ_2, σ_3, and σ_5 are generators of $\mathrm{Aut}(\Gamma_2)$. In (E41), we study the structure of $\mathrm{Aut}(\Gamma_2)$ more.

Next, in order to describe the group structure of $\mathrm{Aut}(\Gamma)$ more simply, we consider semidirect products of groups. For high motivated readers, see [10] for details and more examples. The

semidirect product groups are kinds of generalizations of direct product groups. Let G be a group, K a subgroup of G, and H a normal subgroup of G. Furthermore, if we have

$$G = \{hk | h \in H,\ k \in K\},\ H \cap K = \{1_G\},$$

then we call G the semidirect product group of H and K and denote it by $G = H \rtimes K$.

(E38) Recall the dihedral group $D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$. Set $H := \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ and $K := \{1, \tau\}$. Then we can see that the subset H is a normal subgroup of D_n, $H \cap K = \{1\}$, and $D_n = \{hk | h \in H,\ k \in K\}$. Thus $D_n = H \rtimes K$.

Remark that for any $g \in G$, we can write $g = hk$ for some $h \in H$ and $k \in K$ and that this expression is unique. Namely, if $g = hk = h'k'$ for $h, h' \in H$ and $k, k' \in K$, then we have $(h')^{-1}h = k'k^{-1} \in H \cap K$. Hence $(h')^{-1}h = k'k^{-1} = 1_G$, and hence $h = h'$ and $k = k'$. Therefore, if $|G| < \infty$, we see that $|G| = |H||K|$. We also remark that if $hk = kh$ for any $h \in H$ and $k \in K$, then G is isomorphic to the direct product group of H and K, namely, $G \cong H \times K$. Thus, the semidirect product is a generalization of the direct product.

Now, let Γ be a graph. For any $v, w \in V(\Gamma)$, we number the oriented edges of Γ with v as initial vertex and w as terminal vertex. Then every oriented edge e can be uniquely represented as $e = (v, w, k)$. In particular, we can arrange the numbering such that $\overline{e} = (w, v, k)$ for any $e = (v, w, k) \in E(\Gamma)$.

(E39) See **Figure 7**. We can arrange a numbering of the oriented edges as

$$e = (v, w, 1), \overline{e} = (w, v, 1), f = (v, w, 2), \overline{f} = (w, v, 2), g = (v, w, 3), \overline{g} = (w, v, 3),$$
$$h = (w, w, 1), \overline{h} = (w, w, 2).$$

Let T be the subgroup of $\mathrm{Aut}(\Gamma)$ consisting of automorphisms that fix all vertices pointwise:

$$T := \{t \in \mathrm{Aut}(\Gamma) \,|\, t(v) = v,\ v \in V(\Gamma)\}.$$

Let M be the subgroup of $\mathrm{Aut}(\Gamma)$ consisting of automorphisms that fix the numberings of edges:

$$M := \{m \in \mathrm{Aut}(\Gamma) \mid m(v, w, k) = (v', w', k) \text{ for any } v, w \in V \text{ and any number } k\}.$$

Then we have $\mathrm{Aut}(\Gamma) = T \rtimes M$

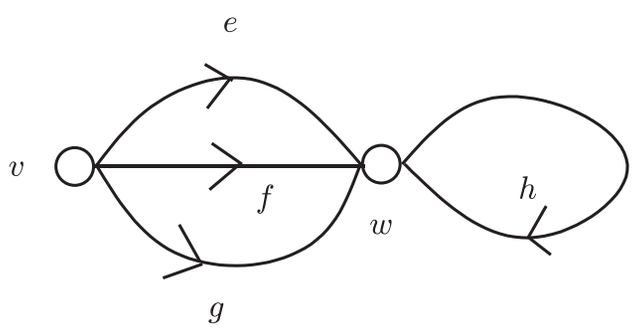

Figure 7. An example of a graph.

(E40) Recall the graph Γ_1 in (E37). Since every automorphism fixes the vertex v, we see that $\mathrm{Aut}(\Gamma_1) = T$ and $M = \{1\}$. Similarly, if a graph Γ has only one vertex, then $\mathrm{Aut}(\Gamma) = T$.

(E41) Recall the graph Γ_2 in (E37). We have $\mathrm{Aut}(\Gamma_2) = T$ and $M = \{1\}$. Set $H := \langle \sigma_2, \sigma_3 \rangle$ and $K := \langle \sigma_5 \rangle$. Then it is seen that $H \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $K \cong \mathbf{Z}/2\mathbf{Z}$, and $\mathrm{Aut}(\Gamma_2) \cong H \rtimes K$.

(E42) Consider the directed graph Γ depicted as the regular n-gon. Then we see that $T = \{1\}$ since if an automorphism fixes all vertices then it must fix all edges. Thus, $\mathrm{Aut}(\Gamma) = M$. Furthermore, we can see that $M \cong D_n = \langle \sigma, \tau \rangle$ where σ is the $2\pi/n$-angled rotation and τ is the reflection.

(E43) Consider the directed graph Γ in **Figure 8**. We arrange a numbering of the oriented edges as

$$e = (w, v, 1),\ \overline{e} = (v, w, 1),\ f = (w, v, 2),\ \overline{f} = (v, w, 2),\ g = (w, v, 3),\ \overline{g} = (v, w, 3).$$

The subgroup T consists of automorphisms which permute the oriented edges e, f, g, and hence $T \cong \mathfrak{S}_3$. On the other hand, the subgroup Q consists of two automorphisms given by the identity map and

$$\sigma : (v, w) \mapsto (w, v),\ (e, f, g) \mapsto (\overline{e}, \overline{f}, \overline{g}),$$

and hence $Q \cong \mathbf{Z}/2\mathbf{Z}$. Therefore $\mathrm{Aut}(\Gamma) \cong \mathfrak{S}_3 \rtimes \mathbf{Z}/2\mathbf{Z}$.

The readers are strongly encouraged to consider further examples by oneself. It makes their understandings better and deeper.

As a remark, we mention the irreducible representations of a semidirect product group. As mentioned in Section 7, the irreducible representations of a direct product group $G \times H$ can be calculated with those of G and H. The situation for semidirect products groups, however, is much more complicated. In general, in order to study the irreducible representations of semidirect product groups, we require some arguments in advanced algebra.

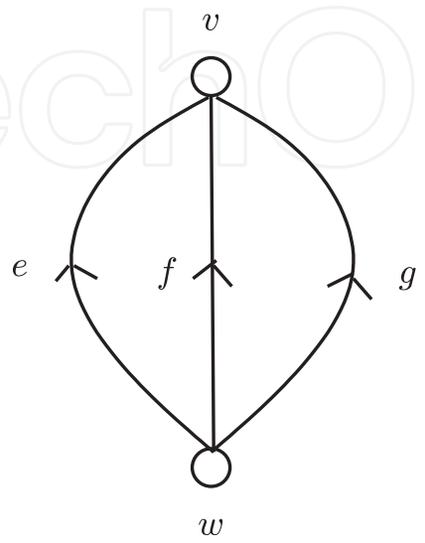

Figure 8. An example of a graph.

Acknowledgements

The author would like to thank Professor Takashiro Akitsu, who is a chemist of our faculty, for introducing to him this work and many useful comments. He considers it a privilege since this is the first interaction across disciplines as a mathematician. He also would like to thank Professor Naoko Kunugi, who is a mathematician majoring in the representation theory of finite groups, for her useful comments about references of the field.

A part of this work was done when the author stayed at the University of Bonn in 2017. He would like to express his sincere gratitude to the Mathematical Institute of the University of Bonn for its hospitality and to Tokyo University of Science for its financial supports.

Author details

Takao Satoh

Address all correspondence to: takao@rs.tus.ac.jp

Department of Mathematics, Faculty of Science Division II, Tokyo University of Science, Tokyo, Japan

References

[1] Satoh T. Sylow's Theorem. Spotlight Series 1. Kindaikagakusya; 2015. 168p. (Japanese)

[2] Armstrong MA. Groups and Symmetry. Undergraduate Texts in Mathematics. Springer-Verlag; 1988. 186p

[3] Rotman JJ. An Introduction to the Theory of Groups. 4th ed. Graduate Texts in Mathematics 148. Springer-Verlag; 1995. 513p

[4] Suzuki M. Group Theory I. Grundlehren der Mathematischen Wissenschaften 247. Springer-Verlag; 1982. 434p

[5] Serre JP. Linear Representations of Finite Groups. Graduate Texts in Mathematics 42. Springer-Verlag; 1977. 170p

[6] James G, Liebeck M. Representations and Characters of Groups. Cambridge University Press: Cambridge Mathematical Textbooks; 1993. 419p

[7] Alperin JL, Bell RB. Groups and Representations. Graduate Texts in Mathematics 162. Springer-Verlag; 1995. 194p

[8] Curtis CW, Reiner I. Representation theory of finite groups and associative algebras. AMS Chelsea Publishing; 2006. 689p

[9] Chiswell I. Introduction to Λ-Trees. World Scientific; 2001. 315p

[10] Brady T. The integral cohomology of $\mathrm{Out}_+(F_3)$. Journal of Pure and Applied Algebra. 1993;**87**:123-167