Chapter 1

Some classic groups

1.1 cyclic group

- What is cyclic group?

  If $\exists q$ s.t. $\langle q \rangle = G$, then G is a cyclic group.

- What is $\langle q \rangle$?

  It is the smallest group that contains the q. And we can prove that $\langle q \rangle$ is equal to

  $$\{ \dots q^{-1}, 1, q, q^2, \dots \}$$

- Can the idea of it be generalized?

  There is also $\langle S \rangle$ (where S is a subset of G) which is the smallest subgroup that contains the S. We can prove that

  $$\langle S \rangle = \{ q_1 \dots q_k \mid k \in \mathbb{Z}, q_i \in S \cup S^{-1} \}$$

  This thing can be more generalized when we reach the section of free groups.

- If G is equal to $\langle a \rangle$, then a is called generator of G.

- Clearly enough, if G is cyclic then G is abelian.

- If G is infinite and is equal to $\langle a \rangle$, then G is isomorphic to $\mathbb{Z}$.

- If G is finite and is equal to $\langle a \rangle$, then G is isomorphic to $\mathbb{Z}_n$, where n is $|G|$.

- What is Euler (totient) function?

  $\varphi(n)$ is defined as the number of the positive intergets that are less than n and are relative primes to n.

- What is the number of the generators?

  If G is finite, and $|G| = n$, then G have $\varphi(n)$ generators.

- Can you prove it?

  This trivial that k is relative prime to n then $\exists a, b \in \mathbb{Z}$ such that

  $$ak + bn = 1$$

  which is to say that if q is generator, then q^{ak} is equals to q, which is to say that $\langle q^{ak} \rangle = G$.

- G is a finite cyclic group, given a positive factor k, there is one and only one subgroup that is $\langle a^{n/k} \rangle$.

- Can you tell the number of the subgroups in a cyclic group?

  It is clear that there are subgroups as many as the factors of $|G|$..

- We can study the Automorphisms of the cyclic groups. We have the conclusion that $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. The latter one is defined as the inversable members under the multiplication in the $\mathbb{Z}/n\mathbb{Z}$.

1.2 Transformation groups

M is a set. The transformation over a M is a monoid. $S(M)$ is the set of the bijective transformation on M. $S(M)$ is a group and is called **symmetric** group. $S(M)$ is sometimes denoted as S_n if $|M| = n$.

Theorem 1.2.1. For a transformation group G on M, if there is onto function or one–one function in G then G is a permutation group.

Proof. (1) If τ is onto, consider $\epsilon\tau(a) = \tau(a)$, then ϵ is id.

(2) If τ is one-one, consider $\tau\epsilon(a) = \tau(a)$, then ϵ is id, because $\epsilon(a) = a$ forall a in G.

$\forall a \in G$, $\exists b \in G, b = a^{-1}$, viz., $ab = \epsilon$. So a, b are inversible and thus are bijectives. Then every a in G is bijective then G is a permutuation group. □

If G is the group whose elements are in $T(M)$. then the fact that G has a bijection suggests that G is a permutuation group, that is, all of the elements of G are bijection; the fact that G has a non–bijective function suggests that all of the elements in G are not bijection.

Example 1.2.2. $M = \{\, (x, y) \mid x, y \in \mathbb{R} \,\}$, $\forall a \in \mathbb{R}$:

$$\tau_a \colon M \to M, (x, y) \mapsto (x + a, 0)$$

Prove that $G = \{\, \tau_a \mid a \in \mathbb{R} \,\}$ is a group.

Theorem 1.2.3 (Cayley)**.** Given a G, there exists a permutuation group that is isomorphic to G.

1.3 Symmetric group

- Something writte as
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
is called as a **permutuation**. And also called **cycles**,
- The above transformation can be written as (132).
- For such thing as $(i_1 i_2 i_3 \dots i_k)$, the order of it is k.
- For the compostion of the transformation, we read from left to right. And if we have σ, and τ, and they are:
$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ \tau(1) & \tau(2) & \tau(3) \end{pmatrix}$$
then we have that $\sigma\tau$ is equals to
$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(\tau 1) & \sigma(\tau 2) & \sigma(\tau 3) \end{pmatrix}$$
You may easily know it from the fact that
$$\begin{pmatrix} 1 & 2 & 3 \\ \tau(1) & \tau(2) & \tau(3) \end{pmatrix} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ \sigma\tau(1) & \sigma\tau(2) & \sigma\tau(3) \end{pmatrix}$$
- Moreover we have that
$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ 1 & 2 & 3 \end{pmatrix}$$
because we have that
$$\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix} \times \begin{pmatrix} j_1 & j_2 & j_3 \\ k_1 & k_2 & k_3 \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & i_3 \\ k_1 & k_2 & k_3 \end{pmatrix}$$

- There is a theorem that easily compute the $\sigma\tau\sigma^{-1}$. If τ is written as $(i_1 i_2 \ldots i_k)$, then we have that

  $$\sigma\tau\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_k))$$

  It is given by the fact that

  $$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ \sigma(i_1) & \sigma(i_2) & \sigma(i_3) \end{pmatrix}$$

  which exactly is saying that $\sigma\tau\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\sigma(i_3))$. One can test the propostion.

  $$\sigma\tau\sigma^{-1}(\sigma(1)) = \sigma\tau(\sigma^{-1}(\sigma(1))) = \sigma\tau(1) = \sigma(i_1)$$

  1 is randomly chosen. One can test all other numbers.

- The compostion of transformation is quite tricky.

- A cycle can be decomposed as the compostion of the **duihuan**. In general, a k–cycle: $(i_1 \ldots i_k)$ can be decomposed as $(i_1 i_k)(i_1 i_{k-1}) \ldots (i_1 i_2)$.

- If there is no identical number in transformation σ, τ, then σ and τ are commutable. that is $\sigma\tau = \tau\sigma$. For a random transformation you can easily find the composition of such form like $\tau\sigma\varphi\ldots$, where the transformations are independent (let us call it temporarily).

- The number of the duihuan in the decomposed form of a k–cycle can be odd or even. If the number is odd then the permutuation is called **odd**, and if the number is even, then the permutuation is called **even**. It can be proved that all the **even** permutuation forms a subgroup of S_n, often denoted as A_n. And moreover, the zhishu of A_n is 2.

- One can prove that if there is a odd permutuation in the permutuation group, then the number of the odd permutuations and the number of even permutuations are equal. Such that **either** the permutuations are all even, **or** half the permutuations are odd and half of the permutuations are even.

Summary Symmetric groups are very important. Why? When it comes to the very section of 'group actions' we will use the properties of symmetric groups. However, most of the properties above is very useless. Why? Because they are.

Chapter 2

Normal subgroups and quotient groups

2.1 What is quotient groups

Definition 2.1.1 (Formal subgroups)**.** N is subgroup of G, and if N suit that $\forall g \in G, gN = Ng$, viz., $N = g^{-1}Ng$, then N is a normal group.

Normal groups have a property that

$$Ng_1Ng_2 = g_1NNg_2 = g_1Ng_2 = Ng_1g_2$$

Consequently, if we have $\{\, [g] \mid g \in G \,\}$, where $g_1 \sim g_2$ iff $Ng_1 = Ng_2$. And then, the above property says that $\{[g]\}$ is closed under group operation. And furthermore, $\{[g]\}$ is a group if we define the operation between $[g_1], [g_2]$ as $[g_1][g_2] = [g_1g_2]$

Definition 2.1.2 (Quotient groups)**.** Given a normal subgroup N we have that $\{\, [g] \mid g \in G \,\}$ is a group, denoted as G/N, and we called G/N a quotient group.

Definition 2.1.3 (Conjugate)**.** Given a group member g the conjugation of g is defined as $h \mapsto g^{-1}hg$. If $\exists g \in G$ s.t. $h_1 = g^{-1}h_2g$, then we say that h_1 and h_2 are conjugate. The relation of conjugate is a equivalence relation.

Example 2.1.4. While it remain a little bit ambiguous that we choose normal subgroups to construct quotient group, we can have a look at quotient in linear space and topological space to further understand what quotient is.

In linear algebra, every subspace of a linear space is a normal group if we treat it as group. Given a linear space V and a subspace W, we have that

$$\dim V/W = \dim V - \dim W$$

It seem that the subspace W is eliminated and that the space which is orthogonal to W is isomorphic to V/W.

Consider the topological space X, and given a equivalence relation of X, we can construct a quotient space Y, where every member is the equivalence class of the relation. **And** the family of open sets $\mathscr{F}'$ suit that for the function $\pi\colon O \mapsto \bigcup_{x\in O}[x]$, we have that $\pi(O)$ is an open set in Y iff O is an open set in X.

The quotient space of topological space X is also called identical space. That is to say, we glue the members in a class into a piece. And that is what we called quotient.

So what is happening here is that the algerbric structure is preserved after we view a collection of elements as one element. $\square$

2.2 A Basic Homomorphism Theorem of Quotient

Next we talk about an important theorem about quotient groups, before which, we first introduce some definitions.

Definition 2.2.1 (kernal)**.** Given a homomorphism $f\colon G \to G'$, the kernal of f (denoted as $\ker f$), is defined as

$$\ker f = f^{-1}(1) \subseteq G$$

and it is easy to show that $\ker f$ is a normal subgroup of G.

Exercise: Prove that $\ker f$ is a normal subgroup of G.

Definition 2.2.2 (Image)**.** The image of f is defined as

$$\operatorname{Im} f = \{\, f(g) \mid g \in G \,\}$$

The image of f is less important than kernal, since `\ker` is a macro provided by LaTeX while that `\Im` or `\im` are not.

Let us state the theorem

Theorem 2.2.3 (a basic theorem of quotients)**.** Given a homomophism $f\colon G \to G'$, we define $\bar{f}$ as that $\bar{f}([g]) = f(g)$, and we have that

$$\bar{f}\colon G/\ker f \to \operatorname{Im} f$$

is an isomorphic.

Proof. We shall prove that $\bar{f}$ is a homomorphism and also a bijective. Then we prove that $\bar{f}$ is isomorphism. □

Is the basic homomorphism theorem really useful? Actually not. It is a trivial fact that we already know. It is better to view the quotient groups in categorical way. Why? After you know about the universal properties, you shall know that the theorem is the case of quotient in category **Grp**. You know the subgroups just happen to be normal groups, because the kernal of a homo φ is normal.

Anyway, it is important to use the theorem, while one may be not needed to use it.

Example 2.2.4. K_4 is called Klein group. The definition is omitted here. One shall prove that

$$S_4/K_4 \simeq S_3$$

by using the theorem or by proving that S_3 is the R of S_4 with the concern of K_4.

Proof. Let $K_4 = \{(1), (12), (34), (12)(34)\}$, and consider K_4 and S_3 as the subgroups of S_4. And it is clear that

$$\forall a, b \in S_3, ab^{-1} \in K_4 \iff ab^{-1} = 1$$

and $ab^{-1} = 1$, we have that $a = b$, so $S_3 \subseteq R$, where R is the represention of S_4 with the concern of K_4. And because that $|S_3| = 6$, and that $|R| = |S_4| \big/ |K_4| = 6$. Thus, $R = S_3$. Then the proof is complete. □