Chapter 1

TODO

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

  $$\langle S \rangle = \{ q^k \mid k \in \mathbb{Z}, q \in S \}$$

- 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 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 $|G|$

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.

If $|M| = n$, then $S(M)$ is sometimes denoted as S_n.

And $|S_n| = n!$.

Transformation group G on M,

Theorem 1.2.1. Transformation group G on M, if there is onto function or one-one function in G then $G = S(M)$

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

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 $G = S(M)$. $\square$

If a bijective is in a group on M then the group is bijective group, that is a group whose elements are bijectives.

If a group is not a bijective group then the group has no bijective or subjective or injective.

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 bijective group that is isomorphic to G.

Proof. Treat the elements in G as functions which is absolutely a bijective. ☐

1.3 Symmetric group

- Something writte as
  $$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
  is called as transformation. And also called **zhihuan**,

- The above transformation can be written as (123), which is to say that the number on position 1 is given to postion 2, and number on position 2 is given to 3, and number on position 3 is given to 1.

  Note that there can be more than one expression of the transformation.

- 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 $\sigma\tau\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\sigma(i_3))$

- The compostion of transformation is quite tricky.

- 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).

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. □

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

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

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

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

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

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. $\square$