Chapter 1

TODO

1.1 cyclic group

What is cyclic group?

$S \subseteq G$ if $\langle S \rangle = G$ then G can be generated by S. Maybe we can use M instead of S.

If S is a singleton $\{g\}$then G is a cyclic group and can be denoted as $\langle g \rangle$.

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

If G is finite and $G = \langle a \rangle$, then G is isomorphic to $\mathbb{Z}_n$

A group G is cyclic then G is abelian.

If a finite group G has a group member whose order is $|G|$, then G is cyclic.

A Euler function $\varphi(n)$ is defined as the number of the positive integers that are less than n and are relative prime to n

G is finite, and $|G| = n$, then G has $\varphi(n)$ generator.

the proof is easy, given a number q , q is relative prime to n, then $\exists u, v \in \mathbb{Z}, uq + v|G| = 1$

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

1.2 Transformation

M is a set. The transformation over a M is a monoid.

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. □

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

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

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

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

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. □