Sep. 22, 2006 (Fri.)

2. Group Theory

The concept of groups is a very fundamental one in Mathematics. It arise as automorphism of certain sets. For example, some geometry can be described as the groups acting on the geometric objects.

In the first section, we are going to recall some definition and basic properties of groups in general. In the second section, we introduce the acting of groups. The groups action can find many applications in geometry, algebra, and the theory of groups itself. In the third section, we are would like to take care of various aspects of reducing or factoring groups into simple ones.

2.1. **Basic group theory.**

Definition 2.1.1. *A group G is a set together with a binary operation $\circ : G \times G \to G$ satisfying:*

1. *there is an $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.*
2. *for all $g \in G$, there is an $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$*
3. *for all $g_1, g_2, g_3 \in G$, we have $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.*

A group is said to be **abelian** *if $x \circ y = y \circ x$ for all $x, y \in G$.*

For simplicity, we will denote xy for $x \circ y$.

A subset $H \subset G$ is a **subgroup** if H is a group by using the binary operation of G, denoted $H < G$.

A **group homomorphism** $f : G \to H$ is a function between groups that respects the structure of groups. That is, a function satisfying $f(xy) = f(x)f(y)$.
The **kernel** of f, denote $\ker(f)$, is defined to be $\{x \in G | f(x) = e_H\}$.

A subgroup $H < G$ is said to be **normal** if $gHg^{-1} = H$ for all $g \in G$, denoted $H \lhd G$. Given a subgroup $H < G$, we note G/H the set of left cosets, i.e. $G/H = \{gH | g \in G\}$. When $H \lhd G$ is normal, then G/H has induced group structure given by $xH \circ yH := xyH$. This is called the quotient group.

We remark that a subgroup is normal if and only if it is the kernel of some homomorphism. The following lemma is useful

Lemma 2.1.2. *Let $f : G \to H$ be a group homomorphism. Let N be a normal subgroup of G contained in* $\ker(f)$*, then there is an induced homomorphism $\bar{f} : G/N \to H$.*

Proof. Define $\bar{f} : G/N \to H$ by $\bar{f}(gN) = f(g)$. Then it's routine to verify it's well-defined and it's a group homomorphism. □

Regarding group homomorphisms, there are some useful facts:

Theorem 2.1.3 (First isomorphism theorem)**.** *Let $f : G \to H$ be a group homomorphism, then there is an induced isomorphism $\bar{f} : G/\ker(f) \cong im(f)$.*
In particular, if f is surjective, then $\bar{f} : G/\ker(f) \cong H$.

Proof. Define $\bar{f} : G/\ker(f) \to H$ by $\bar{f}(g\ker(f)) = f(g)$. Then it's routine to verify it's well-defined and it's a injective group homomorphism. □

Example 2.1.4. *Let G be the set of all maps $T_{a,b} : \mathbb{R} \to \mathbb{R}$ such that $T_{a,b}(x) = ax + b$ with $a \neq 0$. Then G is a group under composition. There are two natural subgroups:*
$A := \{T_{a,0}\} \cong \mathbb{R}^*$, the multiplication group.
$N := \{T_{1,b}\} \cong \mathbb{R}$, the translation group.
There is a group homomorphism $f : G \to \mathbb{R}^*$ by $f(T_{a,b}) = a$. Its kernel is N, which is a normal subgroup of G. So we have $G/N \cong A$.
Moreover, $G = NA = AN$ and $N \cap A = \{e\}$. So in fact G is the **semidirect product** *of A and N.*

Theorem 2.1.5 (Second isomorphism theorem)**.** *Let H, K be subgroups of G. Then we have group isomorphism*

$$H/(H \cap K) \cong HK/K,$$

when
1. $H < N_G(K)$ or especially,
2. $K \lhd G$.

Sketch. Recall that $N_G(K) := \{x \in G | xKx^{-1} = K\}$ denotes the normalizer of K in G. It is the maximal subgroup of G in which K is normal. In particular $K \lhd N_G(K)$. So $K \lhd G$ if and only if $G = N_G(K)$.

Also one can check that if $H < N_G(K)$, then $HK = KH < N_G(K)$ is a subgroup of G. Moreover, $K \lhd HK$.

On the other hand, if $H < N_G(K)$, then $H \cap K \lhd H$. Thus both sides are groups.

Finally, we consider $f : H \to HK/K$ by $f(h) = hK$. It's easy to check that f is surjective with kernel $H \cap K$. By first isomorphism theorem, we proved (1). And (2) is just a special case of (1). □

Given a surjective homomorphism $f : G \to H$, by First isomorphism theorem, $H \cong G/N$ where $N = \ker(f)$ is a normal subgroup. It's natural to study the group structures between them. It's easy to see that there is a map

$$\{K < G/N\} \overset{f^{-1}}{\to} \{L < G | N < L\}.$$

In fact, this map is bijective. Moreover, it sends normal subgroups to normal subgroups.

Theorem 2.1.6 (Third isomorphism theorem)**.** *Given $N \lhd G$ and $K \lhd G$ containing N. Then $K/N \lhd G/N$. Moreover, $(G/N)/(K/N) \cong G/K$.*

Sketch. It's easy to check that $K/N \lhd G/N$ by definition.
In fact, we consider $f : G \to G/K$. Since $N \lhd G$ and N is contained in $\ker(F) = K$, by Lemma 2.1.2, we have an induced map $\bar{f} : G/N \to G/K$ which is clearly surjective. One checks that $\ker(\bar{g}) = K/N$ and we are done by Themreom 2.1.3. □

2.2. **cyclic groups.**

Among all groups, perhaps simplest ones are cyclic groups. Let G be a group. We say that G is cyclic if there is an element $x \in G$ such that every element $g \in G$ can be written as x^n for some $n \in \mathbb{Z}$.

It's clear that $\mathbb{Z}$ under addition is a cyclic group. By the definition, given a cyclic group G, there is a surjective map $f : \mathbb{Z} \to G$, by $n \mapsto x^n$. This is indeed a group homomorphism. Therefore, by Theorem 2.1.3, $G \cong \mathbb{Z}/\ker(f)$.

The reader should find no difficulty showing that subgroups of $\mathbb{Z}$ is either $\{0\}$ or of the form $n\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, every subgroup is normal.

Turning back to the discussion of cyclic groups. There are two cases:
1. $\ker(f) = 0$. Then $G \cong \mathbb{Z}$. This is called an infinite cyclic group.
2. $\ker(f) = n\mathbb{Z}$. Then $G \cong \mathbb{Z}/n\mathbb{Z}$. This is called a cyclic group of order n, denoted $\mathbb{Z}_n$.

There list some properties and leave the proof for the readers.

Proposition 2.2.1. *Let G be a cyclic group.*
1. Every subgroup is cyclic.
2. Homomorphic image of G is cyclic.
3. If G is a cyclic group of order n, for all $d|n$ there exist a subgroup of order d.
4. If G is a cyclic group of order n with a generator x, then the set of generators consist of $\{x^t|(t,n) = 1\}$.