3. Quotients and Products of Groups

3.1 Cosets

H is a subgroup of G and $a, b \in G$,

define an equivalence relation on $G : a \sim b$ if $a = bh$ for some $h \in H$:

1. $\forall a \in G$, $a = a \cdot 1, 1 \in H \rightarrow a \sim a$
2. $a \sim b \rightarrow a = bh$ for some $h \in H \rightarrow b = ah^{-1}$, $h^{-1} \in H \rightarrow b \sim a$
3. $a \sim b$, $b \sim c \rightarrow a = bh_1$, $b = ch_2$ for some $h_1, h_2 \in H$

   $\rightarrow a = (ch_2)h_1 = c(h_2h_1),\ \ h_1h_2 \in H \rightarrow a \sim c$

Under this equivalence relation, an equivalence class is:

$[g] = \{x \in G | x = gh \text{ for some } h \in H\} = \{gh \in G | h \in H\} = gH$

such equivalence class is called a left coset of H in G.

Cor. Two left cosets of H in G are either equal or disjoint. And G is a partition of its distinct left cosets.

Example: $\mathbb{Z}^+$, $H = 3\mathbb{Z}$. Partition: $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$.

H is a subgroup of G and $a, b \in G$. The the following are equivalent:

1. $aH = bH$
2. $a = bh$ for some $h \in H$
3. $b^{-1}a \in H$
4. $a \in bH$

We can construct right cosets in a similar way, starting from defining $a \sim b$ if $a = hb$ for some $h \in H$:

$Hg = \{hg \in G | h \in H\}$

H is a subgroup of G. Define the index of H in G to be the number of left cosets, denoted by $[G : H]$.

Lagrange's Theorem. H is a subgroup of a finite group G. Then $[G : H] = \frac{|G|}{|H|}$.

Cor. $|H|$ divides $|G|$.

Example: $G = K_4 \rightarrow |H| = 1, 2, 4$

Cor. If $x \in G$, then $|x|$ divides $|G|$, since $|x| = | < x > |$ is the order of the cyclic subgroup generated by x.

Cor. A group of prime order is cyclic, since for any non-identity element $x \in G$, $|x|$ divides $|G|$ and $|x| \neq 1$, so $|x| = |G|$, so $< x >= G$.

Remark. If $|G| \neq 1$ or prime, then we can find a non-cyclic group G.

Prop. H is a subgroup of G and K is a subgroup of H. Then $[G : K] = [G : H][H : K]$.

Prop. Any subgroup of index 2 is normal.

3.2 Quotient Groups

We wish to define a group structure on the quotient space.

$\forall g \in G$, $gH = Hg \iff \forall g \in G$, $gHg^{-1} = H \iff H$ is a normal subgroup of G

N is a normal subgroup of G. We define the quotient group of G by N to be the set of all cosets of N in G, with composition given by $(aN)(bN) = abN$. The quotient group is denoted by G/N.

Examples: $K_4 = \{1, a, b, c\}$, $N = \{1, a\} =< a >$.

$K_4/N = \{N, bN\} =< bN >$ cyclic group of order 2, identity element is N

$S_3 = \{id, (12), (13), (23), (123), (132)\}$, $H = \{id, (123), (132)\} =< (123) >$,

$S_3/H = \{H, (12)H\} =< (12)H >$ — cyclic group of order 2

3.3 Integers modulo n

Guotient group $\mathbb{Z}/n\mathbb{Z}$:

Elements are of form $k + n\mathbb{Z}$

Denote $\bar{k} = k + n\mathbb{Z}$,

$\overline{k_1} = \overline{k_2} \iff (-k_1) + k_2 \in n\mathbb{Z} \iff n|k_1 - k_2$

so $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{k-1}\}$. The composition is $\bar{a} + \bar{b} = \overline{a+b}$.

If $\bar{a} = \bar{b}$, we say "a is congruent to b module n", denoted by $a \equiv b \pmod{n}$.

We can define another composition — multiplication: $\bar{a}\bar{b} = \overline{ab}$. Well-defined since $\bar{a} = \bar{a'}, \bar{b} = \bar{b'} \to \overline{ab} = \overline{a'b'}$, but not a group since some elements (e.g. $\bar{0}$) have no inverse.

An element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is called a unit if there exists $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\bar{a}\bar{b} = 1$.

Prop. If $\bar{a}, \bar{c}$ are both units of $\mathbb{Z}/n\mathbb{Z}$, then $\bar{a}\bar{c}$ is also a unit.

The set of all units in $\mathbb{Z}/n\mathbb{Z}$ with multiplication form a group, and denote it by $(\mathbb{Z}/n\mathbb{Z})^\times$, called the group of units.

Examples: $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$, $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$ $\quad (2^2 = 4 \equiv 1 \pmod{3})$

$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ $\quad (3^2 = 9 \equiv 1 \pmod{4})$

$\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. The followings are equivalent:

1. $\bar{a}$ is a unit
2. $\gcd(a, n) = 1$, i.e., relatively prime
3. $\bar{a}$ is a generator for $\mathbb{Z}/n\mathbb{Z}$
4. $f_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f_a(\bar{x}) = \overline{ax}$ is a automorphism.

The Eulers's phi function is $\phi(n) = \#\{k \in \mathbb{N} | 1 \le k \le n, \gcd(k, n) = 1\}$.

Examples: $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$

Fermat's Little Theorem: $n \ge 2$, $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Pf. $\gcd(a, n) = 1 \to \bar{a}$ is a unit, i.e., $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \to \bar{a}|(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)$, $\bar{a}^{\phi(n)} = \bar{1} \to \overline{a^{\phi(n)}} = \bar{1}$ $\to a^{\phi(n)} \equiv 1 \pmod{n}$

Cor. p is a prime. $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Cor. $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

3.4 First Isomorphism Theorem

Lemma. $f : G \to G'$ is a homomorphism. $a, b \in G$.

Then $f(a) = f(b) \iff aN = bN$, where $N = \ker(f)$. (Recall: $\ker(f) = \{g \in G | f(g) = 1'\}$)

First Isomorphism Theorem. $f : G \to G'$ is a surjective homomorphism. Then there is a unique homomorphism $F : G/N \to G'$ ($N = \ker(f)$) such that F is an isomorphism and $f = F \circ \pi$ where $\pi : G \to G/N$, $\pi(g) = gN$ is the quotient map.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/N \arrow[ur, dashed, "\exists! F"'] & \end{tikzcd}$$

Cor. $f : G \to G'$ is a homomorphism. Then $G/\ker(f) \cong \operatorname{Im}(f)$. (force it to be surjective)

Pf. Follows from First Isomorphism Theorem. $Im(f) = \{f(g) \in G' | g \in G\} = G'$ for surjective homomorphism f.

Cor. If G is a finite group. $f : G \to G'$ is a homomorphism. Then $|G| = |\ker(f)| \cdot |\operatorname{Im}(f)|$.

Pf. Follows from previous cor. and Lagrange's Theorem.

Cor. $f : G \to G'$ is a homomorphism. $\gcd(|G|, |G'|) = 1$. Then f is a trivial map, i.e., $\forall g \in G$, $f(g) = 1'$.

Pf. By previous cor., $|\operatorname{Im}(f)|$ divides $|G|$. $\operatorname{Im}(f)$ is a subgroup of G, so $|\operatorname{Im}(f)|$ divides $|G|$. $\gcd(|G|, |G'|) = 1$, so $|\operatorname{Im}(f)| = 1$. $\operatorname{Im}(f) = \{1'\}$.

Example: $G =< a >$ is a cyclic group of order n. $f : \mathbb{Z} \to G, k \mapsto a^k$ is a surjective homomorphism.

$\ker(f) = \{k \in \mathbb{Z} | a^k = 1\} = \{k \in \mathbb{Z} | n | k\} = n\mathbb{Z}$.

By First Isomorphism Theorem, $\mathbb{Z}/n\mathbb{Z} \cong G =< a >$.

So if $G_1 =< a >$ and $G_2 =< b >$ are both cyclic groups of order n, then $G_1 \cong \mathbb{Z}/n\mathbb{Z} \cong G_2$.

Remark: $\pi : G \to G/N$. The quotient map defined by $\pi(g) = gN$ is a homomorphism.

$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$. $\ker(\pi) = N$.

So any normal subgroup N of G is the kernel of some homomorphism defined on G.

So "kernel" $\iff$ "normal subgroup".

3.5 Product Groups

G and G' are groups. Define their product group to be $G \times G'$, the set of all ordered pairs (g, g') where $g \in G$, $g' \in G'$, with law of composition $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$.

Properties:

- $|G \times G'| = |G| \cdot |G'|$
- We can identify G with $\{(g, 1') \in G \times G' | g \in G\}$. $i_1 : G \to G \times G', i_1(g) = (g, 1')$.
  G' with $\{(1, g') \in G \times G' | g' \in G'\}$. $i_2 : G \to G \times G', i_2(g') = (1, g')$.
- Under this identification, G and G' are normal subgroups in $G \times G'$.

G is a group. H and K are its subgroups. Then

$G = H \times K$ if $f : H \times K \to G, f(h, k) = hk$ is an isomorphism.

$G = H \times K$

$\iff$

$H \cap K = \{1\}$, $HK = G$, and H, K are normal subgroups of G.

Example: $K_4 = \{1, a, b, c\} \cong < a > \times < b > \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$

Prop. If r and s are relatively prime positive integers, then a cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.

Pf. $G =< x >$ is a cyclic group of order rs, $H =< x^s >$, $K =< x^r >$

Lemma. If H and K are subgroups of G, with $|H|$ and $|K|$ relatively prime, then $H \cap K = \{1\}$. (Pf. since $|H \cap K|$ divides both $|H|$ and $|K|$.)

Chinese Reminder Theorem. If $\gcd(r, s) = 1$, then $f : \mathbb{Z}/rs\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ is an isomorphism.

In practice, it implies that the system of congruence equations

$$\begin{cases} x \equiv a \pmod r \\ x \equiv b \pmod s \end{cases}$$

has a unique solution up to congruence mod rs.

Remark. This can be generalized to: $\mathbb{Z}/r_1...r_n\mathbb{Z} = \mathbb{Z}/r_1\mathbb{Z} \times ... \times \mathbb{Z}/r_n\mathbb{Z}$

If $\gcd(r, s) \neq 1$, $\mathbb{Z}/rs\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$.

Idea: Suppose $(g, g') \in G \times G'$. $|g| = m$. $|g'| = n$.

$(g, g')^k = (1, 1') \iff (g^k, g'^k) = (1, 1') \iff |g|$ divides k, $|g'|$ divides $k \iff k$ is a common multiple of m, n

So $|(g, g')| = lcm(mn)$.