CHAPTER 3

Left, right cosets

Normal subgroups, characterization: Here:

\[ N \triangleleft G \iff (gN \times hN) = (gh)N \]

Throughout \( G \) is a group

Note: \( H \leq G \) choose \( a, b \in G \) then

\[ aH = bH \iff a = bh \text{ for some } h \in H \]

and \( Ha = Hb \iff a = b'b \text{ for some } b' \in H \) (exercise)

1. \( aH \cap bH \neq \emptyset \iff aH = bH \)

\[ Ha \cap Hb \neq \emptyset \iff Ha = Hb \]

Let \( N \triangleleft G \) and set

\[ G/N = \{ gN : g \in G \} \text{ the set of left cosets} \]

\[ = \{ Ng : g \in G \} \text{ } \text{ normally} \]

Then \( G/N \) is a group under \( (gN \times hN) = (gh)N \)

for all \( g, h \in G \) with identity \( 1N = N \)

Refer to \( G/N \) as "\( G \) mod \( N \)"
And with \((gN)^{-1} = g^{-1}N\) for all \(g \in G\).

Also the map:
\[
G \rightarrow G/N \\
g \rightarrow gN
\]

is a group homomorphism (natural, canonical, etc) called the natural projection.

**Proof**

Last time, showed
\[(gN \cdot hN) = (gh)N\]

is a well-defined product. Group axioms for \(G/N\) are a consequence for \(G\). Properties of natural projection follow.

**Remark** \(G/N\) is referred to as a “quotient” or a “factor” of \(G\).

**Note** \(G/N\) is NOT a subgroup of \(G\).

**Def** Let \(\varphi : G \rightarrow H\) be a group homomorphism.

Define the **kernel** of \(\varphi\) to be
\[
\text{Ker}\varphi = \{ g \in G \mid \varphi(g) = 1_H \} = \varphi^{-1}(1)
\]

Also the **image** of \(\varphi\) is
\[
\text{Im}\varphi = \{ h \in H \mid \exists g \in G : \varphi(g) = h \} = \varphi(G)
\]

In general for \(h \in H\) refer to \(\varphi^{-1}(h)\) as the **fiber** over \(h\).
Lemma \( \varphi : G \rightarrow H \) homomorphism

1. \( \varphi(1_G) = 1_H \)
2. \((\varphi(g))^\prime = \varphi(g^\prime)\) for all \(g \in G\)
3. \(\varphi(g)^n = \varphi(g^n)\)
4. \(\ker \varphi\) is a subgroup of \(G\)
5. \(\Im \varphi\) is a subgroup of \(H\)

Proof - exercise
1. \(\varphi(1_G) \varphi(1_G) = \varphi(1_G) \cdot \varphi(1_G) \cdot \varphi(1_G) = I\)

Lemma \( \varphi : G \rightarrow H \) be a group homomorphism

\(\ker \varphi \leq G\)

Proof.
For \(g \in G\), \(\ker \varphi \subseteq \ker \varphi\)

\[ \varphi(gk^{-1}) = \varphi(g) \varphi(k) \varphi(g^{-1}) \]

\[ = \varphi(g) \cdot 1 \cdot \varphi(g^{-1}) = I \]

N.B. used the "weaker" formulation of normality from last time.

Lemma Let \(N \leq G\). Then \(N\) is the Kernel of the natural projection \(\pi : G \rightarrow G/N\)

Proof. As before, \(N = 1\). \(N\) is the identity of \(G/N\)

\[ \text{Ker} \pi = \{g \in G | gN = N\} = \{g \in G | n \in N\} = N \]
The normal subgroups are exactly the kernels of homomorphisms of $G$.

**Lemma** \( \varphi: G \rightarrow H \) homomorphism

\[ K = \ker \varphi \quad \text{Then} \]
\[ \{ \varphi^{-1}(h) \mid h \in \text{im} \varphi \} \]
\[ = \{ gK \mid g \in G \} = \{ Kg \mid g \in G \} \]

**Proof**

Choose \( h \in \text{Im} \varphi \)

\[ g \in G \quad \text{s.t.} \quad \varphi(g) = h \]

Then \( a \in \varphi^{-1}(h) \iff \varphi(a) = h \iff \varphi(a) = \varphi(g) \]
\[ \iff \varphi(a) \varphi(g^{-1}) = 1 \]
\[ \iff ag^{-1} \in K \iff a \in Kg \]
\[ \therefore \varphi^{-1}(h) = Kg \]

Also \( \ker \varphi \subseteq G \)

\[ gK = Kg \quad \text{for} \quad \forall g \in G \quad \Box \]

Put another way \( G/K \) is exactly the set of nonempty fibers of \( \varphi \).
Remarks: Suppose that \( G \) is an additive abelian group and let \( H \leq G \).

1. For each \( g \in G \), the left coset \( g + H \) is
   \[ \{ g + h \mid h \in H \} \]
   \[ = \{ h + g \mid h \in H \} = H + g \] the right coset

2. \( G/H = \{ g + H \mid g \in G \} \) is a group
   under \( (g + H) + (g' + H) = (g + g') + H \) for \( g, g' \in G \)

Examples

Set \( G = \mathbb{Z} \) (\( \mathbb{Z}^+ \))

and \( H = m \mathbb{Z} = \{ mr \mid r \in \mathbb{Z} \} \) for \( m \neq 0 \)

Then \( H = m \mathbb{Z} \) is a subgroup of \( G \).

The quotient group \( \mathbb{Z}/m \mathbb{Z} \). The quotient group can also be thought of as the set of equivalence classes under

\[ r \sim r' \iff m \mid r-r' \] for \( r, r' \in \mathbb{Z} \)

\( \mathbb{Z}/m \mathbb{Z} \) as a quotient group is isomorphic to the group of integers modulo \( m \).

Moreover the group structures are identical.
Consider the map
\[ f: \mathbb{R}^+ \to \mathbb{C}^* \]
\[ r \mapsto e^{2\pi i r} \]
\[ \text{Im} f = \{ \alpha + bi \mid \alpha^2 + b^2 = 1 \} \]
\[ \ker f = (\mathbb{Z}, +) \subseteq \mathbb{R} \]

for each \( e^{2\pi i \theta} \in \text{Im} f \), the fiber is \( \{ \theta + n \mid n \in \mathbb{Z} \} \)

§ 3.2

\[ \text{Def. } \frac{|G|}{|H|} \text{ is the index of } H \text{ in } G \]

is the (possibly infinite) number of left cosets of \( H \) in \( G \).

(i.e., \( \frac{|G|}{|H|} = |G/H| \) is the set of cosets, \( H \) need not be normal)

Thin LAGRANGE'S THEOREM

\[ G \text{ a finite group, } H \leq G. \text{ Then } \]
\[ \frac{|G|}{|H|} = \frac{|G|}{|H|} \]

Proof

It follows from § 3.1 \( G \) is the disjoint union of left cosets of \( H \) in \( G \).

Moreover, each coset is in bijection with \( H \). (Denote \( g \in G, H = gH \))

Corollary \( G \) be a finite group, \( g \in G \) then \( |g| \mid |G| \). Consequently,

\[ |G| = 1, \text{ Proof } 1|g| = |g|, \text{ by Largrange } |G : \langle g \rangle| = \frac{|G|}{|\langle g \rangle|} \Rightarrow |\langle g \rangle| = 1 \]

or \[ |G| = 1 \]
Examples

1. $G$ a group s.t. $|G| = p$

   Every $g \in G$ has order either 1 or $p$.

   Therefore $g \notin G \setminus \{e\}$

   $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{p-1}\}$  \( \square \)

2. $G \cong \mathbb{Z}/p\mathbb{Z}$

   Also the lattice of subgroups of $G$ is

   \[
   \begin{array}{c}
   \mathcal{G} \\
   \langle e \rangle \\
   \end{array}
   \]

Suppose $G$ an arbitrary group with subgroup $H$ of index 2. \( \text{then } |G:H| = 2 \)

H must be normal \( \iff H \trianglelefteq G \)

Proof: first take $a \in G \setminus H$ then $aH + H \text{ (Why)} 

\neq H$.

Since $|G:H| = 2$, \( G = 1 \cdot H \sqcup aH \)

\( = H \uplus H_a \text{ disjoint union.} \)

\( aH = G \setminus H = Ha \)

On other hand, \( b \in H \), \( bH = Hb = H \) (check)

\( \forall g \in G \), \( gH = Hg \) \( \iff H \trianglelefteq G \) \( \square \)
For arbitrary subgroup $H$ of arbitrary $G$, we also let

$$G/H = \{ gH \mid g \in G \}$$

which is NOT a group, except when $H$ is normal.

Homework returned

Grading