Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

9 Lecture 9 May 22nd 2018

9.1 Subgroups (Continued 5)

9.1.1 Examples of Non-Cyclic Groups

Example 9.1.1
The Klein 4-group is

$$K_4 = \{1, a, b, c\} \text{ where } a^2 = b^2 = c^2 = 1 \text{ and } ab = c.$$

We may also write

$$K_4 = \langle\, a, b : a^2 = 1 = b^2,\, ab = ba \,\rangle.$$

Note that we can replace (a, b) *by* (a, c) *or* (b, c).

Example 9.1.2
The symmetric group of degree 3 *is*

$$S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

where $\sigma^3 = \varepsilon = \tau^2$ *and* $\sigma\tau = \tau\sigma^2$. *We may also express* S_3 *as*

$$S_3 = \langle\, \sigma, \tau : \sigma^3 = \varepsilon = \tau^2,\, \sigma\tau = \tau\sigma^2 \,\rangle$$

Definition 18 (Dihedral Group)
For $n \geq 2$, *the* ***dihedral group*** *of order* $2n$ *is*

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., b^{n-1}$$

where $a^n = 1 = b^2$ *and* $aba = b$. *Note that* a *represents a rotation of* $\frac{2\pi}{n}$ *radians, and* b *represents a reflection through the x-axis*

Recall from Assignment 1 that the dihedral group is a set of rigid motions for transforming a regular polygon back to its original position while changing the index of its vertices.

Example 9.1.3
We may write the dihedral group as

$$D_{2n} = \langle\, a, b : a^n = 1 = b^2,\, aba = b \,\rangle$$

Exercise 9.1.1
Prove the following:

1. $D_4 \cong K_4$
2. $D_6 \cong S_3$

9.2 Normal Subgroup

9.2.1 Homomorphism and Isomorphism

Definition 19 (Homomorphism)
Let G, H be groups. A mapping

$$\alpha : G \to H$$

is called a ***homomorphism*** *if $\forall a, b \in G$,*[1]

$$\alpha(ab) = \alpha(a)\alpha(b).$$

[1] Note that ab uses the operation of G while $\alpha(a)\alpha(b)$ uses the operation of H.

Example 9.2.1 (A classical example)
Consider the determinant map:

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \quad \textit{given by } A \to \det A$$

Note that $\mathbb{R}^*$ is the set of real numbers that has a multiplicative inverse.

Since

$$\det AB = \det A \det B$$

we have that the determinant map is a homomorphism.

This is a classical example to show a homomorphism, especially since the group $GL_n(\mathbb{R})$ uses **matrix multiplication** while $\mathbb{R}^*$ uses regular **arithmetic multiplication**.

Proposition 20 (Properties of Homomorphism)
Let $\alpha : G \to H$ be a group homomorphism. Then

1. $\alpha(1_G) = 1_H$

2. $\forall g \in G \;\; \alpha(g^{-1}) = \alpha(g)^{-1}$
3. $\forall g \in G \; \forall k \in \mathbb{Z} \;\; \alpha(g^k) = \alpha(g)^k$

Proof

1. *Note that*

$$\alpha(1_G)\alpha(g) = \alpha(1_G \cdot g) = \alpha(g) = \alpha(g \cdot 1_G) = \alpha(g)\alpha(1_G)$$

Thus it must be that $\alpha(1_G) = 1_H$ for only the identity of H satisfies this equation.

2. *Since H is a group, we know that*

$$1_H = \alpha(g)\alpha(g)^{-1}.$$

Now with part 1, we have that

$$\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1_G) = 1_H = \alpha(g)\alpha(g)^{-1}.$$

By Proposition 6, we have that $\alpha(g^{-1}) = \alpha(g)^{-1}$.

3. *This is simply a result of applying the definition repeatedly, which we can then perform an induction procedure to complete the proof.* □

Definition 20 (Isomorphism)

Let G, H be groups. Consider a mapping

$$\alpha : G \to H$$

*We say that α is an **isomorphism** if it is a homomorphism and bijective.*

*If α is an isomorphism, we say that G is **isomorphic to** to H, or that G and H are **isomorphic**, and denote that by $G \cong H$.*

Proposition 21 (Isomorphism as an Equivalence Relation)

1. *(Reflexive) The identity map $G \to G$ is an isomorphism.*
2. *(Symmetric) If $\sigma : G \to H$ is an isomorphism, then the inverse map $\sigma^{-1} : H \to G$ is also an isomorphism.*

3. ***(Transitive)*** *If $\sigma : G \to H$ and $\tau : H \to K$, then the composition map $\tau\sigma : G \to K$ is also an isomorphism.*

Proof

1. *The identity map is clearly bijective. For all $g_1, g_2 \in G$, we have that*

$$\alpha(g_1 g_2) = g_1 g_2 = \alpha(g_1)\alpha(g_2).$$

Thus the identity map is a homomorphism, and hence an isomorphism.

2. *Since σ is a bijective map, its inverse σ^{-1} exists and is also a bijective map. Since σ is bijective, we have that*

$$\forall h_1, h_2 \in H \ \exists! g_1, g_2 \in G \quad \sigma(g_1) = h_1, \sigma(g_2) = h_2.$$

Note that since σ has a bijective inverse, we also have

$$g_1 = \sigma^{-1}(h_1) \text{ and } g_2 = \sigma^{-1}(h_2).$$

Then since σ is a homomorphism,

$$\begin{aligned}\sigma^{-1}(h_1 h_2) &= \sigma^{-1}(\sigma(g_1)\sigma(g_2)) = \sigma^{-1}(\sigma(g_1 g_2)) \\ &= g_1 g_2 = \sigma^{-1}(h_1)\sigma^{-1}(h_2).\end{aligned}$$

3. *We know that the composition map of two bijective map is bijective. Let $g_1, g_2 \in G$, then since both τ and σ are homomorphisms*

$$\tau\sigma(g_1 g_2) = \tau(\sigma(g_1)\sigma(g_2)) = \tau\sigma(g_1)\tau\sigma(g_2),$$

where we note that $\sigma(g_1), \sigma(g_2) \in H$.

□

Example 9.2.2
Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r \geq 0\}$. Show that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

Solution
Consider the map

$$\alpha : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) \quad r \mapsto e^r,$$

where e is the natural exponent. Note that the exponential map from $\mathbb{R}$ to

$\mathbb{R}^+$ *is bijective*[2]. *Also,* $\forall r, s \in \mathbb{R}$ *we have that*

$$\alpha(r+s) = e^{r+s} = e^r e^s = \alpha(r)\alpha(s).$$

Therefore, α *is an isomorphism and* $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. □

[2] The image of the map covers all positive real numbers while taking all real numbers, which is the perfect candidate as a map here.

Example 9.2.3

Show that $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$.

Solution

Suppose, for contradiction, that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ *is an isomorphism. In particular, we have that* τ *is onto. Then* $\exists q \in \mathbb{Q}$ *such that* $\tau(q) = 2$. *Let* $\tau(\frac{q}{2}) = \alpha$. *Since* τ *is an isomorphism, we have*

$$\alpha^2 = \tau(\frac{q}{2})\tau(\frac{q}{2}) = \tau(\frac{q}{2} + \frac{q}{2}) = \tau(q) = 2.$$

But that implies that $\alpha = \sqrt{2}$, *which is clearly not rational. Thus, we know that there is no such* τ *and*

$$(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$$

as required. □

9.2.2 Cosets and Lagrange's Theorem

Definition 21 (Coset)

Let H *be a subgroup of a group* G.

$\forall a \in G \quad Ha = \{ha : h \in H\}$ *is the right coset of* H *generated by* a

and

$\forall a \in G \quad aH = \{ah : h \in H\}$ *is the left coset of* H *generated by* a

Note

Note that $1H = H = H1$. *Also, since* $a1 = a$ *and* $1 \in H$, *we have that* $a \in aH$, *and similarly so for* $a \in Ha$.

In general, aH *and* Ha *are not subgroups of* G. *See example*

Also, in general, $aH \neq Ha$, *since not all groups are abelian.*

Proposition 22 (Properties of Cosets)

Let H be a subgroup of G, and let $a, b \in G$. Then

1. $Ha = Hb \iff ab^{-1} \in H$. *In particular,* $Ha = H \iff a \in H$.

2. $a \in Hb \implies Ha = Hb$.

3. $Ha = Hb \veebar Ha \cap Hb = \emptyset$.[3] *Then the distinct right cosets of H forms a partition of G.*[4]

We can create an analogued version of this proposition for the left cosets.

[3] $\veebar \equiv$ XOR

[4] Note that this is true because by definition, we iterate over all elements of G to construct the cosets of the subgroup H. The earlier part of this statement implies that cosets must be distinct (otherwise, they are the same set), and so if we take the union of these cosets, by iterating through all elements of G, we get that

$$\bigcup_{a \in G} Ha = G.$$

Summarizing the above argument, we observe that the distinct cosets partitions G.

Proof

1. *For* ($\implies$),

$$\begin{aligned} Ha = Hb &\implies a = 1a \in Ha = Hb \\ &\implies \exists h \in H \;\; a = hb \\ &\implies ab^{-1} = h \in H. \end{aligned}$$

For ($\impliedby$),

$$\begin{aligned} ab^{-1} \in H &\implies \forall h \in H \;\; ha = h(ab^{-1})b \in Hb \\ &\implies Ha \subseteq Hb \\ ab^{-1} \in H &\implies (ab^{-1})^{-1} = ba^{-1} \in H \\ &\implies \forall h \in H \;\; hb = h(ba^{-1})a \in Ha \\ &\implies Hb \subseteq Ha \end{aligned}$$

Let $b = 1$. Then

$$Ha = H \iff a \in H \qquad \because 1^{-1} = 1$$

2. *Note*

$$a \in Hb \implies \exists h \in H \;\; a = hb \implies ab^{-1} \in H \overset{\text{by } 1}{\implies} Ha = Hb$$

3. *Trivially, if $Ha \cap Hb = \emptyset$, we are done.*

$$\begin{aligned} & Ha \cap Hb \neq \emptyset \\ \implies & \exists x \in Ha \cap Hb \\ \implies & (x \in Ha \overset{by\ 1}{\implies} Hx = Hb) \wedge (x \in Hb \overset{by\ 1}{\implies} Hx = Hb) \\ \implies & Ha = Hb \end{aligned}$$

□

By Proposition 22, we have that G can be written as a disjoint union of cosets of a subgroup H. We now define the following terminology that we shall use for the upcoming content.

Definition 22 (Index)

*Let H be a subgroup of a group G. We call the number of disjoint cosets of H in G as the **index** of H in G, and denote this number by $[G : H]$.*