List of Theorems

Proposition 1	. . . .	18
Proposition 2	Properties of S_n	20
Theorem 3	Cycle Decomposition Theorem	21
Proposition 4	Group Identity and Group Element Inverse	23
Proposition 5	. . . .	26
Proposition 6	Cancellation Laws	29
Proposition 7	. . . .	31
Proposition 8	Intersection of Subgroups is a Subgroup . .	35
Proposition 9	Finite Subgroup Test	35
Theorem 10	Parity Theorem	37
Theorem 11	Alternating Group	38
Proposition 12	Cyclic Group as A Subgroup	40
Proposition 13	Properties of Elements of Finite Order . . .	41
Proposition 14	Property of Elements of Infinite Order . . .	43
Proposition 15	Orders of Powers of the Element	43
Proposition 16	Cyclic Groups are Abelian	44
Proposition 17	Subgroups of Cyclic Groups are Cyclic . . .	45
Proposition 18	Other generators in the same group	46
Theorem 19	Fundamental Theorem of Finite Cyclic Groups	47
Proposition 20	Properties of Homomorphism	50
Proposition 21	Isomorphism as an Equivalence Relation . .	51

12.2.1 Quotient Groups

Let G be a group and K a subgroup of G. Given a set

$$\{Ka \,:\, a \in G\},$$

how can we create a group out of it?

A "natural" way to define an operation on the set of right cosets above is

$$\forall a, b \in G \qquad Ka * Kb = Kab. \tag{$\dagger$}$$

Note that it is entirely possible that for $a_1 \neq a$ and $b_1 \neq b$, we have $Ka = Ka_1$ and $Kb = Kb_1$. In order for Equation (†) to make sense as an operation, it is necessary that

$$Ka = Ka_1 \wedge Kb = Kb_1 \implies Kab = Ka_1b_1.$$

If the condition is satisfied, we say that the "multiplication" $KaKb$ is well-defined.

Lemma 34 (Multiplication of Cosets of Normal Subgroups)
Let K be a subset of G. The following are equivalent:

1. $K \lhd G$;
2. $\forall a, b \in G \;\; KaKb = Kab$ *is well-defined.*

Proof
$(1) \implies (2)$ *Suppose $K \lhd G$. Suppose $Ka = Ka_1$ and $Kb = Kb_1$. Then $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To show that $Kab = Ka_1b_1$, it suffices to show that $(ab)(a_1b_1)^{-1} \in K$. Note that since $K \lhd G$, we have that $aKa^{-1} = K$. Therefore,*

$$\begin{aligned} ab(a_1b_1)^{-1} &= ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a_1^{-1} \\ &= \big(a(bb_1^{-1})a^{-1}\big)(aa_1^{-1}) \in K. \end{aligned}$$

Therefore $Kab = Ka_1b_1$ as required.

$(2) \implies (1)$ *If $a \in G$, we need to show that $\forall k \in K$, $aka^{-1} \in K$. Since $Ka = Ka$ and $Kk = K(1)$* [2]*, by (2), we have that $Kak = Ka(1)$, i.e. $Kak = Ka$. Thus $aka^{-1} = 1 \in K$, implying that $aKa^{-1} \subseteq K$ and hence*

[2] This is cause 1 is in the same coset.

$K \triangleleft G$. $\square$

13 Lecture 13 May 30 2018

13.1 Isomorphism Theorems (Continued)

13.1.1 Quotient Groups (Continued)

Proposition 35

Let $K \triangleleft G$ and write ${}^{G}\!/_{K} = \{Ka : a \in G\}$ for the set of cosets of K.

1. *${}^{G}\!/_{K}$ is a group under the operation $KaKb = Kab$.*
2. *The mapping $\phi : G \to {}^{G}\!/_{K}$ given by $\phi(a) = Ka$ is a surjective homomorphism.*[1]
3. *If $[G : K]$ is finite, then $\left|{}^{G}\!/_{K}\right| = [G : K]$. In particular, if $|G|$ is finite, then $\left|{}^{G}\!/_{K}\right| = \frac{|G|}{|K|}$.*

[1]

Exercise 13.1.1
Is ϕ injective?

Solution
We know that we cannot uniquely express a coset, since for $a, b \in Ka$ such that $a \neq b$, we have that $Ka = Kb$.

Proof

1. *By Lemma 34, the operation is well-defined, and ${}^{G}\!/_{K}$ is closed under the operation. The identity of ${}^{G}\!/_{K}$ is $K = K(1)$ since $\forall Ka \in {}^{G}\!/_{K}$,*

$$KaK(1) = Ka = K(1)Ka.$$

Also, since

$$KaKa^{-1} = K(1) = Ka^{-1}Ka,$$

the inverse of Ka is Ka^{-1}. Finally, by associativity of G, we have that

$$Ka(KbKc) = Kabc = (KaKb)Kc.$$

It follows that ${}^{G}\!/_{K}$ is a group.

2. *Clearly, ϕ is surjective. For $a, b \in G$,*

$$\phi(ab) = Kab = KaKb = \phi(a)\phi(b).$$

   Thus ϕ is a surjective homomorphism.

3. *If $[G : K]$ is finite, then by definition of the index $[G : K]$, we have that $[G : K] = \left| {}^{G}\!/_{K} \right|$. Also, if $|G|$ is finite, then by Theorem 23,*

$$\left| {}^{G}\!/_{K} \right| = [G : K] = \frac{|G|}{|K|}.$$

□

Definition 26 (Quotient Group)
Let $K \lhd G$. The group ${}^{G}\!/_{K}$ of all cosets of K in G is called the ***quotient group*** *of G by K. Also, the mapping*

$$\phi : G \to {}^{G}\!/_{K} \text{ defined by } a \mapsto Ka$$

is called the ***coset*** *(pr* ***quotient****)* ***map****.*

13.1.2 Isomorphism Theorems

Definition 27 (Kernel and Image)
Let $\alpha : G \to H$ be a group homomorphism. The ***kernel*** *of α is defined by*

$$\ker \alpha := \{ g \in G : \alpha(g) = 1_H \} \subseteq G$$

and the image of α is defined by

$$\operatorname{im} \alpha := \alpha(G) = \{ \alpha(g) : g \in G \} \subseteq H.$$

Proposition 36
Let $\alpha : G \to H$ be a group homomorphism.

1. $\operatorname{im} \alpha$ *is a subgroup of H*

2. $\ker\alpha \triangleleft G$

Proof

1. *Note that* $1_H = \alpha(1_G) \in \alpha(G)$ *(i.e. the identity is in* $\operatorname{im}\alpha$*). Also, for* $h_1 = \alpha(g_1)$ *and* $h_2 = \alpha(g_2)$ *in* $\alpha(G)$ *and* $h_1, h_2 \in H$*, we have*

$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G).$$

(i.e. $\operatorname{im}\alpha$ *i closed under its operation). By Proposition 20,* $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$ *(i.e. the inverse of an element is also in* $\operatorname{im}\alpha$*). Thus by the Subgroup Test, we have that* $\operatorname{im}\alpha$ *is a subgroup of* H*.*

2. *For* $\ker\alpha$*,* $\alpha(1_G) = 1_H$*. For* $k_1, k_2 \in \ker\alpha$*, we have*

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1.$$

Also,

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1.$$

By the Subgroup Test, $\ker\alpha$ *is a subgroup of* G*.*

If $g \in G$ *and* $k \in \ker\alpha$*, then*

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

Thus by Proposition 27, $\ker\alpha \triangleleft G$*.*

$\square$

Example 13.1.1
Consider the determinant map

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \text{ defined by } A \mapsto \det A.$$

Then $\ker\det = SL_n(\mathbb{R})$*. Then* $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$*, as proven before.*

Example 13.1.2
Define the ***sign of a permutation*** $\sigma \in S_n$ *by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then the sign mapping, $\operatorname{sgn} : S_n \to \{\pm 1\}$ *defined by* $\sigma \mapsto \operatorname{sgn}(\sigma)$ *is a*