

Notes in Group Theory

Thum Sze Khai

Last edited: 25/03/2021

Please send any error found to [sze.khai0508\(at\)gmail.com](mailto:sze.khai0508@gmail.com).

Contents

1	Preliminaries	2
1.1	Groups	2
1.2	Subgroups	2
1.3	Lagrange theorem	3
1.3.1	Corollaries of Lagrange theorem	3
1.4	Normal Subgroups	3
1.5	Homomorphisms	4
1.6	Miscellaneous theorems	4
2	Some important results	6
2.1	Isomorphism theorems	6
2.2	Cartesian product of groups	7
3	Symmetric groups	9
3.1	Introduction	9
3.2	Cycle notation	9
A	Recommended references	12

1 Preliminaries

We (usually) do not include proof for this section as these are learnt in Algebra I SIM2004.

1.1 Groups

Definition 1.1. (Definition of groups) Let G be a set and (\cdot) an operation on G . Suppose G satisfies

- $\forall a, b \in G; a \cdot b \in G$ (closure),
- $\forall a, b, c \in G; a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity),
- $\exists e \in G; a \cdot e = a = e \cdot a, \forall a \in G$ (identity),
- $\forall a \in G; \exists b \in G$ s.t. $a \cdot b = e = b \cdot a$, where we denote such $b = a^{-1}$ (inverses).

Then we say (G, \cdot) is a group.

We will omit the use of (\cdot) whenever it's clear from context.

Theorem 1.2. *If G is a group, then G has a unique identity e . For every $a \in G$, a^{-1} is also unique.*

Theorem 1.3. *The Cayley table of a group G is a latin square, but the converse is not necessarily true.*

1.2 Subgroups

Definition 1.4. (Subgroups) Let G be a group and $H \subseteq G$. If H satisfies

- $\forall a, b \in H; ab \in H$,
- $\forall a, b, c \in H; a(bc) = (ab)c$,
- $\exists e \in H; ae = a = ea, \forall a \in H$,
- $\forall a \in H; \exists a^{-1} \in H$ s.t. $aa^{-1} = e = a^{-1}a$,

then we say H is a subgroup of G and write $H \leq G$.

Theorem 1.5. *Let G be a group and $H \leq G$. If e_H and e_G are identity of H and G respectively, then $e_H = e_G$.*

Theorem 1.6. *Let G be a group, $H \leq G$, and $a \in H \subseteq G$. If a^{-1}_H and a^{-1}_G are inverses of a in H and G respectively, then $a^{-1}_H = a^{-1}_G$.*

Theorem 1.7. (Subgroup criterion) *Let G be a group and $H \subseteq G$. Then H is a subgroup iff $H \neq \emptyset$ and $xy^{-1} \in H, \forall x, y \in H$.*

1.3 Lagrange theorem

Definition 1.8. (Coset) Let G be a group and $H \leq G$. We define left coset $gH = \{gh : h \in H\}$ for $g \in G$. Similarly right coset is $Hg = \{hg : h \in H\}$

Theorem 1.9. (Left coset equivalent criterion) Let G be a group and $H \leq G$. For $a, b \in H$, $aH = bH$ iff $b^{-1}a \in H$.

Theorem 1.10. Let G be a group and $H \leq G$. If $a, b \in G$, then either $aH = bH$ or $aH \cap bH = \emptyset$.

Theorem 1.11. Let G be a group and $H \leq G$. If $a, b \in G$, then $|aH| = |bH|$. In particular $|gH| = |H|$ for any $g \in G$.

Theorem 1.12. Let G be a group and $H \leq G$. Then the set of cosets $\{gH : g \in G\}$ form a partition of G , i.e. $\cup\{gH : g \in G\} = G$ and the cosets are mutually disjoint.

Theorem 1.13. (Lagrange) Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$.

Definition 1.14. Let G be a group and $H \leq G$. Then the index of H in G is $[G : H] = \frac{|G|}{|H|}$.

Corollary 1.15. Let G be a group and $H \leq G$. Then $[G : H]$ is a positive integer.

1.3.1 Corollaries of Lagrange theorem

Theorem 1.16. Let G be a group and $a \in G$. Then $\text{ord}(a) \mid |G|$.

Corollary 1.17. Let G be a group of order n and $a \in G$. Then $a^n = 1$.

Theorem 1.18. If G is a group of prime order p , then G is cyclic.

Proof. Let $a \in G$ be a non-identity element. Then $|\langle a \rangle| \mid |G| = p$, hence $\langle a \rangle$ has order p since a is non-identity. Therefore $\langle a \rangle = G$ and G is cyclic. \square

1.4 Normal Subgroups

Definition 1.19. (Normal subgroup) Let G be a group and $H \leq G$. If $ghg^{-1} \in H$ for all $h \in H, g \in G$ then H is a normal subgroup and we write $H \triangleleft G$.

Theorem 1.20. (Normal subgroup criterion) Let G be a group and $H \leq G$. The following are equivalent:

- (i) $H \triangleleft G$
- (ii) $(H \neq \emptyset) \wedge (\forall x, y \in H; xy^{-1} \in H) \wedge (\forall h \in H, g \in G; ghg^{-1} \in H)$
- (iii) $H \leq G \wedge (\forall g \in G; gH = Hg)$

(iv) $H \leq G \wedge (\forall g \in G; gHg^{-1} = H)$

Theorem 1.21. Let G be a group and $H \leq G$. If $[G : H] = 2$ then $H \triangleleft G$.

Theorem 1.22. (Quotient group) Let G be a group and $H \triangleleft G$. Let $G/H = \{gH : g \in G\}$ be the set of left cosets. Then G/H forms a group with the operation

$$(aH)(bH) = (ab)H, \quad a, b \in H.$$

We call G/H the quotient group.

Corollary 1.23. Let G be a group and $H \triangleleft G$. Then $|G/H| = [G : H]$.

1.5 Homomorphisms

Definition 1.24. (Homomorphism) Let G and H be groups. A function $f : G \rightarrow H$ is a homomorphism if $f(ab) = f(a)f(b)$ for all $a, b \in G$. If f is surjective then we call f an epimorphism. If f is bijective we call f an isomorphism.

Definition 1.25. (Kernel and image) Let G, H be groups and $f : G \rightarrow H$ a homomorphism. Then the kernel of f is

$$\ker f = \{g \in G : f(g) = e_H\}$$

and the image of f is

$$\text{Im} f = \{f(g) : g \in G\} = \{h : h \in H \text{ s.t. } \exists g \in G; f(g) = h\}$$

Theorem 1.26. Let G and H be groups and $f : G \rightarrow H$ a homomorphism. Then $\ker f \leq G$ and $\text{Im} f \leq H$. Moreover, $\ker f \triangleleft G$.

1.6 Miscellaneous theorems

Theorem 1.27. If H is a subgroup of a cyclic group, then H is cyclic.

Proof. Let $H \leq G = \langle x \rangle$. We may assume $|H| > 1$. Then there exist $h \in H$ s.t. $h = x^i$ for some non-zero integer i . Yet if $i < 0$, since H is a group, then $h^{-1} = x^{-i} \in H$. Therefore there exist natural number n where $x^n \in H$.

Let n_0 be the smallest natural where $x^{n_0} \in H$. We claim that $H = \langle x^{n_0} \rangle$. Clearly $\langle x^{n_0} \rangle \subseteq H$. Let $y \in H$ where $y = x^i$ for some integer i . Similarly we may consider only $i > 0$. By the division algorithm, there exist integer q and $0 \leq r < n_0$ where $i = qn_0 + r$. But

$$y = x^i = x^{qn_0+r} = x^r \in H.$$

Thus we must have $r = 0$ and $n_0 \mid i$. Hence $H \subseteq \langle x^{n_0} \rangle$ and therefore $H = \langle x^{n_0} \rangle$ as needed. \square

Theorem 1.28. Suppose G is a cyclic group of order n . If $d \mid n$ then G contains exactly one subgroup of order d .

Proof. Let $G = \langle a \rangle$, $H \leq G$ and $|H| = d$. From theorem 1.27 we have $H = \langle a^i \rangle$ for some integer i . By hypothesis (or Lagrange theorem) we have $n \mid d$. Furthermore, since $a^{id} = 1$ by corollary 1.17, we have $id = kn$ for some integer k . Hence $i = k \left(\frac{n}{d}\right)$ and $a^i \in \langle a^{\frac{n}{d}} \rangle$, therefore $H \subseteq \langle a^{\frac{n}{d}} \rangle$.

Note that $\text{ord}(a^{\frac{n}{d}}) = d$ since for any natural l where $a^{\frac{n}{d}l} = 1$ implies $\frac{n}{d}l = k'n$ for some integer k' , thus $d \mid l$ and $d \leq l$.

Therefore $H = \langle a^{\frac{n}{d}} \rangle$. Finally it is easy to see that for any $d \mid n$, $\langle a^{\frac{n}{d}} \rangle \leq G$, and we're done. \square

2 Some important results

This section contains results that I can't fit into anywhere.

2.1 Isomorphism theorems

Theorem 2.1. (*First isomorphism theorem*) Let $f : G \rightarrow H$ be an epimorphism with kernel K . Then $K \triangleleft G$ and $G/K \cong H$.

Proof. It is easy to show that $K \triangleleft G$. We define $h : G/K \rightarrow H$ where $h(gK) = f(g)$ for $g \in G$.

The function h is well-defined since $g_1K = g_2K$ implies $g_2^{-1}g_1 \in K$ hence $f(g_2^{-1}g_1) = 1$ which implies $f(g_1) = f(g_2)$ as desired. Note that the reversed direction shows that h is injective.

Then,

$$h(g_1Kg_2K) = h(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = h(g_1K)h(g_2K)$$

so h is a homomorphism.

Clearly h is surjective. Therefore h is an isomorphism, thus $G/K \cong H$. \square

Theorem 2.2. (*Second isomorphism theorem*) Let N and T be subgroups of G with $N \triangleleft G$. Then, $N \cap T \triangleleft T$ and $T/(N \cap T) \cong NT/N$.

Note on the quotient group NT/N : we have the following representation

$$NT/N = \{ntN : nt \in NT\} = \{t(t^{-1}nt)N : nt \in NT\} = \{tN : t \in T\}$$

which is much simpler

Proof. Let $a \in T$, $b \in N \cap T$. Clearly $aba^{-1} \in T$. Since $N \triangleleft G$, we have $aba^{-1} \in N$, hence $aba^{-1} \in N \cap T$ thus $N \cap T \triangleleft T$.

Let $f : T \rightarrow NT/N$ where $f(a) = aN$ for $a \in T$. Clearly f is a surjective homomorphism. Note that $f(a) = N$ iff $a \in N$, since $a \in T$, we have $a \in N \cap T$. Therefore $\ker f = N \cap T$. By theorem 2.1 we have

$$T/(N \cap T) \cong NT/T$$

and we're done. \square

Theorem 2.3. (*Third isomorphism theorem*) Let $K \leq H \leq G$ with $K, H \triangleleft G$. Then $H/K \triangleleft G/K$ and

$$(G/K)/(H/K) \cong G/H.$$

Proof. Let $g \in G$, $h \in H$. Then

$$(gK)^{-1}(hK)(gK) = (g^{-1}hg)K \in H/K$$

since H is normal. Hence $H/K \triangleleft G/K$.

Now let $g : G/K \rightarrow G/H$ by $g(aK) = aH$ for $a \in G$. Since $aK = bK \Rightarrow b^{-1}a \in K \leq H$ hence $b^{-1}a \in H$ thus $aH = bH$, therefore g is well-defined.

Clearly g is a surjective homomorphism. Then $g(aK) = H$ iff $a \in H$, i.e. $aK \in H/K$. Thus $\ker g = H/K$. By theorem 2.1, we are done. \square

2.2 Cartesian product of groups

Definition 2.4. Let A, B be groups. We define the cartesian product of A and B as

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Theorem 2.5. Let A, B be groups. Then $A \times B$ is a group under

$$(a, b) * (c, d) = (ac, bd), \quad \forall a, c \in A, b, d \in B.$$

Proof. Let $(a, b), (c, d) \in A \times B$. Since A, B are closed,

$$(a, b) * (c, d) = (ac, bd) \in A \times B$$

Then, let $(e, f) \in A \times B$. We have

$$\begin{aligned} [(a, b) * (c, d)] * (e, f) &= (ac, bd) * (e, f) = ((ac)e, (bd)f) \\ &= (a(ce), b(df)) = (a, c) * (ce, df) = (a, c) * [(c, d) * (e, f)] \end{aligned}$$

Note that $(1, 1) \in A \times B$. Then for any $(a, b) \in A \times B$, $(a, b) * (1, 1) = (a, b) = (1, 1) * (a, b)$. Hence $(1, 1)$ is the identity.

If $(a, b) \in A \times B$, then $(a^{-1}, b^{-1}) \in A \times B$. Also,

$$(a, b) * (a^{-1}, b^{-1}) = (1, 1) = (a^{-1}, b^{-1}) * (a, b)$$

and we're done. \square

Theorem 2.6. Let A, B be groups and $G = A \times B$. Then $A \times \{1\}$ and $\{1\} \times B$ are normal subgroups of G .

Proof. Let $(x, y) \in G$ and $a \in A$, hence $(a, 1) \in A \times \{1\}$. Clearly, $A \times \{1\} \leq G$. Then

$$(x, y)^{-1} * (a, 1) * (x, y) = (x^{-1}ax, 1) \in A \times \{1\}$$

Hence $A \times \{1\}$ is normal. Similarly for $\{1\} \times B$. \square

Theorem 2.7. Let A, B be groups, $H = A \times \{1\}$ and $K = \{1\} \times B$. Then, $H \cap K = \{1 = (1, 1)\}$, $H, K \triangleleft G$, and $G = HK$.

Proof. (Basically trivial.) □

Theorem 2.8. (*Internal direct product theorem*) Let $H, K \triangleleft G$. If $H \cap K = \{1\}$ and $G = HK$, then $G \cong H \times K$.

Proof. Let $f : G \rightarrow H \times K$ where

$$f(ab) = a \times b \quad \forall a \in H, b \in K$$

We shall show that f is well-defined. Suppose we have $a_1, a_2 \in H, b_1, b_2 \in K$ such that $a_1 b_1 = a_2 b_2$. Then $a_2^{-1} a_1 = b_2 b_1^{-1}$, clearly the left hand side is in H , right hand side is in K , therefore they are identity since $H \cap K = \{1\}$, which yields $a_1 = a_2, b_1 = b_2$. Hence f is well-defined.

Now, $f(a_1 b_1 a_2 b_2) = f(a_1 b_1 a_2 b_1^{-1} b_1 b_2)$. Since H is normal, $a_1 b_1 a_2 b_1^{-1} \in H$, so

$$f(a_1 b_1 a_2 b_2) = (a_1 b_1 a_2 b_1^{-1}, b_1 b_2) = (a_1, b_1)(b_1 a_2 b_1^{-1}, b_2).$$

Then, consider $b_1 a_2 b_1^{-1} a_2^{-1}$. On one hand, $b_1(a_2 b_1 a_2^{-1}) \in K$, on the other hand $(b_1 a_2 b_1^{-1}) a_2^{-1} \in H$. Hence $b_1 a_2 b_1^{-1} a_2^{-1} = 1$ which implies $b_1 a_2 b_1^{-1} = a_2$. Therefore

$$f(a_1 b_1 a_2 b_2) = (a_1, b_1)(a_2, b_2) = f(a_1 b_1) f(a_2 b_2)$$

and f is a homomorphism.

Clearly f is surjective. For injectivity, if we have $f(a_1 b_1) = f(a_2 b_2)$ then $(a_1, b_1) = (a_2, b_2)$ which is equivalent to $a_1 = a_2$ and $b_1 = b_2$. Thus f is bijective and $G \cong H \times K$ as desired. □

Remark. Another formulation of theorem 2.8 is $H, K \leq G$ where

- (i) $H \cap K = \{1\}$,
- (ii) for all $h \in H, k \in K$, we have $hk = kh$,
- (iii) $G = HK$.

It is easy to see how (ii) and (iii) implies $H, K \triangleleft G$. If $H, K \triangleleft G$, then along with (i) we can show that $hkh^{-1}k^{-1} = 1$ hence $hk = kh$ for any $h \in H, k \in K$.

¹(Unworthy comment from TSK) Actually we can take $f : H \times K \rightarrow G$. Then well-defined becomes trivial, the proof of homomorphism is still the same (more or less), surjectivity remains trivial, and the proof of injectivity is similar to proving well-defined in the original proof. So we only have to worry about two parts.

3 Symmetric groups

3.1 Introduction

Definition 3.1. Let $[n] = \{1, 2, 3, \dots, n\}$. A permutation on $[n]$ is a bijective function $\sigma : [n] \rightarrow [n]$.

Theorem 3.2. *The set of all permutation on $[n]$, S_n with composition (\circ) forms a group. We call S_n the symmetric group.*

Proof. Let $\sigma, \varphi \in S_n$. Since σ and φ are bijective, $\sigma \circ \varphi$ is also a bijective function on $[n]$, hence $\sigma \circ \varphi \in S_n$ for any $\sigma, \varphi \in S_n$.

Now let $\psi \in S_n$. Since function composition is associative, we have $\sigma \circ (\varphi \circ \psi) = (\sigma \circ \varphi) \circ \psi$ for any $\sigma, \varphi, \psi \in S_n$.

Let $1 : [n] \rightarrow [n]$ by $1(k) = k$ for $k \in [n]$. Note that $1 \in S_n$. Then $\sigma \circ 1(k) = \sigma(k) = 1 \circ \sigma(k)$ for all $k \in [n]$.

For any $\sigma \in S_n$, σ^{-1} is also a bijective function, hence $\sigma^{-1} \in S_n$. Furthermore, $\sigma \circ \sigma^{-1} = 1 = \sigma^{-1} \circ \sigma$. Therefore S_n is a group under composition as desired. \square

Remark. The symmetric group S_n has order $n!$.

3.2 Cycle notation

There are several ways to represent a permutation. A natural one is the **row notation**.

Let $\sigma \in S_n$. We may write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

However, the row notation is slightly unwieldy. It takes up two lines and it hides some information from us. For example, it is not clear, from the notation, what is the order of σ . Also it's difficult to work out the composition.

We present a new notation, the **cycle notation**. Consider the following permutation under S_6 .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$$

Notice that the number 1, 2, 3 forms a cycle of length 3. Similarly 4 and 5 forms a cycle of length 2. Consider the notation

$$\sigma = (1 \ 2 \ 3)(4 \ 5)$$

We read the notation from right to left. Consider a more complicated cycle notation

$$\psi = (1\ 3\ 4)(3\ 6)(2\ 4\ 6)(5\ 1)$$

Following the notation from right to left, we have

$$\begin{aligned} 1 &\rightarrow 5 \\ 2 &\rightarrow 4 \rightarrow 1 \\ 3 &\rightarrow 6 \\ 4 &\rightarrow 6 \rightarrow 3 \rightarrow 4 \\ 5 &\rightarrow 1 \rightarrow 3 \\ 6 &\rightarrow 2 \end{aligned}$$

which gives

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 3 & 2 \end{pmatrix}$$

So we can actually simplify ψ to $\psi = (1\ 5\ 3\ 6\ 2)$.

We say a cycle notation $\sigma = (\lambda_1^{(1)}\lambda_2^{(1)}\lambda_3^{(1)}\cdots\lambda_{l_1}^{(1)})(\lambda_1^{(2)}\lambda_2^{(2)}\lambda_3^{(2)}\cdots\lambda_{l_2}^{(2)})\cdots(\lambda_1^{(k)}\lambda_2^{(k)}\lambda_3^{(k)}\cdots\lambda_{l_k}^{(k)})$ is a **disjoint cycle notation** if each cycle are disjoint, i.e. no number appears in two cycle.

Theorem 3.3. *Disjoint cycle commutes.*

Theorem 3.4. *(Disjoint cycle notation works) Let S_n be a symmetric group. Then all permutation in S_n has a (essentially unique) disjoint cycle notation.*

Essentially unique means that the order of the disjoint cycle doesn't matter, the "rotation" of individual cycle doesn't matter.

Proof. Let $\sigma \in S_n$. Consider the cycle $(1\ \sigma(1)\ \sigma^2(1)\ \sigma^3(1)\ \cdots)$. There must exist positive integers k, l where $\sigma^k(1) = \sigma^l(1)$. Hence $\sigma^{k-l}(1) = 1$. Let k be the smallest natural where $\sigma^k(1) = 1$. Hence the first cycle is

$$(1\ \sigma(1)\ \sigma^2(1)\ \sigma^3(1)\ \cdots\ \sigma^{k-1}(1)).$$

Now pick $j = [n] \setminus \{1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots, \sigma^{k-1}(1)\}$. Similarly, we have a second cycle

$$(j\ \sigma(j)\ \sigma^2(j)\ \cdots\ \sigma^l(j)).$$

These cycle are disjoint, otherwise it is clear that they are the same cycle. We may repeat this until we exhausted all $1, 2, \dots, n$. \square

Terminology: We call a cycle of length k a k -cycle. A 2-cycle is also called a transposition.

Theorem 3.5. *Symmetric groups are generated by transposition.*

Proof. We only need to show that we may express any cycle as a product of transpositions. Consider a cycle $(a_1 a_2 a_3 \cdots a_n)$. Note that

$$(a_1 a_n)(a_1 a_{n-1})(a_1 a_{n-2}) \cdots (a_1 a_3)(a_1 a_2) = (a_1 a_2 a_3 \cdots a_n)$$

and we're done. \square

Remark. There is more than one way to express a cycle as product of transpositions. For example

$$(a_1 a_2 a_3 \cdots a_n) = (a_1 a_2)(a_2 a_3)(a_3 a_4) \cdots (a_{n-1} a_n)$$

Theorem 3.6. *A permutation with one and only one (non-singular) cycle of length k has order k .*

Corollary 3.7. *Let $\sigma \in S_n$, if $\sigma = c_1 c_2 c_3 \cdots c_k$ where c_i are disjoint cycles, and c_i has length l_i , then $\text{ord}(\sigma) = \text{lcm}(l_1, l_2, \dots, l_k)$.*

A Recommended references

1. Hall, M., The theory of Groups. Dover Publications; Reprint edition, New York, 2018.
2. Barnard, T., Neil, H., Discovering Group Theory: A Transition to Advanced Mathematics, Taylor & Francis Ltd, London, 2016.
3. Rotman, J.J., An introduction to the theory of groups, 4th edition. Springer-Verlag, New York, 1999.