Notes in Group Theory

Thum Sze Khai

Last edited: 24/03/2021

Please send any error found to sze.khai0508(at)gmail.com.

Contents

1 Preliminaries

1.1 Groups

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

- $\forall a, b \in G;\ a \cdot b \in G$ (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 $b = a^{\text{-1}}$ (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 $a \in G$, $a^{\text{-1}}$ 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

1.3 Normal Subgroups

1.4 Homomorphisms

Definition 1.4. Let G and H be groups. A function $f : G \to H$ 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.

2 Isomorphism theorem

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

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

The function h is well-defined since $g_1K = g_2K$ implies ${g_2}^{\text{-1}} g_1 \in K$ hence $f({g_2}^{\text{-1}} g_1) = 1$ 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 $G/K \cong H$. □

Theorem 2.2. *(Second isomorphism theorem) Let N and T be subgroups of G with $N \lhd G$. Then, $N \cap T \lhd T$ 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 $N \lhd G$, we have $aba^{-1} \in N$, hence $aba^{-1} \in N \cap T$ thus $N \cap T \lhd T$.

Let $f : T \to NT/N$ 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. □

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

Now let $g : G/K \to G/H$ 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. □

3 Symmetric groups

3.1 Introduction

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

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 $1 : [n] \to [n]$ 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. □

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

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

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 $j = [n] \setminus \{1, \sigma(1), \sigma^2(1), \sigma^3(1), \cdots, \sigma^{k-1}(1)\}$. 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 $1, 2, \ldots, n$. □

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. □

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 $\sigma = c_1c_2c_3\cdots c_k$ where c_i are disjoint cycles, and c_i has length l_i, then $ord(\sigma) = lcm(l_1, l_2, \ldots, l_k)$.*

4 Direct product

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.