Review V(Slides 280 - 311)

Homormophism & Coset

Hold on! This is difficult!

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

March 25, 2022

VE203 - Discrete Mathmatics

Symmetric Group

Definition

Given $n \in \mathbb{N}\backslash\{0\}$, we have the following symmetric group of degree n,

$$\begin{aligned} S_n &= \{\text{All permutations on } n \text{ letters/numbers}\} \\ &= \mathrm{Sym}\{1, 2, 3, \dots, n\} \\ &= \{f : [n] \to [n] \mid f \text{ bijective}\} \end{aligned}$$

Note that it is a finite group of order $n!$ (the number of bijections from $[n]$ to $[n]$), *i.e.*, $|S_n| = n!$.

- A subgroup of S_n is called a permutation group.
- A permutation of the form (ab) where $a \neq b$ is called a transposition.

Permutation

A permutation that can be expressed as a product of an **even/odd number of transpositions** is called an even/odd permutation.

The set of even permutations in S_n forms a subgroup of S_n, denoted as A_n, is called the alternating group of degree n.

Permutation → transportation: $(132)(5648) = (13)(32)(56)(64)(48)$ (not unique, but only can be either all odd or all even).

Inverse of permutation: $\sigma = (132)(5648) \;\Rightarrow\; \sigma^{-1} = (8465)(231)$ (Separate permutations to be **disjoint** first. Since $\sigma(a_i) = a_j$ implies $\sigma^{-1}(a_j) = a_i$, we only need to reverse the order of the cyclic pattern).

Composition: $(12)(245)(13)(125) = (14532)$.
(Apply the **right** permutation first. Demo!).

Exercise

1. True or false:
   - Can an abelian group have a non-abelian subgroup?
   - Can a non-abelian group have an abelian subgroup?
   - Can a non-abelian group have a non-abelian subgroup?

Answer: No; Yes; Yes.

Exercise

2. Prove the following:
   1. S_n is non-abelian for $n \geq 3$;
   2. A_n is a subgroup of S_n;
   3. $|A_n| = n!/2$.

Homomorphism

Given groups G, G', a homomorphism is a map $f : G \to G'$ such that for

$$f(x \cdot y) = f(x) \cdot f(y)$$

We have:

- $f(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$
- $f(1_G) = 1_{G'}$
- $f(a^{-1}) = f^{-1}(a)$

Compare and Contrast

Recall the concept of structure preserving

$$\begin{tikzcd} y \arrow[r, "f"] \arrow[d, "x \cdot"'] & f(y) \arrow[d, "f(x) \cdot"] \\ x \cdot y & f(x \cdot y) \arrow[l, "f^{-1}"'] \end{tikzcd}$$

Image & Kernel

The image of a homomorphism $f : G \to G'$, often denoted by $\operatorname{im} f$, or $f(G)$, is simply the image of as a map of sets:

$$\operatorname{im} f = \left\{x \in G' \mid x = f(a) \text{ for some } a \in G\right\}.$$

The kernel of f , denoted by $\ker f$, is the set of elements of G that are mapped to the identity in G':

$$\ker f = \{a \in G \mid f(a) = 1_{G'}\}.$$

Comapre and Contrast

Let U, V be real or complex vector spaces and $L \in \mathscr{L}(U, V)$, then we define the range and kernel of L by:

$$\operatorname{ran} L := \{v \in V : \underset{u \in U}{\exists} \; v = Lu\}$$

$$\ker L := \{u \in U : Lu = 0\}$$

Properties

Let $f : G \to G'$ be a group homomorphism, and let $a, b \in G$. Let $K = \ker f$. The following are equivalent:

1. $f(a) = f(b)$
2. $a^{-1}b \in K$
3. $b \in aK$
4. $aK = bK$

! A homomorphism $f : G \to G'$ is injective iff $\ker f = \{1_G\}$.

! Isomorphism $G \cong G' \quad \Leftrightarrow \quad f$ is **bijective**.

! How to check if a **homomorphism** is an **isomorphism**:

$$\text{verify } \ker f = \{1_G\} \text{ (injection) and } \operatorname{im} f = G' \text{ (bijection)}$$

Exercise

3. Prove: Let a homomorphism $f : G \to G'$. If H is a subgroup of G, then $f(H)^{-1}$ is a subgroup of G'.

Solution:

Let $x, y, a \in H$.

1. Closure: $f(x)^{-1}f(y)^{-1} = f(x^{-1})f(y^{-1}) = f\left(x^{-1}y^{-1}\right) = f\left((yx)^{-1}\right) = f(yx)^{-1}$.
2. Identity: $1_G \in H, 1_{G'} = f(1_G) \in f(H)^{-1}$.
3. Inverse: $f(a)^{-1} = f\left(a^{-1}\right) \in f(H)^{-1}$.

Exercise

4. Let $(G, \cdot)$ be a group. Let $g, h \in G$ both have order n, prove that $\langle g \rangle \cong \langle h \rangle$.

Exercise

4. Let $(G, \cdot)$ be a group. Let $g, h \in G$ both have order n, prove that $\langle g \rangle \cong \langle h \rangle$.

Solution:

Define $f : \langle g \rangle \to \langle h \rangle$ by $f(g) = h$ and for all $0 \leq k \leq n, f\left(g^k\right) = f(g)^k$. So, f is a well-defined function, and, by definition, f preserves the group product. It is clear that the function f sends $1_G \mapsto 1_G$, $g \mapsto h$, $\ldots$, $g^{n-1} \mapsto h^{n-1}$, and so f is a bijection.

(Directly taken from Zach's slides)

Cosets

Given a group G, if H is a subgroup of G and $a \in G$, the notation aH will stand for the set of all products ah with $h \in H$,

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

This set is called a **left coset** of H in G.

The number of left cosets of a subgroup is called the index of H in G. The index is denoted by $[G : H]$ (can be infinite, why?).

All left cosets aH of a subgroup H of a group G have the same order.

- Counting formula: $|G| = |H| \cdot [G : H]$.
- Lagrange's Theorem: Let H be a subgroup of a finite group G. The order of H divides the order of G.

Exercise

5. Verify Lagrange's Theorem for the subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6$.

Exercise

5. Verify Lagrange's Theorem for the subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6$.

Solution:

The cosets are

$$0 + H = \{0, 3\}, \quad 1 + H = \{1, 4\}, \quad 2 + H = \{2, 5\}.$$

Notice there are 3 cosets, each containing 2 elements, and that the cosets form a **partition** of the group.

An important consequence of Lagrange's Theorem

Theorem

Let $(G, \cdot)$ be a group and let $g \in G$ have order n. If there exists $m, k \in \mathbb{N}\backslash\{0\}$ with $n = mk$, then the order of g^m is k.

Proof.

Let $m, k \in \mathbb{N}\backslash\{0\}$ with $\mathrm{n = mk}$. Now, $(g^m)^k = g^{mk} = g^n = 1_G =$. If $0 < q < k$ is such that $(g^m)^q = 1_G$, then $g^{mq} = 1_G$. But $mq < mk = n$, which is a contradiction.

Theorem

If $(G, \cdot)$ is a finite group with order n, then for all $g \in G, g^n = 1_G$.

Proof.

Let $(G, \cdot)$ be a finite group with order n. Let $g \in G$. We know that the order of g must be finite, so let k be the order of g. Now, k must divide n, so the exists $m \in N$ such that $n = mk$. So $g^n = g^{mk} = (g^k)^m$ $= 1_G^m = 1_G$.

Exercise

6. Prove that for any subgroup $H \leq G$, the (left) cosets of H partition the group G.

Hint:

We need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.

Normal Subgroup

Given group G, and $a, g \in G$, the element $gag^{-1} \in G$ is called the conjugate of a by g.

A subgroup N of G is a normal subgroup, denoted by $N \trianglelefteq G$, if for all $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Properties:

- $f : G \to G'$ a homomorphism, then $\ker f \trianglelefteq G$.
- Every subgroup of an abelian group is normal.
- The center is always a normal subgroup.
- $gH = Hg$ for all $g \in G$ iff $H \trianglelefteq G$.
- $A_n \trianglelefteq S_n$.

Try your best! Remember them!

Exercise

Important result:

7. Show that any subgroup of index 2 in a group is a normal subgroup.

Exercise

Important result:

7. Show that any subgroup of index 2 in a group is a normal subgroup.

Solution:

Denote the subgroup as H. Obviously, the left cosets of a subgroup of index 2 are $1_H H = H$ and aH, where $a \notin H$; (why?) the right cosets are $H1_H = H$ and Ha. Since the cosets form a partition of the origin group, and $1_H H = H1_H = H$, so the remaining is another coset, namely $aH = Ha$. (left=right) So H is normal.

Distribution of Primes (Part I)

Proposition

Let K be any positive integer larger than 2, then there exists two adjacent primes p and p' $(p' < p)$, such that $p - p' \geq K$.

Proof:

Let $K! + 2 = M$, then $2 \mid M, 2+1 \mid M+1, \cdots, K \mid M+K-2$. Since $M > 2$, we conclude that $M, M+1, \cdots, M+K-2$ are all composite. Let p' be the largest prime that is smaller than M, but the next prime p is denifitely larger than $M+K-2$, namely

$$p - p' \geq (M+K-1) - (M-1) = K.$$

Distribution of Primes (Part I)

Definition

We denote $\pi(x)$ as the number of primes no larger than x. Namely

$$\pi(x) = \sum_{p \le x} 1.$$

We already know that as $x \to \infty$, $\pi(x) \to \infty$. But how fast it grows?

Here, we're going to prove that $\pi(x) = \Theta(x/\ln x)$. Namely, there exists two positive numbers A_1 and A_2, such that

$$A_1 \frac{x}{\ln x} < \pi(x) < A_2 \frac{x}{\ln x} \quad (x \ge 2)$$

This is so called Чебышев (Chebyshev) inequality in number theory.

Distribution of Primes (Part I)

Before prove the above inequality, we need to prove the following two lemmas.

Lemma 1

Let n be any positive integer, set

$$N = \frac{(2n)!}{(n!)^2}$$

then

$$(\pi(2n) - \pi(n)) \ln n \leq \ln N \leq \pi(2n) \ln(2n).$$

Proof of Lemma 1

Let

$$N = \prod_{p \le 2n} p^{\alpha_p}$$

to be the standard decomposition of N, we have

$$\alpha_p = \sum_{r=1}^{\infty} \left[\frac{2n}{p^r}\right] - 2\sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right] = \sum_{r=1}^{\left[\frac{\ln(2n)}{\ln p}\right]} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right),$$

(this is because when $r > \lfloor \ln(2n)/\ln(p) \rfloor$, $p^r > 2n > n$). Obviously,

$$\alpha_p \le \sum_{r=1}^{\left[\frac{\ln(2n)}{\ln p}\right]} 1 = \left[\frac{\ln(2n)}{\ln p}\right] \le \frac{\ln(2n)}{\ln p}.$$

Proof (Cont.)

Therefore

$$\ln N = \sum_{p\leq 2n} \alpha_p \ln p \leq \sum_{p\leq 2n} \ln(2n) = \pi(2n)\ln(2n).$$

On the other hand, if $n < p \leq 2n$, then $p \mid (2n)!$, $\left(p, (n!)^2\right) = 1$, so $p \mid N$. We have

$$N \geq \prod_{n<p\leq 2n} p.$$

Take logrithm on both side,

$$\ln N \geq \sum_{n<p\leq 2n} \ln p > \ln n \sum_{n<p\leq 2n} 1 = (\pi(2n) - \pi(n))\ln n,$$

this complete our proof.

Esitimation of $\ln N$

Now it's time to esitimate how large $\ln N$ is.

Lemma 2

For the same n, N defined in Lemma 1, we have

$$n \ln 2 \leq \ln N \leq 2n \ln 2.$$

Proof:

Considering that N is the coefficient of term x^n when expanding $(1+x)^{2n}$, so

$$N \leq (1+1)^{2n} = 2^{2n}$$

On the other hand,

$$N = \frac{2n(2n-1)\cdots(n+1)}{n!} = 2\left(2 + \frac{1}{n-1}\right)\cdots(2 + \frac{n-1}{1}) \geq 2^n.$$

Reference

- Examples From Zach's Slides (P196)
- Exercises from 2021-Fall-Ve203 TA Zhao Jiayuan
- Yan Shijian, etc. *Basic Number Theory*, fourth edition. Beijing: Higher Education Press, 2020.5 print.