Advanced Modern Algebra

Joseph J. Rotman

September 12, 2019

Contents

1 Group I

1.1 Permutations

Definition 1.1. A **permutation** of a set X is a bijection from X to itself.

Definition 1.2. The family of all the permutations of a set X, denoted by S_X is called the **symmetric group** on X. When $X = \{1, 2, \ldots, n\}$, S_X is usually denoted by X_n and is called the **symmetric group on n letters**

Definition 1.3. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, 2, \ldots, n\}$. If $\alpha \in S_n$ fixes the other integers and if

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$$

then α is called an textbf{r-cycle}. α is a cycle of **length** r and denoted by

$$\alpha = (i_1\ i_2\ \ldots\ i_r)$$

2-cycles are also called the **transpositions**.

Definition 1.4. Two permutations $\alpha, \beta \in S_n$ are **disjoint** if every i moved by one is fixed by the other.

Lemma 1.5. Disjoint permutations $\alpha, \beta \in S_n$ commute

Proposition 1.6. Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.

Proof. Induction on the number k of points moved by α $\square$

Definition 1.7. A **complete factorization** of a permutation α is a factorization of α into disjoint cycles that contains exactly one 1-cycle (i) for every i fixed by α

Theorem 1.8. Let $\alpha \in S_n$ and let $\alpha = \beta_1 \ldots \beta_t$ be a complete factorization into disjoint cycles. This factorization is unique except for the order in which the cycles occur

Proof. for all i, if $\beta_t(i) \neq i$, then $\beta_t^k(i) \neq \beta_t^{k-1}(i)$ for any $k \geq 1$ $\square$

Lemma 1.9. If $\gamma, \alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ has the same cycle structure as γ. In more detail, if the complete factorization of γ is

$$\gamma = \beta_1\beta_2 \ldots (i_1\ i_2\ \ldots) \ldots \beta_t$$

then $\alpha\gamma\alpha^{-1}$ is permutation that is obtained from γ by applying α to the symbols in the cycles of γ

Example. Suppose

$$\beta = (1\ 2\ 3)(4)(5)$$
$$\gamma = (5\ 2\ 4)(1)(3)$$

then we can easily find the α

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

Theorem 1.10. Permutations γ and σ in S_n has the same cycle structure if and only if there exists $\alpha \in S_n$ with $\sigma = \alpha\gamma\alpha^{-1}$

Proposition 1.11. If $n \geq 2$ then every $\alpha \in S_n$ is a product of tranpositions

Proof. $(1\ 2\ \ldots\ r) = (1\ r)(1\ r-1)\ldots(1\ 2)$ □

Definition 1.12. A permutation $\alpha \in S_n$ is **even** if it can be factored into a product of an even number of transpositions. Otherwise **odd**

Definition 1.13. If $\alpha \in S_n$ and $\alpha = \beta_1 \ldots \beta_t$ is a complete factorization, then **signum** α is defined by

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}$$

Theorem 1.14. For all $\alpha, \beta \in S_n$

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$$

Theorem 1.15.

1. Let $\alpha \in S_n$; if $\operatorname{sgn}(\alpha) = 1$ then α is even. otherwise odd
2. A permutation α is odd if and only if it's a product of an odd number of transpositions

Corollary 1.16. Let $\alpha, \beta \in S_n$. If α and β have the same parity, then $\alpha\beta$ is even while if α and β have distinct parity, $\alpha\beta$ is odd

1.2 Groups

Definition 1.17. A **binary operation** on a set G is a function

$$* : G \times G \to G$$

Definition 1.18. A **group** is a set G equipped with a binary operation * s.t.

1. the **associative law** holds
2. **identity**
3. every $x \in G$ has an **inverse**, there is a $x' \in G$ with $x * x' = e = x' * x$

Definition 1.19. A group G is called **abelian** if it satisfies the **commutative law**

Lemma 1.20. Let G be a group

1. The **cancellation laws** holds: if either $x * a = x * b$ or $a * x = b * x$, then $a = b$
2. e is unique
3. Each $x \in G$ has a unique inverse
4. $(x^{-1})^{-1} = x$

Definition 1.21. An expression $a_1 a_2 \ldots a_n$ **needs no parentheses** if all the ultimate products it yields are equal

Theorem 1.22 (Generalized Associativity)**.** If G is a group and $a_1, a_2, \ldots, a_n \in G$ then the expression $a_1 a_2 \ldots a_n$ needs no parentheses

Definition 1.23. Let G be a group and let $a \in G$. If $a^k = 1$ for some $k > 1$ then the smallest such exponent $k \geq 1$ is called the **order** or a; if no such power exists, then one says that a has **infinite order**

Proposition 1.24. If G is a finite group, then every $x \in G$ has finite order

Definition 1.25. A **motion** is a distance preserving bijection $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$. If π is a polygon in the plane, then its **symmetry group** $\Sigma(\pi)$ consists of all the motions φ for which $\varphi(\pi) = \pi$. The elements of $\Sigma(\pi)$ are called the **symmetries** of π

Let π_4 be a square. Then the group $\Sigma(\pi_4)$ is called the **dihedral group** with 8 elements, denoted by D_8

Definition 1.26. If π_n is a regular polygon with n vertices $v_1, \ldots, v_n$ and center O, then the symmetry group $\Sigma(\pi_n)$ is called the {dihedral group} with $2n$ elements, and it's denoted by D_{2n}

1.3 Lagrange's theorem

Definition 1.27. A subset H of a group G is a **subgroup** if

1. $1 \in H$
2. if $x, y \in H$, then $xy \in H$
3. if $x \in H$, then $x^{-1} \in H$

If H is a subgroup of G, we write $H \leq G$. If H is a proper subgroup, then we write $H<$G

Proposition 1.28. A subset H of a group G is a subgroup if and only if H is nonempty and whenever $x, y \in H$, $xy^{-1} \in H$

Proposition 1.29. A nonempty subset H of a finite group G is a subgroup if and only if H is closed; that is, if $a, b \in H$, then $ab \in H$

Definition 1.30. If G is a group and $a \in G$

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$$

$\langle a \rangle$ is called the **cyclic subgroup** of G **generated** by a. A group G is called **cyclic** if there exists $a \in G$ s.t. $G = \langle a \rangle$, in which case a is called the **generator**

Definition 1.31. The **integers mod** m, denoted by $\mathbb{I}_m$ is the family of all congruence classes mod m

Proposition 1.32. Let $m \geq 2$ be a fixed integer

1. If $a \in \mathbb{Z}$, then $[a] = [r]$ for some r with $0 \leq r < m$
2. If $0 \leq r' < r < m$, then $[r'] \neq [r]$
3. $\mathbb{I}_m$ has exactly m elements

Theorem 1.33.

1. If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if $(k, n) = 1$
2. If G is a cyclic group of order n and $\mathrm{gen}(G) = \{\text{all generators of } G\}$, then
$$\left|\mathrm{gen}(G)\right| = \phi(n)$$
where ϕ is the Euler ϕ-function

Proof. 1. there is $t \in \mathbb{N}$ s.t. $a^{kt} = a$ hence $a^{kt-1} = 1$ and $n \mid kt - 1$ □

Proposition 1.34. Let G be a finite group and let $a \in G$. Then the order of a is $|\langle a \rangle|$.

Definition 1.35. If G is a finite group, then the number of elements in G, denoted by $|G|$ is called the **order** of G

Proposition 1.36. The intersection $\bigcap_{i \in I} H_i$ of any family of subgroups of a group G is again a subgroup of G

Corollary 1.37. If X is a subset of a group G, then there is a subgroup $\langle X \rangle$ of G containing X tHhat is **smallest** in the sense that $\langle X \rangle \leq H$ for of G that contains X every subgroup \$\$

Definition 1.38. If X is a subset of a group G, then $\langle X \rangle$ is called the {subgroup generated by} X

A **word** on X is an element $g \in G$ of the form $g = x_1^{e_1} \dots x_n^{e_n}$ where $x_i \in X$ and $e_i = \pm$ for all i

Proposition 1.39. If X is a nonempty subset of a group G, then $\langle X \rangle$ is the set of all words on X

Definition 1.40. If $H \leq G$ and $a \in G$, then the **coset** aH is the subset aH of G, where

$$aH = \{ah : h \in H\}$$

aH **left coset**, Ha **right coset**

Lemma 1.41. $H \leq G, a, b \in G$

1. $aH = bH$ if and only if $b^{-1}a \in H$
2. if $aH \cap bH \neq \emptyset$, then $aH = bH$
3. $|aH| = |H|$ for all $a \in G$

Proof. define a relation $a \equiv b$ if $b^{-1}a \in H$ □

Theorem 1.42 (Lagrange's Theorem)**.** If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$

Proof. Let $\{a_1H, a_2H, \ldots, a_tH\}$ be the family of all the distinct cosets of H in G. Then

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH$$

hence

$$|G| = |a_1H| + \cdots + |a_tH|$$

But $|a_iH| = |H|$ for all i. Hence $|G| = t|H|$ □

Definition 1.43. The **index** of a subgroup H in G denoted by $[G : H]$, is the number of left cosets of H in G

Note that $|G| = [G : H]|H|$

Corollary 1.44. If G is a finite group and $a \in G$, then the order of a is a divisor of $|G|$

Corollary 1.45. If G is a finite group, then $a^{|G|} = 1$ for all $a \in G$

Corollary 1.46. If p is a prime, then every group G of order p is cyclic

Proposition 1.47. The set $U(\mathbb{I}_m)$, defined by

$$U(\mathbb{I}_m) = \{[r] \in \mathbb{I}_m : (r, m) = 1\}$$

is a multiplicative group of order $\varphi(m)$. If p is a prime, then $U(\mathbb{I}_m) = \mathbb{I}_m^\times$.

Corollary 1.48 (Fermat)**.** If p is a prime and $a \in \mathbb{Z}$, then

$$a^p \equiv a \mod p$$

Proof. suffices to show $[a^p] = [a]$ in $\mathbb{I}_p$. If $[a] = [0]$, then $[a^p] = [a]^p = [0]$. Else, since $\left|\mathbb{I}_p^\times\right| = p$, $[a]^{p-1} = [1]$ □

Theorem 1.49 (Euler)**.** If $(r, m) = 1$, then

$$r^{\phi(m)} \equiv 1 \mod m$$

Theorem 1.50 (Wilson's Theorem)**.** An integer p is a prime if and only if

$$(p-1)! \equiv -1 \mod p$$