Advanced Modern Algebra

Joseph J. Rotman

September 13, 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 $a_1 a_2 \dots a_n$ **needs no parentheses** if all the ultimate products it yields are equal

Theorem 1.22 (Generalized Associativity)**.** If G is a group and $a_1, a_2, \dots, a_n \in G$ then the expression $a_1 a_2 \dots a_n$ 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 $v_1, \dots, v_n$ 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 $\text{gen}(G) = \{\text{all generators of } G\}$, then
$$\left|\text{gen}(G)\right| = \phi(n)$$
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 $\left|\langle a \rangle\right|$.

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 every subgroup H of G that contains X

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 $e_i = \pm 1$ 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 $|G| = t|H|$ $\square$

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 $U(\mathbb{I}_m) = \mathbb{I}_m^{\times}$, the nonzero elements of $\mathbb{I}_p$.

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 $\left|\mathbb{I}_p^{\times}\right| = p - 1$, $[a]^{p-1} = [1]$ $\square$

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

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

1.4 Homomorphisms

Definition 1.51. If $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a **homomorphism** if

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$. If f is also a bijection, then f is called an **isomorphism**. G and H are called **isomorphic**, denoted by $G \cong H$

Lemma 1.52. Let $f : G \to H$ be a homomorphism

1. $f(1) = 1$
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x^n) = f(x)^n$ for all $n \in \mathbb{Z}$

Definition 1.53. If $f : G \to H$ is a homomorphism, define

$$\textbf{kernel} f = \{x \in G : f(x) = 1\}$$

and

$$\textbf{image} f = \{h \in H : h = f(x) \text{ for some } x \in G\}$$

Proposition 1.54. Let $f : G \to H$ be a homomorphism

1. $\ker f$ is a subgroup of G and $\operatorname{im} f$ is a subgroup of H
2. if $x \in \ker f$ and if $a \in G$, then $axa^{-1} \in \ker f$
3. f is an injection if and only if $\ker f = \{1\}$

Proof. 1. $f(a) = f(b) \Leftrightarrow f(ab^{-1}) = 1$

□

Definition 1.55. A subgroup K of a group G is called a **normal subgroup** if $k \in K$ and $g \in G$ imply $gkg^{-1} \in K$, denoted by $K \lhd G$

Definition 1.56. If G is a group and $a \in G$, then a **conjugate** of a is any element in G of the form

$$gag^{-1}$$

where $g \in G$

Definition 1.57. If G is a group and $g \in G$, define **conjugation** $\gamma_g : G \to G$ by

$$\gamma_g(a) = gag^{-1}$$

for all $a \in G$

Proposition 1.58.
1. If G is a group and $g \in G$, then conjugation $\gamma_g : G \to G$ is an isomorphism
2. Conjugate elements have the same order

Proof.
1. bijection: $\gamma_g \circ \gamma_{g^{-1}} = 1 = \gamma_{g^{-1}} \circ \gamma_g$

□

Proposition 1.59.
1. If H is a subgroup of index 2 in a group G, then $g^2 \in H$ for every $g \in G$
2. If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G

Definition 1.60. The group of **quaternions** is the group $\boldsymbol{Q}$ of order 8 consisting of the following matrices in $GL(2, \mathbb{C})$

$$\boldsymbol{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

where I is the identity matrix

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Proposition 1.61. The alternating group A_4 is a group of order 12 having no subgroup of order 6

1.5 Quotient group

$\mathcal{S}(G)$ is the set of all nonempty subsets of a group G. If $X, Y \in \mathcal{S}(G)$, define

$$XY = \{xy : x \in X \text{ and } y \in Y\}$$

Lemma 1.62. $K \leq G$ is normal if and only if

$$gK = Kg$$

A natural question is that whether HK is a subgroup when H and K are subgroups. The answer is no. Let $G = S_3, H = \langle (1\ 2) \rangle, K = \langle (1\ 3) \rangle$

Proposition 1.63.

1. If H and K are subgroups of a group G, and if one of them is normal, then $HK \leq G$ and $HK = KH$
2. If $H, K \lhd G$, then $HK \lhd G$

Theorem 1.64. Let G/K denote the family of all the left cosets of a subgroup K of G. If $K \lhd G$, then

$$aKbK = abK$$

for all $a, b \in G$ and G/K is a group under this operation

Proof. $aKbK = abKK = abK$ □

G/K is called the **quotient group** G mod K

Corollary 1.65. Every $K \lhd G$ is the kernel of some homomorphism

Proof. Define the **natural map** $\pi : G \to G/K$, $a \mapsto aK$ □

Theorem 1.66 (First Isomorphism Theorem)**.** If $f : G \to H$ is a homomorphism, then

$$\ker f \lhd G \quad \text{and} \quad G/\ker f \cong \operatorname{im} f$$

If $\ker f = K$ and $\varphi : G/K \to \operatorname{im} f \leq H, aK \mapsto f(a)$, then φ is an isomorphism

Remark

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/K \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Proposition 1.67 (Product Formula)**.** If H and K are subgroups of a finite group G, then

$$|HK||H \cap K| = |H||K|$$

Proof. Define a function $f : H \times K \to HK, (h, k) \mapsto hk$. Show that $\left|f^{-1}(x)\right| = |H \cap K|$.

Claim that if $x = hk$, then

$$f^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}$$

□

Theorem 1.68 (Second Isomorphism Theorem)**.** If $H \lhd G, K \leq G$, then $HK \leq G, H \cap K \lhd G$ and

$$K/(H \cap K) \cong HK/H$$

Proof. $hkH = kk^{-1}hkH = kh'H = kH$ $\square$

Theorem 1.69 (Third Isomorphism Theorem)**.** If $H, K \triangleleft G$ with $K \leq H$, then $H/K \triangleleft G/K$ and

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

Theorem 1.70 (Correspondence Theorem)**.** If $K \triangleleft G, \pi : G \to G/K$ is the natural map, then

$$S \mapsto \pi(S) = S/K$$

is a bijection between $Sub(G; K)$, the family of all those subgroups S of G that contain K, and $Sub(G/K)$, the family of all the subgroups of G/K. If we denote S/K by S^*, then

1. $T \leq S \leq G$ if and only if $T^* \leq S^*$, in which case $[S : T] = [S^* : T^*]$
2. $T \triangleleft S$ if and only if $T^* \triangleleft S^*$, in which case $S/T \cong S^*/T^*$

$$\begin{tikzcd}
G \arrow[d, dash] \arrow[dr] & \\
S \arrow[d, dash] \arrow[dr] & G/K \arrow[d, dash] \\
T \arrow[d, dash] \arrow[dr] & S/K = S^* \arrow[d, dash] \\
K \arrow[dr] & T/K = T^* \arrow[d, dash] \\
 & \{1\}
\end{tikzcd}$$