Chapter 5 Groups of permutations (bijections)

Basic notation and ideas

We study the most "general type" of groups - groups of permutations (bijections).

Definition A bijection from a set A to itself is also called a permutation

Theorem Let A be a set, and let S_A be the set of permutations on A, i.e., bijections from A to A. Then S_A is a group under function composition.

Examples (Important) S_1, S_2, S_3, S_4**.**

Cayley Theorem

Definition If A has n elements, we may assume $A = \{1, \ldots, n\}$, and write S_A as S_n, *the symmetric group of degree* n, which has $n!$ elements.

Remark The group S_A is not Abelian if A has more than 2 elements.

Theorem 6.1 Every group is isomorphic to a subgroup of S_A.

Proof. Use the Left (or right) regular representation of G

Cycles, and the Alternating Groups

Definition and notation

Let $\sigma = (i_1, \ldots, i_m) \in S_n$ be the permutation of sending $\sigma(i_1) = i_2, \ldots, \sigma(i_{m-1}) = i_m$, and $\sigma(i_m) = i_1$, and $\sigma(j) = j$ for all other j.

We call σ an m-cycle in S_n. A 1-cycle is a fixed point, a two cycle is called a **transposition**.

Examaple ...

Theorems 5.1–5.4 Consider S_n with $n > 1$.

(a) Disjoint cycles in S_n commute.

(b) Every permutation in S_n is a product of disjoint cycles.

(c) The order of $\sigma \in S_n$ is the lcm of the cycle lengths in its disjoint cycle decomposition.

(d) Every permutation is a product of transpositions.

Even and odd permutations

Definition A permutation is even (odd) if it is a product of even (odd) number of transpositions.

Theorem 5.5 A permutation is either even or odd. The identity permutation ε is even.

Proof. (1) Use isomorphism to the group of permutations and determinant theory.

(2) p.107–110 in the book. Key step. Proof by induction that if $\varepsilon = \beta_1 \cdots \beta_r$, then $\varepsilon = \hat{\beta}_1 \cdots \hat{\beta}_{r-2}$ by the following trick if $r \geq 3$.

Let $\beta_r = (ab)$. Move $\beta_r = (ab)$ to the left until we see $\beta_1 \eta_j$ has the following form so that we can apply the reduction:

$$(ab)(ab) = \varepsilon, \quad (ac)(ab) = (ab)(bc), \quad (bc)(ab) = (ac)(cb), \quad (cd)(ab) = (ab)(cd).$$

Eventually, ...

□

Theorem 5.7 The set A_n of even permutations in S_n form a subgroup of order $n!/2$.

Proof. Use bijection to count!

Subgroups of permutation groups and applications

(1) Dihedral groups

(2) Rotations of tetrahedron.

(3) Moves in Rubik's cube.

(4) Construct check digit using D_5; see pp. 115-116.

Chapter 6 Isomorphisms

Definition: Two groups are isomorphic if ....

Examples

(1) The function $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ is a group isomorphism.

(2) The group $(\mathbb{Z}_n, +)$ is somorhic to $(G_n, \cdot)$, where

$$G_n = \{\exp(i2k\pi/n) : k = 0, 1, \ldots, n-1\}.$$

(3) Every cyclic group is isomorphic to $(\mathbb{Z}, n)$ or $(\mathbb{Z}, +)$.

(4) [**Theorem 6.1**] Every group is isomorphic to a subgroup of S_A.

(5) The group S_n is isomorphic to the group of $n \times n$ permutation matrices.

Results on group isomorphisms and applications

Theorem 6.2 Suppose $\phi : G_1 \to G_2$ is an isomorphism.

1. $\phi(e_1) = e_2$.
2. $\phi(a^n) = \phi(a)^n$ for any $n \in \mathbb{Z}$.
3. Two elements $a, b \in G_1$ commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G_1 = \langle a \rangle$ if and only if $G_2 = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for every $a \in G_1$.
6. For every integer k and $b \in G_1$, we have

$$|\{x \in G_1 : x^k = b\}| = |\{y \in G_2 : y^k = \phi(b)\}|.$$

In particular, $|\{x \in G_1 : x^k = e_1\}| = |\{y \in G_2 : y^k = e_2\}|$.

Theorem 6.3 Suppose $\phi : G_1 \to G_2$ is an isomorphism.

1. $\phi^{-1} : G_2 \to G_1$ is an isomorphism.
2. G_1 is Abelian if and only if $\phi(G_1) = G_2$ is Abelian.
3. G_1 is cyclic if and only if $\phi(G_1) = G_2$ is.

   In particular, $G_1 = \langle a \rangle$ if and only if $G_2 = \langle \phi(a) \rangle$.
4. If $K \leq G_1$, then $\phi(K) \leq G_2$.
5. If $H \leq G_2$, then $\phi^{-1}(H) \leq G_1$.
6. $\phi(Z(G_1)) = Z(G_2)$.

Definition Let G be a group, and $a \in G$. Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism.

Theorem 6.4 Under function composition, the set $Aut(G)$ of group automorphisms is a group, and the set $Inn(G)$ of inner automorphisms is a subgroup.

Theorem 6.5 [Automorphisms of $\mathbb{Z}_n$] The groups $Aut(\mathbb{Z}_n)$ is isomorphic to $(U(n), \cdot)$ with

$$U(n) = \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}.$$

Chapter 7 Cosets and Lagrange's Theorem

Definition Let G be a group and $H \leq G$. For $a \in G$ define the left coset of H containing a by $aH = \{ah : h \in H\}$ and the right coset of H containing by $Ha = \{ha : h \in H\}$.

Theorem 7.1 [LaGrange's Theoerem and other properties of cosets] Let G be a group, and $H \leq G$. Define a relation on R on G by $(a, b) \in R$ if $a^{-1}b \in H$. Then R is an equivalence relation so that the left cosets are equivalence classes.

(a) We have $aH = bH$ if and only if $a^{-1}b \in H$.

(b) The group G is a union of disjoint left cosets of H.

(c) The map $ah \mapsto bh$ is a bijection between two cosets aH and bH.

(d) If G is finite, then it is a disjoint union of m left cosets of H with $m = |G|/|H|$.

Notation and Terminology The number of cosets of the subgroup H in G is called the index of H in G, and denoted by $|G : H|$. If G is finite, it is equal to $|G|/|H|$.

Corollary Let G be a finite group.

1. If $a \in G$, then $|a|$ is a factor of $|G|$ so that $a^{|G|} = e$.
2. If G has prime order than G is cyclic.

Corollary [Fermat's Little Theorem] If $a \in \mathbb{Z}$ and p is a prime, then $a^p - a$ is divisible by p. More generally, if $x \in \mathbb{Z}_n$, then $k^{\phi(n)} = 1$ if $\gcd(k, n) = 1$, i.e., $k \in U(n)$.

Remarks

1. The converse of Lagrange's Theorem is false. Example 5 in p.149.

   The group A_4 has order 12, but there is no subgroup of order 6.

2. One may consider the right cosets Ha so that $Ha = Hb$ if and only if $ab^{-1} \in H$,

   G is a partition of the right cosets.

3. Left and right cosets are different in general.

4. A subgroup H in G satisfies $aH = Ha$ for all $a \in G$ if and only if $aHa^{-1} = H$ for all $a \in H$. Such a subgroup is called a normal subgroup of G.

Theorem 7.2 Let H, K be finite subgroups of a group. If $HK = \{hk : h \in H, k \in K\}$, then

$$|HK| = |H|\,|K|/|H \cap K|.$$

Theorem 7.3 If G is a group with $|G| = 2p$ for a prime number $p > 2$, then G is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.