Permutation Groups

Prajwal Neupane

1 Ideas

from Dixon, Permutation Groups

1.1 Preliminaries

1. Consider polynomial: $X^5 - X + 1$.
2. Has five distinct roots: one real (r_1), four non-real (z_1, z_2, z_3, z_4)
3. Taking the set of roots and applying the action of complex conjugation leaves the set as: one real (r_1) unchanged, and four-non-real (z_2, z_1, z_4, z_3).
4. Complex conjugation fixes the real element and permutes the non-real elements pair wise.
5. Generally, any automorphism (like complex conjugation) of the field of complex numbers induces a permutation on the set of roots.
6. The set of all such permutations forms a group which is called the **Galois group**.
7. come back to Galois groups. It describes the algebraic symmetries of the polynomial like the rotations/transformations on a cube describe its symmetries.
8. Just as a cube has spatial symmetries (rotations and reflections) that rearrange its faces while preserving its structure, a polynomial has algebraic symmetries (field automorphisms) that rearrange its roots while preserving all polynomial equations with rational coefficients.

1.2 Symmetric Groups

1. $\Omega :=$ arbitary non-empty set of "points".
2. a bijection (one-to-one, onto) of Ω onto itself is a permutation of Ω.
3. Set of all permutations of Ω forms a group under composition of mappings called symmetric group on Ω. $(Sym(\Omega), S^{\Omega}, S_{\Omega})$
4. S_n forms a symmetric group for the set $\Omega = \{1, 2, 3, ..., n\}$
5. Permutation group is a sub-group of $Sym(\Omega)$

6. If Ω and Ω' have same cardinality (there is a bijection $A : \alpha \to \alpha'$) then $Sym(\Omega) \cong Sym(\Omega')$ via $x \to x'$ defined by

$$x' \text{ takes } \alpha' \text{ to } \beta' \text{ and } x \text{ takes } \alpha \text{ to } \beta$$

7. Proof sketch

Proof. for every $\alpha' \in \Omega', \exists \alpha = A^{-1}(\alpha') \in \Omega$
for every $A^{-1}(\alpha') \in \Omega, \exists f \in S^{\Omega}, f(\alpha) = \beta \in \Omega$
for every $\beta \in \Omega, \exists A(\beta) = \beta' \in \Omega'$
We have just defined a map $\phi : S^{\Omega} \to S^{\Omega'}$ which is a permutation of Ω'

$$\phi(f)(\alpha') = A(f(A^{-1}(\alpha')))$$

ϕ takes $f \in S^{\Omega}$ and gives a permutation $g \in S^{\Omega'}$ it is bijective because A, f are bijective.

□

1.2.1 Representing Permutations:

(a) The mapping $x : \Omega \to \Omega$ may be written explicity,

$$x = \begin{pmatrix} \alpha_1 & \alpha_2 & ... & \alpha_n \\ \beta_1 & \beta_2 & ... & \beta_n \end{pmatrix}$$

where, top row is some enumeration of the points of Ω and β_i is the image of α_i under x for each i.

(b) Product of disjoint cycles. A permutation $c \in Sym(\Omega)$ is called an r-cycle $(r = 1, 2, ...)$ if for r distinct points $\gamma_1, \gamma_2, ..., \gamma_r$ of Ω, c maps γ_i onto $\gamma_{i+1} (i = 1, ..., r-1)$, maps γ_r onto γ_1, and leaves all other points fixed.