Algorithms in Finite Groups

MATH 37500: László Babai
Scribe: Ang Li

10/07/14

3 Automorphism groups, wreath product, regular permutation groups

3.1 Automorphism groups of Platonic solids and n-cubes. Wreath product.

Exercise 3.1. Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group. Prove: G is primitive if and only if the stabilizer G_x is a maximal subgroup.

Exercise 3.2. $S_k^{(2)} \leq S_{\binom{k}{2}}$ is primitive for $k \geq 5$.

Exercise 3.3. Petersen's graph is isomorphic to the complement of the line graph of K_5.

Exercise 3.4. The automorphism group of Dodecahedron is not isomorphic to S_5.

Exercise 3.5. $\mathrm{Aut}^+(Dodecahedron) \cong A_5$ and $\mathrm{Aut}(Dodecaheron) \cong A_5 \times C_2$. Here Aut^+ denotes the group of orientation preserving symmetries.

Exercise 3.6. (a) Those congruences (norm-preserving linear transformations) of $\mathbb{R}^n$ which fix the origin form the orthogonal group $\mathrm{O}(n)$ consisting of the orthogonal matrices A defined by the equation $A^T A = I$. (b) Prove that the determinant of such a matrix is ± 1. (c) The *orientation preserving* ("sense-presrving") transformations form the group $\mathrm{SO}(n)$ which consists of those $A \in \mathrm{O}(n)$ with $\det(A) = 1$. Prove: $\mathrm{SO}(n)$ is the unique subgroup of index 2 in $\mathrm{O}(n)$.

Exercise 3.7. (a) Prove: if $A \in \mathrm{SO}(3)$ then A is a rotation. (b) Prove: if $A \in \mathrm{O}(3) \setminus \mathrm{SO}(3)$ then A is a "rotational reflection," i.e., a rotation followed by a reflection in an axis perpendicular to the axis of rotation. (c) Find a rotational reflection that causes the vertices of a regular tetrahedron to be permuted in a 4-cycle.

Exercise 3.8. Prove: $\mathrm{Aut}^+(cube) \cong S_4$ and $\mathrm{Aut}(cube) \cong S_4 \times C_2$.

Exercise 3.9. Let X be a connected graph and Y the union of k disjoint copies of X. Then $\mathrm{Aut}(Y) = \mathrm{Aut}(X) \wr S_k$ where the wreath product acts in the imprimitive (union) action.

Exercise 3.10. Let Q_n denote the graph (1-skeleton) of the n-cube. So $V(Q_n) = \{0,1\}^n$ and two vertices are adjacent of their Hamming distance is 1.
Prove: $\mathrm{Aut}(Q_n)$ includes $\mathbb{Z}_2^n$ and $\mathbb{Z}_2^n \lhd \mathrm{Aut}(Q_n)$.

Exercise 3.11. $\mathrm{Aut}(Q_n)/\mathbb{Z}_2^n \cong S_n$.

Exercise 3.12. $\mathrm{Aut}(Q_n) \cong \mathbb{Z}_2^n \wr S_n$ (wreath product)

Exercise 3.13. Is $\mathbb{Z}(Q_n)$ primitive?

Exercise 3.14. If $A \leq \mathrm{Sym}(\Omega)$ is primitive and not of prime order and $B \leq \mathrm{Sym}(\Phi)$ is transitive then $A \wr B$ in product action on Ω^Φ is primitive.

3.2 Regular permutation groups, permutational isomorphism

Exercise 3.15. Let $G \leq \mathrm{Sym}(\Omega)$ and assume $x, y \in \Omega$ belong to the same orbit of G. Consider the set $G_{x\to y} := \{g : x^g = y\}$. Let $h \in G_{x\to y}$. Prove: $G_{x\to y} = G_x \cdot h = h \cdot G_y$.

Exercise 3.16. If x, y are in the same orbit of $G \leq \mathrm{Sym}(\Omega)$ then G_x and G_y are conjugate.

Exercise 3.17. The *right translation* ρ_g by $g \in G$ is the permutation of G defined by $\rho_g : x \mapsto xg$ $(x \in G)$. The *left translation* λ_g is defined by $\lambda_g : x \mapsto g^{-1}x$ $(x \in G)$. Let $R_G = \{\rho_g \mid g \in G\} \leq \mathrm{Sym}(G)$ denote the group of right translations of G; and $L(G) = \{\lambda_g \mid g \in G\} \leq \mathrm{Sym}(G)$ the group of left translations. Prove: $\rho : g \mapsto \rho_g$ is an isomorphism of G to R_G and $\lambda : G \mapsto \lambda_g$ is an isomorphism of G to L_G.

Exercise 3.18. $[R_G, L_G] = 1$, i.e., R_G and L_G centralize each other.

Exercise 3.19. $C_{\mathrm{Sym}(G)}(R_G) = L_G$ and $C_{\mathrm{Sym}(G)}(L_G) = R_G$.

Definition 3.20. A *permutational isomorphism* between the permutation groups $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\Phi)$ is a bijection $\alpha : \Omega \to \Phi$ such that $H = G^\alpha = \alpha^{-1}G\alpha$.

Exercise 3.21. L_G and R_G are permutationally isomorphic.

Definition 3.22. A permutation group $G \leq \mathrm{Sym}(\Omega)$ is *semiregular* if $(\forall x \in \Omega)(G_x = 1)$. We say that G is a *regular permutation group* if it is semiregular and transitive.

Exercise 3.23. If $G \leq S_n$ is regular then $|G| = n$.

Exercise 3.24. R_G and L_G are regular permutation groups.

Exercise 3.25. If G is a regular permutation group then G is permutationally isomorphic to R_G. (In particular, this will reprove that L_G and R_G are permutationally isomorphic.)

Exercise 3.26. (a) If G is semiregular then $C_{\mathrm{Sym}(\Omega)}(G)$ is transitive.

(b) If G is transitive then $C_{\mathrm{Sym}(\Omega)}(G)$ is semiregular.

(c) If G is regular then $C_{\mathrm{Sym}(\Omega)}(G)$ is regular.

Exercise 3.27. For any permutation group G, if $N \triangleleft G$ then the orbits of N form a G-invariant partition of Ω.
Corollary: If G is primitive and N is a non-trivial normal subgroup of G then N is transitive.

Exercise 3.28. Every transitive abelian group is regular.

Definition 3.29 (Equivalent permutation representations)**.** Let $\varphi : G \to \mathrm{Sym}(\Phi)$ and $\psi : G \to \mathrm{Sym}(\Psi)$ be two permutation actions (permutation representations) of the group G. We say that φ and ψ are equivalent if there exists a bijection $\alpha : \Phi \to \Psi$ such that for all $g \in G$ we have $g^{\varphi}\alpha = \alpha g^{\psi}$.

Exercise 3.30. Given $H \leq G$, there exists a unique permutation action of G such that $G_x = H$. (Uniqueness is up to equivalence of permutation representations.)

Exercise 3.31. The kernel of this action is $\mathrm{Core}(H) = \bigcap_{g \in G} H^g$.

Exercise 3.32. If M, N are normal subgroups in the group G and $M \cap N = 1$ then $[M, N] = 1$ (M and N centralize each other).