Discrete Math, Second Series, 3rd Problem Set (July 23)

REU 2003

Instructor: László Babai
Scribe: Mridul Mehta

Definition 0.1. Suppose G is a group and $H \leq G$. The sets $\{H \cdot a \colon a \in G\}$ are the **right cosets** of H in G. **Left cosets** are defined analogously.

The right cosets of H in G partition G into disjoint subsets so that $G = \dot{\bigcup}_{a \in \mathrm{Rep}} H \cdot a$ where Rep consists of right coset representatives of H in G. Two elements a and b belong to the same right coset if $H \cdot a = H \cdot b$ which happens if and only if $ab^{-1} \in H$. This defines an equivalence relation on G. The same is true of left cosets. For an arbitrary subgroup H, the left and right cosets of H in G are not the same. However, there exists a one-to-one correspondence between the left and right cosets of H in G (which holds even if $|G|$ is infinite). This can be seen using the map $(aH) \mapsto (aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$. (Here $H^{-1} = \{h^{-1} \colon h \in H\}$.)

Definition 0.2. The *index* of a subgroup $H \leq G$ in G is the number of cosets (left or right) of H in G. It is written as $|G : H|$.

The left and right cosets of a normal subgroup are the same. This is because $N \triangleleft G \Rightarrow N^a = N \Rightarrow a^{-1}Na = N \Rightarrow Na = aN$ for any $a \in G$.

Definition 0.3. Given two subsets $L, K \subseteq G$, we define the **product of these subsets** in G to be the set $KL = \{kl \colon k \in K, l \in L\}$. Similarly, we define the **inverse of the subset** K to be $K^{-1} = \{k^{-1} \colon k \in K\}$.

Exercise 0.4. Given a group G, $K \leq G$ if and only if $K \subset G$, $K \neq \emptyset$ and $K \supseteq KK^{-1}$.

Definition 0.5. The cosets of a normal subgroup $N \triangleleft G$ form a group under multiplication of subsets as defined above. This is known as the **quotient group** G/N.

Definition 0.6. A group G is said to be **simple** if $|G| > 1$ and the only normal subgroups of G are $\{1\}$ and G.

Definition 0.7. The set of all nonsingular $n \times n$ matrices over a field $\mathbb{F}$ is a group under matrix multiplication. This is known as the **General Linear Group** and is denoted by $GL(n, \mathbb{F})$.

Exercise 0.8. The center $Z(GL(n, \mathbb{F})) \cong \mathbb{F}^{\times}$. ($\mathbb{F}^{\times}$ is the multiplicative group $\mathbb{F} \backslash \{0\}$.)
Hint. Show that $Z(GL(n, \mathbb{F})) = \{\lambda I \colon \lambda \in \mathbb{F}^{\times}, I \text{ is the identity matrix}\}$.

Definition 0.9. The **projective general linear group** $PGL(n,\mathbb{F})$ is defined to be the quotient $GL(n,\mathbb{F})/Z(GL(n,\mathbb{F}))$.

Definition 0.10. The **special linear group** $SL(n,\mathbb{F})$ is defined to be $\{A \in GL(n,\mathbb{F})\colon \det(A) = 1\}$.

Exercise 0.11. $SL(n,\mathbb{F}) \lhd GL(n,\mathbb{F})$.
Hint. Show that the map $\det : GL(n,\mathbb{F}) \to \mathbb{F}^\times$ is a homomorphism. $\mathrm{Ker}(\det) = SL(n,\mathbb{F})$.

Exercise 0.12. If the homomorphism $f : G \to H$ is onto, then $H \cong G/\ker(f)$.

Therefore, $GL(n,\mathbb{F})/SL(n,\mathbb{F}) \cong \mathbb{F}^\times$.

Definition 0.13. The **projective special linear group** $PSL(n,\mathbb{F})$ is defined to be the quotient $SL(n,\mathbb{F})/Z(SL(n,\mathbb{F}))$.

Exercise 0.14. $Z(SL(n,\mathbb{F})) = SL(n,\mathbb{F}) \cap Z(GL(n,\mathbb{F}))$.

Theorem 0.15. *$PSL(n,\mathbb{F})$ is simple for all $n \geq 2$ except $n = 2$, $|\mathbb{F}| \leq 3$.*

Definition 0.16. G is said to be a p-**group** (p prime) if all the elements of G have order a power of p.

Exercise 0.17. A finite group is a p-group if and only if the order of the group is a power of p.

Example 0.18. $\left\{ \text{Matrices of the form } \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\} \leq SL(n,\mathbb{F}_p)$ is a p-group. ('*'s refer to any values from $\mathbb{F}_p$.)

Exercise 0.19. Find the order of the group shown in the last example.
Hint. It is of the form p^N.

Definition 0.20. A **permutation group of degree** n is a subgroup of S_n.

Example 0.21. $A_n \leq S_n$, $|S_n : A_n| = 2$. $D_n \leq S_n$, $|D_n| = 2n$.

D_n may be defined by taking symmetries of a circle with n equidistant points on the circle. This definition includes the cases $n = 1$ and $n = 2$. We see that $D_1 \cong \mathbb{Z}_2$, $D_2 \cong V_4$ and $D_3 \cong S_3$.

We represent permutations using cycle notation where the permutation $\sigma = (3,4,5,1)(2)$ sends $1 \mapsto 3$, $2 \mapsto 2$, $3 \mapsto 4$, $4 \mapsto 5$ and $5 \mapsto 1$. Every permutation in S_n can be written uniquely as a product of cycles.

Remark 0.22. Given two permutations σ and τ, we shall use the notation $x^{\sigma\tau}$ to mean $(x^\sigma)^\tau$.

Definition 0.23. A permutation acting on a domain Ω can be expressed as a bijective map $\pi : \Omega \to \Omega$. We define the **support** of the permutation as $\mathrm{supp}(\pi) = \{x \in \Omega \colon x^\pi \neq x\}$. We define the **degree** of the permutation as $\deg(\pi) = |\,\mathrm{supp}(\pi)|$.

So, in the above example, we have $\mathrm{supp}(\sigma) = \{1, 3, 4, 5\}$, and $\deg(\sigma) = 4$. Similarly $\mathrm{supp}(\mathit{identity}) = \emptyset$ and $\deg(\mathit{identity}) = 0$.

Definition 0.24. A 2-cycle is known as a **transposition**.

Exercise 0.25. Transpositions generate S_n.

Exercise 0.26. The product of an odd number of transpositions can never be the identity.

Exercise 0.27. $\sigma \in S_n$ is even if and only if σ is a product of an even number of transpositions. Similarly, $\sigma \in S_n$ is odd if and only if σ is a product of an odd number of transpositions.

Theorem 0.28. *A_n is simple for $n \geq 5$.*

Exercise 0.29. Find a normal subgroup isomorphic to V_4 in S_4.

The quotient of S_4 by V_4 is a group of 6 elements, it is in fact S_3.

Exercise 0.30. Find a homomorphism from S_4 to S_3 which has kernel V_4.

Definition 0.31. A **permutation representation** of G is a homomorphism $f : G \to S_n$. This representation is called **faithful** if f is one-to-one.

If $H \leq G$ with $|G : H| = n$, then H defines a permutation representation of $G \to S_n$. We shall denote by G/H the set of left cosets of H in G, by $H\backslash G$ the set of right cosets of H in G, and by $\mathrm{Sym}(\Omega)$ all the permutations of Ω. We consider the map from $G \to \mathrm{Sym}(H\backslash G)$ given by $g \mapsto \{Ha \mapsto Hag\}$.

Exercise 0.32. Prove that the above map defines a permutation of $H\backslash G$ (so that this is a permutation representation).

In the special case when the subgroup $H = \{1\}$, the above permutation representation is known as the **right regular permutation representation** of G. This gives us a homomorphism $\rho : G \to \mathrm{Sym}(G)$ where ρ_g is the permutation $\{x \mapsto xg\}$ (often referred to as 'right translation by g'). Note that the length of each of the cycles in ρ_g is just the order of the element g.

Corollary 0.33. **(Lagrange)** $\mathrm{ord}(g) \,\Big|\, |G|$.

Corollary 0.34. **(Euler-Fermat)** g.c.d. $(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1\ (n)$.

Exercise 0.35. Deduce the above corollary from Cor 0.33

Definition 0.36. Let $f : G \to \mathrm{Sym}(\Omega)$ be a permutation representation (sometimes also referred to as a G-action on Ω). For any $x \in \Omega$, we define the **orbit** of x as $x^G = \{x^g \colon g \in G\}$. (Here by x^g we mean $x^{f(g)}$.)

We have that $y \in x^G \iff (\exists\, g)(y = x^g)$. This defines an equivalence relation on Ω and then equivalence classes are exactly the orbits of the G action on Ω.

Definition 0.37. We say that the G-action is **transitive** if Ω is an orbit i.e., $(\forall\, x, y \in \Omega)(\exists\, g \in G)(y = x^g)$.

Definition 0.38. The **stabilizer** of any element $x \in \Omega$ under a G-action is $G_x = \{g \in G \colon x^g = x\}$.

Exercise 0.39. $G_x \leq G$.

Remark 0.40. There is a one-to-one correspondence between $G_x \backslash G$ and the orbit x^G.

Corollary 0.41. $|G : G_x| = |x^G|$. ($|x^G|$ is referred to as the **length** of the orbit x^G.)

Corollary 0.42. *$|x^G|$ divides $|G|$ and $|G| = |G_x|\,|x^G|$.*

Exercise 0.43. If G is a transitive permutation group of degree p^k, then G has a transitive Sylow subgroup.

Exercise 0.44. The converse to the above statement is trivial and follows immediately from the preceding corollaries: if G has a transitive Sylow subgroup, then the degree of G is a prime power.

Example 0.45. D_6 is a transitive permutation group on the set of 6 points (consider them as the vertices of a regular hexagon). If we label these points as 1 through 6 in order, we note that the partition $\{1, 3, 5\} \cup \{2, 4, 6\}$ is invariant under D_6. Similarly, so is the partition $\{1, 4\} \cup \{2, 5\} \cup \{3, 6\}$.

Definition 0.46. A G-action is **primitive** if there is no non-trivial invariant partition of Ω.

Exercise 0.47. The action of D_5 is primitive, while that of D_6 is not.

Exercise 0.48. A transitive action on a prime number of points is primitive.

A permutation action a domain induces a natural action on unordered pairs of the Domain. This can be seen using the map $S_n \to S_{\binom{n}{2}}$ defined in the natural way so that the permutation $\sigma = (1, 2, 3)(4, 5) \mapsto \sigma^{(2)} = (\{1, 2\}, \{2, 3\}, \{3, 1\})(\{1, 4\}, \{2, 5\}, \{3, 4\}, \{1, 5\}, \{2, 4\}, \{3, 5\})(\{4, 5\})$.

Exercise 0.49. S_n acts primitively on the $\binom{n}{2}$ pairs.

Exercise 0.50. $S_n \to S_{\binom{n}{k}}$ is also primitive except when $k = \frac{n}{2}$ (n even).

Exercise 0.51. A set of transpositions generates S_n if and only if they form a connected graph.

Corollary 0.52. *At least* $(n-1)$ *transpositions are needed to generate* S_n.

Exercise 0.53. Let $\sigma = (1, 2, \dots, n)$ and $\tau = (1, 2)$. Prove that σ and τ generate S_n.

Exercise 0.54. $\operatorname{diam} \Gamma(S_n, \{\sigma, \tau\}) = \Theta(n^2)$. ($a_n = \Theta(n^2) \Rightarrow c_1 n^2 < a_n < c_2 n^2$ for some $0 < c_1 < c_2$.)

Exercise 0.55. $\operatorname{diam} \Gamma(S_n, A) = \Theta(n^2)$ where the generating set A consists of adjacent transpositions.