REU 2007 · Discrete Math · Lecture 2

Instructor: László Babai
Scribe: Shawn Drenning

June 19, 2007. Proofread by instructor.
Last updated June 20, 1 a.m.

Exercise 2.0.1. Let G be an abelian group and $A \subseteq G$ be a subset with $|A| = n$. Show there exists a product-free set $S \subseteq A$ with $|S| \geq \frac{n-1}{3}$.

Exercise 2.0.2. Show that $(1/\mathrm{e}) \sum_{k=0}^{\infty} \frac{k^n}{k!}$ is an integer.

2.1 Relations on Sets

Definition 2.1.1. A relation on a set Ω is a subset $R \subseteq \Omega \times \Omega$. If $(a, b) \in R$, we say aRb.

Example 2.1.2. Let $\Omega = \mathbb{N}$ and R be the relation satisfying $(a, b) \in R$ if and only if a divides b (denoted $a \mid b$). For instance, $(7, 21) \in R$.

Example 2.1.3. Let $\Omega = \mathbb{R}$ and R be the relation satisfying $(a, b) \in R$ if and only if $a < b$. For instance, $(5, 7) \in R$.

The following are several properties we might ask whether or not a relation satisfies:

Definition 2.1.4.

1. A relation is reflexive if $(\forall a)(aRa)$
2. A relation is symmetric if $(\forall a, b)(aRb \Rightarrow bRa)$
3. A relation is transitive if $(\forall a, b, c)(aRb \wedge bRc \Rightarrow aRc)$

A relation satisfying all of the above properties is called an *equivalence relation.*

Question 2.1.5. Which of these three properties do the relations in the above examples satisfy?

Exercise 2.1.6. If $a, b, n \in \mathbb{Z}$, we say $a \equiv b \pmod{n}$ if $n \mid (a - b)$. Prove that for fixed n, the relation $a \equiv b \pmod{n}$ is an equivalence relation on $\mathbb{Z}$. - The equivalence classes are called "modulo n **residue classes**."

Exercise 2.1.7. Let $f : \Omega \to T$ be any function. We define a relation $\sim$ on Ω by $x \sim y$ if $f(x) = f(y)$. Show that this is an equivalence relation. We call this equivalence relation the *equivalence kernel* of f.

Exercise 2.1.8. Prove that every equivalence relation is the *equivalence kernel* of some function.

Exercise 2.1.9. The number of relations on a set of size n is 2^{n^2}.

Exercise 2.1.10. Let B_n be the number of equivalence relations on a set of size n (the n-th "Bell number"). It follows from the previous exercise that $B_n < 2^{n^2}$. In fact it is much smaller. Prove: (a) $B_n < n^n$. (b) Prove that for every k $(1 \leq k \leq n-1)$, $B_n > k^{n-k}$. (c) Prove: $\ln B_n \sim n \ln n$ (asymptotically equal).

Exercise 2.1.11. Prove the recurrence $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

Exercise 2.1.12. $\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = e^{e^x - 1}$.

Exercise 2.1.13. (a) Prove that $B_n = \frac{1}{\mathrm{e}} \sum_{k=0}^{\infty} \frac{k^n}{k!}$. This is known as *Dobinski's formula*. (b) Find the largest term in this sum.

2.2 More Group Theory

Definition 2.2.1. If H is a non-empty subset of G which is a group under the same operation as G, we say H is a subgroup of G and write $H \leq G$.

Exercise 2.2.2. A nonempty subset H of G is a subgroup if and only if for all $a, b \in H$ we have $ab^{-1} \in H$.

Observe: the "subgroup" relatioon is transitive: if $K \leq H$ and $H \leq G$, then $K \leq G$.

Definition 2.2.3. If $A, B \subseteq G$, then $A \cdot B = \{ab \mid a \in A, b \in B\}$.

Exercise 2.2.4. (a) $|AB| \leq |A||B|$; (b) $\emptyset \cdot B = \emptyset$; (c) if $A \neq \emptyset$ then $AG = G$.

Exercise 2.2.5. $H \subseteq G$ is a subgroup if and only if $H \neq \emptyset$ and $HH^{-1} \subseteq H$.

Exercise 2.2.6. The intersection of a family of subgroups of a group is a subgroup.

Definition 2.2.7. Let $S \subseteq G$ and let H be the intersection of all subgroups of G containing S. We say that H is the subgroup of G **generated by** S and write $\langle S \rangle = H$.

Exercise 2.2.8. Let S be a non-empty subset of G. We define

$$S^{-1} = \{s^{-1} \mid s \in S\}$$

and

$$(S \cup S^{-1})^n = \{a_1 a_2 \dots a_n \mid a_i \in S \cup S^{-1}\}.$$

Prove that

$$\langle S \rangle = \bigcup_{n=0}^{\infty} (S \cup S^{-1})^n.$$

Exercise* 2.2.9. (Cauchy-Davenport, Hamidoune) If $A, B \subseteq G$, $A, B \neq \emptyset$, and $\langle A \rangle = G$, then $|AB| \geq \min\{|A| + |B| - 1, G\}$. (Hint: connectivity theory of graphs)

The set of all bijections of a set Ω is a group under composition. We call this group the *symmetric group on* Ω and denote it $\mathrm{Sym}(\Omega)$. We call Ω the *permutation domain* and the elements of $\mathrm{Sym}(\Omega)$ *permutations* of Ω. If $|\Omega| = n$ we often denote $\mathrm{Sym}(\Omega)$ by S_n. We often will write elements of S_n using cycle notation. The symbol $(a_1, \ldots, a_k)$ denotes the "k-cycle" which moves a_i to a_{i+1} $(i = 1, \ldots, k-1)$ and a_k to a_1 (here the a_i are distinct elements of Ω); all other elements of Ω are fixed.

Composition of permutations is performed left to right. For example, $(123) = (13)(23)$ (verify!)

Exercise 2.2.10. Prove: a k-cycle is an even permutation if and only if k is odd.

Exercise 2.2.11. Every permutation can be written as a product of disjoint cycles. This is referred to as the *cycle decomposition* of the permutation. This decomposition is unique apart from the order of the cycles and the possible omission of cycles of length 1.

Definition 2.2.12. Let the cycle-decomposition of a permutation σ consist of a cycle of length n_1, a cycle of length n_2, ..., and a cycle of length n_m, where $n_1 \geq n_2 \geq \cdots \geq n_m$. In this representation, we include all fixed points as cycles of length one. We say that σ has *cycle-type* $(n_1, n_2, \ldots, n_m)$.

Exercise 2.2.13. The order of S_n is $n!$.

Definition 2.2.14. A transposition is a 2-cycle.

Exercise 2.2.15. S_n is generated by the $n-1$ transpositions of the form $(i, i+1)$.

Exercise 2.2.16. (a) Let T be a set of transpositions. View T as the set of edges of a graph. Give a graph theoretic characterization of those T which generate S_n. (b) S_n cannot be generated by fewer than $n-1$ transpositions.

Exercise* 2.2.17. The number of $(n-1)$-tuples of transpositions that generate S_n is n^{n-2}. (Hint: Cayley's Formula in Graph Theory.)

Definition 2.2.18. $\sigma \in S_n$ is **even** if it is a product of an even number of transpositions and **odd** if it is a product of an odd number of transpositions.

Exercise 2.2.19. If σ is even, then σ is not odd. (What you need to prove is that the identity permutation is not odd.)

Theorem 2.2.20 (Lagrange's Theorem). *If $H \leq G$, then $|H| \Big| G|$.*

Proof. Define a relation by $a \sim b$ if ab^{-1}.

Exercise 2.2.21. Verify that this is an equivalence relation.

We call the sets of the form aH (this is shorthand for $\{a\}H$) and Ha the left and right **cosets** of H, respectively. We have $ab^{-1} \in H$ if and only if $a \in Hb$. It follows that (a) the equivalence classes of the equivalence relation defined above are exactly the right cosets of H; and (b) all cosets are of the same size. We call the number of right cosets of H in G the **index** of H and G. This is denoted by $|G : H|$. Since all the cosets have the same number of elements, we must have $|G| = |H||G : H|$. □

Exercise 2.2.22. Prove: if $H \leq G$ then the number of right cosets and the number of left cosets is equal. (Your proof should work for infinite as well as for finite groups.)

Exercise 2.2.23. The only subgroups of $\mathbb{Z}$ are of the form $d\mathbb{Z}$ for $d \in \mathbb{N}$. What is $|\mathbb{Z} : d\mathbb{Z}|$? Show that two cosets of $a + d\mathbb{Z}$ and $b + d\mathbb{Z}$ are equal if and only if $a \equiv b \mod d$. Cosets of $d\mathbb{Z}$ in $\mathbb{Z}$ are called modulo d residue classes.

Definition 2.2.24. The set of all even permutations of S_n is a subgroup of S_n called the **alternating group of degree** n and denoted A_n.

Exercise 2.2.25. The 3-cycles generate A_n.

Exercise 2.2.26. If $n \geq 2$ then $|S_n : A_n| = 2$.

Exercise 2.2.27. For $n \geq 2$, A_n is the only subgroup of index 2 in S_n.

Now we would like to study the number of possible configurations of Rubik's cube obtainable by pulling the cube apart and then reassembling it, without changing the colors on the faces of the "cubies." We think of the 6 face centers as fixed to the center. There are 8! ways to arrange the "corner cubies" and 12! ways to arrange the "edge cubies." Once the location of a corner cubie is fixed, there are 3 ways to place it; once the location of an edge cubie is fixed, there are 2 ways to place it. In all, this gives $8!12!3^8 2^{12}$ configurations. These configurations form a group which we call the "total group" T of Rubik's cube and call the subgroup of configurations obtained through legal moves G.

Exercise 2.2.28. $|T : G| = 12$.

Exercise 2.2.29. We will now describe what is known as **Sam Lloyd's 15 puzzle**. Suppose the numbers $1, 2, \ldots, 15$ and "blank" are arranged in a 4×4 grid. A legal move is to swap the empty cell ("blank") with an adjacent cell. Prove that it is not possible through legal moves to go from

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

to

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(so the first configuration is not "feasible" – the goal being to reach the second configuration). In fact, exactly half of the 16! configurations are feasible.

Exercise 2.2.30. $S_n = \langle (12\ldots n), (12) \rangle$

Definition 2.2.31. Let G be a group and S a subset of G. We define the **Cayley Graph** of G with respect to S to be the graph whose vertices are the elements of G and with an edge between g_1 and g_2 if $g_1 = g_2 s$ for some $s \in S \cup S^{-1}$.

Definition 2.2.32. The **diameter** of group G with respect to a set S of generators is defined to be the diameter of the Cayley graph of G with respect to S and is denoted $\mathrm{diam}(G, S)$.

Exercise 2.2.33. Let $\sigma = (12\ldots n)$ and $\tau = (12)$. Then $\mathrm{diam}(S_n, \{\sigma, \tau\}) = \Theta(n^2)$.

Definition 2.2.34. We say $a, b \in G$ are **conjugates** if $(\exists g \in G)(a = g^{-1}bg)$. **Conjugation** by g is the map $G \to G$ given by $a \mapsto g^{-1}ag$.

Definition 2.2.35. If G and H are groups, a map $\varphi : G \to H$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. A homomorphism that is also a bijection is called an **isomorphism**. An isomorphism from a group to itself is called an **automorphism**. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$ and is a group under composition.

Exercise 2.2.36. Conjugation by g is a group automorphism. Such automorphisms are called *inner automorphisms*. The group of all inner automorphisms of G is denoted $\mathrm{Inn}(G)$.

Observe that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$.

Exercise 2.2.37. Conjugacy is an equivalence relation on G. We call the classes **conjugacy classes**.

Exercise 2.2.38. In S_n, two permutations are conjugate if and only if they have the same cycle structure.

Definition 2.2.39. A map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ is an *isometry* if it preserves distance. More generally, if $A, B \subset \mathbb{R}^n$, $\varphi : A \to B$ is an isometry if it is a distance preserving bijection. The set of all isometries of $\mathbb{R}^2$ is a group under composition. If there is an isometry between two subsets of $\mathbb{R}^n$, we say they are *congruent*.

Exercise 2.2.40. Every isometry of the plane is either

1. a translation, or
2. a rotation, or
3. a reflection (in an axis), or
4. a "glide reflection," that is, a reflection followed by a translation parallel to the axis of reflection.

The conjugates of an isometry are of the same type. In fact, a conjugate of a rotation by angle α is a rotation by $\pm\alpha$ (when is it $-\alpha$?), a conjugate of a translation is a the translation by a vector of the same length, and the same holds for the translation involved in a glide reflection.

Definition 2.2.41. A **partition of a number** n is a sequence of natural numbers $a_1, \dots a_k$ satisfying $a_1 \geq a_2 \geq \ldots \geq a_k \geq 1$ such that $n = a_1 + \ldots + a_k$. The number of partitions of n is denoted $p(n)$.

Note that $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$.

Exercise 2.2.42. The number of conjugacy classes of S_n is $p(n)$.

A most amazing asymptotic formula for $p(n)$ was found Hardy and Ramanujan.

Theorem 2.2.43 (Hardy-Ramanujan). $p(n) \sim \frac{c_1}{n} \mathrm{e}^{c_2\sqrt{n}}$ *where* $c_1 = \frac{1}{4\sqrt{3}}$ *and* $c_2 = \frac{2\pi}{\sqrt{6}}$.

For an elementary proof of the weaker but still surprisingly tight inequality $\ln p(n) < \frac{2\pi}{\sqrt{6}}\sqrt{n}$, see Matoušek and Nešetřil's "Invitation to Discrete Mathematics," Chapter 10.7.

Exercise 2.2.44. Prove from first principles: $\log p(n) = \Theta(\sqrt{n})$.

Definition 2.2.45. $N \leq G$ is a **normal subgroup**, denoted $N \trianglelefteq G$, if N is invariant under conjugation, i. e., $(\forall g \in G)(g^{-1}Ng \subseteq N)$.

Exercise 2.2.46. $N \leq G$ is a normal subgroup if and only if $(\forall g \in G)(g^{-1}Ng = N)$.

Exercise 2.2.47. Let $\varphi : G \to H$ be a homomorphism and $N = \varphi^{-1}(1_H)$. Prove that N is a normal subgroup and the partition by φ is cosets of N.

Definition 2.2.48. If $\varphi : G \to H$ is a homomorphism, we define

$$\mathrm{Im}(\varphi) = \{\varphi(a) \,:\, a \in G\}$$

and

$$\ker(\varphi) = \{g \in G \,:\, \varphi(g) = 1\}.$$

Exercise 2.2.49. $\mathrm{Im}(\varphi) \leq G$ and $\ker(\varphi) \trianglelefteq G$.

Theorem 2.2.50. *For normal subgroups $N \trianglelefteq G$, the cosets Na form a group under the operation of set multiplication defined in 2.2.3.*

Proof. Using the fact that $aN = Na$, we see that $(Na)(Nb) = N(aN)b = Nab$. □

The group of cosets of N is denoted G/N and called a *quotient group*.

Example 2.2.51. $d\mathbb{Z} \leq \mathbb{Z}$ and $\mathbb{Z}/d\mathbb{Z} = \mathbb{Z}_d$.

Exercise 2.2.52. If $\varphi : G \to H$ is a homomorphism then $\mathrm{Im}(\varphi) \cong G/\ker\varphi$.

The sign of a permutation

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

is a homomorphism from S_n onto the multiplicative group $\{-1, 1\}$:

Exercise 2.2.53. For any $\sigma, \tau \in S_n$ we have $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$.

The kernel of sgn is A_n, so $S_n/A_n \cong \mathbb{Z}_2$.

2.3 Symmetries of Platonic solids

We would like to figure out the group of isometries of the Platonic solids. First we consider the tetrahedron T. We denote the group of isometries of T by $O(T)$. Any isometry of T is determined by what it does to the four vertices of T. This gives an injection φ of $O(T)$ into S_4. By looking at reflections across a plane intersecting two of the vertices and bisecting the edge connecting the other two vertices, we see that all transpositions are in the image of φ. We conclude that $\mathrm{Im}(\varphi) = S_4$; therefore $O(T) \cong S_4$.

Exercise 2.3.1. Give a simple explicit description of a spatial congruence that maps under φ to (1234).

We say an isometry of the space is **orientation preserving** if it turns a right hand into a right hand; and it is **orientation reversing** if it turns a right hand into a left hand.

Definition 2.3.2. The group of those congruences of $\mathbb{R}^3$ which fix the origin is called the 3-dimensional **orthogonal group** and is denoted $O(\mathbb{R}^3)$ or $O_3(\mathbb{R})$. Its index-2 subgroup consisting of the orientation preserving congruences that fix the origin is $SO(\mathbb{R}^3)$ or $SO_3(\mathbb{R})$, the **special orthogonal group.**

We have, as usual, a homomorphism $\varphi : O(\mathbb{R}^3) \to \{1, -1\}$ given by $\varphi(x) = 1$ if and only if x is orientation preserving; $\ker(\varphi) = SO(\mathbb{R}^3)$. So, $SO(\mathbb{R}^3) \trianglelefteq O(\mathbb{R}^3)$.

Since the only subgroup of index 2 in S_4 is A_4, we must have that $SO(T) = A_4$.

Now let us find the $O(\text{cube})$. Any vertex v of a cube can be mapped to one of 8 vertices. Once we decide where v is mapped, there are 3 possibilities for where a vertex adjacent to v can be mapped. Once we fix this, we can do one additional reflection. We conclude that $|O(\text{Cube})| = 48$. A cube has four main diagonals. Any member of $O(\text{Cube})$ permutes these diagonals. This gives us a homomorphism φ from $O(\text{Cube})$ into S_4. If we restrict to $SO(\text{Cube})$, φ is injective. As with the tetrahedron, we can verify that all transpositions are in the image of φ. It follows that φ is onto and $SO(\text{Cube}) \cong S_4$. From this we see that $O(\text{Cube}) \cong S_4 \times \mathbb{Z}_2$.

The octahedron can be embedded in the cube so that its six vertices correspond to the centers of the six faces of the cube. It follows that the isometry group of the octahedron is isomorphic to the isometry group of the cube.

Finally, we consider isometries of the dodecahedron. A similar argument to the one we used to count the isometries of the cube shows us that the dodecahedron has 120 isometries.

Definition 2.3.3. The center of G is

$$Z(G) = \{g \in G : g \text{ commutes with all elements of } G\}$$

Exercise 2.3.4. (a) $Z(G) \trianglelefteq G$; (b) $G/Z(G) \cong \mathrm{Inn}(G)$.

Exercise 2.3.5. If $n \geq 3$, $Z(S_n) = \{1\}$.

Since the isometry group of the dodecahedron has non-trivial center, it cannot be S_5.

Exercise 2.3.6. Show that

$$O(\text{dodecahedron}) = SO(\text{dodecahedron}) \times \mathbb{Z}_2$$

and

$$SO(\text{dodecahedron}) \cong A_5.$$

Definition 2.3.7. An **automorphism** of a graph G is a permutation of the set of vertices V that preserves adjacency. The set $\mathrm{Aut}(G)$ of all automorphisms of G is a group under composition. Note that $\mathrm{Aut}(G) \leq \mathrm{Sym}(V)$.

Exercise 2.3.8. The group of automorphisms of the Petersen graph is isomorphic to S_5.

Definition 2.3.9. If V is a vector space over a field $\mathbb{F}$, we define $\mathrm{GL}(V)$ to be the group of automorphisms of V. We define $\mathrm{GL}_n(\mathbb{F})$ to be the set of $n \times n$ invertible matrices with coefficients in $\mathbb{F}$.

Definition 2.3.10. A **representation** of G is a group homomorphism $G \to \mathrm{GL}(V)$. If V is of finite dimension n, this is equivalent to giving a homomorphism into $\mathrm{GL}_n(\mathbb{F})$.

Recall we found two representations of S_4 in $O(\mathbb{R}^3)$, namely the $SO(\text{Cube})$ and $O(\text{tetrahedron})$.

Definition 2.3.11. $G \to \mathrm{GL}(V)$ is *irreducible* if no subspace of V is mapped into itself by each element of G.

Exercise 2.3.12. Find an irreducible representation $S_4 \to O(\mathbb{R}^2)$.

We have the following irreducible representations of S_4:

1. $S_4 \to \{1\}$
2. $\mathrm{sgn} : S_4 \to \{\pm 1\}$
3. $S_4 \to O(\mathbb{R}^2)$ (Ex. 2.3
4. $S_4 \to O(\text{tetrahedron})$
5. $S_4 \to O(\text{Cube})$

Theorem 2.3.13. (Frobenius) *If G is a finite group, the number of irreducible representations over $\mathbb{C}$ of G is equal to the number of conjugacy classes of G.*

Exercise 2.3.14. (Cayley) If $|G| = n$, then $G \leq S_n$.

Exercise 2.3.15. (Frucht) $(\forall G)(\exists \text{ graph } X)(\mathrm{Aut}(X) \cong G)$.

Definition 2.3.16. G is *cyclic* if $G = \langle g \rangle$.

Exercise 2.3.17. If G is cyclic and $|G| = n$, then G is isomorphic to $\mathbb{Z}_n$. If G is cyclic and infinite, then $G \cong \mathbb{Z}$.

Definition 2.3.18. The group of symmetries of a regular n-gon is called a **dihedral group** and denoted D_n.

Observe that $|D_n| = 2n$ and $SO(\text{regular } n\text{-gon}) \cong \mathbb{Z}_n$.

Exercise 2.3.19. The center of D_n is $\{1\}$ if n is odd and $\{1, -1\}$ if n is even.

Exercise 2.3.20. $Z(\mathrm{GL}_n(\mathbb{F})) = \{\lambda I : \lambda \in \mathbb{F}^\times\}$ ("scalar matrices").

Exercise 2.3.21. If A is an $n \times n$ matrix over the integers then A^{-1} is an integer matrix if and only if the determinant of A is ± 1.

Definition 2.3.22. $\mathrm{GL}_n(\mathbb{Z})$ is the group of all $n \times n$ matrices with determinant ± 1.

Exercise 2.3.23. If $\mathbb{F}$ is a field, the determinant map is a homomorphism $\mathrm{GL}_n(\mathbb{F}) \to F^\times$. The kernel of the determinant map is $\mathrm{SL}_n(\mathbb{F})$.