GROUPS AROUND US

Pavel Etingof

Introduction

These are notes of a mini-course of group theory for high school students that I gave in the Summer of 2009. This mini-course covers the most basic parts of group theory with many examples and applications, such as the "Fifteen" puzzle, the game "SET", the Rubik cube, wallpaper patterns in the plane. The notes contain many exercises, which are necessary for understanding the main text. More detailed treatment of group theory in a similar style can be found in M. Artin's wonderful book "Algebra".

Acknowledgments. I am very grateful to my students Valentina Barboy, Esther Bogorov, Konstantin Churin, Ivan Kirillov, Elias Kleinbock, and Michael Perlin for curiosity and motivation, which made it exciting for me to teach this course.

Lecture 1

1. Groups of transformations

1.1. **The definition of a group of transformations.** The notion of a group is one of the most important and ubiquitous notions in the entire field of mathematics. One of its primary functions is to describe symmetry. For this reason, one of the most common ways in which groups arise in nature is as groups of transformations, or symmetries, of various mathematical objects.

Definition 1.1. Let X be a set, and let G be a subset of the set of all invertible transformations (i.e., bijections) $f : X \to X$. One says that G is a **group** if

1) G is closed under composition, i.e., $f \circ g \in G$ if $f, g \in G$;
2) $\mathrm{Id} \in G$; and
3) If $g \in G$ then $g^{-1} \in G$.

Definition 1.2. If G is a finite group, then the **order** $|G|$ of G be the the number of elements in G.

1.2. **The symmetric and alternating groups.** The most obvious example of a group of transformations is the group $\mathrm{Perm}(X)$ of all transformations (or permutations) of X. This group is especially interesting if X is a finite set: $X = \{1, ..., n\}$. In this case the group $\mathrm{Perm}(X)$ is called **the symmetric group**, and is denoted by S_n. The order of this group is $n!$.

The simplest example of a permutation which is not the identity is a **transposition** (ij), $1 \le i < j \le n$. This permutation switches i and j and keeps all other elements fixed. In particular, if $j = i + 1$, then (ij) is called a **transposition of neighbors**. It is clear that any permutation is a composition of transpositions of neighbors.

For every permutation $s \in S_n$, we have a notion of the sign of s. Namely, let $\mathrm{inv}(s)$ is the number of inversions of s, i.e. the number of pairs $i < j$ such that $s(i) > s(j)$. Then s is said to be even (respectively, odd) if $\mathrm{inv}(s)$ is even (respectively, odd), and one defines $\mathrm{sign}(s)$ to be $(-1)^{\mathrm{inv}(s)}$.

Proposition 1.3. For any representation of s as a composition of N transpositions of neighbors, $\mathrm{sign}(s) = (-1)^N$.

Proof. Right multiplication of a permutation by a transposition of neighbors either creates a new inversion or kills an existing one. So N equals the number of inversions modulo 2. $\square$

Corollary 1.4. One has $\mathrm{sign}(s \circ t) = \mathrm{sign}(s)\mathrm{sign}(t)$. In particular, even permutations form a group, which for $n \geq 2$ has order $n!/2$.

The group of even permutations is called **the alternating group** and denoted by A_n.

Exercise 1.5. (i) Let $a_1, ..., a_m \in \{1, ..., n\}$ be distinct elements. Denote by $(a_1...a_m)$ the cyclic permutation of $a_1, ..., a_m$, i.e. $a_1 \mapsto a_2 \mapsto ... \mapsto a_m \mapsto a_1$. Show that any permutation can be uniquely represented as a composition of cycles on disjoint collections of elements (up to order of composition). This representation is called the **cycle decomposition**, and is a convenient way of recording permutations.

(ii) Show that any cycle of even length (in particular, any transposition) is an odd permutation, while any cycle of odd length is an even permutation. Thus, the sign of any permutation s is $(-1)^r$, where r is the number of even length cycles in the cycle decomposition of s.

Exercise 1.6. The "Fifteen puzzle" is a collection of 15 movable square tiles numbered by 1 through 15, which are put in a box of size 4 by 4, so that there is one vacant spot. The solved position is when all the squares are positioned in the increasing order, and the vacant spot is in the lower right corner.

Suppose the puzzle is in some initial position, in which the vacant spot is in the lower right corner. Show that if the puzzle can be solved (by sliding tiles without removing them) then the initial position is an even permutation in S_{15} (in fact, the converse is also true). In particular, the solved position in which 14 and 15 are interchanged is unsolvable.

Hint. Define the parity of a position of the puzzle to be the parity of the permutation s of tiles (0 or 1) plus the parity of the number of the row containing the vacant spot, modulo 2. A slide of a tile to the right or left does not change either of the summands, so does not change the sum. On the other hand, a slide up or down composes the permutation s with a cycle of length 4 (so changes its parity), and at the same time changes the parity of the row number, so the sum remains unchanged. This implies the statement.

What happens for an m-by-n puzzle with one missing tile? Explain why for $m, n \geq 2$, every even permutation with the right lower corner missing is solvable. (Hint: do the 2 by 3 case by hand, then use induction).

Remark. In the late 1880s Sam Loyd offered a $ 1,000 prize for solving the puzzle with the usual order of numbers and 14 and 15 reversed. This had been proved to be impossible in 1879, but many people spent many hours, days and weeks in a fruitless search for a solution!

1.3. **Groups of rotations, motions, symmetries.** Often one considers groups G of all transformations of X that preserve some structure on X (in many cases, of geometric origin). In this case, it is usually obvious that G satisfies conditions 1-3.

Here are some examples of groups of transformations.

1. The group of automorphisms of a graph Γ, i.e. the group of invertible transformations $g : V \to V$ of the set V of vertices of Γ and $g : E \to E$ of the set E of edges of Γ, such that an edge e goes from a vertex x to a vertex y if and only if $g(e)$ goes from $g(x)$ to $g(y)$. (The graph Γ may have multiple edges and self-loops, and may or may not be oriented).

E.g, the group $\mathbb{Z}_n$ of automorphisms of an oriented cycle of length n has n elements (which are residues modulo n, with composition being addition modulo n), while the group of automorphisms of an unoriented cycle of length n, D_{2n}, has $2n$ elements.

2. The group of translations of a space $\mathbb{R}^n$, for example the plane $\mathbb{R}^2$ or 3-space $\mathbb{R}^3$ (i.e., the group of transformations that preserve distances and directions). This group can be identified with $\mathbb{R}^n$ itself, by looking at where the origin goes. The composition is then the usual addition of vectors. We can also consider translations of $\mathbb{R}$ by integers or rational numbers, giving the groups $\mathbb{Z}$ and $\mathbb{Q}$. Another example is the group of dilations (homotheties) of $\mathbb{R}^n$; it can be identified with the set $\mathbb{R}^\times_+$ of positive real numbers, with composition being multiplication. If we also allow central symmetry, we will get the group of all nonzero real numbers $\mathbb{R}^\times$. One can also consider dilations by a rational factor, giving the group $\mathbb{Q}^\times$ of nonzero rational numbers, with composition being multiplication.

3. The group of transformations of the plane or 3-space preserving the origin, distances, and orientation. These groups are denoted by $SO(2)$ and $SO(3)$, respectively, and called the **special orthogonal groups**. It is obvious that $SO(2)$ consists of rotations of the plane around the origin, by some angle θ, $-180^0 \leq \theta < 180^0$ (where a positive angle corresponds to a counterclockwise rotation).

Exercise 1.7. Show that the composition of the reflections with respect to two lines L_1, L_2 through the origin making an angle α with each other is a rotation by the angle 2α around the origin. Deduce that any rotation of the plane around the origin is a composition of two reflections $s \circ t$ with respect to lines through the origin, and the reflection s (or t) can be chosen arbitrarily.

In three dimensions, it is also true that any element of $SO(3)$ is a rotation around an axis, but this is less obvious.

Proposition 1.8. Any element $g \in SO(3), g \neq \mathrm{Id}$ is a counterclockwise rotation around a unique (directed) axis L by a uniquely determined angle $0 < \theta < 180^0$.

Proof. It is clear that any nontrivial rotation uniquely derternines L and θ. So we just need to show that g is indeed a rotation around an axis. We first show that g is a composition of two such rotations. Let i, j, k be the standard basis of the 3-space, and i', j', k' be their images under g. By a rotation, we can align i with i', and by a second rotation j with j' and k with k' (using that i', j', k' is right handed, as g preserves orientation).

Now we show that a composition of two rotations is itself a rotation. Let g, h be rotations around axes L_g, L_h. Clearly, we may assume that $L_g \neq L_h$. Let $P_{g,h}$ be the plane through L_g and L_h, and let t be the reflection with respect to this plane. Then, as follows from Exercise 1.7, there exist reflections r and s such that $g = r \circ t$ and $h = t \circ s$. So $g \circ h = r \circ s$, and thus $g \circ h$ is a rotation around the intersection line of the planes of the reflections r and s by twice the angle between these planes. □

4. The group of origin-preserving symmetries of the plane or 3-space, i.e. transformations which preserve distances and the origin. Any symmetry is either a rotation or the composition of a rotation with a reflection with respect to any fixed line (respectively, plane) through the origin. These groups are denoted by $O(2)$ and $O(3)$, and called the **orthogonal groups**. Note that the central symmetry is a rotation in 2 dimensions, but is not in 3 dimensions.

5. The group of motions of the plane or the 3-dimensional space (Galileo transformations), i.e. transformations that preserve distances and orientation. It is easy to see that any motion is a composition of a rotation and a translation. This is the group of symmetries of the laws of classical (Newtonian) mechanics.

6. The group of distance preserving transformations (isometries) of the plane or 3-space.

7. The group of linear transformations of the n-dimensional space $\mathbb{R}^n$, i.e. transformations which preserve addition of vectors and multiplication of them by scalars. This group is denoted by $GL(n, \mathbb{R})$ and called **the general linear group**).

8. The group of rotations of a polytope, i.e. rotations of the space that map the polytope to itself.

Exercise 1.9. What are the orders of these groups for regular polygons and Platonic solids?

Solution. For the regular polygon with n vertices in the plane, we get a group of order n (in fact, $\mathbb{Z}_n$). If the polygon is in 3-space, it can also be flipped, so we get a group of order $2n$ (in fact, D_{2n}).

For the tetrahedron, we have 3 rotations by 180^0 around axes through midpoints of edges, 8 rotations around axes through vertices (4 by 120^0 and 4 by 240^0, in the counterclockwise direction), and the identity transformation, so altogether 3+8+1=12.

For the cube: 8 vertices, 12 edges, 6 faces. So, rotations around axes through edges: 6; rotations around axes through vertices: $4 \times 2 = 8$; rotations around axes through faces: $3 \times 3 = 9$; and the identity transformation. Altogether 6+8+9+1=24. The same result holds for the octahedron (which is dual to the cube).

For the icosahedron: 12 vertices, 30 edges, and 20 faces. So, rotations around axes through edges: 15; rotations around axes through vertices: $6 \times 4 = 24$; rotations around axes through faces: $10 \times 2 = 20$; and the identity transformation. Altogether 15+24+20+1=60. The same result is valid for the dodecahedron (which is dual to the icosahedron).

9. The group of symmetries of a wallpaper pattern. We will see that there are 17 such groups (we exclude "boring" patterns which are preserved by arbitrary shifts in some direction).

10. The group of symmetries of a (crystal) lattice in 3 dimensions. Such groups are called **crystallographic groups**. There are 230 such groups (Fedorov groups).

2. Abstract groups

2.1. **The definition of an abstract group.** It often happens that groups G_1, G_2 originally defined as groups of transformations of two different sets X_1, X_2 nevertheless turn out to be the same. For instance, we claim that the groups of rotations of the tetrahedron, cube, and icosahedron may be identified with A_4, S_4, and A_5, respectively. To see this, we observe that the group of the tetrahedron acts on the set of 4 vertices by even permutations, the group of the cube acts on the set of 4 main diagonals by all permutations, and the group of the icosahedron acts on the 5 inscribed tetrahedra by even permutations.

This shows that the set X on which a group G acts by transformations is not a natural attribute of G, and thus it would be good to be able to work with the group G without referring to X at all. This leads us to the notion of an abstract group.

To come up with the definition of an abstract group, observe that a group G of transformations of a set X is equipped with the composition law $G \times G \to G$, $(a, b) \mapsto ab$, the identity element $e = \mathrm{Id}$, and the inversion operation $a \mapsto a^{-1}$, which satisfy the following axioms:

Axiom 1. **Associativity**: $(ab)c = a(bc)$, $a, b, c \in G$.

Axiom 2. **The unit axiom**: $ea = ae = a$ for any $a \in G$.

Axiom 3. **The inverse axiom**. $aa^{-1} = a^{-1}a = e$ for any $a \in G$.

This motivates the following definition of an abstract group.

Definition 2.1. A **group** is a set with a multiplication operation $G \times G \to G$, $(a, b) \mapsto ab$, the identity element e, and the inversion operation $a \mapsto a^{-1}$, satisfying axioms 1-3.

Note that the commutativity, $ab = ba$, is not required. If it is satisfied for any $a, b \in G$, one says that G is a **commutative**, or **abelian** group. In such groups, the operation is often denoted by $+$ and called addition (rather than multiplication).

Example 2.2. 1. The trivial group $\{e\}$ is the group consisting of one element.

2. Any group of transformations is an abstract group.

Exercise 2.3. (i) Show that the unit and inverse in a group are unique. Thus, the group structure is completely determined by the multiplication operation.

(ii) Show that if in a group $ac = bc$ or $ca = cb$ then $a = b$ (cancelation property).

Lecture 2

Definition 2.4. A **subgroup** of a group G is a subset $H \subset G$ containing e, which is closed under the multiplication and the inversion, i.e., for $a, b \in H$, one has $ab, a^{-1} \in H$.

Definition 2.5. The **order** of an element $a \in G$ is the smallest positive integer n such that $a^n = e$ (if n does not exist, we agree that the order of a is infinite).

Obviously, if $a \in G$ is an element of order n then it generates a subgroup $\mathbb{Z}_n$ in G, and if a has infinite order, then it generates a subgroup $\mathbb{Z}$ in G. These groups are called **cyclic** groups.

Exercise 2.6. (i) Show that if G is a finite group then every element of G has finite order.

(ii) Express the order of a permutation $s \in S_n$ in terms of its cycle decomposition. (Answer: it is the least common multiple of the cycle lengths).

(iii) What is the smallest n such that S_n contains an element of order 2009? (Answer: $n = 90$).

Definition 2.7. Let G, K be two groups. A **homomorphism** $\phi : G \to K$ is a mapping which preserves multiplication, i.e. $\phi(ab) = \phi(a)\phi(b)$.

Exercise 2.8. (i) Show that any homomorphism preserves the unit and the inversion operation.

(ii) Show that if a homomorphism is invertible, then its inverse is also a homomorphism.

(iii) Show that the composition of two homomorphisms is a homomorphism.

Example 2.9. The function $\mathrm{sign} : S_n \to \{1, -1\}$ is a homomorphism.

Definition 2.10. A homomorphism of groups is an **isomorphism** if it is invertible (i.e., bijective).

Two groups between which there is an isomorphism are called **isomorphic**. In group theory, such groups are regarded as "the same". An important class of problems in group theory is to classify groups satisfying given conditions up to isomorphism ("classification problems").

Exercise 2.11. Let G be a group, and $g \in G$. Show that the map $G \to G$ given by $a \mapsto gag^{-1}$ (called the **conjugation** by g) is an isomorphism.

Definition 2.12. The **direct product** (or **Cartesian product**) of two groups G, K is the group $G \times K$ which consists of pairs (g, k), $g \in G$, $k \in K$, with componentwise multiplication.

Similarly one defines the direct product of more than two groups. In particular, one can define the Cartesian powers G^n of a group G.

Example 2.13. The group of symmetries of a diamond (which is not a square) is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2.2. **Actions of groups on sets.** An important basic notion of group theory is that of an action of a group on a set.

Definition 2.14. An **action** of a group G on a set X is a homomorphism $\phi : G \to \mathrm{Perm}(X)$.

Equivalently, an action of G on X is a map $G \times X \to X$, $(g, x) \mapsto gx$ (called the **action map**), such that $g(hx) = (gh)x$ and $ex = x$. Indeed, if we are given such a map, then we can define ϕ by $\phi(g)(x) = gx$, and vice versa.

Example 2.15. The trivial action: $gx = x$ for all $g \in G$, $x \in X$.

Note that we have already seen many examples of group actions, since if G is a group of transformations of X, then G acts on X in a natural way.

Let us show that the notion of an abstract group is, in fact, equivalent to the notion of a group of transformations. For this, it suffices to show that any abstract group G is in fact a group of transformations of some set X. We take X to be the group G itself, and define the action of G on X by setting the action map $G \times X \to X$ to be the multiplication of G. This gives a homomorphism $\phi : G \to \mathrm{Perm}(G)$ given by $\phi(g)(h) = gh$, which is clearly injective. (The fact that $\phi(gk) = \phi(g)\phi(k)$ follows from the associativity axiom, while the fact that $\phi(g)$ is invertrible follows from the unit and inverse axioms). Thus, we get a realization of any group G as a group of transformations. In particular, we have

Proposition 2.16. Any finite group is isomorphic to a subgroup of S_n for some n.

2.3. **Orbits of group actions.** Let G be a group acting on a set X. The **orbit** of $x \in X$ is the set $Gx \subset X$ (which is stable under the action of G).

Exercise 2.17. Find the orbits of the action of $SO(2)$ on $\mathbb{R}^2$, and of $SO(3)$ on $\mathbb{R}^3$.

Answer: these are concentric circles (respectively, spheres), with the exception of the origin, which is a single orbit.

Proposition 2.18. Two orbits of a group action on a set X are either disjoint or coincide. Thus, X is a disjoint union of orbits.

Proof. Suppose $z \in Gx \cap Gy$. Then there exist $a, b \in G$ such that $z = ax = by$, so $y = b^{-1}z = b^{-1}ax$, and hence $Gy = Gx$. □

Definition 2.19. A G-action on X is called **transitive** if there is only one orbit. In this case X is called a **homogeneous G-space**.

Example 2.20. 1. The sphere is a homogeneous space for the group $SO(3)$ of rotations of the 3-space.

2. The sets of vertices, edges, faces of a Platonic solid are homogeneous spaces for the group of its rotations.

Definition 2.21. The **isotropy group**, or **stabilizer** G_x of a point $x \in X$ is the subgroup of all $g \in G$ such that $gx = x$. The action is **free** if G_x is the trivial group for all x.

It is easy to see that if x, y belong to the same orbit, then the stabilizers G_x, G_y are conjugate (in particular, isomorphic); namely, if $gx = y$ then $gG_xg^{-1} = G_y$.

Example 2.22. Any group G acts on itself by conjugation: $(g, x) \mapsto gxg^{-1}$. Orbits of this action are called **conjugacy classes**, and the stabilizer G_x is called **the centralizer** of x; it is the set of $g \in G$ which commute with x, i.e. $gx = xg$. The **center** $Z(G)$ of G consists of $x \in G$ which form a 1-element conjugacy class, i.e. $G_x = G$. Clearly, $Z(G)$ is a subgroup of G.

Remark 2.23. G is abelian if and only if $Z(G) = G$.

Exercise 2.24. (i) Show that $s, t \in S_n$ belong to the same conjugacy class if and only if they have the same number of cycles of each length. Thus, the number of conjugacy classes in S_n is the number of partitions of n.

(ii) Find conjugacy classes in S_3 and S_4.

Exercise 2.25. Find conjugacy classes in the group A_5 of rotations of the icosahedron, and interpret them in terms of the cycle decompositions in S_5. Are (12345) and (12354) conjugate in A_5?

Exercise 2.26. Find conjugacy classes in $SO(3)$.

2.4. **Cosets and Lagrange's theorem.** Let G be a group, and H be a subgroup of G.

Definition 2.27. A **left coset** of H in G is a set of the form gH, where $g \in G$. Similarly, a **right coset** of H in G is the set of the form Hg, where $g \in G$.

Thus, right cosets are orbits of the action of H on G via $(h, g) \mapsto hg$, and left cosets are orbits of the action of H on G via $(h, g) \mapsto gh^{-1}$. Note that these actions are free, i.e., the map $H \to gH$ given by $h \mapsto gh$ and the map $H \to Hg$ given by $h \to hg$ are bijections (by the cancelation property). Also, $hH = Hh = H$ for all $h \in H$.

Example 2.28. 1. Let $G = \mathbb{R}^2$ and $H = \mathbb{R}$ be the horizontal axis. Then left and right cosets of H in G are the horizontal lines.

2. Let $G = S_3$ and $H = \{\mathrm{Id}, (12)\}$. Then the left cosets of G n H are H, $\{(13), (123)\}$, $\{(23), (132)\}$, while the right cosets are H, $\{(13), (132)\}$, $\{(23), (123)\}$.

Proposition 2.29. If two left cosets of H in G intersect, then they coincide, and similarly for right cosets. Thus, G is a disjoint union of left cosets of H and also a disjoint union of right cosets of H.

Proof. This is a special case of Proposition 2.18. □

Corollary 2.30. (Lagrange's theorem) If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. In particular, the order of every element of G divides the order of G.

Proof. The ratio $|G|/|H|$ is the number of left (or right) cosets of H in G, so it is an integer. □

Definition 2.31. The number of left (or right) cosets of H in G is called **the index** of H in G.

Note that this definition makes sense even when H is infinite. E.g. even numbers form a subgroup $2\mathbb{Z}$ of index 2 in $\mathbb{Z}$.

Corollary 2.32. Any group G of prime order p is isomorphic to the cyclic group $\mathbb{Z}_p$.

Proof. Let $a \in G$, $a \neq e$. Then the order of a is > 1 and must divide p, so it is p. Thus, G contains $\mathbb{Z}_p$, hence $G \cong \mathbb{Z}_p$. □

The set of all left cosets of H in G is denoted by G/H. This set has a natural action of G via $(a, gH) \to agH$ (check that this is well defined!). Moreover, it is easy to see that there is only one orbit, so G/H is a homogeneous G-space. Finally, the stabilizer G_x of the point $x = H$ is nothing but the group H itself.

In fact, any homogeneous G-space X can be identified with G/H, where $H = G_x$ for some $x \in X$. Namely, the bijective map $G/H \to X$ is given by the formula $gH \mapsto gx$ (check that this is well defined!).

Example 2.33. 1. $\mathbb{R}/\mathbb{Z}$ is a circle, $\mathbb{R}^2/\mathbb{Z}^2$ is a torus.

2. The sphere in 3-space is $SO(3)/SO(2)$.

3. The real projective plane (the set of lines through the origin in $\mathbb{R}^3$) is $SO(3)/O(2)$.

Example 2.34. Consider the action of the group G of rotations of an icosahedron on its vertices, faces, and edges. Then the stabilizer of a vertex is $\mathbb{Z}_5$, the stabilizer of an edge is $\mathbb{Z}_2$, and the stabilizer of a face is $\mathbb{Z}_3$. So we have three ways of computing the order of this group: $12 \times 5 = 30 \times 2 = 20 \times 3 = 60$.

Example 2.35. 1. The group S_n acts transitively on the set $P_{m,n}$ of placements of m people into $n \geq m$ seats. The stabilizer of a placement is S_{n-m}. Thus, $P_{m,n} = S_n/S_{n-m}$, so $|P_{m,n}| = \frac{n!}{(n-m)!}$.

2. The group S_n acts transitively on the set $C_{m,n}$ of subsets (combinations) of m elements among $1, ..., n$. The stabilizer of a subset is $S_m \times S_{n-m}$. Thus, $C_{m,n} = S_n/(S_m \times S_{n-m})$, so $|C_{m,n}| = \frac{n!}{m!(n-m)!} = \binom{n}{m}$.

Exercise 2.36. Show that if a group G has a prime power order $p^n > 1$ then the center $Z(G)$ is nontrivial.

Solution: By Lagrange's theorem, the order of every conjugacy class of G is a power of p. Also, the sum of these orders is p^n. Since one of these orders equals 1 (for the identity element), at least p of these orders must be equal to 1.

2.5. **Counting colorings.** How many distinct ways are there to color the faces of a regular dodecahedron in red and blue? (We call two colorings distinct if they cannot be transformed into each other by a rotation). It turns out that this question can be solved using group theory. Namely, one can use the following theorem, called the **Polya enumeration theorem.**

Theorem 2.37. Suppose that a finite group G acts on a finite set X. Then number of colorings of X in n colors inequivalent under the action of G is

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)},$$

where $c(g)$ is the number of cycles of g as a permutation of X.

Proof. Let X_n be the set of colorings of X in n colors. Our job is to compute the number of G-orbits on X_n. Instead of counting G-orbits, let us count pairs (g, C), where $C \in X_n$ is a coloring, and $g \in G_C$ is an element of G preserving C. The orbit of C has $|G|/|G_C|$ elements, and each element in this orbit will appear $|G_C|$ times in our counting, so each orbit will appear $|G|$ times. Hence, we will get the correct answer $N(n)$ if we divide the final count by $|G|$.

Now, to count pairs (g, C), let's count for every $g \in G$ all the colorings C with which it can appear. These C are just colorings invariant under g. Decomposing X into orbits (=cycles) of g, we see that the color along the cycle has to be constant, and this is the only restriction. Thus, the number of possible C is just $n^{c(g)}$. Summing over all $g \in G$, we get the theorem. □

Example 2.38. We can now find the number of colorings of the faces of a dodecahedron in n colors. Recall that its group of rotations is $G = A_5$ of order 60. The element 1 has 12 cycles, so it contributes n^{12}. An element of order 2 is a rotation around the line connecting midpoints of two opposite edges, so it has 6 cycles of length 2, and contributes n^6. There are 15 such elements, so we get $15n^6$. An element of order 3 is a rotation around the axis passing through two opposite vertices. It has 4 cycles of length 3, so we get n^4. There are 20 such elements, so we get $20n^4$. Finally, an element of order 5 has 4 cycles of length $1, 1, 5, 5$ (so n^4), and there are 24 such elements, so we get $24n^4$. Overall,

$$N(n) = \frac{n^{12} + 15n^6 + 44n^4}{60}.$$

Note that this is always an integer, even if it's not clear from the formula. For example, for two colors, we get $N(2) = 96$. For three colors, we have $N(3) = 9099$.

Exercise 2.39. Compute the number of colorings of other regular polytopes in n colors. Specialize to $n = 2$.

Example 2.40. How many distinct necklaces can one make out of m triangular beads of two colors? (The beads have to point in the same direction along the necklace). The group of symmetries is $G = \mathbb{Z}_m$. An element $k \in G$ has order $m/GCD(k, m)$, and has $GCD(k, m)$ cycles of length $m/GCD(k, m)$. So we get that the number of necklaces is

$$N = \frac{1}{m} \sum_{k=0}^{m-1} 2^{GCD(k,m)}.$$

For example, if $m = p$ is a prime, then we get

$$N = 2 + \frac{2^p - 2}{p}.$$

Note that this is an integer by Fermat's Little Theorem. For instance, there are 8 distinct necklaces on 5 beads, and 20 on 7 beads.

The Polya enumeration theorem has a weighted generalization, which allows one to count colorings with a prescribed number of colors of each type. To do so, let us introduce a counting variable t_i for the i-th color. We want to get a generating function (polynomial) $P(t_1, ...t_n)$ such that the number of colorings with r_i occurrences of the i-th color will be the coefficient of $t_1^{r_1}...t_n^{r_n}$ in this polynomial.

To compute P, consider an element $g \in G$, and let's compute the contribution of colorings fixed by g. Let $c_m = c_m(g)$ be the number of cycles of length m in g; so $\sum_m c_m = c(g)$. It is clear that the polynomial counting colorings just of cycles of length m is $(t_1^m + ... + t_n^m)^{c_m}$. Thus, we get the following general version of the Polya enumeration:

Theorem 2.41. We have

$$P(t_1, ..., t_n) = \frac{1}{|G|} \sum_{g \in G} \prod_{m \geq 1} (t_1^m + ... + t_n^m)^{c_m(g)}.$$

The previous version is obtained just by setting $t_i = 1$ for all i.

Example 2.42. Let us compute the polynomial $P(t_1, t_2)$ for colorings of a dodecahedron in 2 colors. In fact, since it is homogeneous, it's enough to compute $P(t, 1)$. We have

$$P(t,1) = \frac{1}{60}((t+1)^{12} + 15(t^2+1)^6 + 20(t^3+1)^4 + 24(t+1)^2(t^5+1)^2) =$$
$$t^{12} + t^{11} + 3t^{10} + 5t^9 + 12t^8 + 14t^7 + 24t^6 + 14t^5 + 12t^4 + 5t^3 + 3t^2 + t + 1.$$

In particular, this means that the number of colorings with 6 red and 6 blue faces is 24.

Lecture 3

2.6. **Rings and fields.**

Definition 2.43. A **ring** is an abelian group R with a multiplication operation $R \times R \to R$, $(a, b) \mapsto ab$, such that

1) $(ab)c = a(bc)$ (associativity of multiplication);

2) there is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all a; and

2) $a(b + c) = ab + ac, (b + c)a = ba + ca$, $a, b, c \in R$ (the distributive law).

A ring R is **commutative** if $ab = ba$ for all $a, b \in R$.

A **field** is a commutative ring R in which every nonzero element a has an inverse a^{-1} such that $aa^{-1} = 1$.

Thus, the set of invertible elements of a ring R is a group, called the **multiplicative group** of R and denoted by $R^\times$.

Example 2.44. $\mathbb{Z}$ is a commutative ring, while $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. Also, $\mathbb{Z}_n$ is a commutative ring, which is a field if $n = p$ is a prime. In this case it is often denoted by $\mathbb{F}_p$ (to remember that it is a field). An example of a not necessarily commutative ring is the ring of matrices of size n over any ring R, $\mathrm{Mat}(n, R)$ (with usual matrix multiplication).

2.7. **Vector spaces.** Let F be a field, and consider the n-dimensional vector space F^n over F. Let $e_1, ..., e_n$ be the standard basis of F^n, i.e., $e_i = (0, ..., 1, ..., 0)$, where 1 stands on the i-th place. Any vector $(x_1, ..., x_n)$ can be written as $x_1e_1 + ... + x_ne_n$.

A (linear) **subspace** of F^n is a subset V that is closed under addition and multiplication by elements of F.

If $V \neq F^n$, then we may identify V (preserving addition and multiplication by elements of F) with a subspace of F^{n-1}. Indeed, let i be such that the vector e_i does not belong to V (it must exist since $V \neq F^n$). Let $V' \subset F^{n-1}$ be the subset of vectors obtained by deleting the i-th coordinate from vectors of V. Then the natural map $V \to V'$ is an isomorphism (check it!).

By iterating this process, we can identify any subspace V of F^n with F^m for some $m \leq n$.

In fact, the number m has an intrinsic meaning. Namely, let us say that $v_1, ..., v_r \in V$ are **linearly independent** if the relation $a_1v_1 + ... + a_rv_r = 0$, $a_i \in F$, implies that all $a_i = 0$.

Proposition 2.45. m is the maximal number of linearly independent vectors in V.

Proof. Since $V \cong F^m$, it admits m linearly independent vectors, so we need to show that F^m does not admit $m+1$ of them. This is shown by induction in m. Namely, let $v_1, ..., v_{m+1} \in F^m$. If the last coordinate of all of them is zero, then they are in F^{m-1} and we can use the induction assumption. Otherwise, at least one of them (say, v_{m+1}) has a nonzero last coordinate. Then there are numbers $b_1, ..., b_m \in F$ such that the last coordinates of the vectors $v_i - b_iv_{m+1}$ vanish for $i = 1, ..., m$. So these vectors are in F^{m-1}, and again we are done by the induction assumption. □

Definition 2.46. The number m is called the **dimension** of V, and denoted by $\dim V$. A **basis** of V is any collection of m linearly independent vectors in V.

It follows from the above that if $v_1, ..., v_m$ is a basis of V, then any vector in V can be uniquely written as $a_1v_1 + ... + a_mv_m$, $a_i \in F$.

An **affine subspace** U of F^n is a coset (i.e., shift) of a linear subspace U_0; namely, $U = v + U_0$ for some $v \in V$. If $\dim U_0 = 1$, we say that U is a **line**; if $\dim U_0 = 2$, we say that U is a **plane**.

2.8. **Linear transformations and matrices.** Let R be a commutative ring. A **linear transformation** of R^n is a transformation that preserves addition of vectors and multiplication of vectors by scalars. Thus, any linear transformation g is determined by $ge_1, ..., ge_n$, which can be arbitrary vectors.

Let us write ge_j as $\sum_{j=1}^n g_{ij}e_i$, where $g_{ij} \in R$. In this way, we attach to each linear transformation g a square matrix (=table) $[g] = (g_{ij})$, and vice versa. Then the composition of linear transformations becomes the standard multiplication law for matrices.

Thus the group $GL(n, R)$ of invertible linear transformations of R^n can also be defined as the group of invertible n by n matrices $g = (g_{ij})$. The invertibility condition is equivalent to the condition that the determinant of g is in $R^\times$ (i.e., nonzero if $R = F$ is a field). For instance, for $n = 2$, the determinant is $g_{11}g_{22} - g_{12}g_{21}$, so $GL(2, R)$ is the group of 2 by 2 matrices with entries in R such that $g_{11}g_{22} - g_{12}g_{21} \in R^\times$.

Note that if $R = F$ is a field, then g is invertible if and only if $ge_1, ..., ge_n$ is a basis of F^n; so bases of F^n are in bijective correspondence with elements $g \in GL(n, F)$.

Thus, we can define groups $GL(n, \mathbb{Z})$, $GL(n, \mathbb{Q})$, $GL(n, \mathbb{R})$, $GL(n, \mathbb{C})$, $GL(n, \mathbb{F}_p)$ (the latter group is finite).

Exercise 2.47. Find the order of $GL(n, \mathbb{F}_p)$, where p is a prime.

Solution. For any field F, $GL(n, F)$ acts transitively on the set of nonzero vectors in F^n. For $F = \mathbb{F}_p$, there are $p^n - 1$ such vectors. The stabilizer H of e_n is the set of matrices g with last column $(0, 0, ..., 1)$ and the diagonal block $(g_{ij}), 1 \le i, j \le n - 1$ being invertible. So if $N_n = |GL(n, \mathbb{F}_p)|$ then

$$N_n = N_{n-1}p^{n-1}(p^n - 1).$$

Hence, by induction,

$$N_n = p^{n(n-1)/2}(p - 1)...(p^n - 1).$$

Exercise 2.48. Show that $GL_2(\mathbb{F}_2) = S_3$.

2.9. **The game of SET.** The game of SET has an intrinsic connection to group theory since a SET is just a line in the 4-dimensional space $\mathbb{F}_3^4$ over $\mathbb{F}_3$.

Exercise 2.49. How many SETs are there?

Solution: The number of lines through the origin is $\frac{3^4-1}{3-1} = 40$. Such a line may be shifted to make an arbitrary line. There are 3^4 ways to do so for each line, but then we get each line 3 times. So altogether we have $3^3 = 27$ distinct ways of shifting, and thus $27 \cdot 40 = 1080$ distinct SETs.

Exercise 2.50. What is the chance that when you deal 12 SET cards, there will be no SET containing the first card?

Solution: $\frac{78 \times 76 \times ... \times 60}{79 \times ... \times 70} = 0.46....$

Exercise 2.51. You deal 12 SET cards. What is the average number of SETs you can find?

Solution: The number of 12-tuples of cards is $\binom{81}{12}$. Then number of those of them that contain a given SET is $\binom{78}{9}$. The total number of SETs is 1080. So the average number of SETs per deal is

$$1080 \times \binom{78}{9} / \binom{81}{12} = \frac{220}{79},$$

aproximately 2.78.

Exercise 2.52. Show that if you remove 26 SETs from the complete collection of SET cards, then the remaining triple is a SET.

Solution: A set can be defined as a collection of distinct vectors x, y, z such that $x+y+z = 0$. Since the sum of all vectors in $\mathbb{F}_3^4$ is zero, we get the result.

Exercise 2.53. What is the probability that a given collection of 3,4,5 SET cards does not contain a SET?

Solution: For 3 cards, it's 78/79, approximately 0.987 (two cards are chosen arbitrarily, for the third one there is one forbidden case out of 79). For 4 cards: there is a 78/79 chance to pick the first three so they are not a SET. Now for the 4th card there are 3 forbidden possibilities. So the chance is $\frac{78}{79} \cdot \frac{75}{78} = \frac{75}{79}$, approximately 0.95. The case of 5 cards is a bit more complicated. Let the first 4 cards correspond to vectors x, y, z, t (no two of them lie on the same line). There are two possibilities. The first possibility is that these vectors are not in the same plane. In this case, we may assume that they are $0, -e_1, -e_2, -e_3$, and the forbidden vectors for the 5th card are $e_1, e_2, e_3, e_1 + e_2, e_1 + e_3, e_2 + e_3$, all distinct. The chance of x, y, z, t not being in the same plane is $(78/79) \cdot (72/78) = 72/79$, so we get $(72/79) \cdot (71/77)$. Now, the chance that x, y, z, t are in the same plane is 3/79; given this, we can assume (up to permutation) that these vectors are $0, -e_1, -e_2, -e_1 - e_2$, so the forbidden vectors are all the other vectors of the plane spanned by e_1, e_2, and there are 5 of them, so we get a chance of 72/77. So altogether we get $\frac{72 \cdot 74}{79 \cdot 77}$, which is approximately 0.875.

Exercise 2.54. A superSET is a collection of at least two SET cards such that any two of them are contained in a SET (made out of the cards of this superSET).

(i) How many cards can there be in a superSET?

(ii) Find the number of superSETs of each size.

(iii) How many SETS are contained in a superSET of each size?

Solution: (i) The number of cards in a superSET is 3,9,27, or 81, since it is an affine subspace of $\mathbb{F}_3^4$.

(ii) For size 9, we have to count 2-planes in the 4-space over $\mathbb{F}_3$. First count the 2-planes through the origin. For the first basis vector we have $3^4 - 1 = 80$ possibilities, for the second one $3^4 - 3 = 78$, but this is all modulo $GL(2, \mathbb{F}_3)$, which has order 48. So altogether we have $80 \cdot 78/48 = 130$ such planes. Thus, the total number of planes is $9 \cdot 130 = 1170$.

For size 27, we have to count 3-hyperplanes in the 4-space. Those that pass through the origin correspond to linear equations $a_1x_1 + ... + a_4x_4 = 0$, where not all a_i are zero, and a_i can be scaled simultaneously. There are $(3^4 - 1)/2 = 40$ such equations (up to scaling). So altogether we have $3 \cdot 40 = 120$ such hyperplanes.

(iii) For size 9, $3 \cdot 4 = 12$ SETs; for size 27, $9 \cdot 13 = 117$ SETs.

2.10. **The projective SET.** The **projective SET** is a game of 31 cards, on which there are red, green, blue, brown, and black triangles. Each triangle may be present only once or not at all, and all combinations occur exactly once, except the empty card. A SET is a collection of 3 cards on which a triangle of each color either does not occur at all or occurs twice (i.e., on two different cards). The game is played as the usual SET, starting with 8 cards.

Like the usual SET, projective SET can be interpreted in terms of group theory. Namely, the cards can now be viewed as nonzero vectors in $\mathbb{F}_2^5$. Specifically, to every card we attach a vector whose first coordinate (0 or 1) indicates the absence or presence of a red triangle, the second - green triangle, the third - blue triangle, the forth - brown triangle, and the fifth - black triangle. Then it is easy to see that a SET is nothing but a collection of vectors a, b, c such that $a + b + c = 0$, i.e. a 2-plane in $\mathbb{F}_2^5$ through the origin with the origin deleted.

One can also consider the deck of cards as the collection of lines through the origin, called the 4-dimensional projective space, $\mathbb{F}_2\mathbb{P}^4$. Then SETs are projective lines in this space, hence the name "projective SET".

Exercise 2.55. (i) How many projective SETs are there?

Answer: 155.

(ii) How many projective SETs are, on average, in a deal of 8 cards?

Answer: 56/29.

(iii) A projective superSET is a collection S of cards such that any two cards are contained in a set inside S. What are the possible values of $|S|$?.

Answer: $3, 7, 15, 31$.

(iv) How many superSETs are there for each size?

Answer: $155, 155, 31, 1$.

Note that the first two numbers coincide. Can you explain why?

2.11. **Normal subgroups.** If G is a group and H is a subgroup of G, then G/H is a homogeneous G-space, but in general not a group. The naive definition $aH \cdot bH = abH$ does not really work, since we can have $a_1H = a_2H$, but $a_1bH \neq a_2bH$. The simplest example is $G = S_3$, $H = \{1, (12)\}$, $a_1 = (13)$, $a_2 = (123)$, $b = (13)$ (we have $a_1b = \mathrm{Id}$, $a_2b = (23)$). However, this definition works in the special situation when H is a normal subgroup.

Definition 2.56. H is a **normal subgroup** of G if its left and right cosets coincide.

Equivalently, H is normal if it is preserved by conjugations by $g \in G$. If H is normal, then $aHbH = abH$, so the above definition works, and G/H is naturally a group. This group is called the **quotient group** of G by H.

Example 2.57. 1. Any subgroup of an abelian group is normal. We have $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, where $n\mathbb{Z}$ is the group of integers divisible by n.

2. G is a normal subgroup in $G \times K$, and $(G \times K)/G = K$.

3. Any subgroup of index 2 is normal (since there are only two right (left) cosets of H in G, and the nontrivial one must be the complement of H in G, whether it is a right or a left coset). The quotient is $\mathbb{Z}_2$.

4. The center $Z(G)$ is normal in G.

5. The group of translations of the Euclidean space is normal in the group of motions (the quotient being the group of rotations), but the group of rotations is not.

6. The group of elements of S_4 which have two cycles of length 2 or are trivial is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and normal.

Definition 2.58. The **kernel** $\mathrm{Ker}\phi$ of a group homomorphism $\phi : G \to K$ is the set of $g \in G$ such that $\phi(g) = e$. The **image** $\mathrm{Im}\phi$ of ϕ is the set of elements of the form $\phi(g) \in K$, where $g \in G$.

Proposition 2.59. (i) The image of ϕ is a subgroup of K.
(ii) The kernel of ϕ is a normal subgroup of G.
(iii) the quotient group $G/\mathrm{Ker}\phi$ is naturally isomorphic to $\mathrm{Im}\phi$.

Exercise 2.60. Prove this proposition.

Example 2.61. $S_4/(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_3$. Indeed, we have a surjective homomorphism $S_4 \to S_3$ obtained by the action of the group of rotations of the cube on the coordinate axes, or by action of S_4 on the splittings of $1, 2, 3, 4$ into two pairs. The kernel is easily seen to be $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercise 2.62. Show that any group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Exercise 2.63. Show that if G is a group of order p^n, where p is a prime, then G admits a surjective homomorphism $\phi : G \to \mathbb{Z}_p$.

Solution: The proof is by induction in n. The base is clear. Let us prove the induction step. As shown above, $Z(G)$ is nontrivial, so has an element z of order p. If $G = (z)$, there is nothing to prove. Otherwise, by the induction assumption, $G/(z)$ has a surjective homomorphism into $\mathbb{Z}_p$, hence so does G.

Exercise 2.64. Show that any group G of order $2p$, where p is an odd prime, is either $\mathbb{Z}_{2p}$ or D_{2p}. In particular, every group of order 6 is either $\mathbb{Z}_6$ or S_3.

Solution: If there is an element of order $2p$, then the group is $\mathbb{Z}_{2p}$. Otherwise, we claim there is always an element of order p. Indeed, otherwise, since orders of elements can only be $1, 2, p$, we have elements $a \neq b$ such that a, b, ab have order 2. Then these elements generate a $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is impossible by Lagrange's theorem. Thus, there is a subgroup $\mathbb{Z}_p \subset G$, which is normal, since it is of index 2. Let $g \in G$ be an element outside this subgroup. Then $g^2 = 1$ (otherwise there is an element of order $2p$). Also, if a is the generator of $\mathbb{Z}_p$, $(ga)^2 = 1$, so $ga = a^{-1}g$, and we get D_{2p}.

Lecture 4

2.12. **Classification of finitely generated abelian groups.** Let G be a group, and S be a subset in G. We say that G is **generated by** S if any element of G is a product of elements of S and their inverses. A group is **finitely generated** if it can be generated by a finite set.

Example 2.65. The symmetric group S_n is generated by the transpositions of neighbors $(i, i+1)$.

Exercise 2.66. Let a, b, c be elements of the group of rotations of the icosahedron which preserve a face, its edge, and an endpoint of this edge, respectively. Then G is generated by any two of these three elements.

The following important theorem (whose proof is beyond the scope of these notes) classifies finitely generated abelian groups.

Theorem 2.67. Any finitely generated abelian group is uniquely representable as a direct product of (finitely many) cyclic groups of infinite or prime power orders.

Exercise 2.68. Show explicitly why $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$.

Note that it follows from this theorem that if $n = p_1^{m_1}...p_k^{m_k}$ is a prime factorization, then $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{m_1}} \times ... \times \mathbb{Z}_{p_k^{m_k}}$. An attentive reader will notice that this is nothing but the celebrated Chinese Remainder Theorem in elementary number theory.

Exercise 2.69. Show that the group $\mathbb{Q}$ of rational numbers (which is infinitely generated) is not a a direct product of cyclic groups.

Solution: $\mathbb{Q}$ has no nontrivial homomorphisms to cyclic groups.

2.13. **Groups of order** 8**.** According to the previous subsection, there are three abelian groups of order 8 - $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. This is also easy to show directly. Let us now consider the nonabelian groups of order 8. We have seen that such a group must have a nontrivial center $Z(G)$, and $G/Z(G)$ cannot be cyclic. So $|Z(G)| = 2$ (i.e. $Z(G) = \mathbb{Z}_2$), and $G/Z(G) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Let i, j be two elements of G that project to generators of $G/Z(G)$, and let z be the generator of $Z(G)$. Then we must have $ij = zji$, and we can have $i^2 = e, j^2 = e$, or $i^2 = z, j^2 = e$, or $i^2 = z, j^2 = z$, up to swapping i, j. The first two cases are in fact equivalent, by replacing i with ij, and is nothing but the group of symmetries of the square, D_8. The last case gives **the quaternnion group** Q_8.

Exercise 2.70. Show that D_8 is not isomorphic to Q_8.

Hint. Count elements of order 2.

Thus, we have classified all the groups of order < 12.

2.14. **Semidirect products.** Let G be a group, K another group, and suppose that G acts on K by group automorphisms (i.e., isomorphisms onto itself). We will write gk as ${}^g k$. Then one can define the semidirect product $G \ltimes K$, which is the usual product of sets with the operation $(k_1, g_1)(k_2, g_2) = (k_1 {}^{g_1} k_2, g_1 g_2)$. For example, if the action of G on K is trivial, this is the usual direct product. Note also that K is a normal subgroup in $G \ltimes K$, and $(G \ltimes K)/K = G$.

The following series of examples shows that semidirect products are ubiquitous.

Example 2.71. 1. The group D_{2n} of symmetries of the n-gon is $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$, where the action of $\mathbb{Z}_2$ on $\mathbb{Z}_n$ is by $a \to -a$.

2. The group S_n is $\mathbb{Z}_2 \ltimes A_n$, where the action is by conjugation by any odd permutation.
3. $S_4 = S_3 \ltimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$.
4. The group of symmetries of the n-dimensional cube is $S_n \ltimes \mathbb{Z}_2^n$.
5. The groups of motions of the plane and 3-space are $SO(2) \ltimes \mathbb{R}^2$ and $SO(3) \ltimes \mathbb{R}^3$.
6. The group of symmetries of the SET game is $GL(4, \mathbb{F}_3) \ltimes \mathbb{F}_3^4$.

Example 2.72. The Sudoku group (i.e. the group of symmetries of the Sudoku game $(D_8 \ltimes (S_3 \ltimes S_3^3)^2) \times S_9$ (permutations of rows and columns inside triples, permutation of triples of rows and columns, symmetries of the square, permuting digits). The order of this group is $8 \cdot 3^8 \cdot 9!$, which is approximately 5 trillions. If you apply an element of this group to a Sudoku problem, you get a formally equivalent problem, which most likely looks totally different. This allows one to indefinitely make a living selling collections of Sudoku problems if one has only one Sudoku problem to start with. Namely, you can make about 700 Sudoku problems for each human on earth!

2.15. **Simple groups.**

Definition 2.73. A group G is called **simple** if it is not trivial, and does not contain any nontrivial normal subgroups, i.e. normal subgroups other than G itself and the trivial group.

Example 2.74. 1. The group $\mathbb{Z}_p$ is simple for prime p.

2. $SO(2)$ is not simple, but $SO(3)$ is simple.

Exercise 2.75. Show that A_5 is a simple group, but A_4 is not.

Solution: As we saw, conjugacy classes in A_5 have sizes $1, 15, 20, 12, 12$. No subset of these numbers containing 1 adds up to a divisor of 60 different from 1 and 60. This implies the statement, since a normal subgroup of a group G is a union of (some) conjugacy classes of G. A_4 is not simple since it contains a normal subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proposition 2.76. The alternating group A_n for $n \geq 5$ is simple.

Proof. Suppose $H \neq \{e\}$ is a normal subgroup of A_n. Then H contains a nontrivial conjugacy class C of A_n.

Let us show that this conjugacy class has $\geq n$ elements. Indeed, assume that the cycle decomposition of an element of C involves a cycle of length ≥ 3. Then C contains a permutation in which 1 is contained in such a cycle. If the cycle has length $p+1$, then there are at least $(n-1)...(n-p)$ ways to fill the remaining positions of the cycle, so the size of conjugacy class is at least $(n-1)(n-2)...(n-p)/2 \geq (n-1)(n-2)/2 \geq n$. Thus, it remains to consider the case where the only cycles are of length 1 and 2. In this case, we have a permutation where 1 is in a cycle of length 2. There are $n-1$ ways to fill this cycle, and for each such way, there are more than one way to fill the rest, unless this is just a transposition (here we use that $n \geq 5$). Finally, the conjugacy class of transpositions has $n(n-1)/2 \geq n$ elements.

Thus, $|H| > n$.

Now we can proceed by induction. We have proved the base of induction, $n = 5$. Now assume that A_{n-1} is simple. Let H be normal in A_n. If $H \cap A_{n-1}$ is nontrivial, then H

contains A_{n-1}, so H contains (123), and hence (ijk) for any i, j, k. But (ijk) generate A_n, so $H = A_n$.

It remains to consider the case $H \cap A_{n-1}$ being trivial. In this case, A_{n-1} embeds into A_n/H, so $|H| \leq n$. Thus, H is the trivial group. □

Simple groups are important because any finite group can be decomposed into simple ones in a unique way, similarly to how a molecule can be decomposed into atoms. More precisely, we have the following theorem, called **the Jordan-Hölder theorem**.

Theorem 2.77. Let G be a finite group. Then there exists a sequence of subgroups $G = G_0 \supset G_1 \supset ... \supset G_n = \{e\}$ such that G_{i+1} is normal in G_i, and the groups $H_i := G_{i-1}/G_i$ are simple. Moreover, the sequence of groups $H_1, ..., H_n$, up to permutation, depends only on G and not on G_i.

Definition 2.78. The sequence $H_1, ..., H_n$ is called **the composition series** of G.

This theorem implies that if we understand finite simple groups, then to some extent we will understand all the finite groups. (With the understanding that this is not the full picture, since there are many complicated ways in which simple groups H_i can be "glued together" into G. This is similar to the distinction in chemistry between ordinary chemical formula and structural formula of a substance).

Proof. To prove the existence of G_i, we can choose G_i to be a maximal normal subgroup in G_{i-1} (not equal G_{i-1} itself). Now we prove uniqueness of the composition series by induction in $|G|$. Assume that there are two collections of subgroups, G_i and G_i'. If $G_1 = G_1'$, the statement follows from the induction assumption. Otherwise, we have homomorphisms $f : G \to H_1, f' : G \to H_1'$, which combine into a surjective homomorphism $f'' : G \to H_1 \times H_1'$. Let K be the kernel of this homomorphism. Let $L_1, ..., L_r$ be the composition series of K (well defined by the induction assumption). Then G_1 has composition series

$$(H_2, ..., H_n) = (H_1', K_1, ..., K_r),$$

and G_1' has composition series

$$(H_2', ..., H_m') = (H_1, K_1, ..., K_r).$$

Thus, adding H_1 to the first series and H_1' to the second one, we get

$$(H_1, H_2, ..., H_n) = (H_1', H_2', ..., H_m'),$$

as desired. □

Exercise 2.79. (i) Show that if H is a normal subgroup in G then the composition series of G is obtained by combining the composition series of H and G/H.

(ii) Show that if G is a group of order p^n, where p is a prime, then its composition series consists of n copies of $\mathbb{Z}_p$.

Exercise 2.80. Find the composition series of S_n.

Solution: For $n = 3$, $\mathbb{Z}_2, \mathbb{Z}_3$. For $n = 4$, three copies of $\mathbb{Z}_2$ and $\mathbb{Z}_3$. For $n \geq 5$, $\mathbb{Z}_2$ and A_n.

Definition 2.81. A finite group G is **solvable** if all its composition factors are cyclic.

A theorem of Burnside (whose proof is beyond the scope of these notes) states that any group whose order has only two prime divisors (i.e. of order $p^a q^b$, where p, q are primes) is solvable. Also, the fact that the groups S_n are solvable for $n \leq 4$ but not solvable for $n \geq 5$ is the reason why equations of order < 5 can be solved in radicals, and equations of order 5 and higher cannot, in general.

Since any finite group can be decomposed into simple groups, it is important to classify finite simple groups. This is an extremely difficult problem - one of the most difficult problems in all mathematics. At the moment, it is believed that this problem is solved, but the solution (completed around 1980) takes many thousands of pages and is written by many people, and there is no complete certainty that it does not contain mistakes.

The answer is that there are the following kinds of cyclic groups:

1) cyclic groups of prime order;

2) alternating groups A_n for $n \geq 5$;

3) simple groups of Lie type (basically, consisting of matrices over finite fields satisfying some special algebraic equations). E.g., $SL_2(\mathbb{F}_p)/\{\pm 1\}$ is simple for $p \geq 5$ (where SL_2 stands for matrices with determinant 1).

4) 26 sporadic groups. The smallest of them has order 7920, the largest one (the Monster) about 10^{53}.

Lecture 5

3. Finite subgroups of $SO(2)$ and $SO(3)$

Exercise 3.1. Show that any finite subgroup of $SO(2)$ is a cyclic group $\mathbb{Z}_n$.

Theorem 3.2. The finite subgroups of $SO(3)$ are $\mathbb{Z}_n$, D_{2n}, the tetrahedral group A_4, the cube group S_4, and the icosahedral group A_5.

Proof. Let G be a finite subgroup of $SO(3)$. Consider the action of G on the sphere. Any nontrivial element of G is a rotation around an axis by a nontrivial angle. So the only fixed points are the intersection points of the axis with the unit sphere, which are two opposite poles.

If P is a pole then the stabilizer of P is the group G_P of $g \in G$ which are rotations around the line connecting P with the center of the sphere. Such group is obviously cyclic, of some order m. Now let $P_1, ..., P_k$ represent orbits of poles and have orders $m_1, ..., m_k$. Then their orbits have orders n/m_i. Thus the number of pairs (g, P) where P is a pole and g a nontrivial element preserving it is

$$\sum_i \frac{n(m_i - 1)}{m_i}.$$

On the other hand, this is twice as many as the number of nontrivial elements of G, as any such element preserves exactly two poles. So we have

$$2(n-1) = \sum_i \frac{n(m_i - 1)}{m_i},$$

or

$$2(1 - \frac{1}{n}) = \sum_{i=1}^{k} (1 - \frac{1}{m_i}).$$

To classify solutions of this equation, assume $n > 1$ and note that it can be written as

$$\sum_{i=1}^{k} \frac{1}{m_i} = k - 2 + \frac{2}{n}.$$

As $m_i \geq 2$, we have $k = 2$ or 3. If $k = 2$ then we get

$$\frac{n}{m_1} + \frac{n}{m_2} = 2,$$

which implies that $m_1 = m_2 = n$ and we have the cyclic group $\mathbb{Z}_n$. If $k = 3$ then we get

$$\frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3} = n + 2,$$

which implies, assuming $m_1 \leq m_2 \leq m_3$, that $m_1 = 2$. If $m_2 = 2$, then $m_3 = n/2$, so G has a cyclic subgroup of index 2, which is normal, so it must be the dihedral group D_n (with its usual action on the sphere). Now, if $m_2 \geq 3$ then there are only three solutions for m_i: $(2, 3, 3), (2, 3, 4), (2, 3, 5)$, giving $n = 12, 24, 60$. It is easy to check that these situations correspond to cases of A_4, S_4, and A_5. □

4. The wallpaper groups

4.1. **Classification of wallpaper groups.**

Definition 4.1. A **wallpaper group** is a group G of symmetries of the plane $\mathbb{R}^2$ which contains a lattice L (generated by two linearly independent vectors v, u), which is a subgroup of finite index in G.

The name of wallpaper groups comes from the fact that they are groups of symmetries of a wallpaper pattern (periodically repeating in two directions).

Theorem 4.2. There are 17 wallpaper groups, up to an isomorphism.

The rest of the section is dedicated to the (sketch of) proof of this theorem.

First consider orientation preserving wallpaper groups. We will assume that L is the largest lattice contained in G. Also, let K be the image of G in $SO(2)$. Then $K = \mathbb{Z}_m$ for some m, and $G = K \ltimes L$ (as $G \cap \mathbb{R}^2 = L$). We claim the $m = 1, 2, 3, 4$ or 6 (for $m = 4$ we need the square lattice, and for $m = 3$ or $m = 6$ the hexagonal lattice). Indeed, let $v \in L$ be a nonzero vector, and R be the generating rotation of K (by angle α). Then $Rv + R^{-1}v = mv$, where m is an integer. But $|mv| \leq 2|v|$, so $m = 2, 1, 0, -1, -2$, which corresponds to the 5 cases above.

Thus, we have 5 wallpaper groups preserving orientation. One of the common ways to denote them is called "orbifold notation", invented by John Conway. This notation has to do with the orbit space (**orbifold**) $\mathbb{R}^2/G$. It is obtained by folding and gluing the **fundamental domain** of G (which is a region containing exactly one representative of each orbit) along its boundary. It is easy to see that topologically, this gives a torus for $m = 1$ and a sphere in all other cases. But if we remember the stabilizers, all these spheres are different. Namely, for $m = 2$ there are 4 special points of order 2 (so it is denoted 2222), for $m = 3$ there are 3 special points of of order 3 (so it is denoted 333), for $m = 4$ there are 2 special points of order 4 and one special point of order 2 (so it is denoted by 442), and for $m = 6$ there are special points of order $6, 3, 2$ (so it is denoted 632). The case of $m = 1$ is denoted just by "o" (no special points).

Now consider groups that contain orientation reversing symmetries. Such a group G contains a group G_+ which is of index 2 and orientation preserving (hence one the five groups above). Suppose first that G contains a reflection. In this case, the classification is determined by which of the centers of rotational symmetry (i.e., special points) lie on the reflection line. The reflection is denoted by *, and the centers of rotation symmetry which are on the reflection line are written after the * (dihedral symmetry), while the centers of rotational symmetry not on the line are written before the *. We get the following list:

G_+=2222: 0, 2, or 4 centers of rotation lie on the reflection line. The first case is denoted 22* (two centers of rotation modulo symmetry, both not on the reflection line), the second 22*2 (three centers, one on the reflection line, two are not), and the third *2222 (four centers on the reflection line).

G_+=333: 1 or 3 centers of rotation lie on the reflection line. The first case is denoted 3*3, the second *333.

G_+=442: 1 or 3 centers of rotation on the reflection line. The first case is denoted by 4*2, the second by *422.

G_+=632: all 3 centers of rotation lie on the reflection line. This case denoted by *632.

$G_+ = L$ (case "o"): in this case we can have (for a rectangular lattice) a reflection in a vertical line through the origin. This creates two reflections in two parallel lines differing by a half-period, so this case is denoted by **. Another possibility is a reflection of a rhombic lattice in the diagonal line (which we take to be vertical). This contains a **gliding symmetry** $x \to -x$, $y \to y + 1$, which is not obtained from rotations and reflections; such a symmetry is denoted by "x" in Conway notation. This symmetry is preserved by the reflection, so we put the x after the *, i.e. *x.

This makes 15 cases altogether. Finally, consider the case when there are no reflections, which gives two remaining possibilities. If there are no reflections, an element of G which is not in G_+ has to be a gliding symmetry. The gliding symmetry has order 2 on the torus, and has no fixed points. So if there is no rotations, there are no fixed points, and we get that G acts freely on $\mathbb{R}^2$, and $\mathbb{R}^2/G$ is the Klein bottle. This case is denoted by xx, since in this case we have two gliding symmetries with lines differing by a half-period. Otherwise, since the gliding symmetry has no fixed points on $\mathbb{R}^2/G_+$, there must be an even number of centers of rotations of each type. This only happens in the case 2222, so we get 22x (two centers of rotation modulo symmetry, which are not fixed by the symmetry).

4.2. **Recognition of planar patterns.** Let us now describe how to recognize planar patterns according to the above classification. Let m be the maximal order of rotational symmetry of the pattern.

m=1: No reflections, no glides: o. Glides, but no reflections: xx. Reflections, but no glides: **. Reflections and glides: *x.

m=2: 1) No reflections. No glides: 2222. Glides: 22x.

2) With reflections. 2 centers of rotation modulo symmetry: 22*. 3 centers: 2*22. 4 centers: *2222.

m=3: No reflections: 333. Reflections and 2 centers of symmetry: 3*3. 3 centers: *333.

m=4: No reflections: 442. Reflections and 2 centers of symmetry: 4*2. 3 centers: *442.

m=6: No reflections: 632: Reflections: *632.

5. The group of the Rubik cube

Let G be the group of the Rubik cube, i.e. the group of all the transformations which can be obtained by alternating the elementary transformations (rotations of faces by 90^0).

Clearly, any such trasformation g permutes the 12 edge cubies (with a possible flip of each) and the 8 corner cubies (with a possible 120^0 or 240^0 rotation of each), and is determined completely by its action on the edge and corner cubies. Thus, G is a subgroup of $S := (S_{12} \ltimes \mathbb{Z}_2^{12}) \times (S_8 \ltimes \mathbb{Z}_3^8)$.

If any configuration could be transformed into any other by elementary transformations, then G would coincide S. However, it turns out that there are three invariants of a configuration, with values in $\mathbb{Z}_2$, $\mathbb{Z}_2$, adn $\mathbb{Z}_3$, respectively, which are the only obstructions to identification of two configurations using elementary transformations. For this reason, we have the following result.

Theorem 5.1. G is a normal subgroup of index 12 in S, which is the kernel of a certain homomorphism $\phi = (\phi_1, \phi_2, \phi_3) : S \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

This means that if we take the Rubik cube apart and randomly put it together, then the probability that the cube can be solved is 1/12.

Proof. Let $g \in S$, $g = (a, x, b, y)$, $a \in S_{12}, b \in S_8, x = (x_1, ..., x_{12}) \in \mathbb{Z}_2^{12}$, $y = (y_1, ..., y_8) \in \mathbb{Z}_3^8$. Then $\phi_1(g) := \text{sign}(a)\text{sign}(b)$, $\phi_2(g) := \sum x_i$, $\phi_3(g) := \sum y_i$.

Let us explain why G is contained in Kerϕ.

First, G is contained in the kernel of ϕ_1, because for g being an elementary transformation, both a and b are cycles of length 4, hence both odd. Also, G is contained in the kernel of ϕ_3 because elementary transformations have order 4.

Finally, let us show that G is contained in the kernel of ϕ_2. To do so, let us put zeros and ones on the edge cubies, so that in the initial position, the horizontal faces have zeros and all other faces have ones. We'll say that an edge cubie is positively oriented if 0 is perpendicular to the x-axis and 1 to the y-axis, or 0 to the y-axis and 1 to the z-axis, or 0 to the z-axis and 1 to the x-axis; otherwise we say that the edge cubie is negatively oriented. Clearly, a rotation of a Rubik cube face flips the orientation of all of its four edge cubies, which implies that the number of positively oriented edge cubies modulo 2 is preserved. This implies that G is indeed contained in the kernel of ϕ_2.

It remains to see why G equals $K = \text{Ker}\phi$. This is nontrivial, but follows from the algorithm of solving the Rubik's cube. Namely, it is known that one can

1) flip any two edge cubies in the same face simultaneously;

2) turn one corner cubie clockwise 120 degrees and another in the same face counterclockwise by 120 degrees;

3) cyclically permute three edge cubies in the same face;

4) cyclically permute three vertex cubies in the same face.

It is easy to see that combining these transformations with face rotations, we can get any element of K, as desired.

□