INTRODUCTORY LECTURE ON GROUPS

1. Motivate Isomorphism Immediately

The same group can appear in various manifestations, so it behooves us to see the underlying common structure rather than the misleading specifics. Specifically, introduce the nonabelian group of order 6 in four ways (have different small groups of students explore each for ten minutes, then reconcile their results):

- As D_3 (bring a triangle). Get the students to describe the six elements geometrically (identity, two rotations, three reflections).
- As S_3. Get the students to describe the six elements as permutations.
- As the presented group $\langle a, b \,|\, a^3 = b^2 = 1,\ ba = a^2b\rangle$. Get the students to spell out the words: $1, a, a^2, b, ab, a^2b$.
- As $\mathrm{SL}_2(F_2)$.
- Then return to D_3, let a be counterclockwise rotation through 120 degrees, let b be vertical reflection. Show that $a^3 = b^2 = 1$, $ba = a^2b$.
- Then return to S_3, let $a = (1\,2\,3)$ and let $b = (1\,2)$. Get the relations again.
- Label the triangle vertices suitably.
- Get a compatible description of $\mathrm{SL}_2(F_2)$ as well.

2. Groups Arise as Ensembles of Symmetries

The dihedral and symmetric groups *act* on sets. (The dihedral group acts on the six possible triangle positions, but we saw that it may as well act on the three triangle vertices.) So do matrix groups. Similar examples:

- Rotations of the cube (picture): Find all 24, see that we get S_4.
- Rotations of the tetrahedron (picture): Which 12 do we get?
- Rotations of the icosahedron (use the model first): Find all 60, then use pictures from the quintic book to see a subgroup of S_5.
- $\mathrm{SO}_3(\mathbb{R})$ as the rotations of $\mathbb{R}^3$.

3. Especially, Groups Arise from Polynomials

Let the initial working environment be the rational field $\mathbb{Q}$. Consider a cubic polynomial

$$f(X) = X^3 + pX + q, \quad p, q \in \mathbb{Q}.$$

This polynomial has a real root because its degree is odd, and so it has three complex roots r_1, r_2, r_3, possibly all real, possibly repeating. Then:

The permutations of the roots that fix $\mathbb{Q}$ pointwise form a group.

Since there are three roots, the group is a subgroup of S_3, but is it all of S_3? For example, can we exchange r_1 and r_2?

The answer depends on the polynomial. Its roots satisfy the conditions

$$\begin{aligned} r_1 + r_2 + r_3 &= \quad 0, \\ r_1r_2 + r_2r_3 + r_3r_1 &= \quad p, \\ r_1r_2r_3 &= -q. \end{aligned}$$

Methods that we will learn later show that the **discriminant** of the polynomial, the product of the squares of the differences of the roots,

$$D = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

can be expressed in terms of the coefficients,

$$D = -4p^3 - 27q^2.$$

For example, the polynomial

$$f(X) = X^3 - 3X + 1$$

has discriminant

$$(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2 = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 81,$$

and hence

$$(r_1 - r_2)(r_1 - r_3)(r_2 - r_3) \in \{\pm 9\}.$$

Hence we can not exchange r_1 and r_2 while fixing $\mathbb{Q}$, since the exchange also exchanges 9 and -9.

Galois invented/discovered group theory precisely in this context. He realized that

> *The group of admissible permutations of the roots describes the difficulty of solving the polynomial. If the group can be decomposed in a certain way then the polynomial can be solved correspondingly by radicals.*

Galois found crucial ideas of group theory in the process of his investigations.

Especially, the cubic polynomial $X^3 - 3X + 1$ is easier to solve than the general cubic because the group of admissible permutations of its roots is smaller than S_3.

4. These Examples Motivate the Group Axioms

- Associativity: The composition of maps is associative because for *any* x,

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)) = f((g \circ h)(x)) = (f \circ (g \circ h))(x),$$

  and so

$$((f \circ g) \circ h) = (f \circ (g \circ h)).$$

- Identity: The do-nothing permutation will always be admissible.
- Inverses: A permutation having certain properties will be reversed by another.

5. The Importance of Maps Between Groups is Often That They Respect the Group Laws

- $\cdot^\alpha : (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ where $\alpha \in \mathbb{Q}$ satisfies $(xy)^\alpha = x^\alpha y^\alpha$.
- $|\ | : (\mathbb{C}_{\neq 0}, \cdot) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ satisfies $|zw| = |z|\,|w|$.
- $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}_{\neq 0}, \cdot)$ satisfies $\exp(x+y) = \exp(x)\exp(y)$.
- $\det : \mathrm{GL}_n(A) \longrightarrow A^\times$ satisfies $\det(AB) = \det(A)\det(B)$.
- $\bmod n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ satisfies $(x+y) \bmod n = (x \bmod n) + (y \bmod n)$ and $xy \bmod n = (x \bmod n)(y \bmod n)$.
- $\deg : k(X)^\times \longrightarrow \mathbb{Z}$ satisfies $\deg(fg) = \deg(f) + \deg(g)$.
- $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$ satisfies $\mathrm{sgn}(\pi\rho) = \mathrm{sgn}(\pi)\mathrm{sgn}(\rho)$.