MA30237 - Group Theory

Overview and motivation – aka Propaganda!

David M. J. Calderbank Thomas Cottrell

4W 3.41, d.m.j.calderbank@bath.ac.uk

Semester 1, 2020-21

Groups and symmetry

What is group theory?

- The mathematical study of symmetry in its most general form.

Why study group theory?

- Symmetry is everywhere: both in obvious places, and less obvious ones.

To illustrate, we consider two kinds of symmetry: one in geometry, one in algebra.

- Both cases have **transformations** that capture the symmetries we are interested in.
- Then study *symmetry properties* of certain **objects** w.r.t. these transformations.
- Each object has a **symmetry group** that describes these properties in precise mathematical terms.

Geometric symmetry

Transformations: Isometries.

- An *isometry* of the plane is a bijection $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distances, i.e., $\forall\, x, y \in \mathbb{R}^2$, the distance from $f(x)$ to $f(y)$ equals the distance from x to y.

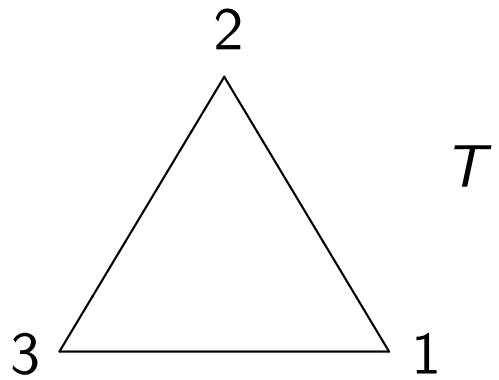
Objects: Figures in the plane (i.e., subsets $A \subseteq \mathbb{R}^2$).

Symmetry group: Isometries that preserve the figure.

- More precisely, for any $A \subseteq \mathbb{R}^2$, let $G_A = \{\text{isometries } f : \mathbb{R}^2 \to \mathbb{R}^2 \text{ st. } f(A) = A\}$.
- G_A is a *group* with composition $f \circ g$ of isometries f, g as the group operation.

Example G1

Let the figure be an equilateral triangle T:



G_T contains • three rotations r, $r^2 := r \circ r$ and $r^3 = e = \mathrm{id}$, where r is an anticlockwise rotation of $2\pi/3$ around the centre of T, and

• three reflections s_1, s_2, s_3 along medians of T through the vertices $1, 2, 3$ respectively.

Question. How do these symmetries act on the vertices?

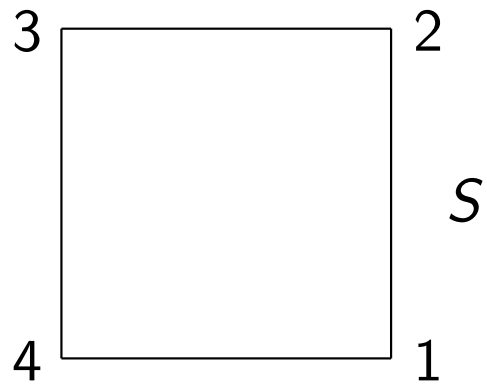
r sends 1 to 2, 2 to 3 and 3 to 1: this is the permutation $(1\ 2\ 3)$.

Similarly r^2 acts by $(1\ 3\ 2)$ and s_1, s_2, s_3 by $(2\ 3)$, $(1\ 3)$, $(1\ 2)$ resp.

Conclude $G_T = S_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

Example G2

Let the figure be a square S:



What is the symmetry group G_S and how does it act on the vertices? Can it be all of S_4?

It can't be because a square has opposite vertices, which must be sent to opposite vertices by any isometry!

For example any symmetry which sends 1 to 2 must send 3 to 4, so $(1\ 2)(3\ 4)$ is induced by a symmetry but $(1\ 2)$ and $(1\ 2\ 3)$ aren't.

Algebraic symmetry

Transformations: Field automorphisms.

A *automorphism* of a field $\mathbb{F}$ is a bijection $f : \mathbb{F} \to \mathbb{F}$ that preserves addition, the zero element, multiplication and the unit element:

$$f(a+b) = f(a) + f(b) \qquad f(0) = 0$$
$$f(ab) = f(a)f(b) \qquad f(1) = 1.$$

Claim. If f is an automorphism of field $\mathbb{F}$ containing $\mathbb{Q}$, then f fixes all the elements in $\mathbb{Q}$.

Why? Any rational number is a ratio of integers, and any integer is plus or minus $1 + 1 + \cdots + 1$ (some number of times). But $f(1) = 1$.

Now turn this idea into a proof...

Proof of claim

First suppose that $n \in \mathbb{Z}^+$ (i.e., a positive integer). Then

$$\begin{aligned} f(n) &= f(1+1+\cdots+1) \\ &= f(1)+f(1)+\cdots+f(1) = 1+1+\cdots+1 = n. \end{aligned}$$

Next observe that for any $a \in \mathbb{F}$ and any $b \neq 0$,

$$f(a)+f(-a) = f(a+(-a)) = f(0) = 0,$$

and

$$f(b)\cdot f(1/b) = f(b\cdot 1/b) = f(1) = 1,$$

so $f(-a) = -f(a)$ and also $f(1/b) = 1/f(b)$.

Hence if n is a negative integer, $f(n) = -f(-n) = -(-n) = n$.

Finally if $q = a/b$ for some integers a, b, where $b \neq 0$, then

$$f(q) = f(a\cdot 1/b) = f(a)\cdot f(1/b) = f(a)\cdot 1/f(b) = a/b = q$$

and we have proved the claim. □

Roots of polynomials

Objects: Polynomials over $\mathbb{Q}$ (elements of $\mathbb{Q}[x]$). Let

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

be a polynomial with coefficients $a_j \in \mathbb{Q}$ and roots $t_1, \ldots t_n \in \mathbb{C}$.

Claim. Let $\mathbb{F}$ be a field containing $\mathbb{Q}$ and $t_1, \ldots t_n$. Then for any automorphism f of $\mathbb{F}$ and any root t of P, $f(t)$ is also a root of P.

Proof.
$$\begin{aligned} P(f(t)) &= a_n f(t)^n + a_{n-1} f(t)^{n-1} + \cdots + a_0 \\ &= f(a_n) f(t)^n + f(a_{n-1}) f(t)^{n-1} + \cdots + f(a_0) \\ &= f(a_n t^n) + f(a_{n-1} t^{n-1}) + \cdots + f(a_0) \\ &= f(a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0) \\ &= f(0) = 0, \end{aligned}$$

where in line two, we use $a_j = f(a_j)$ since $a_j \in \mathbb{Q}$ for all j. □

Hence f permutes $t_1, \ldots t_n$, i.e., $f(t_j) = t_{\sigma(j)}$ for some $\sigma \in S_n$.

The Galois group of a polynomial P

Fact. For any polynomial P over $\mathbb{Q}$, there is a smallest field $\mathbb{F}_P = \mathbb{Q}(t_1, \ldots t_n)$ containing $\mathbb{Q}$ and the roots $t_1, \ldots t_n$ of P.

The symmetry group of P, called its *Galois group*, is defined by:

$$G_P = \{\sigma \in S_n : \sigma \text{ is induced by an automorphism of } \mathbb{F}_P\}.$$

Thus $\sigma \in G_P$ if $\exists$ an automorphism $f : \mathbb{F}_P \to \mathbb{F}_P$ such that $\forall\, j \in \{1, \ldots n\}$, $f(t_j) = t_{\sigma(j)}$.

Trivial Example. Determine G_P where $P(x) = x^2 - 3x + 2$.

Solution. $P(x) = x^2 - 3x + 2 = (x-1)(x-2)$ has roots $t_1 = 1$ and $t_2 = 2$, which are in $\mathbb{Q}$, hence are fixed by every automorphism. Thus $G_P = \{\text{id}\}$ (and $\mathbb{F}_P = \mathbb{Q}(1, 2) = \mathbb{Q}$ in this case).

Example A1

Determine G_T where $T(x) = x^3 - 2$.

T has roots $t_1 = \sqrt[3]{2}$, $t_2 = \sqrt[3]{2}\,\omega$ and $t_3 = \sqrt[3]{2}\,\omega^2$, where $\omega = e^{2\pi i/3}$.

In this case $\mathbb{F}_T = \mathbb{Q}(\sqrt[3]{2}, \omega)$, i.e., is generated by $\sqrt[3]{2}$ and ω.

Complex conjugation $z \mapsto \overline{z}$ is a field automorphism (recall that $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\,\overline{b}$).

Since $\omega^2 = e^{4\pi i/3} = e^{-2\pi i/3} = \overline{\omega}$, complex conjugation swaps t_2 and t_3 but fixes t_1. So the permutation $(2\ 3)$ is in G_T.

Now consider field automorphisms $f : \mathbb{F}_T \to \mathbb{F}_T$ which fix ω (and hence also ω^2). So we only need to say what f does to $t_1 = \sqrt[3]{2}$. Suppose $f(t_1) = t_2 = \sqrt[3]{2}\,\omega$; then to make a field automorphism we must define $f(t_2) = f(\sqrt[3]{2}\,\omega) = f(\sqrt[3]{2})f(\omega) = \sqrt[3]{2}\,\omega^2 = t_3$. This field automorphism thus induces the permutation $(1\ 2\ 3)$.

By composing these symmetries, it follows that $G_T = S_3$.

Example A2

Determine G_S where $S(x) = x^4 - 4x^2 - 2$.

There are two roots for x^2, given by $2 \pm \sqrt{6}$, so roots of S are $t_1 = \sqrt{2+\sqrt{6}}$, $t_2 = \sqrt{2-\sqrt{6}}$, $t_3 = -t_1$ and $t_4 = -t_2$.

What is G_S? Can it be all of S_4?

It can't! We proved already that for any field automorphism f, $f(-a) = -f(a)$, so two roots which are negatives of each other are sent to two roots which are negatives of each other.

For example any automorphism sending t_1 to t_2 must send $t_3 = -t_1$ to $t_4 = -t_2$. So $(1\ 2)(3\ 4) \in G_S$ but $(1\ 2)$ and $(1\ 2\ 3)$ aren't.

So $S(x)$ is just like the square, and $T(x)$ is just like the triangle!

From Geometry to Group Theory

Symmetry in geometry has been studied since ancient Egyptians and Babylonians.

- Euclidean geometry studies properties that are preserved by isometries (e.g., angle, length, area, triangles).
- During 18th and 19th centuries, 'non-Euclidean' geometries were introduced (e.g., hyperbolic, spherical, affine and projective geometries)
- Felix Klein (1872) realized that these geometries are described by symmetries (the permitted transformations).

In contrast, the appearance of symmetry in algebra was *totally unexpected*, and *completely revolutionary*.

This sparked the development of group theory, thanks almost entirely to the work of one extraordinary mathematician, one night in 1832, the night before he was killed in a duel, aged only 21.

This mathematician was **Évariste Galois**.

Solving polynomials by radicals

A polynomial equation $P(x) = 0$ is *solvable by radicals* if its roots can be computed from coefficients of P by repeatedly applying arithmetic operations and kth root operations $\sqrt[k]{\cdot}$.

Examples. Any quadratic equation $ax^2 + bx + c = 0$ is solvable by radicals, using e.g. for $a \neq 0$ the famous formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The cubic equation $x^3 + ax^2 + bx + c = 0$ is solved by:

$$x = -\frac{a}{3} + \sqrt[3]{\frac{-2a^3+9ab-27c+\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}} + \sqrt[3]{\frac{-2a^3+9ab-27c-\sqrt{(2a^3-9ab+27c)^2+4(-a^2+3b)^3}}{54}}.$$

There is also a very complicated formula for quartics!

General quintics are not solvable by radicals

For years, many thought there would be general formulae for all polynomials—they would just get (rapidly!) more complicated.

This was quashed by Abel in 1824, who showed that there is no general formula for solving quintic equations by radicals...

...And Galois explained why: taking a kth root introduces symmetry, because there are k such roots, which are permuted by a cyclic group of order k. Galois concluded that if P is solvable by radicals then G_P must be built from cyclic groups in a specific way. Such groups are now called *solvable*.

Theorem (Galois). P is solvable by radicals iff G_P is solvable.

Fact. For all $n \in \mathbb{Z}^+$ there is a degree n polynomial P with $G_P = S_n$.

Theorem. S_n is solvable iff $n \leqslant 4$. (We will prove this!)

Corollary. $\forall\, n \geqslant 5\ \exists$ a degree n polynomial which is not solvable by radicals.

Summary: whither group theory?

Symmetry pervades mathematics. This unit makes some small steps towards understanding the following questions.

- Q1 What symmetries are out there?
  In other words, what groups are there? (Classification)
- Q2 What are their properties? In other words, how are these groups built out of simpler pieces? (Structure Theory)

Any finite group is built from pieces called *simple groups*, and is solvable if and only if its pieces are cyclic groups.

In 1981, it was announced that all finite simple groups had been classified. The proof is spread across many articles by many mathematicians, totalling more than 10000 journal pages. We probably won't have time to cover it in this course...

...and it is therefore not examinable.