Comment. 0.1. Hey Aaron, I'm leaving comments on your todonotes using this environment. Feel free to make up problems for the topics you mentioned. We can then rearrange, clean, purge the rest of the notes and make them more coherent and presentable.

1 The Discriminant

Many of the problems have too many hints. We should throw away the hints and suggestions which are too trivial for MC students, it's better to have them discuss and struggle in class. We should also have some hard optional problems (like the $\mathbb{Z}/p$ polynomial counting) which students can try to solve in TAU.

> In mathematics you don't understand things. You just get used to them.
>
> John von Neumann

We'll start by analyzing polynomials using good old calculus. There is an algebraic invariant, called the *discriminant*, that has a geometric interpretation coming from calculus on one hand and an algebraic interpretation coming from the properties of the roots of the polynomials on the other.

The **discriminant of a polynomial** is a number which can be computed using only the coefficients of the polynomial and which is 0 precisely when the polynomial has repeated roots. There is no reason, a priori, to expect that such an number should exist but it does, and you've encountered it already for the quadratic equation.

1.1 Quadratic

Let us start with the simplest case. Consider the quadratic polynomial x^2+bx+c with roots α_1 and α_2.

Q.1. Express b, c in terms of α_1, α_2.

Q.2. What are the conditions on the coefficients b, c under which

a) $\alpha_1 = \alpha_2$,

b) α_1, α_2 are both real,

c) α_1, α_2 are both non-real.

Is it possible for exactly one of α_1 and α_2 to be real?

Note that the answers to these questions depend on a single number. This number, denoted Δ (delta), is called the **discriminant** of the quadratic polynomial.

Q.3. Express the discriminant Δ in terms of α_1, α_2.

1.2 Cubic

Moving on to the next degree, consider the following cubic with roots $\beta_1, \beta_2, \beta_3$.

$$P(x) = x^3 + a_2x^2 + a_1x + a_0$$

Q.1. Express a_2, a_1, a_0 explicitly in terms of $\beta_1, \beta_2, \beta_3$.

We'll first get rid of the coefficient on x^2 to simplify our computations.

Q.2. a) Find the coefficients of the polynomial $P_k(x)$ whose roots are

$$\beta_1 + k, \beta_2 + k, \beta_3 + k$$

where k is a constant, in terms of the coefficients of $P(x)$.

b) Find the value of k for which the coefficient of x^2 in $P_k(x)$ is 0.

The value of k only depends on the coefficients of $P(x)$ and hence we can simplify our polynomial **without knowing the roots**.

c) For the polynomial $P(x) = x^3 + 3x^2 + 1$ use find the polynomial $P_k(x)$ whose x^2 coefficient is 0. What is the relationship between the roots of $P(x)$ and $P_k(x)$?

d) Repeat the same exercise for the polynomial $x^3 - 3x^2 + 3x - 1$.

1.3 Graphing the cubic

From now on we'll assume that our cubic is of the form:

$$P(x) = x^3 + px + q \tag{1.1}$$

We'll further assume $p < 0$ for simplicity. Such a cubic is sadly called a **depressed cubic**. With roots $\beta_1, \beta_2, \beta_3$ we've the relations

$$\begin{aligned} 0 &= \beta_1 + \beta_2 + \beta_3 \\ p &= \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 \\ -q &= \beta_1\beta_2\beta_3 \end{aligned}$$

There are four possible cases for the roots.

Case 0	all three roots equal
Case 1	all three roots distinct and real
Case 2	one repeated real root
Case 3	two complex roots

Q.3. a) Convince yourselves that these cases are mutually exclusive and that are no other possibilities. Can $P(x)$ have no real root? Can $P(x)$ have a repeated complex root? all three roots complex (not real)?

b) Case 0 is trivial, what are the roots in this case? What are p, q in this case?

Q.4. Draw the (qualitatively correct) graphs of $P(x)$ in each of the four cases.

Q.5. By analyzing the graph of $P(x)$, determine the relationship between the roots of $P(x)$ and $P'(x)$ for each of the three cases: Case 1 (distinct real), Case 2 (repeated real), Case 3 (complex).

Each of these cases are in fact completely determined by the coefficients p, q. This is because $P'(x)$ is a friendly quadratic equation whose roots are easy to find.

Q.6. a) Find the roots of $P'(x)$.

b) Use your answers to the previous questions to determine the conditions on the coefficients p, q corresponding to the three cases.

Assuming you did the calculations correctly you should get conditions of the following form for some number Δ.

$$\begin{aligned} \Delta > 0 &\implies P(x) \text{ has three real roots} \\ \Delta = 0 &\implies P(x) \text{ has a repeated root} \\ \Delta < 0 &\implies P(x) \text{ has exactly one real root} \end{aligned}$$

These are exactly the relations we had for a quadratic!

1.4 The Discriminant of the Cubic

By the previous section the roots of our polynomial are distinct real, repeated or complex according to whether the value of the polynomial is -ve, 0 or +ve at the roots of it's derivative $\sqrt{-p/3}$, or the opposite for $-\sqrt{-p/3}$.

Q.7. Simplify the condition

$$P\left(\sqrt{-p/3}\right) = 0$$

to the form $-4p^3 - 27q^2 = 0$. Similar simplifications are possible for the conditions $P(\sqrt{-p/3}) < 0$ and > 0.

Using the other root $-\sqrt{-p/3}$ we surprisingly get the *exact* same conditions. Thus we've (almost) proved the following theorem.

Theorem 1.1. *The cubic $P(x) = x^3 + px + q$ has distinct real, repeated, or complex roots, according to whether the* ***discriminant*** *of $P(x)$*

$$\Delta = -4p^3 - 27q^2$$

is positive, 0 or negative.

Q.8. Determine whether the following polynomials have distinct real, repeated or complex roots.

a) $x^3 + 1$

b) $x^3 - 1$

c) $x^3 - 3x + 2$

d) $x^3 - 3x + 1$

e) (optional) $x^3 + 3x^2 + 1$

Q.9. a) What is the value of q for which $x^3 - 3x + q$ has distinct real roots, repeated roots, and complex roots respectively.

b) In the case when $x^3 - 3x + q$ has repeated roots, find the roots.

1.5 The Roots & the Discriminant

As in the case of a quadratic ($b^2 - 4c = (\alpha_1 - \alpha_2)^2$) there is a surprising relation between Δ and the roots $\beta_1, \beta_2, \beta_3$.

Theorem 1.2.

$$-4p^3 - 27q^2 = (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2$$

The proof of this theorem is very cumbersome, we'll only verify it for some cases.

Is there a way to motivate this? Or have an *elegant* proof which is something less that brute verification.

Q.10. a) Argue directly that

$$\begin{aligned} P(x) \text{ has distinct real roots} &\Rightarrow (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2 > 0 \\ P(x) \text{ has a repeated root} &\Rightarrow (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2 = 0 \end{aligned}$$

b) For the complex roots case, assume that β_1 is real and, β_2 and β_3 are complex. Show that

$$\beta_2 = -\beta_1/2 + i\beta' \text{ and } \beta_2 = -\beta_1/2 - i\beta'$$

for some real number β'. Prove that in this case

$$(\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2 < 0$$

Q.11. For $\beta_1 = 0$, $\beta_2 = 1$, $\beta_3 = -1$,

a) Compute $(\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2$.

b) Compute the coefficients p, q of the polynomial $P(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$.

c) Compute $-4p^3 - 27q^2$.

Q.12. (optional) If you're feeling ambitious prove Proposition 1.2 by expanding and simplifying the left and the right hand sides.

1.6 Symmetries & the Discriminant

There are generalizations of 1.2 for all degrees i.e. we can always express "the product of the squares of pairwise differences of roots" as a polynomial in the coefficients.

The coefficients satisfy the equations

$$\begin{aligned} 0 &= \beta_1 + \beta_2 + \beta_3 \\ p &= \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 \\ -q &= \beta_1\beta_2\beta_3 \end{aligned}$$

The right hand sides of these equations are called **elementary symmetric polynomials** (a symmetric polynomial is a multivariable polynomial which remains unchanged if we permute the β_i's). They are called *elementary* because of the following theorem.

Theorem 1.3 (Fundamental Theorem of Symmetric Polynomials)**.** *Every symmetric polynomial can be expressed uniquely as a polynomial in the elementary symmetric ones.*

This theorem is surprisingly easy to prove once you know your induction well. Try the next problem to get an idea of how the proof of this theorem goes in general.

Q.13. a) Express $\beta_1^2 + \beta_2^2 + \beta_3^2$ in terms of p, q. [*]

b) Why is the expression $\beta_1^2\beta_2 + \beta_2^2\beta_3 + \beta_3^2\beta_1$ not symmetric? What terms can you add to it to make it symmetric. Express the resulting polynomial in terms of p, q. [†]

The discriminant $(\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2$ is also symmetric in $\beta_1, \beta_2, \beta_3$ (do you see why?) and hence can be written as a polynomial in the elementary symmetric ones, which turns out to be $-4p^3 - 27q^2$.

This is the simplest connection between symmetries and polynomials. Galois' insight involved studying polynomials with *fewer* symmetries.

Comment. 1.4. I love the idea of having problems connecting repeated roots, discriminant, and polynomials having same roots. If you can think of some concrete problems feel free to add them here.

Comment. 1.5. Polynomials over finite fields might be a little too much. But we can add these questions in as a bonus, optional problems for the more advanced students.

possibly add subsection on counting number of square-free polynomials over Z/p it's a fun motivic induction on the number of square factors

maybe also discuss number of pairs of polynomials with a common root, the formula being the same is no coincidence

[*] Hint: Expand $(\beta_1 + \beta_2 + \beta_3)^2$.

[†] Hint: Expand $(\beta_1 + \beta_2 + \beta_3)(\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1)$

2 Solving the cubic

There is no unique way to find the roots of the cubic. We'll choose the method that is motivated by Galois theory. It'll look extremely mysterious but this is the method that generalizes to show that there is no formula for solving a general fifth degree polynomial.

The fundamental theorem of algebra guarantees the existence of *real or complex roots* to any polynomial, as such complex numbers naturally show up when studying polynomials.

Q.1. a) Find the three roots of the polynomial $x^3 - 1$.

b) Show that if one complex root of this equation is ω then the other complex root is ω^2. Conclude that $\overline{\omega} = \omega^2$.

c) Compute $\omega + \omega^2$.

d) Plot ω, ω^2 on the complex plane.

ω and ω^2 (and also 1) are called the **third roots of unity** as they satisfy $x^3 = 1$.

Q.2. What are the *second* and the *fourth* roots of unity? Plot them on the complex plane.

2.1 The Solution

The method for solving the cubic is somewhat like induction, we reduce the problem to a lower degree one. We need to find intermediate constants μ_1 and μ_2 which satisfy a known *quadratic* and from which $\beta_1, \beta_2, \beta_3$ can be easily recovered.

Define

$$\mu_1 = \beta_1 + \beta_2\omega + \beta_3\omega^2 \tag{2.1}$$

$$\mu_2 = \beta_1 + \beta_2\omega^2 + \beta_3\omega \tag{2.2}$$

Recall that we also have a third equation

$$0 = \beta_1 + \beta_2 + \beta_3 \tag{2.3}$$

Q.3. Determine $\mu_1.\mu_2$ in terms of p, q.

Q.4. a) Verify that the following solves the equations (2.1), (2.2), and (2.3)

$$\beta_1 = \frac{\mu_1 + \mu_2}{3} \ , \ \beta_2 = \frac{\omega^2\mu_1 + \omega\mu_2}{3} \ , \ \beta_3 = \frac{\omega\mu_1 + \omega^2\mu_2}{3}$$

Note that we have three simultaneous (non-degenerate) equations and three variables so there is a unique solution.

b) Compute $\beta_1.\beta_2.\beta_3$ in terms of μ_1, μ_2.

c) Use this to compute $\mu_1^3 + \mu_2^3$ in terms of p, q.

Q.5. Find the coefficients of the quadratic polynomial whose roots are μ_1^3, μ_2^3 and hence find μ_1^3 and μ_2^3 in terms of p, q.

Assuming you did the computations in the previous problems correctly, you should now have the following method for finding the roots of the cubic $P(x) = x^3 + px + q$,

- Solve the quadratic
$$x^2 + 27q.x - 27p^3 = 0$$
and pick μ_1^3 to be any one of the two roots and hence find μ_1.[‡]
- Find μ_2 using
$$\mu_1\mu_2 = -3p$$
- The three roots are given by
$$\beta_1 = \frac{\mu_1 + \mu_2}{3}\ ,\ \beta_2 = \frac{\omega^2\mu_1 + \omega\mu_2}{3}\ ,\ \beta_3 = \frac{\omega\mu_1 + \omega^2\mu_2}{3}$$

If the cubic is not depressed then we first need to shift the roots to get rid of the x^2 coefficient.

Q.6. Use the above method to find the roots of

a) $x^3 - 1$

b) $x^3 + 1$

c) $x^3 - 3x + 2$

d) $x^3 - x$

[‡] Just as (unless $a = 0$) the equation $x^2 = a^2$ has 2 solutions $\pm a$ the equation $x^3 = a^3$ has 3 solutions $a, a\omega, a\omega^2$. Hence we need to *choose* a value of μ_1 once we know what μ_1^3 is. The choice does not matter as choosing a different cube root simply permutes the roots. But the same is true for μ_2 and suddenly we have 9 choices instead of 3, hence we use the equation $\mu_1\mu_2 = -3p$ to determine μ_2.

2.2 Symmetries & the Cubic

What just happened?

The secret reason why the above method worked is that μ_1^3, μ_2^3 remain unchanged when we cyclically permute the three roots, but not when we swap just two of them.

Q.7. a) Compute $\omega\mu_1$ and $\omega^2\mu_1$, similarly for μ_2.

b) Use these to show that if we cyclically permute $\beta_1, \beta_2, \beta_3$ then μ_1^3 and μ_2^3 remain unchanged.

c) Verify that if we swap β_2 and β_3 then μ_1^3 and μ_2^3 also get swapped.

d) (optional) Show that if we swap β_1 and β_2 (or β_1 and β_3) then μ_1^3 and μ_2^3 also get swapped.

e) Argue that $\mu_1^3 + \mu_2^3$ and $\mu_1^3.\mu_2^3$ are symmetric in $\beta_1, \beta_2, \beta_3$ (but not μ_1^3, μ_2^3 individually), and hence they are the roots of a quadratic whose coefficients are polynomials in p, q.[§]

Galois' work then proves that this is the only method that can give us a *general* formula involving radicals. He then went on to show that no such intermediate variables exist for a fifth degree polynomial.

There is another pair which we've already encountered that also has these symmetries.

$$\begin{aligned}\sqrt{\Delta} &= (\beta_1 - \beta_2)(\beta_2 - \beta_3)(\beta_3 - \beta_1)\\ -\sqrt{\Delta} &= (\beta_2 - \beta_1)(\beta_3 - \beta_2)(\beta_1 - \beta_3)\end{aligned}$$

Q.8. Verify that both $\sqrt{\Delta}$ and $-\sqrt{\Delta}$ remain unchanged under cyclic permutation of roots and get swapped when we swap two of the β_i's.

This isn't a coincidence, you can rewrite the solutions you found in terms of $\pm\sqrt{\Delta}$. In fact *any* variables with these symmetries should provide us with a solution to the cubic, which variables we use is a matter of convenience.

Q.9. Go back to your formulae for μ_1^3 and μ_2^3 and express them them terms of p, q and Δ.

[§] These statements are false for μ_1 and μ_2 (instead of μ_1^3 and μ_2^3) and so there is no quadratic, with coefficients polynomials in p, q, whose roots are μ_1, μ_2.

3 Solving the Quartic

The purpose of computation is insight, not numbers.

Richard Hamming

Moving on to the fourth degree, the idea is the same. The method gets much more complicated, and isn't quite useful in practice. You should aim at understanding the ideas and move on.

Consider a *depressed quartic* with roots $\gamma_1, \gamma_2, \gamma_3, \gamma_4$:

$$P(x) = x^4 + a_2x^2 + a_1x + a_0$$

As before, to simplify the calculations we're forcing

$$0 = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$$

If $a_0 = 0$ we can factor out an x and reduce the quartic to a cubic. So we'll assume this is not the case.

Q.1. Express a_2, a_1, a_0 in terms of $\gamma_1, \gamma_2, \gamma_3, \gamma_4$.

We need to find an intermediate third degree polynomial with roots $\lambda_1, \lambda_2, \lambda_3$ which have *fewer* symmetries than a_2, a_1, a_0.

... and here they are:

$$\begin{aligned}\lambda_1 &= \gamma_1\gamma_2 + \gamma_3\gamma_4\\ \lambda_2 &= \gamma_1\gamma_3 + \gamma_2\gamma_4\\ \lambda_3 &= \gamma_1\gamma_4 + \gamma_2\gamma_3\end{aligned}$$

Q.2.
a) How many ways are there to permute the 4 roots $\gamma_1, \gamma_2, \gamma_3, \gamma_4$?

b) Of these, which permutations leave *all* the λ_i's unchanged?

c) What do the rest of the permutations do to the λ_i's?

d) Conclude that $\lambda_1 + \lambda_2 + \lambda_3$, $\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1$ and $\lambda_1\lambda_2\lambda_3$ are symmetric in $\gamma_1, \gamma_2, \gamma_3, \gamma_4$.

By the previous exercise the coefficients of the cubic polynomial whose roots are $\lambda_1, \lambda_2, \lambda_3$ are polynomials in a_2, a_1, a_0.

Q.3. Verify the following identities (only for the intrepid)

$$\begin{aligned} a_2 &= \lambda_1 + \lambda_2 + \lambda_3 \\ -4a_0 &= \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 \\ a_1^2 - 4a_0a_2 &= \lambda_1\lambda_2\lambda_3 \end{aligned}$$

and hence $\lambda_1, \lambda_2, \lambda_3$ are the roots of

$$R(x) = x^3 - a_2x^2 - 4a_0x + (4a_0a_2 - a_1^2)$$

Thus we've reduced the problem from a quartic to a cubic. The last step is recovering $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ from $\lambda_1, \lambda_2, \lambda_3$. For this notice that

$$\begin{aligned} \lambda_1 &= \gamma_1\gamma_2 + \gamma_3\gamma_4 \\ a_0 &= \gamma_1\gamma_2\gamma_3\gamma_4 \end{aligned}$$

and hence $\gamma_1\gamma_2$ and $\gamma_3\gamma_4$ are the roots of the quadratic $x^2 - \lambda_1 x + a_0$. Similarly for the others. We have the identities

$$\lambda_1^2 = (\lambda_1\lambda_2).(\lambda_1\lambda_3).(\lambda_1\lambda_4)/a_0$$

which we can use to find λ_1^2 and then test the two possible square roots to see which one works. The other λ_i's can be found by inspection.

Q.4. Find the roots of the following polynomials:

a) $x^4 - 1$

b) $x^4 + 1$

4 Symmetry groups

> Mathematics is the art of giving the same name to different things.
>
> Henri Poincare

4.1 Multiplying permutations

Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. The **symmetry group of n elements**, S_n, is defined to be the set of all permutations of n elements. We think of the permutations as *functions* $[n] \to [n]$. For example, the element $\sigma = (1\,2\,4\,3)$ denotes the function $\sigma : [4] \to [4]$ which sends $\sigma(1) = 1, \sigma(2) = 2, \sigma(3) = 4, \sigma(4) = 3$,

$$\begin{aligned} 1 &\mapsto 1 \\ 2 &\mapsto 2 \\ 3 &\mapsto 4 \\ 4 &\mapsto 3 \end{aligned}$$

This simple change in perspective now allows us to **multiply** two permutations, by simply composing the corresponding functions. For example, the element $\sigma = (1243)$ and $\tau = (4123)$ the *product* $\sigma \cdot \tau = (4\,1\,3\,2)$

$$\begin{aligned} 1 \mapsto^{\sigma} 1 \mapsto^{\tau} 4 \\ 2 \mapsto^{\sigma} 2 \mapsto^{\tau} 1 \\ 3 \mapsto^{\sigma} 4 \mapsto^{\tau} 3 \\ 4 \mapsto^{\sigma} 3 \mapsto^{\tau} 2 \end{aligned}$$

Note that this is like *applying* σ to τ.

Q.1. For $e = (1\,2), \tau = (2\,1) \in S_2$ compute: $e \cdot e, e \cdot \tau, \tau \cdot e, \tau \cdot \tau$

Q.2. For $\sigma = (2\,3\,1), \tau = (2\,1\,3) \in S_3$ compute

a) $\sigma \cdot \sigma$, $\sigma \cdot \sigma \cdot \sigma$

b) $\sigma \cdot \tau$, $(\sigma \cdot \tau) \cdot (\sigma \cdot \tau)$

c) $\tau \cdot \sigma$

d) Write all the elements of S_3 in terms of σ and τ.

Because $\sigma \cdot \tau \neq \tau \cdot \sigma$ we say that S_3 is **non-abelian**.

4.2 Subgroups

Q.3. Let $e = (1\,2\,3\,\cdots\,n) \in S_n$. Let σ be any permutation in S_n.

a) Compute $e \cdot \sigma$ and $\sigma \cdot e$.

b) Find an element τ such that $\tau \cdot \sigma = e$ and $\sigma \cdot \tau = e$.

Hence e is called the (group) **identity** in S_n and $\tau = \sigma^{-1}$ is called the **inverse** of σ.

c) Explicitly find the inverses of all the elements of S_3.

A set with (associative) multiplication, an identity, and inverses is called a **group**.

A subset $G \subseteq S_n$ which is itself a group is called a **subgroup** of S_n i.e. G is a subgroup of S_n if

- (contains identity) $e \in G$
- (closed under inverses) $g \in G \implies g^{-1} \in G$
- (closed under multiplication) $g, h \in G \implies g \cdot h \in G$

Q.4. Show that $\{e\}$ is a subgroup of any S_n. This is called the **trivial group**.

Q.5. Let $\sigma = (3\,1\,2), \tau = (2\,1\,3) \in S_3$.

a) Show that $\{e, \tau\}$ is a subgroup of S_3.

b) What element(s) do you need to add to $\{e, \sigma\}$ to make it a subgroup of S_3?

c) What element(s) do you need to add to $\{e, \tau, \sigma\}$ to make it a subgroup of S_3?

Q.6. List all the subgroups of S_3.

Q.7. For $\sigma = (2\,3\,\cdots\,n\,1) \in S_n$,

a) Find σ^k.

b) Find σ^{-1}.

c) What are the elements that needs to be added to the set $\{e, \sigma\} \subseteq S_n$ to make it a subgroup?

4.3 Group Actions

Groups naturally occur as symmetries of mathematical objects, S_n is the symmetry group of a set of n elements. But the same group can show up as the symmetries of multiple objects. We think of the group as **acting** on the object via some self-transformations.

For example, S_3 *acts* an equilateral triangle with vertices labelled $\{1, 2, 3\}$ via geometrical transformations (rotations and reflections): $\sigma = (2\ 1\ 3)$ *acts* via rotating the triangle counterclockwise by $2\pi/3$ and $\tau = (2\ 1\ 3)$ *acts* via reflecting along one of the bisectors. On the other hand S_3 does not act naturally on, say, an isosceles triangle, in this case the natural symmetry group is S_2 which acts by reflecting along *the* bisector. For a scalene triangle, the natural symmetry group is the trivial group.

Q.8. a) How many geometrical transformations are there of a square?

b) S_4 does not act naturally on a square. What is an example of an element of S_4 which does not correspond to any geometrical transformation?

c) What is the *subgroup* of S_4 that acts via geometrical transformations?

Q.9. Generalize the above problem to a regular n-gon. These groups are called the **dihedral groups**, denoted D_{2n}. (why $2n$?)

Q.10. If we restrict only to rotations and do not allow reflections, then S_4 does not naturally act on a tetrahedron.

a) What is an example of an element of S_4 which does not correspond to any rotation of the tetrahedron?

b) Describe how the other elements of S_4 act on the tetrahedron.

c) How many rotational symmetries does the tetrahedron have? What is the rotational symmetry group?

The rotational symmetry group of a cube is also extremely interesting and easy to understand, try reading about it online.

5 Symmetries & Polynomials

> Out of nothing I have created a strange new universe.
>
> Janos Bolyai

We need one last definition, that of a normal subgroup, to understand the Galois' ideas using the language of group theory.

5.1 Cycle decomposition and Normality

Every permutation naturally breaks up as cycles. For example $(3\,4\,1\,5\,2) \in S_5$ breaks up as,

$$(3\,4\,1\,5\,2) \rightsquigarrow 1 \mapsto 3 \mapsto 1 \text{ and } 2 \mapsto 4 \mapsto 5 \mapsto 2$$

We say that $(3\,4\,1\,5\,2)$ has a **cycle decomposition** $[1\,3][2\,4\,5]$ and **cycle type** $2+3$. The order of the cycles and of the elements within the cycles is not relevant. We can rewrite the above permutation as having a cycle decomposition $[4\,5\,2][1\,3]$ and cycle type $3+2$.

The cycle decomposition is the more common way of writing permutations, but it is harder to multiply two permutations when they're written in the cycle notation and needs some getting used to.

Q.1. Determine cycle decompositions and cycle types of all the elements of S_3.

Q.2. What are the possible cycle types for elements in S_4? How many elements are there in each cycle type (this is a long problem, patience is the key here).

A subgroup $G \subseteq S_n$ is called **normal** if it satisfies the following property:

if it contains one element of a certain cycle type then it contains *all* the elements of that cycle type.

Q.3. Determine which of the subgroups of S_3 are normal.¶

Q.4.
a) Find the cycle type of $e \in S_n$.
b) What other elements of S_n have the same cycle type as e?
c) Argue that the trivial group is a normal subgroup of S_n. (Also note that S_n itself is a normal subgroup.)

¶Just so that we're all on the same page S_3 has 6 subgroups: $\{e\}$, $\{e, (1\,3\,2)\}$, $\{e, (3\,2\,1)\}$, $\{e, (2\,1\,3)\}$, $\{e, (2\,3\,1), (3\,1\,2)\}$, and S_3 itself.

5.2 Normal subgroups of S_n

Suppose a permutation $\sigma \in S_n$ has a cycle type $a_1 + a_2 + \cdots + a_k$ then we say that σ is an **even permutation** if $(a_1 - 1) + (a_2 - 1) + \cdots + (a_k - 1)$ is even, **odd** otherwise. This is also called the **parity** of the permutation.

For example, $\sigma = (3\,4\,1\,5\,2)$ has cycle type $2 + 3$ and $(2-1)+(3-1) = 1+2 = 3$ is odd, hence the parity of $(3\,4\,1\,5\,2)$ is an odd permutation.

Q.5. a) Determine which permutations of S_3 are even and which ones are odd.

b) Determine which cycle types of S_4 correspond to even permutations and which ones to odd permutations, hence count the number of even and odd permutations in S_4.

c) What is the parity of the identity $e = (1\,2\,\cdots\,n) \in S_n$?

As it turns out the subset containing all the even permutations forms a normal subgroup of S_n, denoted A_n, called the **alternating group** and has size $n!/2$. (We'll assume this fact.)

Q.6. a) What is the subgroup A_3?

b) What is the subgroup A_4? Have you encountered this subgroup before?

A_n is the only true friend S_n has.

Theorem 5.1. *Every S_n, for $n > 4$, has exactly 3 normal subgroups $\{e\}$, A_n and S_n*

There is no deep reason why this theorem is true, it is simply a matter a computing the normal subgroups carefully. This is a recurring phenomenon in group theory, seemingly elementary mathematical objects have very structured symmetric groups, and these then give rise to very beautiful and deep mathematics.

dumb objection, but arguably there might be some deep reason like SL_n is simple as an algebraic group and $A_n = SL_n(F_1)$, but of course F_1 makes no sense

Comment. 5.2. Haha, with a tropical geometer around the camp this summer let's add this in :D

5.3 Normal subgroups of S_4

By direct computations we can find all the normal subgroups of S_4. We'll need the following theorem about subgroups.

Theorem 5.3. *The size of a subgroup divides the size of the total group.*

Q.7. a) Verify the above theorem for S_3.

b) Verify the above theorem for $\{e\}, A_4, S_4$, as subgroups of S_4.

c) Verify the above theorem of the dihedral groups D_{2n} which are subgroups of S_n.

We already know 3 normal subgroups of S_4: $\{e\}, A_4, S_4$. It turns out there is exactly one more called the **Klein 4-group**, denoted K_4.

Q.8. a) What are the possible sizes of subgroups of S_4?

b) Show that S_4 has exactly 4 normal subgroups: $\{e\}, K_4, A_4, S_4$.
(You'll need to use the number of elements in each cycle type of S_4 that you've already computed in **Q.2.** Remember that if a normal subgroup contains one element of a certain cycle type then it must contain all the elements with that cycle type.)

This is the fortunate accident that allows us to solve the quartic. This does not occur for any other S_n.

discuss klein 4 group in context of S_4/A_4 as symmetries of cube

Comment. 5.4. This is a very nice idea. I wish I had thought of this!

5.4 The Cubic and the Quartic

Comment. 5.5. Oh, this is an interesting observation, I had not thought of this. Yes definitely let's put this in somewhere where we introduce symmetry groups.

discuss cross ratio as fixed by klein 4, maybe this goes earlier?

Comment. 5.6. I actually do not know either of these two comments very well. If you want to make some problems please go for it, I'll also learn something.

possibly discuss recovering the quartic from a degree 2 extension of the cubic

possible bonus exercise on connection to genus 1 curves and associated elliptic curves, 2-torsion?

We'll now return to polynomials and understand our methods using the language of symmetric groups.

The symmetry groups S_n naturally acts on a set of n variables, but more importantly it also acts on the set of all polynomials in n variables. For example, the permutation $(1\ 3\ 2)$ sends $\beta_1\beta_2^2 + \beta_3$ to $\beta_1\beta_3^2 + \beta_2$. Let us go back to the cubic and quartic and analyze them using this new language.

Recall that we had the following intermediate variables for the cubic

$$\sqrt{\Delta} = (\beta_1 - \beta_2)(\beta_2 - \beta_3)(\beta_3 - \beta_1) \text{ and } -\sqrt{\Delta} = (\beta_2 - \beta_1)(\beta_3 - \beta_2)(\beta_1 - \beta_3)$$

Q.9. a) Identify the *subgroup* of S_3 that fixes *both* $\sqrt{\Delta}$ and $-\sqrt{\Delta}$.

b) What is the subgroup of S_3 that fixes all the symmetric variables corresponding to the coefficients: $\beta_1\beta_2\beta_3$, $\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1$, and $\beta_1 + \beta_2 + \beta_3$.

c) What is the subgroup of S_3 that fixes the individual variables $\beta_1, \beta_2, \beta_3$.

This problem generalizes to all n.

Similarly we had the following intermediate variables for the quartic

$$\lambda_1 = \gamma_1\gamma_2 + \gamma_3\gamma_4 \text{ and } \lambda_2 = \gamma_1\gamma_3 + \gamma_2\gamma_4 \text{ and } \lambda_3 = \gamma_1\gamma_4 + \gamma_2\gamma_3$$

Q.10. Identify the *subgroup* of S_4 that fixes *all* the elements $\lambda_1, \lambda_2, \lambda_3$.

Notice that all the groups you've computed above are normal subgroups.

Galois correspondence: Galois' theorem states that there is a one-to-one correspondence between (sequence of) *intermediate variables*[‖] in the roots of polynomials of degree n and (sequence of) normal subgroups of S_n. As mentioned earlier a general polynomial can be solved by radicals only if there exists (sequence of) intermediate variables of lower degrees.

I had a vague idea of talking about cyclotomic polynomials and subgroups of cyclic groups. I ran out of time for one, and could not come up with manageable problems for another. I would love it if you have any suggestions about this.

For any S_n the correspondence is

$$\begin{aligned} \{e\} &\leftrightarrow \text{ roots} \\ A_n &\leftrightarrow \{+\sqrt{\Delta}, -\sqrt{\Delta}\} \\ S_n &\leftrightarrow \text{ coefficients} \end{aligned}$$

For S_3 this correspondence is enough as we've already seen that μ_1^3, μ_2^3 could be expressed in terms of $\pm\sqrt{\Delta}$, and it is possible to recover the roots from these.

For $S_n, n \geq 4$ knowing $\{+\sqrt{\Delta}, -\sqrt{\Delta}\}$ is not enough to recover the roots.

However we get lucky for S_4, as S_4 has a special normal subgroup K_4 and the variables $\{\lambda_1, \lambda_2, \lambda_3\}$ corresponding to this normal subgroup do indeed satisfy a lower degree (cubic) polynomial and the roots can be recovered from these.

$$K_4 \leftrightarrow \{\lambda_1, \lambda_2, \lambda_3\}$$

But because S_5 does not have this accidental normal subgroup, there are not enough intermediate variables which could allow us to find a general formula using radicals. This then is the underlying reason why a quintic polynomial cannot be solved using radicals: as S_5 has very few normal subgroups!!![**]

For further reading: If you're interested in learning more about this you should start by some group theory in more details. One of my favorite algebra book for beginners is *Algebra*, by Michael Artin.

[‖] We need the concept of a *field* to make this more precise.

[**] A more precise statement is that A_5 has no normal subgroups.