Symmetries and Polynomials

Aaron Landesman and Apurva Nakade

April 6, 2021

Introduction

In this class we'll learn how to solve a cubic. We'll also sketch how to solve a quartic. We'll explore the connections between these solutions and group theory. Towards the end, we'll hint towards the deep connection between polynomials and groups via Galois Theory. This connection allows one to convert the classical question of whether a general quintic can be solved by radicals to a group theory problem, which can be relatively easily answered.

The 5 day outline is as follows:

1. The first two days are dedicated to studying polynomials. On the first day, we'll study a simple invariant associated to every polynomial, the discriminant.
2. On the second day, we'll solve the cubic equation by a method motivated by Galois theory.
3. Days 3 and 4 are a "practical" introduction to group theory. On day 3 we'll learn about groups as symmetries of geometric objects.
4. On day 4, we'll learn about the commutator subgroup of a group.
5. Finally, on the last day we'll connect the two theories and explain the Galois correspondence for the cubic and the quartic.

There are plenty of optional problems along the way for those who wish to explore more. Tricky optional problems are marked with $*$, and especially tricky optional problems are marked with $**$.

1 The Discriminant

Today we'll introduce the discriminant of a polynomial. The discriminant of a polynomial P is another polynomial Q which tells you whether P has any repeated roots over $\mathbb{C}$. Here, $\mathbb{C}$ denotes the complex numbers.

1.1 Quadratic Polynomials

Definition 1.1 (Quadratic discriminant)**.** Let $P(x) = x^2 + bx + c$ be a polynomial with b and c real numbers. The discriminant $\Delta(P)$ is by definition $b^2 - 4c$.

Exercise 1.2. If the polynomial $P(x) = x^2 + bx + c$ has roots α and β, express b and c in terms of α and β.

Exercise 1.3. Still assuming the polynomial P has real coefficients, what does the sign of the discriminant (i.e., whether $\Delta(P) > 0, < 0$ or $= 0$) tell you about the roots α and β? [1]

Exercise 1.4. Express the discriminant of the polynomial $P(x) = x^2 + bx + c$ in terms of the roots α and β.

1.2 The discriminant in general

Definition 1.5. For $P(x)$ a polynomial of the form $P(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$, define the discriminant $\Delta(P) := \prod_{1 \leq i < j \leq n} (r_i - r_j)^2$.

Exercise 1.6. Verify that for $P(x)$ of degree 2, the definition of the discriminant of a general polynomial from Definition 1.5 agrees with that of a quadratic polynomial given in Definition 1.1. [2]

Exercise 1.7. Show that for P a polynomial, $\Delta(P) = 0$ if and only if P has a repeated root over $\mathbb{C}$.

1.3 Cubic discriminants

Exercise 1.8. Show that a cubic polynomial $P(x) := x^3 + ax + bx + c$ with real coefficients always has a real root. [3]

Exercise 1.9. Using Exercise 1.8, show that a cubic polynomial either has

1. 3 real roots or
2. 2 complex conjugates roots (of the form $a + bi, a - bi$ for a, b real numbers) and one real root. [4]

Exercise 1.10. For $P(x) = x^3 + ax^2 + bx + c$ a cubic polynomial with real coefficients, show $\Delta(P) = 0$ if and only if there is a repeated root over $\mathbb{C}$, $\Delta(P) > 0$ if and only if P has three distinct real roots, and $\Delta(P) < 0$ if and only if P has two complex conjugate roots and one real root. Compare your answer to Exercise 1.3.

Your homework is to complete up through Exercise 1.10. If you finish that, and still have time try the following questions.

1.4 Further optional questions on discriminants

Exercise 1.11 (Optional 1)**.** An amazing fact about the discriminant is that it can always be written as a polynomial in terms of the coefficients. For the quadratic this was shown in Definition 1.1 and Exercise 1.4. Now let's see this for a **depressed cubic** (i.e. a cubic with coefficient of x^2 equal to 0). Consider the cubic

$$P(x) = x^3 + px + q.$$

Assume that not all three roots are the same.

1. By definition, the **critical points** of $P(x)$ are roots of $P'(x) = 3x^2 + p$. Find the critical points of $P(x)$, and call them x_1, x_2.
2. Show that $P(x_1) \cdot P(x_2) = 4(p/3)^3 + q^2$.
3. Argue that $P(x)$ has a repeated root over $\mathbb{C}$ if and only if $P(x_1) \cdot P(x_2) = 0$.

Remark 1.12. This is very close to the statement that $\Delta(P) = 0$ iff $P(x)$ has a repeated root, which is not coincidental. By a direct computation one can show that the discriminant of the cubic $P(x)$ equals

$$\Delta(P) = -27P(x_1) \cdot P(x_2) = -4p^3 - 27q^2$$

1.5 Counting polynomials of discriminant 0

The following questions are quite tricky, but fun. Only attempt them if you've already solved Exercise 1.11.

Exercise 1.13 (Optional 2)**.** ** Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where now the coefficients a_i are in $\mathbb{Z}/p$ (i.e., take on values between 0 and $p-1$), and the discriminant is also considered as a number in $\mathbb{Z}/p$. To make sense of discriminant, you may assume that every such polynomial factors uniquely as a product of irreducible polynomials with coefficients in $\mathbb{Z}/p$. Show there are p^n such polynomials, and exactly p^{n-1} of them have discriminant 0. Conclude that the number of square-free polynomials of degree n over $\mathbb{Z}/p$ is $p^n - p^{n-1}$. [5]

Exercise 1.14 (Optional 3)**.** ** Using a similar method to that of Exercise 1.13, count the number of pairs of degree n polynomials (P, Q) for $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $Q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ with $a_i \in \mathbb{Z}/p, b_i \in \mathbb{Z}/p$ so that P and Q have no common irreducible factor. [6]

Remark 1.15. If you did the two prior exercises Exercise 1.13 and Exercise 1.14 correctly, you may notice a striking similarity between the two answers. There is indeed a deeper connection, but the answer lies deep. Loosely speaking, if you take a polynomial $P(x)$ with no repeated factors, you can send it to the pair of polynomials $(P(x) + P'(x), P(x))$. Here $P'(x)$ denotes the derivative of $P(x)$. If $P(x) = \sum_i a_i x^i$ then $P'(x) = \sum_i i \cdot a_i x^{i-1}$.

Exercise 1.16. Verify that the above indeed defines a map from the space of polynomials with no repeated factors to the space of pairs of polynomials with no common factors.

In some sense (which we do not explain) this map explains why the counts from Exercise 1.13 and Exercise 1.14 are so similar.

2 Solving the Cubic

In this section, we will discover a method to solve the cubic, motivated by Galois theory.

We'll continue working with with the *depressed* cubic (the coefficient of x^2 is 0)

$$P(x) = x^3 + px + q$$

with roots r_1, r_2, r_3 and come back to the more general case later.

Exercise 2.1. Express the coefficients of $P(x)$ (namely 0, p, and q) in terms of r_1, r_2, r_3.

Exercise 2.2. We need some identities about the *cube roots of unity* before proceeding.

1. Find the three roots of the polynomial $x^3 - 1$ over the complex numbers.
2. Show that if ω is a non-real root of $x^3 - 1$ then the other non-real root is ω^2. Conclude that $\overline{\omega} = \omega^2$. The complex numbers ω, ω^2, and 1 are called the **cube roots of unity**.
3. Compute $\omega + \omega^2$.
4. Plot ω, ω^2 on the complex plane.

The method for solving the cubic is somewhat like induction. We reduce the problem of solving the cubic to that of solving a quadratic. For this we need to find *intermediate constants* which satisfy a known quadratic and from which r_1, r_2, r_3 can be easily recovered. To this end we define

$$\begin{aligned} \mu_1 &:= r_1 + r_2\omega + r_3\omega^2 \\ \mu_2 &:= r_1 + r_2\omega^2 + r_3\omega \end{aligned} \tag{2.1}$$

Our *intermediate constants* are not μ_1 and μ_2 but μ_1^3 and μ_2^3.

Exercise 2.3. Verify that

$$r_1 = \frac{\mu_1 + \mu_2}{3}\,,\, r_2 = \frac{\omega^2\mu_1 + \omega\mu_2}{3}\,,\, r_3 = \frac{\omega\mu_1 + \omega^2\mu_2}{3} \tag{2.2}$$

are the solutions to Equations (2.1) and $r_1 + r_2 + r_3 = 0$.

Exercise 2.4.

1. Show that $27r_1r_2r_3 = \mu_1^3 + \mu_2^3$. Express this in terms of p and q.[7]
2. Show that $\mu_1\mu_2 = -3p$.[8]
3. Conclude that μ_1^3, μ_2^3 are the roots of the quadratic $x^2 + 27qx - 27p^3$. Solve it to find μ_1^3, μ_2^3.
4. Verify that the discriminant of this quadratic is a multiple of the discriminant $\Delta(P) = -4p^3 - 27q^2$ of the original cubic $P(x)$.

With all this work done, here's the algorithm for finding the roots of a depressed cubic $x^3 + px + q$:

1. Find μ_1^3 and μ_2^3 by solving the quadratic $x^2 + 27qx - 27p^3$.
2. This does not determine μ_1 and μ_2 uniquely. Pick μ_1 as any of the three *cube roots* of μ_1^3 and use $\mu_1\mu_2 = -3p$ to find μ_2.
3. Use Equations (2.2) to find r_1, r_2, r_3.

Exercise 2.5.

1. Use this method to find the roots of $x^3 - 3x + 2$.
2. Find a general formula for the roots of $x^3 + px + q$.

Remark 2.6 (The idea for solving the quartic)**.** A similar inductive technique works for the quartic, however the method is too tedious to do by hand. Suppose we're trying to find the roots r_1, r_2, r_3, r_4 of a quartic

$$P(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

then the strategy is to find 3 intermediate constants $\lambda_1, \lambda_2, \lambda_3$ such that

1. they satisfy a cubic polynomial whose coefficients can be obtained from the original coefficients and
2. the roots r_i can recovered from the λ_i "easily."

Such variables indeed exist:

$$\begin{aligned} \lambda_1 &:= r_1r_2 + r_3r_4 \\ \lambda_2 &:= r_1r_3 + r_2r_4 \\ \lambda_3 &:= r_2r_3 + r_1r_4. \end{aligned} \tag{2.3}$$

Your homework is to complete up through Exercise 2.5 and read Remark 2.6. If you finish that, and still have time try the following questions.

2.1 Further optional questions

Exercise 2.7 (Optional 2)**.** If our cubic is not depressed to begin with we can make a change of variable and make it one.

1. Show that if $f(x) = x^3 + ax^2 + bx + c$ is a cubic polynomial with real coefficients, one can apply a change of variables of the form $y = x + \alpha$ (for $\alpha \in \mathbb{R}$) so that $f(y) = y^3 + py + q$.
2. Express α, p, q explicitly in terms of a, b, c.

This problem finally provides a complete algorithm for a general cubic.

Exercise 2.8 (Optional 2)**.** Retain the notation from Remark 2.6. Here's how you recover the r_i from the λ_i.

1. Show that r_1r_2 and r_3r_4 are the roots of $x^2 - \lambda_1 x + a_0$. This gives us all the r_ir_j.
2. Figure out a way to recover r_i if you know all the r_ir_j.

We'll later see why the λ_i satisfy a cubic with coefficients which can be written in terms of the a_i.

2.2 Roots of Unity

Solutions of the polynomial equation $x^n = 1$ are called n^{th} **roots of unity**, where n is a positive integer. An n^{th} root of unity is called **primitive** if it not an m^{th} root of unity for any $m < n$.

Exercise 2.9 (Optional 3)**.**

1. Show that the n^{th} roots of unity are $e^{2\pi ik/n}$ where $0 \leq k < n$ is a positive integer. Plot them on the complex plane.
2. Show that there are exactly $\phi(n)$ primitive n^{th} roots of unity, where $\phi(n)$ is the number of positive integers less than n relatively prime to n.

If $\zeta_1, \ldots, \zeta_k$ are all the primitive n^{th} roots of unity then the polynomial

$$\Phi_n(x) := \prod_{i=1}^{k}(x - \zeta_i)$$

is called the n^{th} **cyclotomic polynomial**.

3. Compute the cyclotomic polynomials $\Phi_2(x), \Phi_3(x), \Phi_4(x), \Phi_5(x)$.
4. Compute the cyclotomic polynomials $\Phi_p(x)$ where p is prime.
5. Express $x^n - 1$ as a product of cyclotomic polynomials.
6. ** Use the previous part to show that $\Phi_n(x)$ has integer coefficients.[9]
7. * Find a formula for $\Phi_n(x)$ in terms of $x^n - 1$. [10]
8. * Show that $\Phi_p(x)$ is an irreducible polynomial over the integers.[11]

It is also the case that the $\Phi_n(x)$ is irreducible over the integers for all positive integers n. However, this fact has no easy proof.

3 Symmetry Groups

Today we will explore symmetry groups of objects. Surprisingly, these will help us understand how to solve cubic and quartic equations in future days.

3.1 Symmetries of the triangle

Definition 3.1. For X a subset of $\mathbb{R}^n$, we define the **automorphisms** of $X \subset \mathbb{R}^n$ to be the set of reflections and rotations of $\mathbb{R}^n$ which send X to X.

Exercise 3.2. Show that an equilateral triangle in $\mathbb{R}^2$ has exactly 6 automorphisms. Here, we include the **identity automorphism**, denoted id, which fixes every point of the triangle. Write down these automorphisms explicitly in terms of rotations and reflections.

Remark 3.3. Note that the composition of two automorphisms is again an automorphism. Also, every automorphism has an inverse because you can simply "undo" the rotation or reflection. This makes the set of automorphisms into a **group**.

Exercise 3.4. Let s denote the automorphism of the equilateral triangle which is rotation by 120° and let r denote a reflection interchanging two vertices of the equilateral triangle. Show that $r^2 = \text{id}$, (where r^2 means apply r twice) $s^3 = \text{id}$, and $rs = s^2r$ (here rs means you first apply s, then apply r).

Exercise 3.5. Show that all 6 automorphisms from Exercise 3.2 can be expressed as compositions of the elements r and s defined in Exercise 3.4. In this case we say that r and s **generate** the automorphism group of the equilateral triangle.

3.2 Dihedral Groups

We now generalize from the case of triangles to all polygons.

Exercise 3.6. A regular n-gon in $\mathbb{R}^2$ has $2n$ automorphisms. What are they? This set of automorphisms is called the **dihedral group of size** $2n$, denote D_{2n}.

We suggest you skip the following problem if you are pressed for time.

Exercise 3.7 (Optional)**.** Let s denote the rotation of a regular n-gon by $(360/n)^\circ$ about its center and r denote an automorphism of a regular n-gon which is a reflection. Show that $r^2 = \text{id}$, $s^n = \text{id}$, and $rs = s^{n-1}r$. Show that r and s generate all automorphisms of the regular n-gon by showing the $2n$ automorphisms are $1, s, s^2, \ldots, s^{n-1}, r, rs, \ldots, rs^{n-1}$.

Remark 3.8. Of the $2n$ automorphisms of the regular n-gon, n are rotations. It is easy to see that the subset of rotations is closed under composition. In this case we say that the rotations preserving the regular n-gon form a **subgroup** of all automorphisms. This subgroup is called **the cyclic group of order** n, denoted C_n.

3.3 Symmetric Groups

Definition 3.9. We define the **symmetric group on n elements,** S_n to be the set of bijections $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$

Strictly speaking, the symmetric group is a little more than just this set. Given two bijections, you can compose them to get a third bijection. This makes the set of these bijections into a group.

Exercise 3.10. Show that S_n (the symmetric group on n elements) has size $n!$.

Exercise 3.11. Show that S_3 can be identified with the automorphisms of the equilateral triangle.

Exercise 3.12. Show that the automorphisms of the tetrahedron in $\mathbb{R}^3$ are identified with S_4. [12]

Exercise 3.13. Show that inside the group of all automorphisms of the tetrahedron (of size $24 = 4!$, which is the size of S_4), there are 12 rotations. Show that these rotations form a subgroup of S_4. This is known as the **alternating group on** 4 **elements**, denoted A_4.

Your homework is to complete up through Exercise 3.13. If you finish that, and still have time try the following questions.

3.4 Further optional questions on symmetry groups

Exercise 3.14 (Optional 1)**.** * Inside all automorphisms of the cube, there is a subgroup of rotations. What is the size of this group? Can you identify this group? [13]

Exercise 3.15 (Optional 2)**.** Let G be the group from Exercise 3.14, which you found was the group of rotations of the cube. Identify the group of rotations of the octahedron with the same group G. [14]

Exercise 3.16 (Optional 3)**.** ** Determine the number of rotations of the dodecahedron. Do the same for the number of rotations of the icosahedron. Identify these two groups. That is, construct a bijection between these groups respecting composition. Show that these are subgroups of S_5. [15]

4 Commutators and symmetric polynomials

Today we discuss commutators of groups in order to apply them to solving the cubic and quartic. Tomorrow we will explain how these commutators let us solve the cubic and quartic equations.

Definition 4.1. For G a group and $g_1, \ldots, g_n \in G$, the subgroup of G **generated by** $g_1, \ldots, g_n$ is the smallest subgroup of G containing $g_1, \ldots, g_n$. That is, the elements of the subgroup generated by $g_1, \ldots, g_n$ are all products in $g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}$.

Definition 4.2. Let G be a group. The **commutator subgroup** of G, denoted $[G, G]$ is the subgroup of G generated by elements of the form $ghg^{-1}h^{-1}$ for g, h elements of G. Here g^{-1} denotes the inverse of g.

Remark 4.3. It is important that the commutator subgroup is the group *generated* by all commutators (i.e., all elements of the form $ghg^{-1}h^{-1}$) and not just the set of all commutators. Indeed, the product of two commutators need not be closed a commutator, and hence the set of commutators may not be a subgroup. That said, in most of the examples we consider below, it will coincidentally work out that the set of commutators already forms a group, but this is a coincidence of small groups.

Remark 4.4. We will mostly be concerned with the case that G is the symmetric group, or some group of automorphisms of a subset $X \subset \mathbb{R}^n$. In the case of $X \subset \mathbb{R}^n$, if g and h are two automorphisms of X, $ghg^{-1}h^{-1}$ means that you first apply h^{-1}, then apply g^{-1}, then apply h, then apply g.

Exercise 4.5. Let $G = S_3$ (it may help to think about this as automorphisms of an equilateral triangle). Let r denote the reflection (in terms of S_3 this sends $1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$) and s denote rotation by 120° (in S_3 this sends $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$). Show that $rsr^{-1}s^{-1} = s$. Show that the commutator $[S_3, S_3]$ is generated by $s = rsr^{-1}s^{-1}$, and hence is exactly the subgroup with elements $\{\mathrm{id}, s, s^2\}$.

Exercise 4.6. Let $G = C_3$ (the group of rotations of the triangle). Show that the commutator is just the identity automorphism, $[C_3, C_3] = \{\mathrm{id}\}$. In other words, show that for any $g, h \in C_3$, $ghg^{-1}h^{-1} = \mathrm{id}$. More generally, show that if $G = C_n$, $[C_n, C_n] = \{\mathrm{id}\}$.

Exercise 4.7. Let X be a rectangle. The group of automorphisms of X is called K_4, the **Klein-**4 group.

1. Show that the Klein-4 group has size 4 and is generated by reflections about the x-axis and y-axis.
2. Show that $[K_4, K_4] = \{\mathrm{id}\}$.

4.1 Alternating Groups

Definition 4.8. The nth **alternating group**, denoted A_n is by definition $A_n := [S_n, S_n]$, the commutator of S_n.

Exercise 4.9 (Reality check)**.** Verify that $A_3 = C_3$.

Your homework is to complete up to Exercise 4.9. If you have time, attempt the following optional problems

4.2 Further optional questions on Geometric computations of commutators

We now give some geometric ways to see various commutator subgroups of S_4.

Exercise 4.10 (Optional 1)**.** Using that the automorphisms of the tetrahedron can be identified with S_4 from Exercise 3.13 (by the action of S_4 on the 4 vertices of the tetrahedron), show that the rotations of the tetrahedron can be identified with A_4. For this problem, you may assume that A_4 has size 12, and it is the only subgroup of S_4 of size 12.

Exercise 4.11 (Optional 2)**.** The Klein-4 group (introduced in Exercise 4.7) can be viewed as a subgroup of S_4. Specifically, the three non-identity elements are given by the three ways of swapping two pairs of disjoint elements. (For example, one of them would be $1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 3$.)

1. Using the identification of automorphisms of the tetrahedron with S_4 from Exercise 3.12 (by the action of S_4 on the 4 vertices of the tetrahedron), describe the 4 automorphisms of S_4 lying in the Klein-4 subgroup.

2. Show these are all given by rotations, so $K_4 \subset A_4$ using Exercise 3.13. (Technically speaking, we did not verify that the group of rotations was $A_4 = [S_4, S_4]$. Feel free to assume this, or prove it as an extra challenge. If you want help proving it or would like to develop a better understanding A_4, ask for Appendix A.)

3. * Can you use this description to show $K_4 = [A_4, A_4]$? (Again, ask for Appendix A if you would like to prove this algebraically.)

Exercise 4.12 (Optional 3)**.** * Recall that in Exercise 3.14, we identified the rotations of the cube with S_4. Geometrically describe which rotations lie in the subgroup $A_4 \subset S_4$. Geometrically describe which rotations lie in the subgroup $K_4 \subset S_4$. Can you use these geometric descriptions to verify $A_4 = [S_4, S_4]$ and $K_4 = [A_4, A_4]$?

Exercise 4.13 (Optional 4)**.** Given four distinct ordered complex numbers a, b, c, d, the **cross ratio** is defined as

$$\mathrm{r}(a, b; c, d) := \frac{(c-a)(d-b)}{(c-b)(d-a)}.$$

Note that S_4 acts on the set $\{a, b, c, d\}$ by permuting the elements of this set. Show that $K_4 \subset S_4$ preserves the cross ratio. That is, if $\sigma \in K_4$ then then $\mathrm{r}(a, b; c, d) = \mathrm{r}(\sigma(a), \sigma(b); \sigma(c), \sigma(d))$. Find an example of some set of four complex numbers (a, b, c, d) for which K_4 is exactly the subgroup of S_4 that preserves the cross ratio.

5 The Galois Correspondence

So far we've talked about solving cubic and quartics and some concepts from Group theory. Today we'll see the connection between these and hint towards the deeper connection called the Galois Correspondence.

5.1 Symmetries & Polynomials

Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with roots $r_1, r_2, \ldots, r_n$.

Exercise 5.1. For $n = 3$, find a_i as a function of the r_i. (We've already done this for the depressed cubic.) Similar identities hold for all n.

Remark 5.2. Each a_i is a (multi-variable) polynomial in the roots r_i. These polynomials are called the **elementary symmetric polynomials**. They are called 'symmetric' because they remain unchanged upon permuting the roots r_i. We say that the symmetric group S_n acts on the polynomials by permuting the variables, and the 'symmetric' polynomials are exactly the ones which are unchanged or **fixed** by this group action.

The reason for the 'elementary' in 'elementary symmetric' is the following theorem:

Theorem 5.3. *Any symmetric polynomial can be expressed as a polynomial in the elementary symmetric polynomials. Hence, any symmetric polynomial $Q(r_1, r_2, \ldots, r_n)$ in the roots r_i of a polynomial $P(x)$ can be expressed as a polynomial in its coefficients a_i.*

Exercise 5.4. As an example, show that $r_1^2 + r_2^2 + r_3^2 = a_2^2 - 2a_1$ for $n = 3$.

Remark 5.5. You can assume Theorem 5.3 without proof. The proof of this theorem, which is a careful application of the multinomial theorem and induction, also gives an algorithm for finding these polynomials.

We've already encountered several examples of this:

Exercise 5.6 (Discriminant). Verify that for any polynomial $P(x)$ the discriminant $\Delta(P) = \prod_{1 \le i < j \le n}(r_i - r_j)^2$ is symmetric. Conclude that $\Delta(P)$ can be expressed in terms of the coefficients of $P(x)$! This explains the existence of the formulae $\Delta = b^2 - 4c$ and $-4p^3 - 27q^2$ in quadratic and cubic cases.

Remark 5.7 (Cubic). Recall that for the cubic $P(x) = x^3 + px + q$, we defined the intermediate variables

$$\mu_1 = r_1 + r_2\omega + r_3\omega^2$$
$$\mu_2 = r_1 + r_2\omega^2 + r_3\omega$$

By an explicit computation, one can show that $\mu_1^3 + \mu_2^3$ and $\mu_1^3\mu_2^3$ are symmetric in r_1, r_2, r_3, which explains the existence of the formulae $\mu_1^3 + \mu_2^3 = -27q$ and $\mu_1^3\mu_2^3 = -27p$.

Exercise 5.8 (**Quartic**)**.** Recall that for a quartic $P(x)$, we defined the intermediate variables

$$\lambda_1 = r_1r_2 + r_3r_4$$
$$\lambda_2 = r_1r_3 + r_2r_4$$
$$\lambda_3 = r_2r_3 + r_1r_4$$

1. Show that $\lambda_1 + \lambda_2 + \lambda_3$, $\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3$, and $\lambda_1\lambda_2\lambda_3$ are symmetric in r_i.
2. Conclude that the coefficients of $(x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ can be expressed in terms of the coefficients of $P(x)$.

Hopefully now you're convinced that there was some reason behind choosing these intermediate variables. Which brings us to the question: Do such variables exist for all degrees?

Exercise 5.9. Let $P(x)$ be a cubic polynomial.

1. Check that $\omega\mu_1 = r_3 + r_1\omega + r_2\omega^2$.
2. Show that μ_1^3 (and similarly μ_2^3) remains unchanged if we cyclically permute r_1, r_2, r_3.
3. Show that μ_1^3 and μ_2^3 get interchanged if we swap r_2 and r_3. (The same is in fact true if we swap any two of the r_i.)

We say that μ_1^3, μ_2^3 are **fixed** by A_3 (because A_3 consists of the cyclic permutations and *id*).

Exercise 5.10. Let $P(x)$ be a quartic polynomial.

1. Show that each of the λ_i remains unchanged if we swap r_1 with r_2 and r_3 with r_4. Similarly for the other pairs of pairs.
2. Convince yourself that these and *id* are the only permutations in S_4 that leave each of the the λ_i unchanged.

We say that the λ_i are **fixed** by the Klein 4 group K_4.

Exercise 5.11. For an arbitrary polynomial $P(x)$ let $\sqrt{\Delta(P)} := \prod_{1 \le i < j \le n}(r_i - r_j)$.

1. Show that $\sqrt{\Delta(P)}$ changes sign if we swap r_1 with r_2.
2. Show that $\sqrt{\Delta(P)}$ remains unchanged if perform even number of swaps; r_i with r_j.

We say that $\sqrt{\Delta(P)}$ is **fixed** by the entire A_n. For a justification of this, ask for Appendix B.

5.2 The Correspondence

Let us explicitly describe the correspondence between polynomials and symmetry groups:

Cubic: To solve the cubic, we used variables fixed by $A_3 \subset S_3$, namely $\{\mu_1^3, \mu_2^3\}$.

- The fact that we can solve for the solutions of the original cubic in terms of the μ_i^3 corresponds to the fact that $[S_3, S_3] = A_3$.
- The fact that we can solve for the μ_i^3 corresponds to the fact that $[A_3, A_3] = \{\mathrm{id}\}$.

Quartic: To solve the quartic, we used variables fixed by $K_4 \subset S_4$, namely $\{\lambda_1, \lambda_2, \lambda_3\}$.

- The fact that we can solve for the solutions of the original quartic in terms of the λ_i corresponds to the fact that K_4 and S_4 are related by a sequence of commutators $[S_4, S_4] = A_4$ and $[A_4, A_4] = K_4$.
- The fact that we can solve for the λ_i corresponds to the fact that $[K_4, K_4] = \{\mathrm{id}\}$.

What happens for $n > 4$? The sequence of successive commutators for symmetric groups looks like

$$\begin{aligned}
&S_3 \supset [S_3, S_3] = A_3 \supset [A_3, A_3] = \{\mathrm{id}\} \\
&S_4 \supset [S_4, S_4] = A_4 \supset [A_4, A_4] = K_4 \supset [K_4, K_4] = \{\mathrm{id}\} \\
&S_n \supset [S_n, S_n] = A_n \supset [A_n, A_n] = A_n \supset [A_n, A_n] = A_n \cdots \qquad \text{if } n \geq 5
\end{aligned}$$

Taking iterated commutators of S_n for $n \geq 5$ does not eventually shrink to the identity. Because of this, the methods for solving the cubic and quartic do not generalize to a higher degree polynomials.

Theorem 5.12. *A general polynomial of degree ≥ 5 cannot be solved using radicals.*

Sketch of a sketch of a proof.

1. If we can solve a general degree n polynomial by radicals, then we should be able to find a sequence of intermediate variables which satisfy lower degree polynomials. This part is not hard if you think about what a solution in terms of radicals means.

2. Such intermediate variables should be fixed by subgroups of S_n which can be obtained by successively taking commutators of S_n. This is the crucial discovery of Galois that establishes the connection between groups and polynomials.

3. For $n \geq 5$ no such subgroups exist because for $n \geq 5$ the commutators stabilize: $[S_n, S_n] = A_n$ and $[A_n, A_n] = A_n$. (For a series of exercises proving this, ask for Appendix B.)

□

Figure 1: It turns out that one can solve quintics in terms of "generalized radicals" if one also allows something called the "Bring radical." The Bring radical allows you to find a solution to an equation of the form $x^5 + ax + 1$. Image from `https://en.wikipedia.org/wiki/Talk%3ABring_radical`

A Commutators of S_4

In this appendix, we outline some exercises to compute commutators of S_4. To this end, it will be useful to have cycle notation.

Exercise A.1. Define a "cycle notation" for elements in S_n. See Figure 2 for a pictorial description.

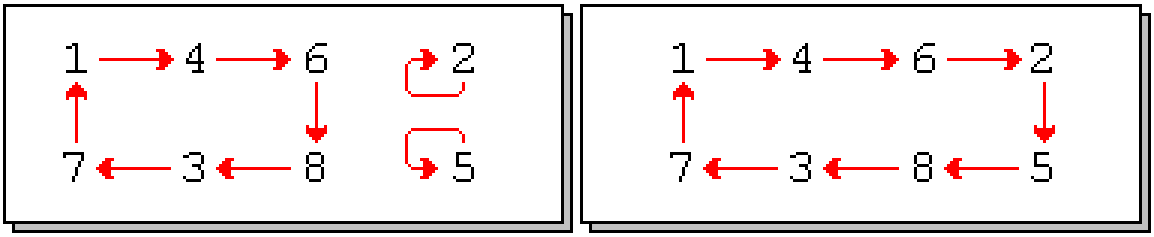

Figure 2: This is a depiction of two elements thought of as elements of S_8. The first corresponds the the permutation fixing 2 and 5, and sending $1 \mapsto 4, 4 \mapsto 6, 6 \mapsto 8, 8 \mapsto 3, 3 \mapsto 7, 7 \mapsto 1$. The corresponding cycle notation for the first picture is $(146837)(2)(5)$ (where each parenthesized group of numbers correspond to a cycle in the above diagram). Similarly, the second permutation has cycle notation (14625837).

Remark A.2. If $s \in S_n$ is an element with certain cycle notation, we often omit all singletons from the cycle notation. So, for example, we denote the element of S_8 with cycle notation $(146837)(2)(5)$ simply as (146837).

You may prove the following facts, or assume them if you'd like:

Fact A.3.

1. The symmetric group is generated by elements with cycle notation of the form (ij). These elements are called **transpositions**. That is, transpositions switch (transpose) two numbers in $\{1, \ldots, n\}$ and preserve the rest.
2. If a group is generated by a collections of elements, the commutator subgroup is generated by commutators of those elements.

Exercise A.4. Using Fact A.3, show that A_n is generated by commutators of transpositions.

Exercise A.5. Compute A_4 as a subgroup of S_4 in the following steps:

1. Show that $(123)(4)$ is the commutator of (12) (the transposition switching 1 and 2) and (13).
2. Show that in general, the commutator of two transpositions is either a 3-cycle when the transpositions have one element in common (i.e., an element with cycle notation of the form (abc) for $a, b, c \in \{1, 2, 3, 4\}$ distinct integers) or it is the identity permutation.
3. Conclude from Exercise A.4 that 3-cycles generate A_4.
4. Compute the set of elements in A_4. Show it has size 12. [16]

Exercise A.6. Compute the commutator $[A_4, A_4]$. Show it has order 4 and is explicitly given by the elements id, $(12)(34)$, $(13)(24)$, $(14)(23)$. This is the Klein-4 group.

B Commutators of S_n and A_n

For this appendix, we assume you have already read Appendix A. In particular, we assume you are familiar with cycle notation and the notion of transpositions. The purpose of this appendix is to show A_n is its own commutator for $n \geq 5$. We do this in two subsections. In the first subsection, we give an alternate definition of A_n, and show that this agrees with the previous definition Definition 4.8. In the second section, we show $[A_n, A_n] = A_n$ for $n \geq 5$.

B.1 Equivalence of two definitions of A_n

In this subsection, we give an alternate definition of A_n, from which it will be easier to show $[A_n, A_n] = A_n$ for $n \geq 5$. Recall above we defined the alternating group A_n as the commutator $[S_n, S_n]$. For the purposes of this appendix, we make the following alternate definition, and then verify A_n is in fact $[S_n, S_n]$.

Definition B.1 (Separate definition for this appendix)**.** The **alternating group**, A_n, is the subgroup of S_n consisting of all elements $g \in S_n$ that can be written as a product of an even number of transpositions.

Exercise B.2. Verify that the definition of A_n, Definition B.1, is well defined by showing that A_n is in fact a subgroup.

Exercise B.3. ** Suppose $g \in S_n$ can be written as products of transpositions in two ways, say $g = t_1 \cdots t_n$ and $g = r_1 \cdots r_m$ for t_i, r_j transpositions. Show $n \equiv m \bmod 2$. [17]

Exercise B.4. Show that $\#A_n = \#S_n/2 = n!/2$. [18]

Exercise B.5. In this exercise, we show A_n is generated by 3-cycles.

1. Show that every 3 cycle (i.e., a permutation written in cycle notation as (ijk)) lies in A_n.
2. Show that every element in A_n is a product of 3-cycles. [19]
3. Conclude A_n is generated by 3-cycles.

Exercise B.6. In this exercise, we check $[S_n, S_n] = A_n$.

1. Show that $[S_n, S_n] \subset A_n$. [20]
2. Show every 3-cycle is a commutator. [21]
3. Use Exercise B.5 to conclude that $[S_n, S_n] = A_n$.

B.2 Commutator of A_n

We now use our new definition of A_n, Definition B.1, to prove $[A_n, A_n] = A_n$ when $n \geq 5$. The proof is surprisingly easy, given what we have shown so far. We start with the following warm-up computation.

Exercise B.7 (Warm up)**.** Show that in A_5, the commutator of (123) and (345) is (235). That is, check $(123)(345)(132)(354) = (235)$.

Exercise B.8. If $n \geq 5$, check that every 3-cycle can be expressed as a commutator of two 3-cycles. [22]

Exercise B.9. Show $[A_n, A_n] = S_5$. [23]

Notes

[1]*Hint:* If the discriminant is > 0 show that the roots are real, if it is equal to 0, show they are the same, if it is less than 0, show they are complex numbers which are not real.

[2]*Hint:* Use Exercise 1.4.

[3]*Hint:* Graph the cubic and show it intersects the line $P(x) = 0$.

[4]*Hint:* Factor out the real root, and use your understanding of quadratic polynomials.

[5]*Hint:* You may assume that every such polynomial $p(x)$ can be written uniquely as $f(x)g(x)^2$, where $f(x)$ is square-free. (Here, f and g are polynomials with $\mathbb{Z}/p$ coefficients.) Then count the number of such polynomials with $\deg f = k$ by induction on k.

[6]Hint: Use a method similar to that of Exercise 1.13. As a further hint, show that every pair of degree n polynomials (P, Q) can be written uniquely as $(f \cdot p, f \cdot q)$ where p and q have no common factors. Now count the number of such pairs by induction on the degree of f.

[7]Hint: Compute $r_2 r_3$ first.

[8]Hint: Don't forget that $(r_1 + r_2 + r_3)^2 = 0$.

[9]Hint: Induction on n.

[10]Hint: Mobius inversion!

[11]Hint: Replace x by $x + 1$ and use the Eisenstein criterion.

[12]*Hint:* Consider the action of the automorphisms of the 4 vertices.

[13]Hint: Look at the long diagonals.

[14]Hint: Look at the four diagonals joining opposite sides. Alternatively, use Exercise 3.14 and that the octahedron is "dual" to the cube (the faces of the cube correspond to the vertices of the octahedron and the faces of the octahedron correspond to the vertices of the cube).

[15]Hint: For identifying this as a subgroup of S_5, one can show there are 5 cubes which can be inscribed in a dodecahedron, and the rotations permute these cubes.

[16]Hint: You should get that A_4 contains all three cycles, together with the four elements id, $(12)(34)$, $(13)(24)$, $(14)(23)$.

[17]Hint: This is a bit tricky, and there are many ways to do it. Here is one nice one: Let $\sigma \in S_n$ be some permutation. Draw a picture with $1, 2, \cdots, n$ listed at the top and the bottom. Draw curves connecting i to $\sigma(i)$ so that the lines always intersect transversely (i.e., no two curves are tangent at an intersection point). Check that the number of intersections of lines is well defined modulo 2. Using that this number of intersections is well defined mod2, check that the parity of the number of intersections agrees with the parity of the number of transpositions. Use this to conclude.

[18]Hint: Use Definition B.1 to define a map $S_n \to C_2$ (where C_2 is the cyclic group of order 2) so that A_n is the set of elements mapping to the identity.

[19]Hint: Show that if i, j, k, l are distinct then $(ij)(kl)$ can be expressed as a product of two 3-cycles. Then, expand any element as a product of transpositions and express any pair of transpositions as a product of one or two 3-cycles.

[20]Hint: Expand commutators as products of transpositions and count their parity.

[21]Hint: Consider the commutator of two transpositions.

[22]Hint: Relabel the numbers from Exercise B.7.

[23]Hint: Recall from Exercise B.5 that A_n is generated by 3-cycles. Then use Exercise B.5.