Polynomials III - Cubics Revisited With Group Theory

Yan Tao

March 2022

1 Complex Conjugation and Polynomials

Recall that complex conjugation was defined by $\overline{a - bi} = a - bi$ and $\overline{re^{i\theta}} = re^{-i\theta}$.

Problem 1 *Prove that*

- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{zw} = \overline{z}\,\overline{w}$
- *For any real number* x, $\overline{x} = x$.

Problem 2 *Let* $p(x) = a_n x^n + ... + a_0$ *be a polynomial in real coefficients and let the complex number* z *be a root. Using the previous problem, prove that* $\overline{z}$ *is also a root of* p.

2 Extensions of the Rational Numbers

Recall that we defined the complex numbers by adding $i = \sqrt{-1}$ and defined addition and multiplication by treating it as a variable. This process is called *adjunction*, and we call the resulting number system the reals with i *adjoined*, and we write this $\mathbb{R}(i)$. Of course, $\mathbb{C} = \mathbb{R}(i)$ by definition.

This is an example of what is more generally called an *extension* of the reals. Because every complex number can be written as a sum of two things with real coefficients $(a + bi)$, the complex numbers are said to be a *degree 2* extension of the reals. Degree 2 extensions are also called *quadratic extensions*, and degree 3 extensions are called *cubic extensions*, and so on.

Unfortunately, the complex numbers are really the only interesting extension of the reals. But there are many interesting extensions of the rational numbers $\mathbb{Q}$, so let us focus on that.

Problem 3 *Show that $\mathbb{Q}(\sqrt{2})$ is a degree 2 extension of the rationals.*

Problem 4 *Show that $\mathbb{Q}(\sqrt[3]{2})$ is a degree 3 extension of the rationals. (Hint: When trying to multiply things in this number system, you will get $(\sqrt[3]{2})^2$. Can this be written as a sum of 1 and $\sqrt[3]{2}$, with **rational coefficients**?)*

In Problem 1, we saw that the function $f(z) = \overline{z}$ satisfies:

$$\begin{aligned} &f(z+w) = f(z) + f(w) \\ &f(zw) = f(z)f(w) \\ &f(x) = x \text{ for all } x \in \mathbb{R} \end{aligned}$$

We can define similar operations over the rationals:

Definition 1 *Let K be an extension of $\mathbb{Q}$ and $f : K \to K$ be a function. f is an* ***automorphism of*** *K* ***over*** *$\mathbb{Q}$ if all of the following hold:*

- *f is a bijection.*
- *$f(x + y) = f(x) + f(y)$ for all $x, y \in K$*
- *$f(xy) = f(x)f(y)$ for all $x, y \in K$*
- *$f(x) = x$ for all rational numbers x*

Denote the set of automorphisms of K over $\mathbb{Q}$ by $Aut(K/\mathbb{Q})$.

It is easy to see that $f(z) = \overline{z}$ is also a bijection. So complex conjugation is an example of an *automorphism of* $\mathbb{C}$ *over* $\mathbb{R}$. In this worksheet, we will focus on automorphisms over $\mathbb{Q}$.

Problem 5 *Show that for any extension K of $\mathbb{Q}$, $Aut(K/\mathbb{Q})$ is a group under the operation of composition. In particular, find the identity element.*

Problem 6 *Let $K = \mathbb{Q}(\sqrt{2})$. Show that $f(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of K over $\mathbb{Q}$.*

We shall revisit $\mathbb{Q}(\sqrt[3]{2})$ later, as it's quite a bit more complicated.

3 Splitting Fields and Galois Groups

Recall last quarter we defined polynomials which are *irreducible, reducible, or split*:

Definition 2 *Let p be a **non-constant** polynomial with coefficients in $\mathbb{C}$ (respectively, $\mathbb{R}$ or $\mathbb{Q}$)*

- *p is **reducible over** $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$) if it is divisible by a polynomial q over $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$), where q is not constant and also has smaller degree than p.*
- *p is **irreducible over** $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$) if it is not reducible over $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$).*
- *p **splits over** $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$) if it factors into linear factors over $\mathbb{C}$ (respectively, over $\mathbb{R}$ or $\mathbb{Q}$); i.e. if there exist $r_1, ..., r_n$ all in $\mathbb{C}$ (respectively, $\mathbb{R}$ or $\mathbb{Q}$) such that $p(x) = (x - r_1)...(x - r_n)$.*

The same definitions still make sense over any extension of a number system, of course. But even though every polynomial splits over $\mathbb{C}$ (the Fundamental Theorem of Algebra), we don't need every complex number to be able to split a polynomial.

Definition 3 *Given a polynomial p in rational coefficients, a **splitting field** of p is a minimal-degree extension of the rational numbers over which p splits.*

Often (not always, but it will be the case in every example we'll see), minimal degree will mean that *we adjoin as few things as possible* so that we account for all roots of p. Since the Fundamental Theorem of Algebra says that every polynomial splits over the complex numbers, we will only need to adjoin complex numbers.

Problem 7 *Show that $\mathbb{Q}(\sqrt{2})$ is a splitting field of $x^2 - 2$. (Hint: To show minimality, consider what a degree 1 extension is.)*

Definition 4 *When p is irreducible over the rationals, the group of automorphisms of its splitting field K over $\mathbb{Q}$ is called its **Galois group** and is denoted $Gal(K/\mathbb{Q})$, or sometimes just $Gal(p)$, instead of $Aut(K/\mathbb{Q})$.*

Let $p(x) = a_n x^n + ... + a_0$ be a degree n irreducible polynomial over $\mathbb{Q}$ (in particular, all the coefficients $a_n, ..., a_0$ have to be rational). Take a splitting field K, and let's take a look at what $\mathrm{Gal}(K/\mathbb{Q})$ does to p.

Problem 8 *Let f be an automorphism of K over $\mathbb{Q}$.*

- Show that if $x \in K$ is a root of p, then so is $f(x)$.

- Show that the restriction of f to the roots (that is, $f : \{\text{roots of f}\} \to \{\text{roots of f}\}$) is a bijection.

- Show that there are at most $n!$ different automorphisms of K over $\mathbb{Q}$. (Hint: How many roots does p have? Because K is of minimal degree by definition, f should be uniquely determined by what it does to the roots of p - try to see why this is the case!)

- Show that $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of the permutation group S_n.

4 Examples of Galois Groups

Problem 9 *Prove that every irreducible quadratic has Galois group $\mathbb{Z}/2$.*

Next week we will learn some tricks for computing Galois groups, but for cubics the guess-and-check strategy will suffice.

Problem 10 *Show that $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $x^3 - 2$. What else can we adjoin to make this a splitting field?*

Problem 11 *Show that the Galois group of $x^3 - 2$ is S_3. (Hint: Find all roots of $x^3 - 2$ in the complex numbers, and consider all permutations of these roots. Does there exist a $f \in Gal(K/\mathbb{Q})$ which gives these permutations?)*

Problem 12 *Find a splitting field for $8x^3 - 6x + 1$ (you'll have to trust me - this is irreducible!). (Hint: Show that if a is a root, then $2a^2 - 1$ and $-2a^2 - a + 1$ are the other roots.)*

Problem 13 *Show that the Galois group of $8x^3 - 6x + 1$ is $\mathbb{Z}/3$.*

Problem 14 *Show that the only possible Galois groups for an irreducible cubic are* $\mathbb{Z}/3$ *and* S_3 *(Hint: Use the cubic formula - we know none of the roots can be rational.)*

Problem 15 *Under what circumstances is the Galois group* $\mathbb{Z}/3$ *or* S_3*?*