Galois Groups Using Field Extensions

This is based on *Visual Group Theory* by Nathan Carter.

Simplification is an essential part of polynomial equations.
Even difficult polynomial equations, like this one:

$$\frac{(12-x)(13+\frac{x}{2})}{19-\frac{x+1}{x-1}} = 100 + \frac{50}{x-9}$$

Can be simplified into this form:

$$x^4 + 4x^3 + 3157x^2 - 31354x + 31192 = 0$$

Meaning, polynomials on one side and zero on the other. It still looks pretty complicated, but the thing is, this form has an advantage over the other because there's a centuries old proven technique for solving it.

There is a formula for quadratic polynomial equations

$$ax^2 + bx + c = 0$$

Cubic polynomial equations:

$$ax^3 + bx^2 + cx + d = 0$$

And quartic polynomial equations:

$$x^4 + 4x^3 + 3157x^2 - 31354x + 31192 = 0$$

On the quintics though, is where all progress stopped for a while:

$$ax^5 + bx^4 + cx^3 + dx^2 + fx + g = 0$$

This required the use of *fields*.

A set of numbers S with addition and multiplication is a ***field*** if
1) S and its addition operation form an abelian group. Which basically means that it has all the 4 properties of a group plus an additional condition of "commutative", $(a \cdot b) = (b \cdot a)$ for all $a, b \in G$.

2) Removing the identity element (the zero) from that group leaves a set that, under multiplication, also forms an abelian group.
3) Addition and multiplication relate through the distributive law $a(b + c) = ab + ac$.

If you think about it, a set of natural numbers $\mathbb{N}$ cannot be a field, because they do not satisfy condition 1 and 2. A set of integers $\mathbb{Z}$ also cannot be a field because they do not satisfy the 2nd condition. But the next in-line, rational numbers $\mathbb{Q}$, do satisfy all of the conditions, and are therefore a field.

The process of solving a polynomial can be viewed as extending the field $\mathbb{Q}$ to include the roots, or solutions, of the polynomial.

For example, we know that quadratic equations often require us to take a square root to obtain a solution. Some square roots are rational numbers that give rational numbers $\sqrt{\frac{9}{4}} = \frac{3}{2}$

But what about if we have $\sqrt{2}$? This number is in the field of real numbers $\mathbb{R}$, beyond $\mathbb{Q}$.

Some equations, like this one $x^2 - 2x + 2 = 0$, give solutions that aren't even real numbers when plugged into the quadratic formula.

$$x = \frac{2 \pm \sqrt{4 - 8}}{2} = \frac{2 \pm 2i}{2} = 1 \pm i.$$

This takes us beyond $\mathbb{R}$ into $\mathbb{C}$, the realm of complex numbers.

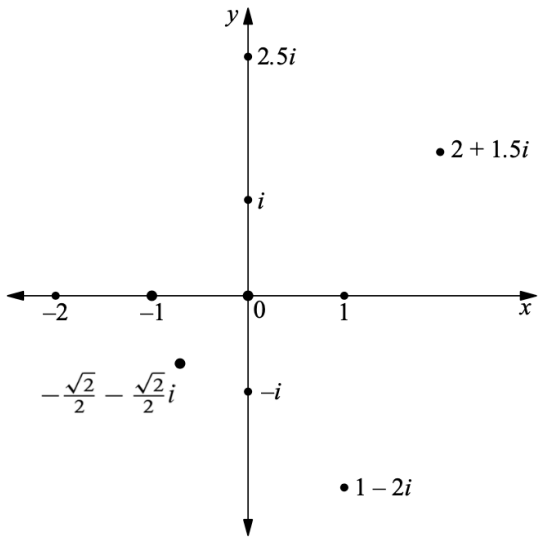
It all comes back analyzing operations that reach out of $\mathbb{Q}$ – how far outside of $\mathbb{Q}$ should be reach when analyzing operations?

All polynomials whose coefficients are in $\mathbb{C}$ have their roots in $\mathbb{C}$ as well. Because of that, $\mathbb{C}$ is an algebraically closed field. Fields like R (the real numbers) or Q (the rationals) are **not** algebraically closed because there are polynomials with coefficients in those fields whose roots do not lie within them.

All complex numbers can be written in the form $a + bi$.

Because of this two part structure, we can visualize each of these as a point on a coordinate plane, where x is the real number line.

(Consider becoming a member of the channel!) Thanks!



There is actually symmetry we can observe from each of these roots. Each is a mirror reflection of itself over the x axis, and a vertical flip would therefore respect the shape of the root set. These are called ***complex conjugates***.

The formal definition of this is that, for any complex number $a + bi$, we call $a - bi$ a complex conjugate. If c is any complex number, we write $\overline{c}$ to mean its complex conjugate.

For example, in $x^2 - 2x + 2$, the roots of which are $1 \pm i$, $1 + i$ and $1 - i$ are conjugates. So we therefore write $\overline{1 + i} = 1 - i$.

Mind that we only mean the vertical flip above and below the x axis, because not all four roots of a polynomial are one another's complex conjugates, as is the case with $x^4 + 1$.

$c = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ then $\overline{c} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ but $\overline{c} \neq -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ and $\overline{c} \neq -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$

If we're talking about real numbers on their own, they're their own complex conjugates
$\overline{6} = 6 \; and \; \overline{0} = 0$

This is known as the ***complex conjugate root theorem***. It states that if r is a root of a polynomial, then its conjugate $\overline{r}$ is a root of the same polynomial. Meaning that every polynomial root has a mirror symmetry over the x axis of the complex plane.

To prove that, take the general form of a polynomial.

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

If one of the possible roots is r, then it will yield 0

$$a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 = 0$$

Therefore, $\bar{r}$ is also a root. Let's prove that by taking the conjugate

$$\overline{a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0} = 0,$$

And simplify the left side, because it's unmanageably long. I'd like to prove that conjugation can be separated over each term of a sum of complex numbers

$$\overline{(a+bi)+(c+di)} = \overline{a+bi} + \overline{c+di}$$

By using simple algebra we will show that the two sides are equal

$$\overline{(a+bi)+(c+di)} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i$$
$$\overline{a+bi} + \overline{c+di} = a - bi + c - di = (a+c)-(b+d)i$$

So, once we apply it to the original polynomial we simplify things a bit

$$\overline{a_n r^n} + \overline{a_{n-1} r^{n-1}} + \cdots + \overline{a_2 r^2} + \overline{a_1 r} + \overline{a_0} = 0$$

Each of these is a conjugate of the multiplied expressions a_i and r^i. To simplify it even further, we'd split the conjugation over the two terms in each multiplication, using a rule like this.

$$\overline{(a+bi)(c+di)} = (\overline{a+bi})(\overline{c+di})$$

We'll apply it without proving it.

$$\overline{a_n}\,\overline{r^n} + \overline{a_{n-1}}\,\overline{r^{n-1}} + \cdots + \overline{a_2}\,\overline{r^2} + \overline{a_1}\,\overline{r} + \overline{a_0} = 0$$

Since each coefficient a_i is a real number, and it's own conjugate, we can simplify further

$$a_n \overline{r^n} + a_{n-1} \overline{r^{n-1}} + \cdots + a_2 \overline{r^2} + a_1 \overline{r} + a_0 = 0$$

And finally, natural number exponents just mean repeated multiplication, allowing to split up the powers as well

$$a_n\bar{r}^n + a_{n-1}\bar{r}^{n-1} + \cdots + a_2\bar{r}^2 + a_1\bar{r} + a_0 = 0.$$

From this we prove that $\bar{r}$ is the root of the same polynomial.

What we just saw is just one type of symmetry in Galois Theory. To find another one, we need to get acquainted with an important concept.

To understand it, we need to go back to factoring.

Take $12x^3 - 44x^2 + 35x + 17$; we know one of its rational roots to be $-\frac{1}{3}$. Knowing that, we can "factor out" the linear term $(x + \frac{1}{3})$, which corresponds to the root.

But to avoid fractions, the linear factor is rewritten as $(3x + 1)$. This adjustment works because multiplying the entire polynomial by 3 doesn't change its roots.
Using polynomial division, the original cubic polynomial is factored as:
$(3x + 1)(4x^2 - 16x + 17)$

However, what about examples like this $(4x^2 - 16x + 17)$
The roots of this quadratic are complex numbers

$$x = \frac{16 \pm \sqrt{16^2 - 4 \cdot 4 \cdot 17}}{2 \cdot 4} = \frac{16 \pm \sqrt{-16}}{8} = 2 \pm \frac{1}{2}i$$

Since the roots are not rational, and cannot be factored further into polynomials with rational coefficients, we call that **irreducible over** $\mathbb{Q}$. These are of interest to us because their roots are outside of $\mathbb{Q}$, and thus we need to expand our number system beyond $\mathbb{Q}$.

Thus we need new notation, besides arithmetic and the natural numbers, which pushed for the creation of the radical sign.

Like, there is no rational number solution to $x^2 - 2 = 0$, so mathematicians created the symbol $\sqrt{2}$ to say that that is the solution – the number whose square is 2 .

Theorems like Eisenstein Criterion helps to find irreducible polynomials. It states that a polynomial with integer coefficients is irreducible if we can find a prime number p that satisfies these two requirements:

1) the coefficient of the highest power of x is not a multiple of p

2) The constant term (the one without the x) is not a multiple of p^2.

We can use irreducible polynomials to analyze radicals that reach outside $\mathbb{Q}$. These operations are called **field extensions**.

Let's take a simple example, $x^2 - 2 = 0$. How far outside of $\mathbb{Q}$ do we need to go to solve it?

The result has to be a number system capable of arithmetic, a field, not just $\sqrt{2}$. And, I want to reach out of $\mathbb{Q}$ with the smallest field possible. That field is called $\mathbb{Q}(\sqrt{2})$; It contains all of the numbers that $\mathbb{Q}$ does, $\sqrt{2}$, and all the numbers we can get from $\sqrt{2}$ using arithmetic.
All of these are inside of $\mathbb{Q}(\sqrt{2})$ for example. Although there are other, more complicated ones.

$$-\sqrt{2} \qquad 6+\sqrt{2} \qquad \left(\sqrt{2}+\frac{3}{2}\right)^3 \qquad \frac{\sqrt{2}}{16+\sqrt{2}}$$

They can be simplified to a smaller form. For example, expanding $(\sqrt{2}+\frac{3}{2})^3$

$$\left(\sqrt{2}+\tfrac{3}{2}\right)^3 = \left(\sqrt{2}\right)^3 + \tfrac{9}{2}\left(\sqrt{2}\right)^2 + \tfrac{27}{4}\sqrt{2} + \tfrac{27}{8} = 12\tfrac{3}{8} + 8\tfrac{3}{4}\sqrt{2}$$

Interestingly, the result is that any element of $\mathbb{Q}(\sqrt{2})$ can be simplified into the form $a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Which is similar to what we saw earlier with $\mathbb{C}$.

$\mathbb{Q}(\sqrt{2})$ is larger than $\mathbb{Q}$ but smaller than $\mathbb{R}$. Now that we know what is inside of $\mathbb{Q}(\sqrt{2})$, let's see how Galois theory will show its symmetry.

The Galois group of a polynomial is the group of symmetries of its roots. These symmetries are captured by how the roots can be permuted (or swapped around) while respecting the algebraic relationships defined by the polynomial.

For $x^2 - 2 = 0$, the two roots $\sqrt{2}$ and $-\sqrt{2}$ can either: stay as they are (do nothing), which is equivalent to the "identity" permutation, or be switched.

The set of possible permutations of the roots is written as $Perm\{\sqrt{2}, -\sqrt{2}\}$.

Can we use the equations of arithmetic to tell the roots of $\pm\sqrt{2}$ apart?
If we can, the roots have no symmetry. If we can't, they can be easily swapped.

Since arithmetic does not have the square root symbol, we will call the roots r_1 and r_2 instead, in order to be able to mention them in an arithmetic equation.

We might try to write it like this $r_1 = \sqrt{2}$, $r_2 = -\sqrt{2}$, using the equation $r_1 = r_2 + 2\sqrt{2}$. Fine, we distinguished the *roots* themselves from one another, but we're cheating by using the symbol $\sqrt{2}$. Therefore, it's not an equation from $\mathbb{Q}$. We could allow for a statement like $r_1 r_2 = -2$, but this fails to distinguish the two roots, because you could assign $\pm\sqrt{2}$ in either order, and the answer would still be true. If we put it into an equation like $r_1 + r_2 = 0$ we would have the same problem.

As many times as we will try, we will never find a way to distinguish the roots of $x^2 - 2$ using only equations of arithmetic. Thus, the two roots look identical from Q's point of view.

This is true for all of $\mathbb{Q}(\sqrt{2})$. Thus this is how Galois Theory is the study of these symmetries and their field extensions.

Please, if you find this document useful, let us know. Or if you found typos and things to improve, let us know as well. Your feedback is very important to us, since we are working hard to deliver the best material possible. Contact us at: dibeos.contact@gmail.com