Section 6: Field and Galois theory

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Some history and the search for the quintic

The quadradic formula is well-known. It gives us the two roots of a degree-2 polynomial $ax^2 + bx + c = 0$:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There are formulas for cubic and quartic polynomials, but they are *very* complicated. For years, people wondered if there was a quintic formula. Nobody could find one.

In the 1830s, 19-year-old political activist Évariste Galois, with no formal mathematical training proved that no such formula existed.

He invented the concept of a group to solve this problem.

After being challenged to a dual at age 20 that he knew he would lose, Galois spent the last few days of his life frantically writing down what he had discovered.

In a final letter Galois wrote, "*Later there will be, I hope, some people who will find it to their advantage to decipher all this mess.*"

Hermann Weyl (1885–1955) described Galois' final letter as: "*if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.*" Thus was born the field of group theory!

Arithmetic

Most people's first exposure to mathematics comes in the form of counting.

At first, we only know about the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$, and how to add them.

Soon after, we learn how to subtract, and we learn about negative numbers as well. At this point, we have the integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Then, we learn how to divide numbers, and are introducted to fractions. This brings us to the rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$.

Though there are other numbers out there (irrational, complex, etc.), we don't need these to do basic arithmetic.

Key point

To do arithmetic, we need *at least* the rational numbers.

Fields

Definition

A set F with addition and multiplication operations is a field if the following three conditions hold:

- F is an abelian group under addition.
- $F \setminus \{0\}$ is an abelian group under multiplication.
- The distributive law holds: $a(b+c) = ab + ac$.

Examples

- The following sets are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (prime p).
- The following sets are *not* fields: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$ (composite n).

Definition

If F and E are fields with $F \subset E$, we say that E is an extension of F.

For example, $\mathbb{C}$ is an extension of $\mathbb{R}$, which is an extension of $\mathbb{Q}$.

In this chapter, we will explore some more unusual fields and study their automorphisms.

An extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$?

This field must contain all sums, differences, and quotients of numbers we can get from $\sqrt{2}$. For example, it must include:

$$-\sqrt{2}, \qquad \tfrac{1}{\sqrt{2}}, \qquad 6+\sqrt{2}, \qquad \left(\sqrt{2}+\tfrac{3}{2}\right)^3, \qquad \tfrac{\sqrt{2}}{16+\sqrt{2}}.$$

However, these can be simplified. For example, observe that

$$\left(\sqrt{2}+\tfrac{3}{2}\right)^3 = (\sqrt{2})^3 + \tfrac{9}{2}(\sqrt{2})^2 + \tfrac{27}{4}\sqrt{2} + \tfrac{27}{8} = \tfrac{99}{8} + \tfrac{35}{4}\sqrt{2}.$$

In fact, *all* of these numbers can be written as $a+b\sqrt{2}$, for some $a, b \in \mathbb{Q}$.

Key point

The smallest extension of $\mathbb{Q}$ that contains $\sqrt{2}$ is called "$\mathbb{Q}$ adjoin $\sqrt{2}$," and denoted:

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\} = \left\{\tfrac{p}{q} + \tfrac{r}{s}\sqrt{2} : p, q, r, s \in \mathbb{Z},\ q, s \neq 0\right\}.$$

$\mathbb{Q}(i)$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $i = \sqrt{-1}$?

This field must contain

$$-i, \qquad \tfrac{2}{i}, \qquad 6+i, \qquad \left(i+\tfrac{3}{2}\right)^3, \qquad \tfrac{i}{16+i}\,.$$

As before, we can write all of these as $a+bi$, where $a, b \in \mathbb{Q}$. Thus, the field "$\mathbb{Q}$ adjoin i" is

$$\mathbb{Q}(i) = \{a+bi : a, b \in \mathbb{Q}\} = \left\{\frac{p}{q} + \frac{r}{s}\,i : p, q, r, s \in \mathbb{Z},\ q, s \neq 0\right\}.$$

Remarks

- $\mathbb{Q}(i)$ is much smaller than $\mathbb{C}$. For example, it does *not* contain $\sqrt{2}$.
- $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, but $\mathbb{Q}(i)$ is not.
- $\mathbb{Q}(\sqrt{2})$ contains all of the roots of $f(x) = x^2 - 2$. It is called the splitting field of $f(x)$. Similarly, $\mathbb{Q}(i)$ is the splitting field of $g(x) = x^2 + 1$.

$\mathbb{Q}(\sqrt{2}, i)$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $i = \sqrt{-1}$?

We can do this in two steps:

(i) Adjoin the roots of the polynomial $x^2 - 2$ to $\mathbb{Q}$, yielding $\mathbb{Q}(\sqrt{2})$;

(ii) Adjoin the roots of the polynomial $x^2 + 1$ to $\mathbb{Q}(\sqrt{2})$, yielding $\mathbb{Q}(\sqrt{2})(i)$;

An element in $\mathbb{Q}(\sqrt{2}, i) := \mathbb{Q}(\sqrt{2})(i)$ has the form

$$\begin{aligned} &\alpha + \beta i && \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \\ &= (a + b\sqrt{2}) + (c + d\sqrt{2})i && a, b, c, d \in \mathbb{Q} \\ &= a + b\sqrt{2} + ci + d\sqrt{2}i && a, b, c, d \in \mathbb{Q} \end{aligned}$$

We say that $\{1, \sqrt{2}, i, \sqrt{2}i\}$ is a basis for the extension $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. Thus,

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\}$$

In summary, $\mathbb{Q}(\sqrt{2}, i)$ is constructed by starting with $\mathbb{Q}$, and adjoining all roots of $h(x) = (x^2 - 2)(x^2 + 1) = x^4 - x^2 - 2$. It is the splitting field of $h(x)$.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $\sqrt{3}$?

This time, our field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, constructed by starting with $\mathbb{Q}$, and adjoining all roots of the polynomial $h(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$.

It is not difficult to show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for this field, i.e.,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}.$$

Like with did with a group and its subgroups, we can arrange the subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in a lattice.

I've labeled each extension with the degree of the polynomial whose roots I need to adjoin.

Just for fun: What *group* has a subgroup lattice that looks like this?

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Field automorphisms

Recall that an automorphism of a group G was an isomorphism $\phi\colon G \to G$.

Definition

Let F be a field. A field automorphism of F is a bijection $\phi\colon F \to F$ such that for all $a, b \in F$,

$$\phi(a+b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\,\phi(b)\,.$$

In other words, ϕ must preserve the structure of the field.

For example, let $F = \mathbb{Q}(\sqrt{2})$. Verify (HW) that the function

$$\phi\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})\,, \qquad \phi\colon a + b\sqrt{2} \longmapsto a - b\sqrt{2}\,.$$

is an automorphism. That is, show that

- $\phi((a+b\sqrt{2}) + (c+d\sqrt{2})) = \cdots = \phi(a+b\sqrt{2}) + \phi(c+d\sqrt{2})$
- $\phi((a+b\sqrt{2})(c+d\sqrt{2})) = \cdots = \phi(a+b\sqrt{2})\,\phi(c+d\sqrt{2})$.

What other field automorphisms of $\mathbb{Q}(\sqrt{2})$ are there?

A defining property of field automorphisms

Field automorphisms are central to Galois theory! We'll see why shortly.

Proposition

If ϕ is an automorphism of an extension field F of $\mathbb{Q}$, then

$$\phi(q) = q \qquad \text{for all } q \in \mathbb{Q}.$$

Proof

Suppose that $\phi(1) = q$. Clearly, $q \neq 0$. (Why?) Observe that

$$q = \phi(1) = \phi(1 \cdot 1) = \phi(1)\,\phi(1) = q^2\,.$$

Similarly,

$$q = \phi(1) = \phi(1 \cdot 1 \cdot 1) = \phi(1)\,\phi(1)\,\phi(1) = q^3\,.$$

And so on. It follows that $q^n = q$ for every $n \geq 1$. Thus, $q = 1$. $\square$

Corollary

$\sqrt{2}$ is irrational. $\square$

The Galois group of a field extension

The set of all automorphisms of a field forms a group under composition.

Definition

Let F be an extension field of $\mathbb{Q}$. The Galois group of F is the group of automorphisms of F, denoted $\mathrm{Gal}(F)$.

Here are some examples (without proof):

- The Galois group of $\mathbb{Q}(\sqrt{2})$ is C_2:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})) = \langle f \rangle \cong C_2\,, \qquad \text{where } f\colon \sqrt{2} \longmapsto -\sqrt{2}$$

- An automorphism of $F = \mathbb{Q}(\sqrt{2}, i)$ is completely determined by where it sends $\sqrt{2}$ and i. There are four possibilities: the identity map e, and

$$\left\{ \begin{array}{r} h(\sqrt{2}) = -\sqrt{2} \\ h(i) = i \end{array} \right. \qquad \left\{ \begin{array}{r} v(\sqrt{2}) = \sqrt{2} \\ v(i) = -i \end{array} \right. \qquad \left\{ \begin{array}{r} r(\sqrt{2}) = -\sqrt{2} \\ r(i) = -i \end{array} \right.$$

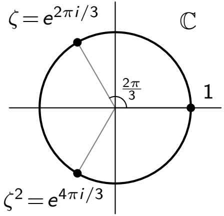
Thus, the Galois group of F is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) = \langle h, v \rangle \cong V_4$.

$\mathbb{Q}(\zeta, \sqrt[3]{2})$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains all roots of $g(x) = x^3 - 2$?

Let $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. This is a 3rd root of unity; the roots of $x^3 - 1 = (x-1)(x^2 + x + 1)$ are $1, \zeta, \zeta^2$.



Note that the roots of $g(x)$ are

$$z_1 = \sqrt[3]{2}, \qquad z_2 = \zeta\sqrt[3]{2}, \qquad z_3 = \zeta^2\sqrt[3]{2}.$$

Thus, the field we seek is $F = \mathbb{Q}(z_1, z_2, z_3)$.

I claim that $F = \mathbb{Q}(\zeta, \sqrt[3]{2})$. Note that this field contains z_1, z_2, and z_3. Conversely, we can construct ζ and $\sqrt[3]{2}$ from z_1 and z_2, using arithmetic.

A little algebra can show that

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}.$$

Since $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ lies in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so does $2(\zeta + \frac{1}{2}) = \sqrt{3}i = \sqrt{-3}$. Thus,

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3}i, \sqrt[3]{2}).$$

Subfields of $\mathbb{Q}(\zeta, \sqrt[3]{2})$

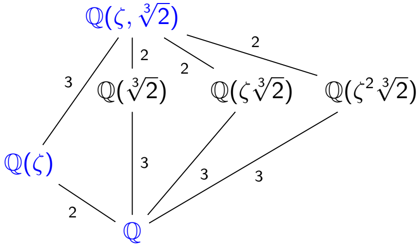
What are the subfields of

$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}\,?$$

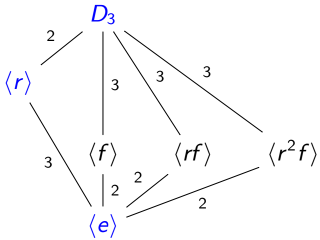
Note that $(\zeta^2)^2 = \zeta^4 = \zeta$, and so $\mathbb{Q}(\zeta^2) = \mathbb{Q}(\zeta) = \{a + b\zeta : a, b \in \mathbb{Q}\}$.

Similarly, $(\sqrt[3]{4})^2 = 2\sqrt[3]{2}$, and so $\mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

There are two more subfields. As we did before, we can arrange them in a lattice:



Look familiar?



Compare this to the subgroup lattice of D_3.

Summary so far

Roughly speaking, a field is a group under both addition and multiplication (if we exclude 0), with the distributive law connecting these two operations.

We are mostly interested in the field $\mathbb{Q}$, and certain extension fields: $F \supseteq \mathbb{Q}$. Some of the extension fields we've encountered:

$$\mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{2}, i), \qquad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \qquad \mathbb{Q}(\zeta, \sqrt[3]{2}).$$

An automorphism of a field $F \supset \mathbb{Q}$ is a structure-preserving map that fixes $\mathbb{Q}$.

The set of all automorphisms of $F \supseteq \mathbb{Q}$ forms a group, called the Galois group of F, denoted $\mathrm{Gal}(F)$.

There is an intriguing but mysterious connection between subfields of F and subgroups of $\mathrm{Gal}(F)$. This is at the heart of Galois theory!

Something to ponder

How does this all relate to solving polynomials with radicals?

Polynomials

Definition

Let x be an unknown variable. A polynomial is a function

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \,.$$

The highest non-zero power of n is called the degree of f.

We can assume that all of our coefficients a_i lie in a field F.

For example, if each $a_i \in \mathbb{Z}$ (not a field), we could alternatively say that $a_i \in \mathbb{Q}$.

Let $F[x]$ denote the set of polynomials with coefficients in F. We call this the set of polynomials over F.

Remark

Even though $\mathbb{Z}$ is not a field, we can still write $\mathbb{Z}[x]$ to be the set of polynomials with integer coefficients. Most polynomials we encounter have integer coeffients anyways.

Radicals

The roots of low-degree polynomials can be expressed using arithmetic and radicals.

For example, the roots of the polynomial $f(x) = 5x^4 - 18x^2 - 27$ are

$$x_{1,2} = \pm\sqrt{\frac{6\sqrt{6}+9}{5}}, \qquad x_{3,4} = \pm\sqrt{\frac{9-6\sqrt{6}}{5}}.$$

Remark

The operations of arithmetic, and radicals, are really the "only way" we have to write down generic complex numbers.

Thus, if there is some number that cannot be expressed using radicals, we have no way to express it, unless we invent a special symbol for it (e.g., π or e).

Even weirder, since a computer program is just a string of 0s and 1s, there are only countably infinite many possible programs.

Since $\mathbb{R}$ is an uncountable set, there are numbers (in fact, "almost all" numbers) that can *never* be expressed algorithmically by a computer program! Such numbers are called "uncomputable."

Algebraic numbers

Definition

A complex number is algebraic (over $\mathbb{Q}$) if it is the root of some polynomial in $\mathbb{Z}[x]$. The set $\mathbb{A}$ of all algebraic numbers forms a field (this is not immediately obvious).

A number that is not algebraic over $\mathbb{Q}$ (e.g., π, e) is called transcendental.

Every number that can be expressed from the natural numbers using arithmetic and radicals is algebraic. For example, consider

$$\begin{aligned} x = \sqrt[5]{1+\sqrt{-3}} \qquad &\Longleftrightarrow \qquad x^5 = 1+\sqrt{-3} \\ &\Longleftrightarrow \qquad x^5 - 1 = \sqrt{-3} \\ &\Longleftrightarrow \qquad (x^5-1)^2 = -3 \\ &\Longleftrightarrow \qquad x^{10} - 2x^5 + 4 = 0\,. \end{aligned}$$

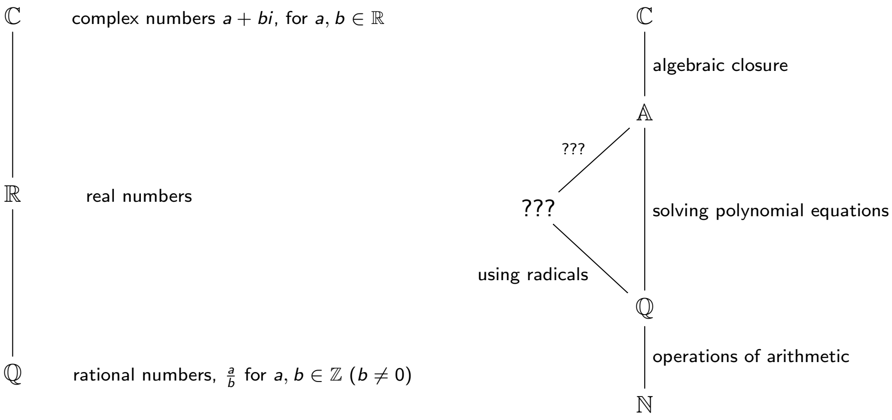
Question

Can *all* algebraic numbers be expressed using radicals?

This question was unsolved until the early 1800s.

Hasse diagrams

The relationship between the natural numbers $\mathbb{N}$, and the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{A}$, and $\mathbb{C}$, is shown in the following Hasse diagrams.



Some basic facts about the complex numbers

Definition

A field F is algebraically closed if for any polynomial $f(x) \in F[x]$, all of the roots of $f(x)$ lie in F.

Non-examples

- $\mathbb{Q}$ is not algebraically closed because $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has a root $\sqrt{2} \notin \mathbb{Q}$.
- $\mathbb{R}$ is not algebraically closed because $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has a root $\sqrt{-1} \notin \mathbb{R}$.

Fundamental theorem of algebra

The field $\mathbb{C}$ is algebraically closed.

Thus, every polynomial $f(x) \in \mathbb{Z}[x]$ completely factors, or splits over $\mathbb{C}$:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n), \qquad r_i \in \mathbb{C}.$$

Conversely, if F is *not* algebraically closed, then there are polynomials $f(x) \in F[x]$ that do *not* split into linear factors over F.

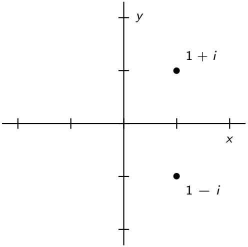
Complex conjugates

Recall that complex roots of $f(x) \in \mathbb{Q}[x]$ come in conjugate pairs: If $r = a + bi$ is a root, then so is $\overline{r} := a - bi$.

For example, here are the roots of some polynomials (degrees 2 through 5) plotted in the complex plane. All of them exhibit symmetry across the x-axis.

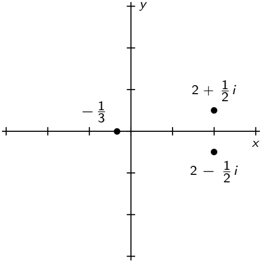
$f(x) = x^2 - 2x + 2$

Roots: $1 \pm i$



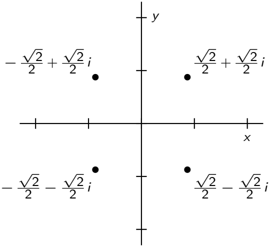
$f(x) = 12x^3 - 44x^2 + 35x + 17$

Roots: $-\frac{1}{3},\ 2 \pm \frac{1}{2} i$



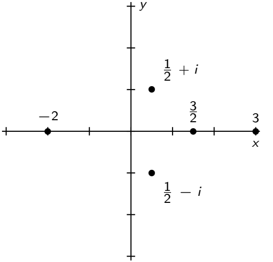
$f(x) = x^4 + 1$

Roots: $\pm \frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}$



$f(x) = 8x^5 - 28x^4 - 6x^3 + 83x^2 - 117x + 90$

Roots: $-2,\ \frac{3}{2},\ 3,\ \frac{1}{2} i \pm i$



Irreducibility

Definition

A polynomial $f(x) \in F[x]$ is reducible over F if we can factor it as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ of strictly lower degree. If $f(x)$ is not reducible, we say it is irreducible over F.

Examples

- $x^2 - x - 6 = (x+2)(x-3)$ is reducible over $\mathbb{Q}$.
- $x^4 + 5x^2 + 4 = (x^2+1)(x^2+4)$ is reducible over $\mathbb{Q}$, but it has no roots in $\mathbb{Q}$.
- $x^3 - 2$ is irreducible over $\mathbb{Q}$. If we could factor it, then one of the factors would have degree 1. But $x^3 - 2$ has no roots in $\mathbb{Q}$.

Facts

- If $\deg(f) > 1$ and has a root in F, then it is reducible over F.
- Every polynomial in $\mathbb{Z}[x]$ is reducible over $\mathbb{C}$.
- If $f(x) \in F[x]$ is a degree-2 or 3 polynomial, then $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.

Eisenstein's criterion for irreducibility

Lemma

Let $f \in \mathbb{Z}[x]$ be irreducible. Then f is also irreducible over $\mathbb{Q}$.

Equivalently, if $f \in \mathbb{Z}[x]$ factors over $\mathbb{Q}$, then it factors over $\mathbb{Z}$.

Theorem (Eisenstein's criterion)

A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$ is irreducible if for some prime p, the following all hold:

1. $p \nmid a_n$;
2. $p \mid a_k$ for $k = 0, \dots, n-1$;
3. $p^2 \nmid a_0$.

For example, Eisenstein's criterion tells us that $x^{10} + 4x^7 + 18x + 14$ is irreducible.

Remark

If Eisenstein's criterion fails for all primes p, that does *not* necessarily imply that f is reducible. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Q}$, but Eisenstein cannot detect this.

Extension fields as vector spaces

Recall that a vector space over $\mathbb{Q}$ is a set of vectors V such that

- If $u, v \in V$, then $u + v \in V$ (closed under addition)
- If $v \in V$, then $cv \in V$ for all $c \in \mathbb{Q}$ (closed under scalar multiplication).

The field $\mathbb{Q}(\sqrt{2})$ is a 2-dimensional vector space over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

This is why we say that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Notice that the other field extensions we've seen are also vector spaces over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\},$$
$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}.$$

As $\mathbb{Q}$-vector spaces, $\mathbb{Q}(\sqrt{2}, i)$ has dimension 4, and $\mathbb{Q}(\zeta, \sqrt[3]{2})$ has dimension 6.

Definition

If $F \subseteq E$ are fields, then the degree of the extension, denoted $[E : F]$, is the dimension of E as a vector space over F.

Equivalently, this is the number of terms in the expression for a general element for E using coefficients from F.

Minimial polynomials

Definition

Let $r \notin F$ be algebraic. The minimal polynomial of r over F is the irreducible polynomial in $F[x]$ of which r is a root. It is unique up to scalar multiplication.

Examples

- $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
- $i = \sqrt{-1}$ has minimal polynomial $x^2 + 1$ over $\mathbb{Q}$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
- $\zeta = e^{2\pi i/3}$ has minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$, and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.
- $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

What are the minimal polynomials of the following numbers over $\mathbb{Q}$?

$$-\sqrt{2}\,, \qquad -i\,, \qquad \zeta^2\,, \qquad \zeta\sqrt[3]{2}\,, \qquad \zeta^2\sqrt[3]{2}\,.$$

Degree theorem

The degree of the extension $\mathbb{Q}(r)$ is the degree of the minimal polynomial of r.

The Galois group of a polynomial

Definition

Let $f \in \mathbb{Z}[x]$ be a polynomial, with roots $r_1, \dots, r_n$. The splitting field of f is the field

$$\mathbb{Q}(r_1, \dots, r_n)\,.$$

The splitting field F of $f(x)$ has several equivalent characterizations:

- the smallest field that contains all of the roots of $f(x)$;
- the smallest field in which $f(x)$ splits into linear factors:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n) \in F[x]\,.$$

Recall that the Galois group of an extension $F \supseteq \mathbb{Q}$ is the group of automorphisms of F, denoted $\mathrm{Gal}(F)$.

Definition

The Galois group of a polynomial $f(x)$ is the Galois group of its splitting field, denoted $\mathrm{Gal}(f(x))$.

A few examples of Galois groups

- The polynomial $x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$, so
$$\mathrm{Gal}(x^2 - 2) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})) \cong C_2\,.$$
- The polynomial $x^2 + 1$ splits in $\mathbb{Q}(i)$, so
$$\mathrm{Gal}(x^2 + 1) = \mathrm{Gal}(\mathbb{Q}(i)) \cong C_2\,.$$
- The polynomial $x^2 + x + 1$ splits in $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/3}$, so
$$\mathrm{Gal}(x^2 + x + 1) = \mathrm{Gal}(\mathbb{Q}(\zeta)) \cong C_2\,.$$
- The polynomial $x^3 - 1 = (x-1)(x^2 + x + 1)$ also splits in $\mathbb{Q}(\zeta)$, so
$$\mathrm{Gal}(x^3 - 1) = \mathrm{Gal}(\mathbb{Q}(\zeta)) \cong C_2\,.$$
- The polynomial $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ splits in $\mathbb{Q}(\sqrt{2}, i)$, so
$$\mathrm{Gal}(x^4 - x^2 - 2) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) \cong V_4\,.$$
- The polynomial $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so
$$\mathrm{Gal}(x^4 - 5x^2 + 6) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V_4\,.$$
- The polynomial $x^3 - 2$ splits in $\mathbb{Q}(\zeta, \sqrt[3]{2})$, so
$$\mathrm{Gal}(x^3 - 2) = \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3\ ???$$

The tower law of field extensions

Recall that if we had a chain of subgroups $K \leq H \leq G$, then the index satisfies a tower law: $[G : K] = [G : H][H : K]$.

Not surprisingly, the degree of field extensions obeys a similar tower law:

Theorem (Tower law)

For any chain of field extensions, $F \subset E \subset K$,

$$[K : F] = [K : E][E : F] \, .$$

We have already observed this in our subfield lattices:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\underbrace{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})}_{\text{min. poly: } x^2-3}][\underbrace{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}}_{\text{min. poly: } x^2-2}] = 2 \cdot 2 = 4 \, .$$

Here is another example:

$$[\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = [\underbrace{\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})}_{\text{min. poly: } x^2+x+1}][\underbrace{\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}}_{\text{min. poly: } x^3-2}] = 2 \cdot 3 = 6 \, .$$

Primitive elements

Primitive element theorem

If F is an extension of $\mathbb{Q}$ with $[F:\mathbb{Q}]<\infty$, then F has a primitive element: some $\alpha\notin\mathbb{Q}$ for which $F=\mathbb{Q}(\alpha)$.

How do we find a primitive element α of $F=\mathbb{Q}(\zeta,\sqrt[3]{2})=\mathbb{Q}(i\sqrt{3},\sqrt[3]{2})$?

Let's try $\alpha=i\sqrt{3}\sqrt[3]{2}\in F$. Clearly, $[\mathbb{Q}(\alpha):\mathbb{Q}]\leq 6$. Observe that

$$\alpha^2=-3\sqrt[3]{4},\quad \alpha^3=-6i\sqrt{3},\quad \alpha^4=-18\sqrt[3]{2},\quad \alpha^5=18i\sqrt[3]{4}\sqrt{3},\quad \alpha^6=-108.$$

Thus, α is a root of x^6+108. The following are equivalent (why?):

(i) α is a primitive element of F;
(ii) $[\mathbb{Q}(\alpha):\mathbb{Q}]=6$;
(iii) the minimal polynomial $m(x)$ of α has degree 6;
(iv) x^6+108 is irreducible (and hence must be $m(x)$).

In fact, $[\mathbb{Q}(\alpha):\mathbb{Q}]=6$ holds because both 2 and 3 divide $[\mathbb{Q}(\alpha):\mathbb{Q}]$:

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(i\sqrt{3})]\underbrace{[\mathbb{Q}(i\sqrt{3}):\mathbb{Q}]}_{=2},\qquad [\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt[3]{2})]\underbrace{[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]}_{=3}.$$

An example: The Galois group of $x^4 - 5x^2 + 6$

The polynomial $f(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$ has splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

We already know that its Galois group should be V_4. Let's compute it explicitly; this will help us understand it better.

We need to determine all automorphisms ϕ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know:

- ϕ is determined by where it sends the basis elements $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
- ϕ must fix 1.
- If we know where ϕ sends two of $\{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$, then we know where it sends the third, because

$$\phi(\sqrt{6}) = \phi(\sqrt{2}\sqrt{3}) = \phi(\sqrt{2})\,\phi(\sqrt{3})\,.$$

In addition to the identity automorphism e, we have

$$\begin{cases} \phi_2(\sqrt{2}) = -\sqrt{2} \\ \phi_2(\sqrt{3}) = \quad\sqrt{3} \end{cases} \qquad \begin{cases} \phi_3(\sqrt{2}) = \quad\sqrt{2} \\ \phi_3(\sqrt{3}) = -\sqrt{3} \end{cases} \qquad \begin{cases} \phi_4(\sqrt{2}) = -\sqrt{2} \\ \phi_4(\sqrt{3}) = -\sqrt{3} \end{cases}$$

Question

What goes wrong if we try to make $\phi(\sqrt{2}) = \sqrt{3}$?

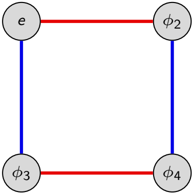
An example: The Galois group of $x^4 - 5x^2 + 6$

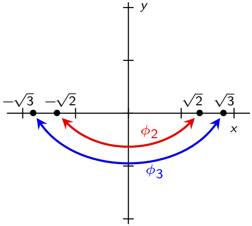
There are 4 automorphisms of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $x^4 - 5x^2 + 6$:

$$\begin{aligned}
e\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
\phi_2\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
\phi_3\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\phi_4\colon a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{aligned}$$

They form the Galois group of $x^4 - 5x^2 + 6$. The multiplication table and Cayley diagram are shown below.

	e	ϕ_2	ϕ_3	ϕ_4
e	e	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	e	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	e	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	e





Remarks

- $\alpha = \sqrt{2} + \sqrt{3}$ is a primitive element of F, i.e., $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- There is a group action of $\mathrm{Gal}(f(x))$ on the set of roots $S = \{\pm\sqrt{2}, \pm\sqrt{3}\}$ of $f(x)$.

The Galois group acts on the roots

Theorem

If $f \in \mathbb{Z}[x]$ is a polynomial with a root in a field extension F of $\mathbb{Q}$, then any automorphism of F permutes the roots of f.

Said differently, we have a group action of $\mathrm{Gal}(f(x))$ on the set $S = \{r_1, \ldots, r_n\}$ of roots of $f(x)$.

That is, we have a homomorphism

$$\psi\colon\ \mathrm{Gal}(f(x)) \longrightarrow \mathrm{Perm}(\{r_1, \ldots, r_n\})\,.$$

If $\phi \in \mathrm{Gal}(f(x))$, then $\psi(\phi)$ is a permutation of the roots of $f(x)$.

This permutation is what results by "pressing the ϕ-button" – it permutes the roots of $f(x)$ via the automorphism ϕ of the splitting field of $f(x)$.

Corollary

If the degree of $f \in \mathbb{Z}[x]$ is n, then the Galois group of f is a subgroup of S_n.

The Galois group acts on the roots

The next results says that "$\mathbb{Q}$ can't tell apart the roots of an irreducible polynomial."

The "One orbit theorem"

Let r_1 and r_2 be roots of an irreducible polynomial over $\mathbb{Q}$. Then

(a) There is an isomorphism $\phi\colon \mathbb{Q}(r_1) \longrightarrow \mathbb{Q}(r_2)$ that fixes $\mathbb{Q}$ and with $\phi(r_1) = r_2$.

(b) This remains true when $\mathbb{Q}$ is replaced with any extension field F, where $\mathbb{Q} \subset F \subset \mathbb{C}$.

Corollary

If $f(x)$ is irreducible over $\mathbb{Q}$, then for any two roots r_1 and r_2 of $f(x)$, the Galois group $\mathrm{Gal}(f(x))$ contains an automorphism $\phi\colon r_1 \longmapsto r_2$.

In other words, if $f(x)$ is irreducible, then the action of $\mathrm{Gal}(f(x))$ on the set $S = \{r_1, \dots, r_n\}$ of roots has only one orbit.

Normal field extensions

Definition

An extension field E of F is normal if it is the splitting field of some polynomial $f(x)$.

If E is a normal extension over F, then every irreducible polynomial in $F[x]$ that has a root in E splits over F.

Thus, if you can find an irreducible polynomial that has *one, but not all of its roots* in E, then E is *not* a normal extension.

Normal extension theorem

The degree of a normal extension is the order of its Galois group.

Corollary

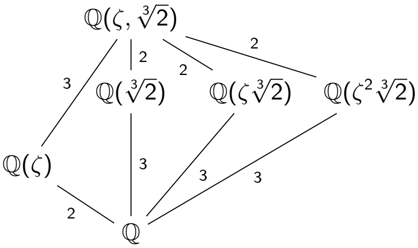
The order of the Galois group of a polynomial $f(x)$ is the degree of the extension of its splitting field over $\mathbb{Q}$.

Normal field extensions: Examples

Consider $\mathbb{Q}(\zeta, \sqrt[3]{2}) = \mathbb{Q}(\alpha)$, the splitting field of $f(x) = x^3 - 2$.

It is also the splitting field of $m(x) = x^6 + 108$, the minimal polynomial of $\alpha = \sqrt[3]{2}\sqrt{-3}$.

Let's see which of its intermediate subfields are normal extensions of $\mathbb{Q}$.



- $\mathbb{Q}$: Trivially normal.
- $\mathbb{Q}(\zeta)$: Splitting field of $x^2 + x + 1$; roots are $\zeta, \zeta^2 \in \mathbb{Q}(\zeta)$. Normal.
- $\mathbb{Q}(\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta^2\sqrt[3]{2})$: Contains only one root of $x^3 - 2$, not the other two. Not normal.
- $\mathbb{Q}(\zeta, \sqrt[3]{2})$: Splitting field of $x^3 - 2$. Normal.

By the normal extension theorem,

$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2\,, \qquad |\,\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6\,.$$

Moreover, you can check that $|\,\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}))| = 1 < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

The Galois group of $x^3 - 2$

We can now conclusively determine the Galois group of $x^3 - 2$.

By definition, the Galois group of a polynomial is the Galois group of its splitting field, so $\mathrm{Gal}(x^3 - 2) = \mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))$.

By the normal extension theorem, the order of the Galois group of $f(x)$ is the degree of the extension of its splitting field:

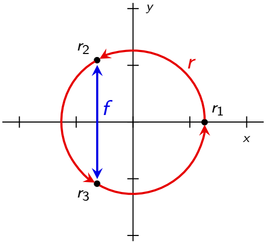
$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6\,.$$

Since the Galois group acts on the roots of $x^3 - 2$, it must be a subgroup of $S_3 \cong D_3$.

There is only one subgroup of S_3 of order 6, so $\mathrm{Gal}(x^3 - 2) \cong S_3$. Here is the action diagram of $\mathrm{Gal}(x^3 - 2)$ acting on the set $S = \{r_1, r_2, r_3\}$ of roots of $x^3 - 2$:

$$\begin{cases} r \colon \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \\ r \colon \zeta \longmapsto \zeta \end{cases}$$

$$\begin{cases} f \colon \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ f \colon \zeta \longmapsto \zeta^2 \end{cases}$$



Paris, May 31, 1832

The night before a duel that Évariste Galois knew he would lose, the 20-year-old stayed up late preparing his mathematical findings in a letter to Auguste Chevalier.

Hermann Weyl (1885–1955) said "*This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.*"

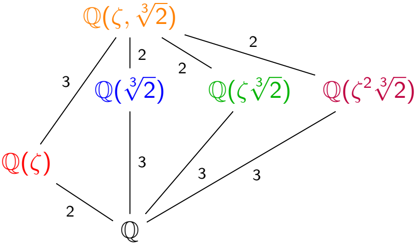
Fundamental theorem of Galois theory

Given $f \in \mathbb{Z}[x]$, let F be the splitting field of f, and G the Galois group. Then the following hold:

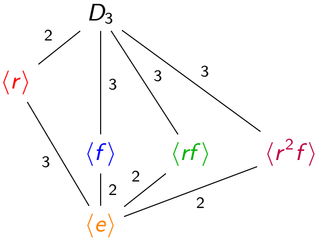
(a) The subgroup lattice of G is identical to the subfield lattice of F, but upside-down. Moreover, $H \lhd G$ if and only if the corresponding subfield is a normal extension of $\mathbb{Q}$.

(b) Given an intermediate field $\mathbb{Q} \subset K \subset F$, the corresponding subgroup $H < G$ contains precisely those automorphisms that fix K.

An example: the Galois correspondence for $f(x) = x^3 - 2$



Subfield lattice of $\mathbb{Q}(\zeta, \sqrt[3]{2})$



Subgroup lattice of $\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2})) \cong D_3$.

- The automorphisms that fix $\mathbb{Q}$ are precisely those in D_3.
- The automorphisms that fix $\mathbb{Q}(\zeta)$ are precisely those in $\langle r \rangle$.
- The automorphisms that fix $\mathbb{Q}(\sqrt[3]{2})$ are precisely those in $\langle f \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta\sqrt[3]{2})$ are precisely those in $\langle rf \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ are precisely those in $\langle r^2 f \rangle$.
- The automorphisms that fix $\mathbb{Q}(\zeta, \sqrt[3]{2})$ are precisely those in $\langle e \rangle$.

The normal field extensions of $\mathbb{Q}$ are: $\mathbb{Q}$, $\mathbb{Q}(\zeta)$, and $\mathbb{Q}(\zeta, \sqrt[3]{2})$.

The normal subgroups of D_3 are: D_3, $\langle r \rangle$ and $\langle e \rangle$.

An example: the Galois correspondence for $f(x) = x^8 - 2$

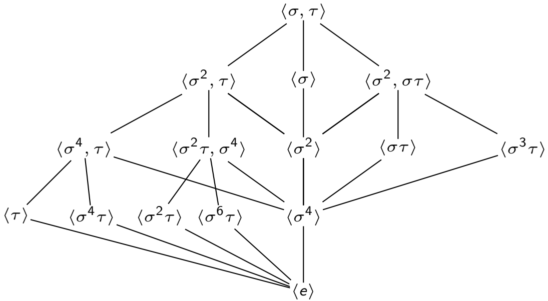
The splitting field of $x^8 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[8]{2}, i)$, a degree-16 extension over $\mathbb{Q}$. Its Galois group is the quasidihedral group $G = QD_8$:

$$QD_8 = \langle \sigma, \tau \mid \sigma^8 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle .$$

Let $\zeta = e^{2\pi i/8}$

$$\sqrt[8]{2} \overset{\sigma}{\longmapsto} \zeta\sqrt[8]{2}$$
$$i \longmapsto i$$

$$\sqrt[8]{2} \overset{\tau}{\longmapsto} \sqrt[8]{2}$$
$$i \longmapsto -i$$



Exercise

The subfields of $\mathbb{Q}(\sqrt[8]{2}, i)$ are: $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[8]{2})$, $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{Q}(\sqrt[4]{2}i)$, $\mathbb{Q}(\sqrt[8]{2}i)$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[4]{2}, i)$, $\mathbb{Q}((1+i)\sqrt[4]{2})$, $\mathbb{Q}((1-i)\sqrt[4]{2})$, $\mathbb{Q}(\zeta\sqrt[8]{2})$, $\mathbb{Q}(\zeta^3\sqrt[8]{2})$. Construct the subfield lattice.

Solvability

Definition

A group G is solvable if it has a chain of subgroups:

$$\{e\} = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_{k-1} \lhd N_k = G\,.$$

such that each quotient N_i/N_{i-1} is abelian.

Note: Each subgroup N_i need not be normal in G, just in N_{i+1}.

Examples

- $D_4 = \langle r, f \rangle$ is solvable. There are many possible chains:

$$\langle e \rangle \lhd \langle f \rangle \lhd \langle r^2, f \rangle \lhd D_4\,, \qquad \langle e \rangle \lhd \langle r \rangle \lhd D_4\,, \qquad \langle e \rangle \lhd \langle r^2 \rangle \lhd D_4.$$

- Any abelian group A is solvable: take $N_0 = \{e\}$ and $N_1 = A$.

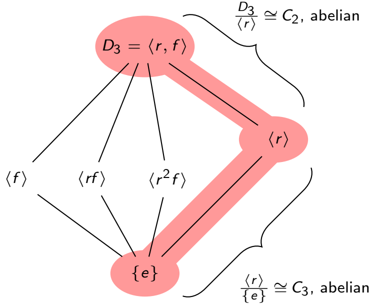
- For $n \geq 5$, the group A_n is simple and non-abelian. Thus, the only chain of normal subgroups is

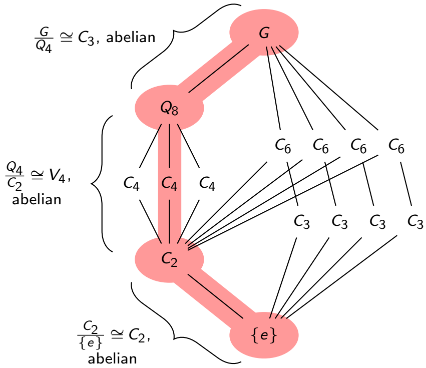
$$N_0 = \{e\} \lhd A_n = N_1\,.$$

  Since $N_1/N_0 \cong A_n$ is non-abelian, A_n is not solvable for $n \geq 5$.

Some more solvable groups

$D_3 \cong S_3$ is solvable: $\{e\} \lhd \langle r \rangle \lhd D_3$.





The group above at right is denoted $G = \mathrm{SL}(2,3)$. It consists of all 2×2 matrices with determinant 1 over the field $\mathbb{Z}_3 = \{0, 1, -1\}$.

$\mathrm{SL}(2,3)$ has order 24, and is the smallest solvable group that requires a three-step chain of normal subgroups.

The hunt for an unsolvable polynomial

The following lemma follows from the Correspondence Theorem. (Why?)

Lemma

If $N \lhd G$, then G is solvable if and only if both N and G/N are solvable.

Corollary

S_n is not solvable for all $n \geq 5$. (Since $A_n \lhd S_n$ is not solvable).

Galois' theorem

A field extension $E \supset \mathbb{Q}$ contains only elements expressible by radicals if and only if its Galois group is solvable.

Corollary

$f(x)$ is solvable by radicals if and only if it has a solvable Galois group.

Thus, any polynomial with Galois group S_5 is not solvable by radicals!

An unsolvable quintic!

To find a polynomial not solvable by radicals, we'll look for a polynomial $f(x)$ with $\text{Gal}(f(x)) \cong S_5$.

We'll restrict our search to degree-5 polynomials, because $\text{Gal}(f(x)) \leq S_5$ for any degree-5 polynomial $f(x)$.

Key observation

Recall that for any 5-cycle σ and 2-cycle (=transposition) τ,

$$S_5 = \langle \sigma, \tau \rangle .$$

Moreover, the *only* elements in S_5 of order 5 are 5-cycles, e.g., $\sigma = (a\ b\ c\ d\ e)$.

Let $f(x) = x^5 + 10x^4 - 2$. It is irreducible by Eisenstein's criterion (use $p = 2$). Let $F = \mathbb{Q}(r_1, \dots, r_5)$ be its splitting field.

Basic calculus tells us that f exactly has 3 real roots. Let $r_1, r_2 = a \pm bi$ be the complex roots, and r_3, r_4, and r_5 be the real roots.

Since f has distinct complex conjugate roots, complex conjugation is an automorphism $\tau \colon F \longrightarrow F$ that transposes r_1 with r_2, and fixes the three real roots.

An unsolvable quintic!

We just found our transposition $\tau = (r_1\ r_2)$. All that's left is to find an element (i.e., an automorphism) σ of order 5.

Take any root r_i of $f(x)$. Since $f(x)$ is irreducible, it is the minimal polynomial of r_i. By the Degree Theorem,

$$[\mathbb{Q}(r_i) : \mathbb{Q}] = \deg(\text{minimum polynomial of } r_i) = \deg f(x) = 5\,.$$

The splitting field of $f(x)$ is $F = \mathbb{Q}(r_1, \dots, r_5)$, and by the normal extension theorem, the degree of this extension over $\mathbb{Q}$ is the order of the Galois group $\mathrm{Gal}(f(x))$.

Applying the tower law to this yields

$$|\,\mathrm{Gal}(f(x))| = [\mathbb{Q}(r_1, r_2, r_3, r_4, r_5) : \mathbb{Q}] = [\mathbb{Q}(r_1, r_2, r_3, r_4, r_5) : \mathbb{Q}(r_1)]\,\underbrace{[\mathbb{Q}(r_1) : \mathbb{Q}]}_{=5}.$$

Thus, $|\,\mathrm{Gal}(f(x))|$ is a multiple of 5, so Cauchy's theorem guarantees that G has an element σ of order 5.

Since $\mathrm{Gal}(f(x))$ has a 2-cycle τ and a 5-cycle σ, it must be all of S_5.

$\mathrm{Gal}(f(x))$ is an unsolvable group, so $f(x) = x^5 + 10x^4 - 2$ is unsolvable by radicals!

Summary of Galois' work

Let $f(x)$ be a degree-n polynomial in $\mathbb{Z}[x]$ (or $\mathbb{Q}[x]$). The roots of $f(x)$ lie in some splitting field $F \supseteq \mathbb{Q}$.

The Galois group of $f(x)$ is the automorphism group of F. Every such automorphism fixes $\mathbb{Q}$ and permutes the roots of $f(x)$.

This is a group action of $\text{Gal}(f(x))$ on the set of n roots! Thus, $\text{Gal}(f(x)) \leq S_n$.

There is a 1–1 correspondence between subfields of F and subgroups of $\text{Gal}(f(x))$.

A polynomial is solvable by radicals iff its Galois group is a solvable group.

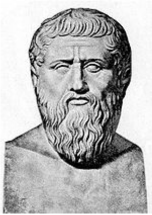
The symmetric group S_5 is not a solvable group.

Since $S_5 = \langle \tau, \sigma \rangle$ for a 2-cycle τ and 5-cycle σ, all we need to do is find a degree-5 polynomial whose Galois group contains a 2-cycle and an element of order 5.

If $f(x)$ is an irreducible degree-5 polynomial with 3 real roots, then complex conjugation is an automorphism that transposes the 2 complex roots. Moreover, Cauchy's theorem tells us that $\text{Gal}(f(x))$ must have an element of order 5.

Thus, $f(x) = x^5 + 10x^4 - 2$ is not solvable by radicals!

Geometry and the Ancient Greeks



Plato (5th century B.C.) believed that the only "perfect" geometric figures were the straight line and the circle.

In Ancient Greek geometry, this philosophy meant that there were only two instruments available to perform geometric constructions:

1. the ruler: a single unmarked straight edge.
2. the compass: collapses when lifted from the page

Formally, this means that the only permissible constructions are those granted by Euclid's first three postulates.

Geometry and the Ancient Greeks

Around 300 BC, ancient Greek mathematician Euclid wrote a series of thirteen books that he called The Elements.

It is a collection of definitions, postulates (axioms), and theorems & proofs, covering geometry, elementary number theory, and the Greek's "geometric algebra."

Book 1 contained Euclid's famous *10 postulates*, and other basic propositions of geometry.

Euclid's first three postulates

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as center.

Using only these tools, lines can be divided into equal segments, angles can be bisected, parallel lines can be drawn, n-gons can be "squared," and so on.

Geometry and the Ancient Greeks

One of the chief purposes of Greek mathematics was to find exact constructions for various lengths, using only the basic tools of a ruler and compass.

The ancient Greeks were unable to find constructions for the following problems:

Problem 1: Squaring the circle

Draw a square with the same area as a given circle.

Problem 2: Doubling the cube

Draw a cube with twice the volume of a given cube.

Problem 3: Trisecting an angle

Divide an angle into three smaller angles all of the same size.

For over 2000 years, these problems remained unsolved.

Alas, in 1837, Pierre Wantzel used field theory to prove that these constructions were impossible.

What does it mean to be "constructible"?

Assume P_0 is a set of points in $\mathbb{R}^2$ (or equivalently, in the complex plane $\mathbb{C}$).

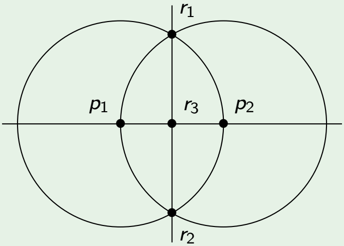
Definition

The points of intersection of any two distinct lines or circles are constructible in one step.

A point $r \in \mathbb{R}^2$ is constructible from P_0 if there is a finite sequence $r_1, \dots, r_n = r$ of points in $\mathbb{R}^2$ such that for each $i = 1, \dots, n$, the point r_i is constructible in one step from $P_0 \cup \{r_1, \dots, r_{i-1}\}$.

Example: bisecting a line

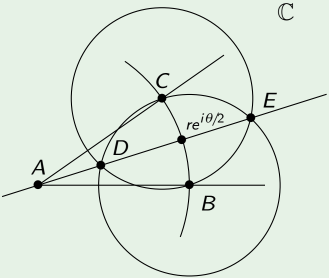
1. Start with a line $p_1 p_2$;
2. Draw the circle of center p_1 of radius $p_1 p_2$;
3. Draw the circle of center p_2 of radius $p_1 p_2$;
4. Let r_1 and r_2 be the points of intersection;
5. Draw the line $r_1 r_2$;
6. Let r_3 be the intersection of $p_1 p_2$ and $r_1 r_2$.



Bisecting an angle

Example: bisecting an angle

1. Start with an angle at A;
2. Draw a circle centered at A;
3. Let B and C be the points of intersection;
4. Draw a circle of radius BC centered at B;
5. Draw a circle of radius BC centered at C;
6. Let D and E be the intersections of these 2 circles;
7. Draw a line through DE.



Suppose A is at the origin in the complex plane. Then $B = r$ and $C = re^{i\theta}$.

Bisecting an angle means that we can construct $re^{i\theta/2}$ from $re^{i\theta}$.

Constructible numbers: Real vs. complex

Henceforth, we will say that a point is constructible if it is constructible from the set

$$P_0 = \{(0,0),\ (1,0)\} \subset \mathbb{R}^2 .$$

Say that $z = x + yi \in \mathbb{C}$ is constructible if $(x, y) \in \mathbb{R}^2$ is constructible. Let $K \subseteq \mathbb{C}$ denote the constructible numbers.

Lemma

A complex number $z = x + yi$ is constructible if x and y are constructible.

By the following lemma, we can restrict our focus on real constructible numbers.

Lemma

1. $K \cap \mathbb{R}$ is a subfield of $\mathbb{R}$ if and only if K is a subfield of $\mathbb{C}$.
2. Moreover, $K \cap \mathbb{R}$ is closed under (nonnegative) square roots if and only if K is closed under (all) square roots.

$K \cap \mathbb{R}$ closed under square roots means that $a \in K \cap \mathbb{R}^+$ implies $\sqrt{a} \in K \cap \mathbb{R}$.

K closed under square roots means that $z = re^{i\theta} \in K$ implies $\sqrt{z} = \sqrt{r}e^{i\theta/2} \in K$.

The field of constructible numbers

Theorem

The set of constructible numbers K is a subfield of $\mathbb{C}$ that is closed under taking square roots and complex conjugation.

Proof (sketch)

Let a and b be constructible real numbers, with $a > 0$. It is elementary to check that each of the following hold:

1. $-a$ is constructible;
2. $a + b$ is constructible;
3. ab is constructible;
4. a^{-1} is constructible;
5. $\sqrt{a}$ is constructible;
6. $a - bi$ is constructible provided that $a + bi$ is.

Corollary

If $a, b, c \in \mathbb{C}$ are constructible, then so are the roots of $ax^2 + bx + c$.

Constructions as field extensions

Let $F \subset K$ be a field generated by ruler and compass constructions.

Suppose α is constructible from F in one step. We wish to determine $[F(\alpha) : F]$.

The three ways to construct new points from F

1. Intersect two lines. The solution to $ax + by = c$ and $dx + ey = f$ lies in F.
2. Intersect a circle and a line. The solution to

$$\begin{cases} ax + by = c \\ (x-d)^2 + (y-e)^2 = r^2 \end{cases}$$

   lies in (at most) a quadratic extension of F.
3. Intersect two circles. We need to solve the system

$$\begin{cases} (x-a)^2 + (y-b)^2 = s^2 \\ (x-d)^2 + (y-e)^2 = r^2 \end{cases}$$

   Multiply this out and subtract. The x^2 and y^2 terms cancel, leaving the equation of a line. Intersecting this line with one of the circles puts us back in Case 2.

In all of these cases, $[F(\alpha) : F] \leq 2$.

Constructions as field extensions

In others words, constructing a number $\alpha \notin F$ in one step amounts to taking a degree-2 extension of F.

Theorem

A complex number α is constructible if and only if there is a tower of field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$

where $\alpha \in K_n$ and $[K_{i+1} : K_i] \leq 2$ for each i.

Corollary

The set $K \subset \mathbb{C}$ of constructible numbers is a field. Moreover, if $\alpha \in K$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some integer n.

Next, we will show that the ancient Greeks' classical construction problems are impossible by demonstrating that each would yield a number $\alpha \in \mathbb{R}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is not a power of two.

Classical constructibility problems, rephrased

Problem 1: Squaring the circle

Given a circle of radius r (and hence of area πr^2), construct a square of area πr^2 (and hence of side-length $\sqrt{\pi} r$).

If one could square the circle, then $\sqrt{\pi} \in K \subset \mathbb{C}$, the field of constructible numbers.

However,

$$\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$$

and so $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Hence $\sqrt{\pi}$ is not constructible.

Problem 2: Doubling the cube

Given a cube of length ℓ (and hence of volume ℓ^3), construct a cube of volume $2\ell^3$ (and hence of side-length $\sqrt[3]{2}\ell$).

If one could double the cube, then $\sqrt[3]{2} \in K$.

However, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of two. Hence $\sqrt[3]{2}$ is not constructible.

Classical constructibility problems, rephrased

Problem 3: Trisecting an angle

Given $e^{i\theta}$, construct $e^{i\theta/3}$. Or equivalently, construct $\cos(\theta/3)$ from $\cos(\theta)$.

We will show that $\theta = 60^\circ$ cannot be trisected. In other words, that $\alpha = \cos(20^\circ)$ cannot be constructed from $\cos(60^\circ)$.

The triple angle formula yields

$$\cos(\theta) = 4\cos^3(\theta/3) - 3\cos(\theta/3)\,.$$

Set $\theta = 60^\circ$. Plugging in $\cos(\theta) = 1/2$ and $\alpha = \cos(20^\circ)$ gives

$$4\alpha^3 - 3\alpha - \frac{1}{2} = 0\,.$$

Changing variables by $u = 2\alpha$, and then multiplying through by 2:

$$u^3 - 3u - 1 = 0\,.$$

Thus, u is the root of the (irreducible!) polynomial $x^3 - 3x - 1$. Therefore, $[\mathbb{Q}(u) : \mathbb{Q}] = 3$, which is not a power of 2.

Hence, $u = 2\cos(20^\circ)$ is not constructible, so neither is $\alpha = \cos(20^\circ)$.

Classical constructibility problems, resolved

The three classical ruler-and-compass constructions that stumped the ancient Greeks, when translated in the language of field theory, are as follows:

Problem 1: Squaring the circle

Construct $\sqrt{\pi}$ from 1.

Problem 2: Doubling the cube

Construct $\sqrt[3]{2}$ from 1.

Problem 3: Trisecting an angle

Construct $\cos(\theta/3)$ from $\cos(\theta)$. [Or $\cos(20^\circ)$ from 1.]

Since none of these numbers these lie in an extension of $\mathbb{Q}$ of degree 2^n, they are not constructible.

If one is allowed a "marked ruler," then these constructions become possible, which the ancient Greeks were aware of.

Construction of regular polygons

The ancient Greeks were also interested in constructing regular polygons. They knew constructions for 3-, 5-, and 15-gons.

In 1796, nineteen-year-old Carl Friedrich Gauß, who was undecided about whether to study mathematics or languages, discovered how to construct a regular 17-gon.

Gauß was so pleased with his discovery that he dedicated his life to mathematics.

He also proved the following theorem about which n-gons are constructible.

Theorem (Gauß, Wantzel)

Let p be an odd prime. A regular p-gon is constructible if and only if $p = 2^{2^n} + 1$ for some $n \geq 0$.

The next question to ask is for which n is $2^{2^n} + 1$ prime?

Construction of regular polygons and Fermat primes

Definition

The n^{th} Fermat number is $F_n := 2^{2^n} + 1$. If F_n is prime, then it is a Fermat prime.

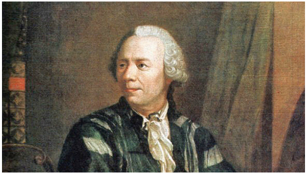
The first few Fermat primes are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$.

They are named after Pierre Fermat (1601–1665), who conjectured in the 1600s that all Fermat numbers $F_n = 2^{2^n} + 1$ are prime.

Construction of regular polygons and Fermat primes

In 1732, Leonhard Euler disproved Fermat's conjecture by demonstrating

$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417$.



It is not known if any other Fermat primes exist!

So far, every F_n is known to be composite for $5 \leq n \leq 32$. In 2014, a computer showed that $193 \times 2^{3329782} + 1$ is a prime factor of

$$F_{3329780} = 2^{2^{3329780}} + 1 > 10^{10^{10^6}}.$$

Theorem (Gauß, Wantzel)

A regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_m$, where $p_1, \dots, p_m$ are distinct Fermat primes.

If these type of problems interest you, take Math 4100! (Number theory)