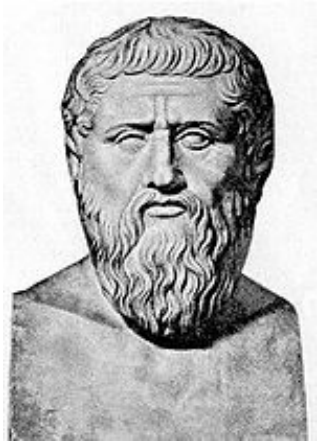
Chapter 10: Fields and Galois theory

Matthew Macauley

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

Math 4120, Visual Algebra

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


EVCLIDIS
ELEMENTORVM
LIBRI XV.
Accessit liber XVI. De Solidorum Regularium cuiuslibet intra quodlibet comparatione.
OMNES PERSPICVIS DEMONSTRATIONIBVS, accuratisque Scholijs illustrati: nunc quarto editi, ac multarum rerum accessione post primam editionem locupletati.
Authore
CHRISTOPHORO CLAVIO
Bambergensi è Societate Iesv.
FRANCOFVRTI,
Ex Officina Typographica Nicolai Hoffmanni,
Sumptibus Ionae Rhodij.
M. DC. VII.

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.

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 centuries, 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, and turned problems in field theory into ones in group theory.

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!

Fields

To do arithmetic, we need to be working in a field.

Definition

A set K with $+$ and $\cdot$ is a field if the following three conditions hold:

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

A field homomorphism $\phi\colon K \to L$ is just a ring homomorphism betweeen fields:

$$\phi(x+y) = \phi(x) + \phi(y), \qquad \phi(xy) = \phi(x)\phi(y), \quad \text{for all } x, y \in K.$$

Key idea

Since fields are simple, every nonzero field homomorphism is an embedding.

In other words, we can't ever take the quotient of a field K; we can only "extend" it, into a larger field $K \hookrightarrow L$.

Field extensions

Definition

If K and L are fields with $K \subset L$, we say that L is an extension of K, and write L/K.

The term "field extension" may refer to either

- a pair $K \subseteq L$ of a subfield K and extension field L;
- an embedding $K \hookrightarrow L$ where $K \subseteq L$.

Key observation

If L/K is a field extension, then L is a vector space over K.

Definition

The degree of the extension L/K is the vector space dimension, $[L : K] := \dim_K(L)$.

Example

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

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

This is a 2-dimensional $\mathbb{Q}$-vector space, with basis $\left\{1, \sqrt{m}\right\}$.

The smallest extension field containing a set S

Definition

Suppose L/K is a field extension, and $K \subseteq S \subseteq L$. The extension of K generated by S is

$$K(S) := \bigcap \{E \mid E/K \text{ is an extension s.t. } S \subseteq E \subseteq L\}.$$

We call this: "K adjoin S."

The field $K(S)$ can also be characterized as the elements that can be obtained from S using finitely many field operations.

If $S = \{\alpha\}$, then $K(\alpha) := K(\{\alpha\})$ is a simple extension, and α is a primitive element.

Note that $K(\alpha)$ is the result of:

- starting with the polynomial ring $K[x]$ and substituting α for x,
- constructing the field of fractions

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in K[x],\ g(\alpha) \neq 0 \right\}.$$

If we want to adjoin multiple elements, $\alpha_1, \ldots, \alpha_n$, we can write $K(\alpha_1, \ldots, \alpha_n)$.

Splitting fields and algebraic closure

Definition

The splitting field of $f(x) \in K[x]$ is the field $K(r_1, \ldots, r_n)$.

The name comes from the fact that in this field, $f(x)$ completely factors, or splits:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n), \qquad r_i \in K(r_1, \ldots, r_n).$$

Definition

A field K is algebraically closed if every polynomial $f(x) \in K[x]$ splits.

Fundamental theorem of algebra

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

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

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 $\sqrt{-1} \notin \mathbb{R}$.

Splitting fields of $\mathbb{Q}$

The splitting field of $f(x) = x^2 - 2$ is $\mathbb{Q}(\sqrt{2})$, the smallest field that contains both roots.

That is, $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ splits in $\mathbb{Q}(\sqrt{2})[x]$.

The splitting field of $g(x) = (x^2 - 2)(x^2 + 1)$ can be constructed in two steps:

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

(ii) Adjoin the roots of $x^2 + 1$ 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

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

$\mathbb{Q}(\sqrt{2}, i)$ is a 4-dimensional $\mathbb{Q}$-vector space, with basis $\{1, \sqrt{2}, i, \sqrt{2}i\}$:

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

That is, the degree of this extension is $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.

Subfield lattices

The field

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

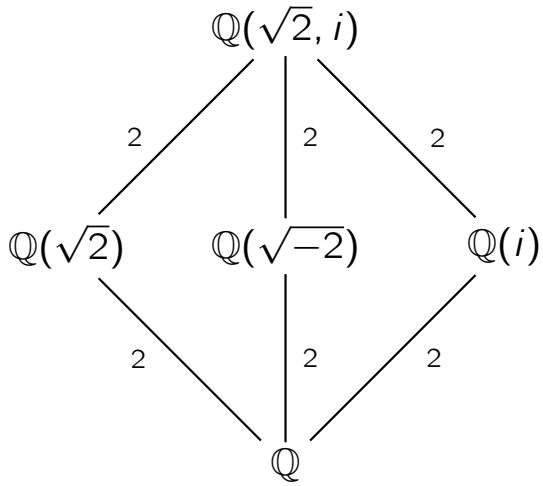
has several subfields, which are $\mathbb{Q}$-vector subspaces:

$$\mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{-2}), \qquad \mathbb{Q}.$$

Like with did with a group and its subgroups, we can arrange them in a lattice.

Each edge is labeled with the degree of the extension.

Alternatively, the label d of $K \subseteq L$ is the degree of a particular polynomial...



To construct $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, ajoin a root of $x^2 - 2$ (get both).

To construct $\mathbb{Q}(i)/\mathbb{Q}$, ajoin a root of $x^2 + 1$ (get both).

To construct $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, ajoin a root of $x^2 + 2$ (get both).

To construct $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, ajoin the root of $(x^2 - 2)(x^2 + 1)$.

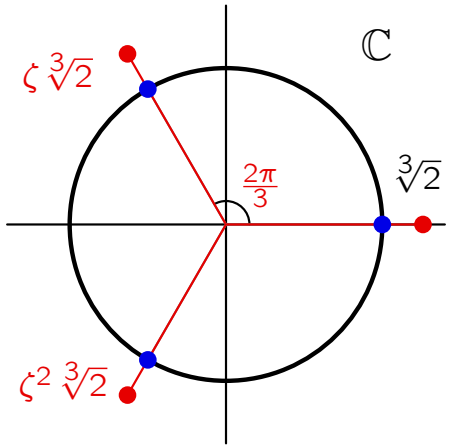
Another extension field of $\mathbb{Q}$

The polynomial $f(x) = x^3 - 2$ splits over $\mathbb{C}$ as

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta)(x - \sqrt[3]{2}\zeta^2), \qquad \zeta = e^{2\pi i/3} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i.$$

Its splitting field (i.e., smallest field over which it factors) is

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



But this field contains $\zeta\sqrt[3]{2}/\sqrt[3]{2} = \zeta$.

Thus, $\mathbb{Q}(\sqrt[3]{2}, \zeta) \subseteq K$; and "$\supseteq$" clearly holds.

There are other ways to write this field. Since $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \in \mathbb{Q}(\zeta, \sqrt[3]{2})$, so does $2(\zeta + \frac{1}{2}) = \sqrt{3}i = \sqrt{-3}$. Thus,

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

This field is an extension of $\mathbb{Q}$ of degree $6 = [\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}]$:

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

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

What are the subfields of

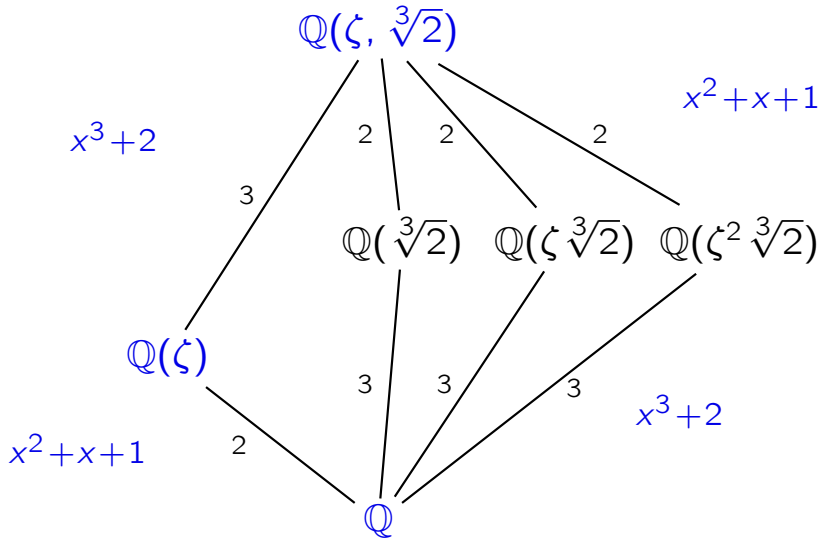
$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} \mid a, b, c, d, e, f \in \mathbb{Q}\right\}?$$

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

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

Each root generates a subfield: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$ and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$.

Here is the subfield lattice:

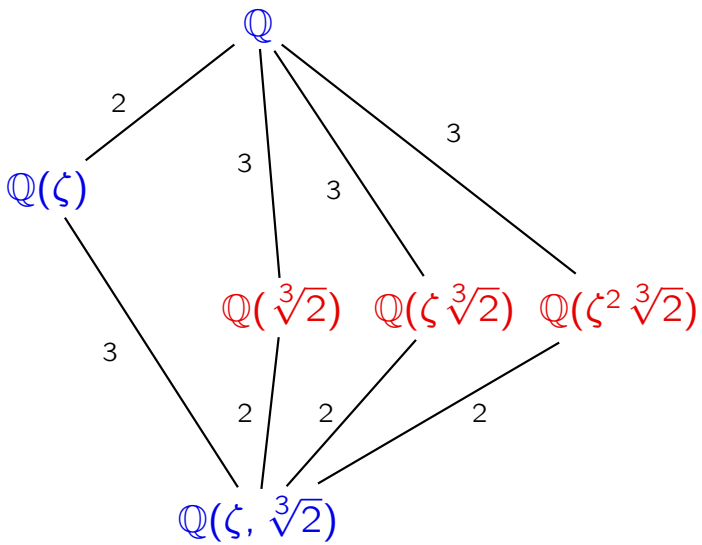


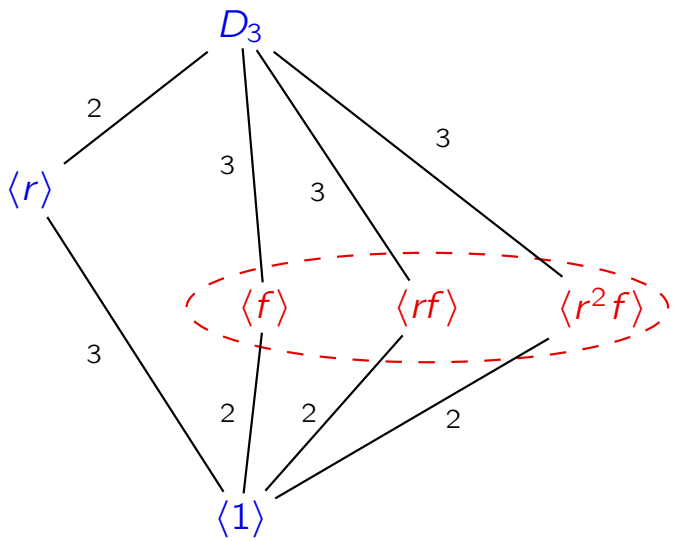
This lattice should look very familiar. . . but also a little different.

Subfield lattices

The similarity between the subfield lattice of $\mathbb{Q}(\zeta, \sqrt[3]{2})$ and subgroup lattice of D_3 is not a coincidence!

Because of this, we will henceforth draw all subfield lattices upside-down.





To construct $\mathbb{Q}(\zeta)/\mathbb{Q}$, ajoin a root of $x^2 + x + 1$ (get both).

To construct $\mathbb{Q}(\zeta^i \sqrt[3]{2})/\mathbb{Q}$, for $i = 0, 1, 2$, adjoin only one root of $x^3 + 2$.

To construct $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}(\zeta)$, adjoin one root of $x^2 + x + 1$ (get both).

To construct $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}(\zeta^i \sqrt[3]{2})$, for $i = 0, 1, 2$, adjoin one root of $x^2 + x + 1$ (get both).

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 and transcendental numbers

Definition

A complex number is algebraic (over $\mathbb{Q}$) if it is the root of a 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

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

Question

Can *all* algebraic numbers be expressed using radicals?

This question was unsolved until the early 1800s.

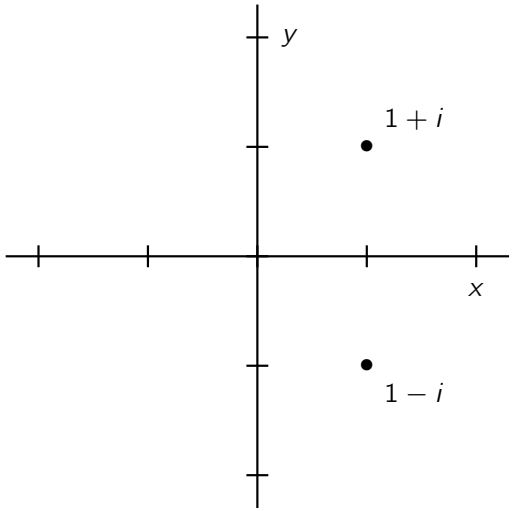
Complex conjugates

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.

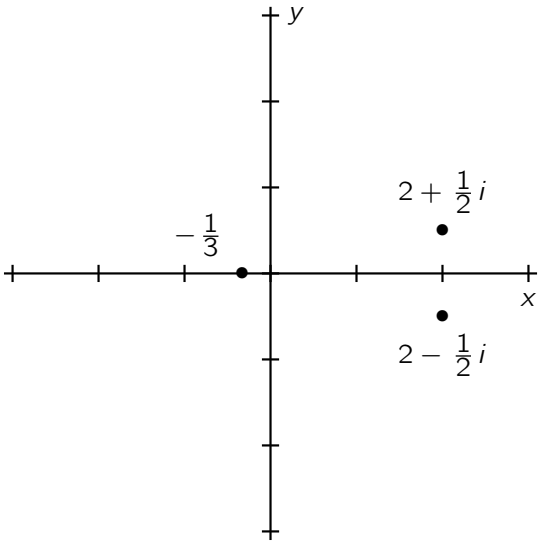
$f(x) = x^2 - 2x + 2$

Roots: $1 \pm i$



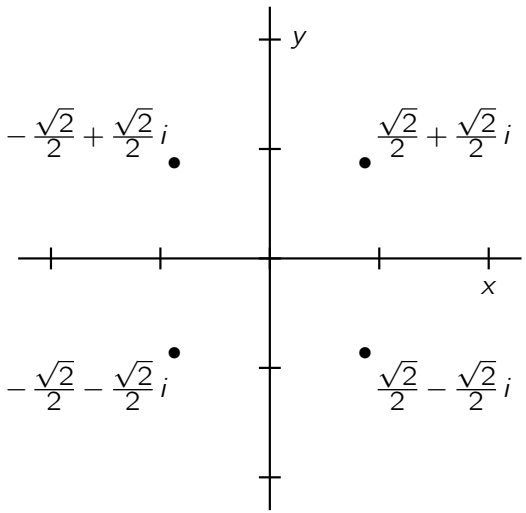
$f(x) = 12x^3 - 44x^2 + 35x + 17$

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



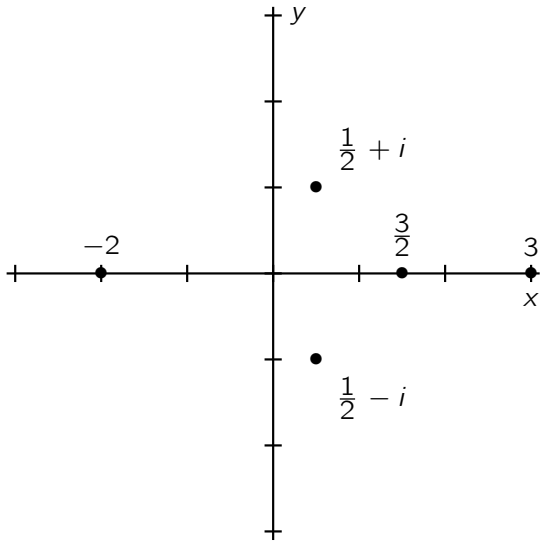
$f(x) = x^4 + 1$

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 $\mathbb{Q}$, but reducible over $\mathbb{Q}(\sqrt[3]{2})$.

Remarks

- 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 $\mathbb{C}$.
- Eisenstein's criterion is helpful for establishing irreducibility over $\mathbb{Q}$.

Extension fields as vector spaces

Recall that if E/F is a field extension, then E is an F-vector space.

The dimension of a vector space is the size of a basis.

Definition

The degree of an extension E/F, denoted $[E : F]$, is the dimension of E as an F-vector space.

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

Here are some examples of extensions we've seen:

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, i) &= \left\{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\right\} & [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] &= 4\\ &= \left\{\alpha + \beta i \mid \alpha, \beta \in \mathbb{Q}(\sqrt{2})\right\} & [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] &= 2\end{aligned}$$

$$\begin{aligned}\mathbb{Q}(\sqrt[3]{2}, \zeta) &= \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} \mid a, \ldots, f \in \mathbb{Q}\right\} & [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] &= 6\\ &= \left\{\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4} \mid \alpha, \beta, \gamma \in \mathbb{Q}(\zeta)\right\} & [\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\zeta)] &= 3\\ &= \left\{p + q\zeta \mid p, q \in \mathbb{Q}(\zeta)\right\} & [\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})] &= 2\end{aligned}$$

Field homomorphisms and extensions

A field homomorphism $\phi\colon F \to E$ is just a ring homomorphism betweeen fields:

$$\phi(x+y) = \phi(x) + \phi(y), \qquad \phi(xy) = \phi(x)\phi(y), \quad \text{for all } x, y \in F.$$

Key idea

Since fields have no nontrivial ideals, every nonzero field homomorphism is an embedding.

A field extension may refer to either

- a pair $F \subseteq E$ of a subfield E extension field F;
- an embedding $F \hookrightarrow E$ where $F \subseteq E$.

Two extensions $F \to E$ and $K \to L$ are equivalent if there are isomorphisms $\phi\colon F \to K$ and $\sigma\colon K \to L$ such that the following diagram commutes:

$$\begin{array}{ccc} F & \xrightarrow{\phi} & K \\ \downarrow & & \downarrow \\ E & \xrightarrow{\sigma} & L \end{array}$$

We'll see that $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ and $\mathbb{Q} \subseteq \mathbb{Q}(x)$ are equivalent extensions.

Do you think that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\zeta\sqrt[3]{2})$ are equivalent?

Algebraic extensions

Definition

A simple extension $K(\alpha)$ is algebraic if $f(\alpha) = 0$ for some $f(x) \in K[x]$. We say

"*α is algebraic over K.*"

Proposition

There is a unique monic polynomial $m(x) \in K[x]$ for which $m(\alpha) = 0$, called the minimal polynomial of α over K, and it is irreducible.

Proof

The polynomials $f(x)$ in $K[x]$ for which $f(\alpha) = 0$ form an ideal I.

Uniqueness. Since $K[x]$ is Euclidean (and thus a PID), we can write $I = (m(x))$ for some unique monic polynomial. ✓

Irreducibility. Suppose $m(x) = f(x)g(x)$, with $f(x)$ and $g(x)$ having lower degree.

Then $m(\alpha) = f(\alpha)g(\alpha) = 0$ implies $f(\alpha) = 0$ or $g(\alpha) = 0$, contradiciting minimality. ✓

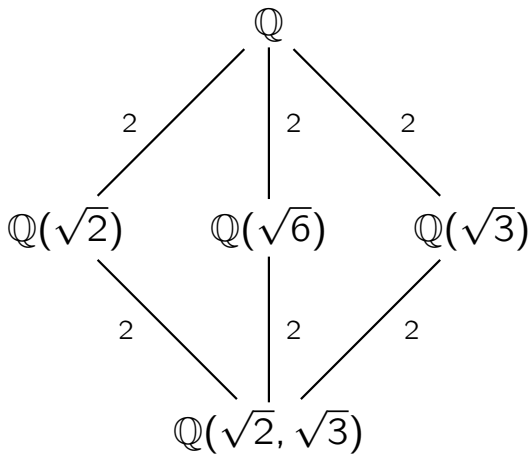
Algebraic extensions

Let's find the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over various extension fields.

It is elementary to check that

$$\sqrt{2}\alpha = 2 + \sqrt{6}, \qquad \sqrt{3}\alpha = 3 + \sqrt{6}, \qquad \alpha^2 = 5 + 2\sqrt{6}, \qquad \alpha^2 = 49 + 20\sqrt{6}.$$

- Over $\mathbb{Q}$: $m(x) = x^4 - 10x^2 + 1$.
- Over $\mathbb{Q}(\sqrt{2})$: $m(x) = x^2 - 2\sqrt{2}x - 1$.
- Over $\mathbb{Q}(\sqrt{3})$: $m(x) = x^2 - 2\sqrt{3}x + 13$.
- Over $\mathbb{Q}(\sqrt{6})$: $m(x) = x^2 - (5 + 2\sqrt{6})$.
- Over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$: $m(x) = x - (\sqrt{2} + \sqrt{3})$.



Key idea

The degree of the extension $F(\alpha)$ is the degree of the minimal polynomial $m(\alpha)$.

Elements in simple extension

Polynomial lemma

If $[F(\alpha) : F] < \infty$, then every $s \in F(\alpha)$ can be written uniquely as $s = r(\alpha)$, for some $r(x) \in F[x]$ with $\deg(r(x)) < \deg(m_\alpha(x))$.

Proof

Existence. Given $s \in F(\alpha)$, write $s = f(\alpha)/g(\alpha)$, for $f, g \in F[x]$.

Note that $m(x) \nmid g(x)$ since $g(\alpha) \neq 0$, and since $m_\alpha(x)$ is irreducible,

$$\begin{aligned} \gcd\big(g(x), m_\alpha(x)\big) = 1 \quad &\Longrightarrow \quad a(x)g(x) + b(x)m_\alpha(x) = 1 \text{ for some } a(x), b(x) \in F[x] \\ &\Longrightarrow \quad a(\alpha)g(\alpha) + \underbrace{b(\alpha)m_\alpha(\alpha)}_{=0} = 1 \\ &\Longrightarrow \quad s = f(\alpha)a(\alpha) \end{aligned}$$

Divide $m(x)$ into $h(x) := f(x)a(x)$, to get

$$h(x) = q(x)m(x) + r(x), \qquad \deg(r(x)) < \deg(m(x)).$$

Plugging in α yields $h(\alpha) = r(\alpha)$. ✓

Uniqueness. If $s = r_1(\alpha) = r_2(\alpha)$, then $\underbrace{r_1(x) - r_2(x)}_{\deg < \deg(m(x))} \in (m(x)) \quad \Rightarrow \quad r_1 - r_2 = 0$ □

Elements in simple extension

Corollary

If α, β have the same minimal polynomial $m(x)$ over F, then $F(\alpha) \cong F(\beta)$.

Proof

By the polynomial lemma, the following map is a bijection:

$$\sigma\colon F(\alpha) \longrightarrow F(\beta), \qquad \sigma\colon c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \longmapsto c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}.$$

We have $\sigma(x+y) = \sigma(x) + \sigma(y)$; it suffices to show $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in F(\alpha)$.

Let $x = f(\alpha)$, $y = g(\alpha)$, $xy = h(\alpha)$, for polynomals of degree less than $\deg m(x)$.

$$f(\alpha)g(\alpha) - h(\alpha) = xy - xy = 0 \quad \Longrightarrow \quad m(x) \mid \big[f(x)g(x) - h(x)\big].$$

Thus, $m(x)q(x) = f(x)g(x) - h(x)$ for some $q(x) \in F[x]$, which rearranged is:

$$f(x)g(x) = m(x)q(x) + h(x), \quad \deg(h(x)) < \deg(m(x)).$$

Plug in α to get $f(\alpha)g(\alpha) = h(\alpha)$. Similarly, $f(\beta)g(\beta) = h(\beta)$. Note that

$$\sigma(xy) = h(\beta) = f(\alpha)f(\beta) = \sigma(x)\sigma(y),$$ □

Algebraic extensions

Degree theorem

The degree of an algebraic extension $[F(\alpha) : F]$ is the degree of the minimal polynomial $m_\alpha(x)$ in $F[x]$.

Proof

It suffices to show that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis.

By the polynomial lemma (existence), this set spans.

By the polynomial lemma (uniqueness), it is linearly independent. $\square$

Definition

The extension E/F is algebraic if every element of E is algebraic over F.

Algebraic extensions

Definition

An extension E/F is finite if $[E : F] < \infty$.

Lemma

Every finite extension is algebraic.

Proof

Suppose $[E : F] = n < \infty$. Pick any $\alpha \in E$. Then $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent, so

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0, \qquad \text{for some } c_i \in F.$$

The converse fails: $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$ is not finite over $\mathbb{Q}$.

As a corollary, the algebraic numbers $\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ are a field.

By the lemma, $\alpha \in \mathbb{A}$ iff $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Let $\alpha, \beta \in \mathbb{A}$.

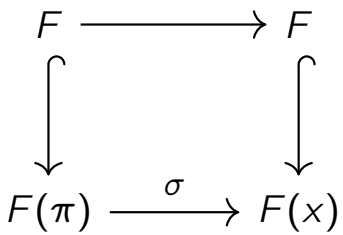
$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$$

Therefore, assuming $a \neq 0$,

$$[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] < \infty, \quad [\mathbb{Q}(-\alpha) : \mathbb{Q}] < \infty, \quad [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] < \infty, \quad [\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}] < \infty.$$

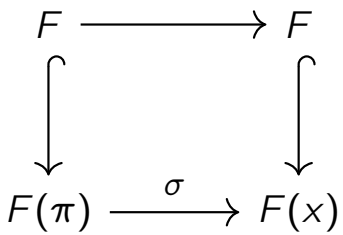
Transcendental extensions

All simple transcendental extensions are equivalent:



Transcendental extensions

All simple transcendental extensions are equivalent:



Field automorphisms

Recall that every automorphism of an extension field F of $\mathbb{Q}$ fixes all elements of $\mathbb{Q}$.

Definition

If K/F is a field extension, let $\mathbf{Aut}(K/F)$ be the automorphism of K that fix F.

Proposition (HW)

If K/F is a field extension, then $\mathbf{Aut}(K)$ is a group and $\mathbf{Aut}(K/F)$ is a subgroup.

Field automorphisms

Key idea

Elements of $\mathbf{Aut}(K/F)$ permute the roots of irreducible polynomials.

Proposition

Let K/F be a field extension, and $r \in K$ algebraic over F with minimal polynomial $m_r(x)$. If $\sigma \in \mathbf{Aut}(K/F)$, then $\sigma(r)$ is also root of $m_r(x)$.

Suppose r is a root of $f(x)$; say

$$r^n + c_{n-1}r^{n-1} + \cdots + c_1 r + c_0 = 0.$$

Apply $\sigma \in \mathbf{Aut}(K/F)$:

$$\begin{aligned}
\sigma(f(r)) &= \sigma(r^n + c_{n-1}r^{n-1} + \cdots + c_1 r + c_0) \\
&= \sigma(r^n) + \sigma(c_{n-1}r^{n-1}) + \cdots + \sigma(c_1 r) + \sigma(c_0) \\
&= (\sigma(r))^n + \sigma(c_{n-1})(\sigma(r))^{n-1} + \cdots + \sigma(c_1)\sigma(r) + \sigma(c_0) \\
&= (\sigma(r))^n + c_{n-1}(\sigma(r))^{n-1} + \cdots + c_1\sigma(r) + c_0
\end{aligned}$$

Field automorphisms

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

Definition

An automorphism of a field 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

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, $q = 1$. □

Corollary

$\sqrt{2}$ is irrational. □

The Galois group of a field extension

We showed that if $E/\mathbb{Q}$, then every automorphism of E must fix $\mathbb{Q}$.

Definition

The Galois group of a field extension E/F, denoted $\mathsf{Gal}(E/F)$, is the group of automorphisms of E that fix F.

Here are some examples (without proof):

- $\mathsf{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \langle f \rangle \cong C_2$, where $f : \sqrt{2} \longmapsto -\sqrt{2}$
- An automorphism of $\mathbb{Q}(\sqrt{2}, i)$ is determined by the image of $\sqrt{2}$ and i.

  There are four possibilities: the identity map e, and

$$\begin{cases} h(\sqrt{2}) = -\sqrt{2} \\ h(i) = i \end{cases} \qquad \begin{cases} v(\sqrt{2}) = \sqrt{2} \\ v(i) = -i \end{cases} \qquad \begin{cases} r(\sqrt{2}) = -\sqrt{2} \\ r(i) = -i \end{cases}$$

  Thus, the Galois group of F is $\mathsf{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \langle h, v \rangle \cong V_4$.
- $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \langle r, f \rangle$, where

$$\begin{cases} r(\sqrt[3]{2}) = \zeta\sqrt[3]{2} \\ r(\zeta) = \zeta \end{cases} \qquad \begin{cases} f(\sqrt[3]{2}) = \sqrt[3]{2} \\ f(\zeta) = \bar{\zeta} = \zeta^2 \end{cases}$$

The Galois group of a polynomial

Definition

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

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

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 $\mathsf{Gal}(F)$.

Definition

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

A few examples of Galois groups

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

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:

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

Theorem (Tower law)

For any chain of field extensions, $K \subset L \subset M$,

$$[M : K] = [M : L][L : K].$$

Proof

Let $\{x_i\}_{i \in I}$ be a basis for M/L, and $\{y_j\}_{j \in J}$ a basis for L/M.

We'll show that $\{x_i y_j\}_{i \in I, j \in J}$ is a basis for M/K.

Independent. Suppose $\sum_{i,j} k_{ij} x_i y_i = 0$. Rearranging this yields

$$\sum_j \Big(\underbrace{\sum_i k_{ij} x_i}_{=0} \Big) y_j = 0 \quad \Longrightarrow \quad \text{all } k_{ij} = 0.$$

Spans. Consider $m \in M$. We can write:

$$m = \sum_j \ell_j y_j, \text{ for } \ell_j \in L, \quad \text{and} \quad \ell_j = \sum_i k_{ij} x_i, \text{ for } k_i \in K.$$

Substituting yields $m = \sum_{i,j} \kappa_{i,j} x_i y_j$. □

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 $F = \mathbb{Q}(\sqrt{2} + \sqrt{3})$? Let's try $\alpha = \sqrt{2} + \sqrt{3} \in F$.

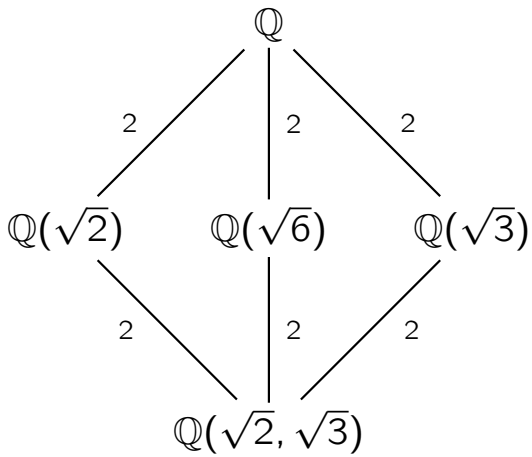
Which of the five subfields is $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$*?*

The following are equivalent (why?):

(i) α is primitive in F;

(ii) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$;

(iii) the minimal polynomial $m(x)$ of α has degree 4;



Also, note that

$$\alpha^4 = 49 + 20\sqrt{6}, \qquad \alpha^2 = 5 + 2\sqrt{6}, \qquad \alpha^4 - 10\alpha = -1.$$

The minimal polynomial of α is $m(x) = x^4 - 10x^2 + 1$

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

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

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

Question

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

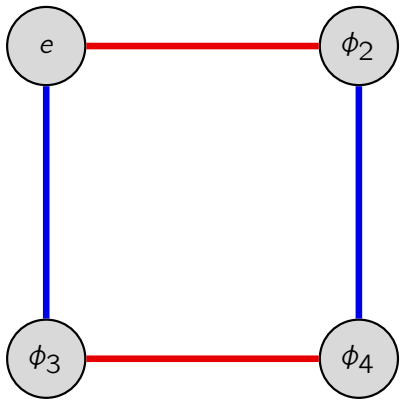
An example: The Galois group of $x^4 - 5x^2 + 6$

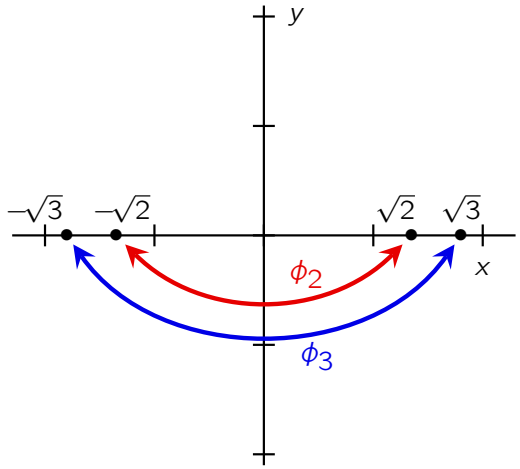
There are 4 automorphisms of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $x^4 - 5x^2 + 6$:

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

They form the Galois group of $x^4 - 5x^2 + 6$. The multiplication table and Cayley graph 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 $\mathsf{Gal}(f(x))$ 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 an action of $\mathsf{Gal}(f(x))$ on the set $S = \{r_1, \ldots, r_n\}$ of roots of $f(x)$.

That is, we have a homomorphism

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

If $\phi \in \mathsf{Gal}(f(x))$, 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 $\mathsf{Gal}(f(x))$ contains an automorphism $\phi\colon r_1 \longmapsto r_2$.

In other words, if $f(x)$ is irreducible, then the action of $\mathsf{Gal}(f(x))$ on the set $S = \{r_1, \ldots, r_n\}$ 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.

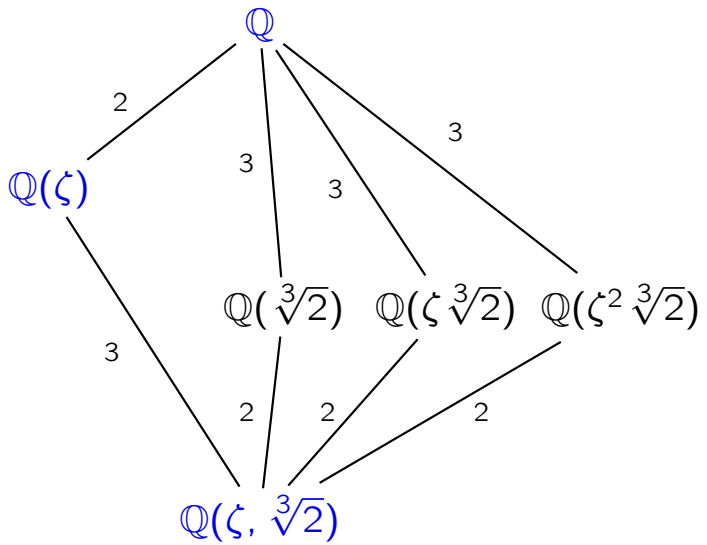
Corollary

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,

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

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

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 $\mathsf{Gal}(x^3 - 2) = \mathsf{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))$.

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

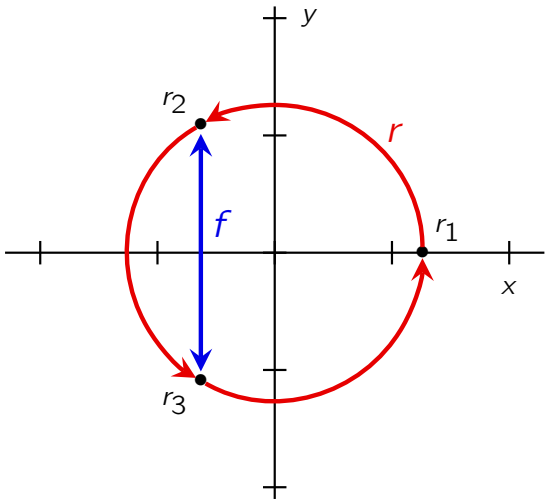
$$|\,\mathsf{Gal}(\mathbb{Q}(\zeta, \sqrt[3]{2}))| = [\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 6\,.$$

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 $\mathsf{Gal}(x^3 - 2) \cong S_3$. Here is the action graph of $\mathsf{Gal}(x^3 - 2)$ acting on the set $S = \{r_1, r_2, r_3\}$ of roots of $x^3 - 2$:

$$\begin{cases} r : \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \\ r : \zeta \quad\;\; \longmapsto \zeta \end{cases}$$

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



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.*"

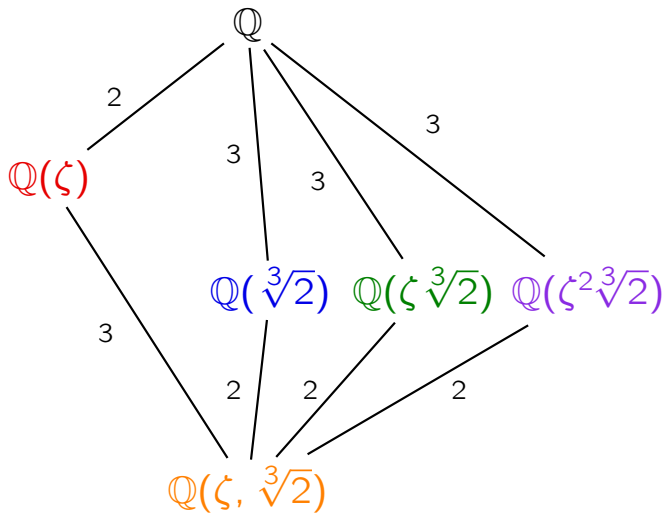
Fundamental theorem of Galois theory

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

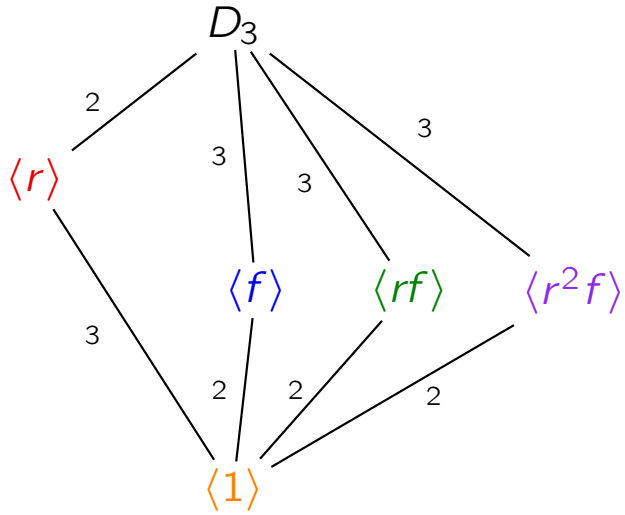
(a) The subgroup lattice of G is identical to the subfield lattice of F, but upside-down. Moreover, $H \lhd G$ if and only if the corresponding subfield is a normal extension of $\mathbb{Q}$.

(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 $\mathbb{Q}(\zeta, \sqrt[3]{2}) \cong D_3$



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

- 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 $f(x) = x^8 - 2$

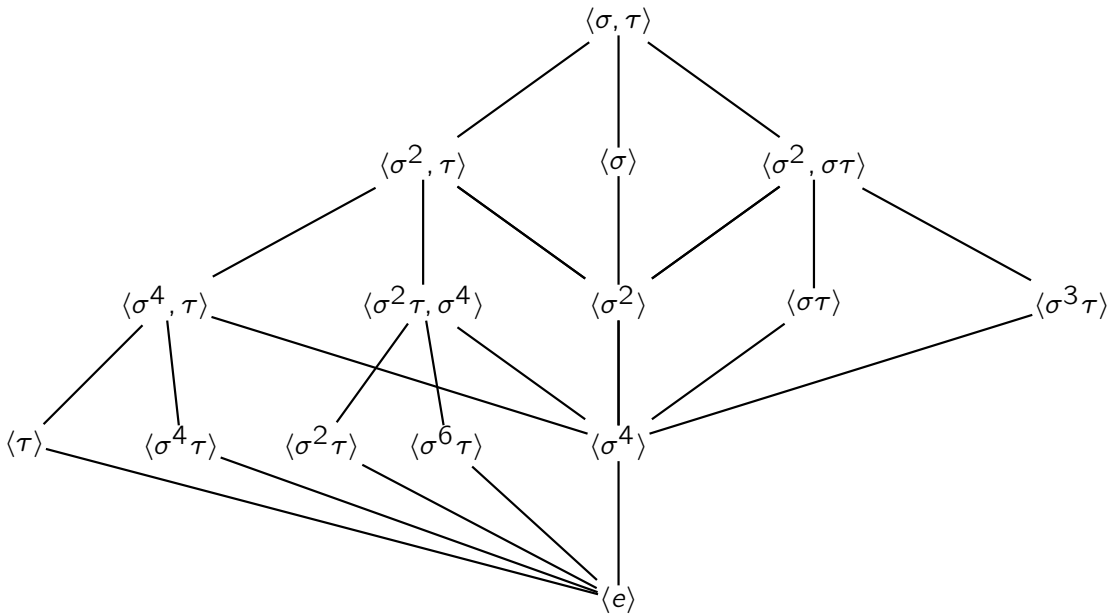
The splitting field of $x^8 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[8]{2}, i)$, a degree-16 extension over $\mathbb{Q}$. Its Galois group is the semidihedral group $G = \mathrm{SD}_8$:

$$\mathrm{SD}_8 = \langle \sigma, \tau \mid \sigma^8 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle .$$

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 $N_1 = A$.

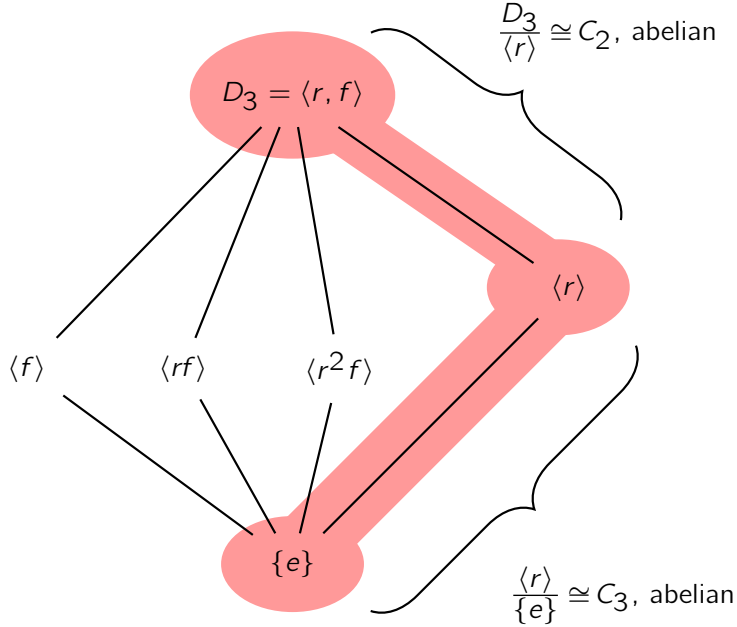
- For $n \geq 5$, the group A_n is simple and non-abelian. Thus, the only chain of normal subgroups is

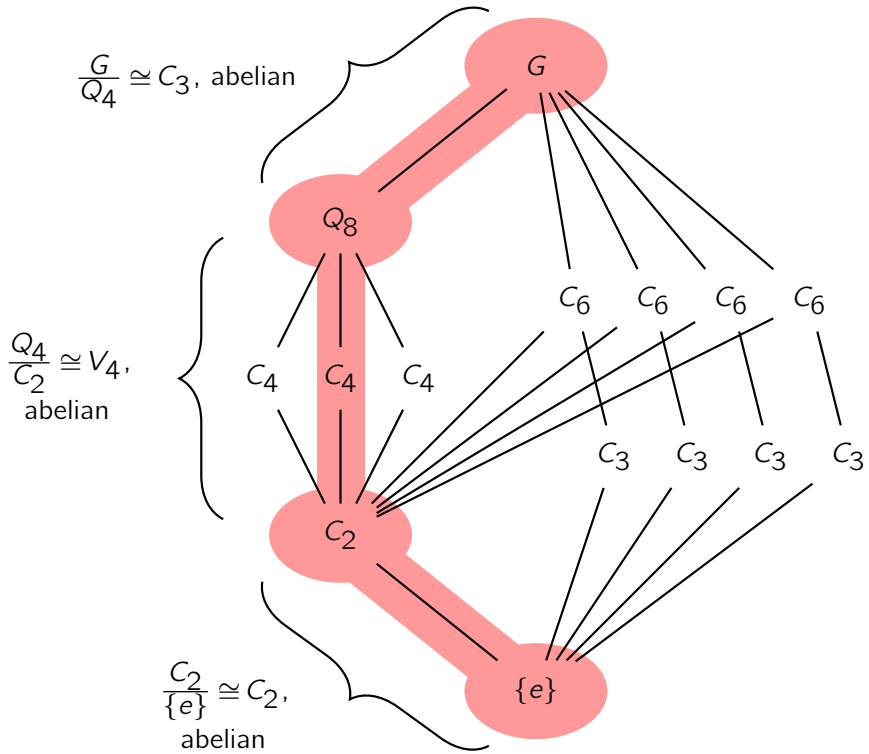
$$N_0 = \{e\} \lhd A_n = N_1\,.$$

  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 $G = \mathbf{SL}(2, 3)$. It consists of all 2×2 matrices with determinant 1 over the field $\mathbb{Z}_3 = \{0, 1, -1\}$.

$\mathbf{SL}(2, 3)$ 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 $\mathsf{Gal}(f(x)) \cong S_5$.

We'll restrict our search to degree-5 polynomials, because $\mathsf{Gal}(f(x)) \leq S_5$ 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 $F = \mathbb{Q}(r_1, \ldots, r_5)$ 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,

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

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

Applying the tower law to this yields

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

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

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

$\textbf{Gal}(f(x))$ 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 $\mathsf{Gal}(f(x))$ on the set of n roots! Thus, $\mathsf{Gal}(f(x)) \leq S_n$.

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

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 $\mathsf{Gal}(f(x))$ must have an element of order 5.

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

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 $\mathbb{C}$).

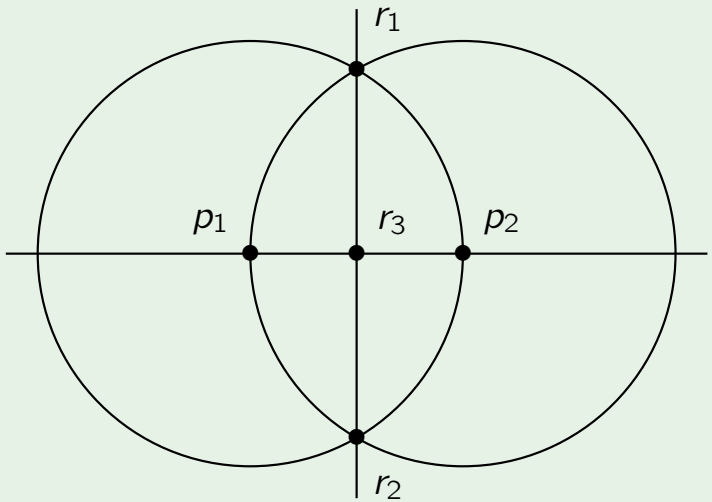
Definition

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

Example: bisecting a line

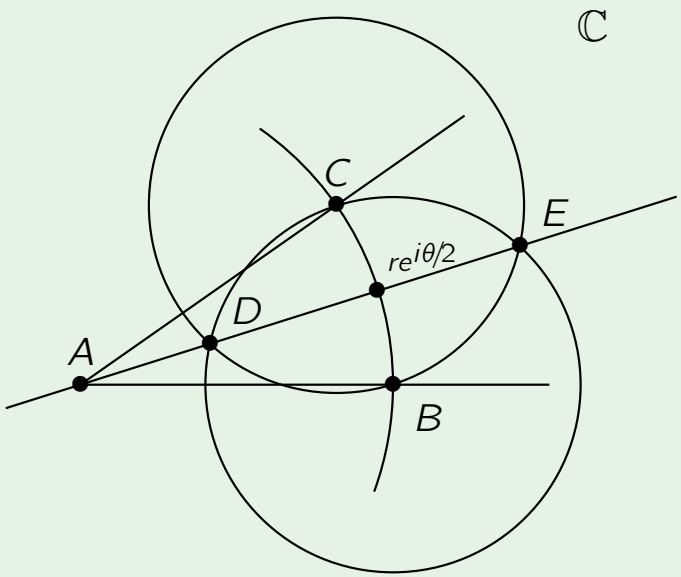
1. Start with a line p_1p_2;
2. Draw the circle of center p_1 of radius p_1p_2;
3. Draw the circle of center p_2 of radius p_1p_2;
4. Let r_1 and r_2 be the points of intersection;
5. Draw the line r_1r_2;
6. Let r_3 be the intersection of p_1p_2 and r_1r_2.



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 $p_1, \ldots, p_m$ are distinct Fermat primes.

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