Lecture 6.6: The fundamental theorem of Galois theory

Matthew Macauley

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

Math 4120, Modern Algebra

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.*"

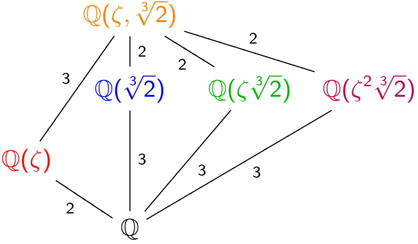
Fundamental theorem of Galois theory

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

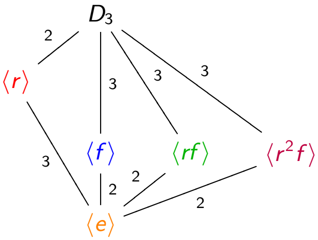
(a) The subgroup lattice of G is identical to the subfield lattice of F, but upside-down. Moreover, $H \lhd G$ if and only if the corresponding subfield is a normal extension of $\mathbb{Q}$.

(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 $\langle e \rangle$.

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 $N_1 = A$.

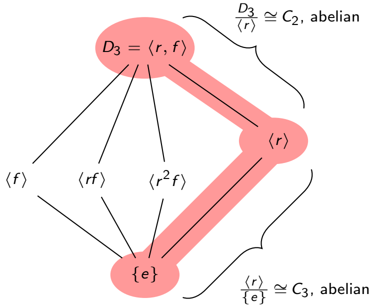
- For $n \geq 5$, the group A_n is simple and non-abelian. Thus, the only chain of normal subgroups is

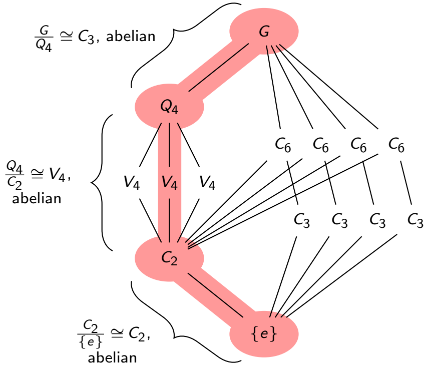
$$N_0 = \{e\} \lhd A_n = N_1\,.$$

  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 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 $E \supseteq \mathbb{Q}$ 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 $\mathrm{Gal}(f(x)) \cong S_5$.

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

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

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!