MAU34101 Galois theory

4 - Solvability by radicals

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2021–2022
Version: December 3, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Solvable groups

Commutators and the derived subgroup

Let G be a group with identity 1_G, and let $x, y \in G$.

Definition (Commutator)

The commutator of x and y is $[x, y] = xyx^{-1}y^{-1}$.

Observe that $[x, y] = (xy)(yx)^{-1}$,
so x and y commute iff. $[x, y] = 1_G$, whence the name.

Definition (Derived subgroup)

The derived subgroup $D(G)$ of G is the subgroup spanned by the commutators.

We have $z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}]$ for all $x, y, z \in G$,
so $D(G)$ is actually normal in G.

Also note that $D(G) = \{1_G\}$ iff. G is Abelian.

Commutators and the derived subgroup

Definition (Abelianisation)

The Abelianised of G is $G^{ab} = G/D(G)$.

G^{ab} is Abelian by construction.
In fact, for all $N \triangleleft G$, the quotient G/N is Abelian iff. N contains $D(G)$, and in this case G/N is a quotient of G^{ab}.

Example

Let $n \in \mathbb{N}$, and let $G = S_n$.

Since the sign ε is a morphism and since $\{\pm 1\}$ is Abelian, we always have $\varepsilon([x,y]) = [\varepsilon(x), \varepsilon(y)] = +1$, so $D(S_n) \leqslant A_n$.

One proves that in fact, $D(S_n) = A_n$. Therefore $S_n^{\mathrm{ab}} \overset{\varepsilon}{\simeq} \{\pm 1\}$ for $n \geqslant 2$.

Normal series

Let still G be a group.

Definition (Normal series)

A normal series of length $r \in \mathbb{N}$ for G is a chain

$$\{1_G\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G.$$

The quotients H_{j+1}/H_j are called the factors of the series.

Example

For $G = S_3$, we have the series $\{\mathrm{Id}\} \triangleleft A_3 \triangleleft S_3$, with factors $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.

For $G = S_4$, we have the series $\{\mathrm{Id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$, with factors $V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$, $A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$, and $S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$.

Observe that in both cases, G is **NOT** simply the product of the factors.

The derived series

Define inductively $D^0(G) = G$, $D^1(G) = D(G)$, $D^2(G) = D(D(G))$, $\cdots$, $D^{n+1}(G) = D(D^n(G))$, $\cdots$.

Suppose that there exists $s \in \mathbb{N}$ such that $D^s(G) = \{1_G\}$. Then we get the normal series

$$\{1_G\} = D^s(G) \lhd D^{s-1}(G) \lhd \cdots \lhd D^1(G) \lhd D^0(G) = G$$

which is called the derived series of G.

Its factors are Abelian, since $D^n(G)/D^{n+1}(G) = D^n(G)/D(D^n(G)) = \big(D^n(G)\big)^{\text{ab}}$.

Solvable groups

Theorem (Characterisations of solvability)

Let G be a finite group. TFAE:

- *There exists a normal series for G with Abelian factors,*
- *There exists a normal series for G with cyclic factors,*
- *There exists $s \in \mathbb{N}$ such that $D^s(G) = \{1_G\}$.*

See notes for the proof.

Definition

A finite group satisfying the above conditions is called solvable.

Solvable groups: examples and counter-examples

Example

If G is Abelian, then G is solvable (take $s = 1$).

Example

We have written series which prove that S_3 and S_4 are solvable.

Counter-example

However, for $n \geqslant 5$, we have that $D(S_n) = A_n$;
but then $D(A_n) \lhd A_n$ is nontrivial since A_n is not Abelian
$\rightsquigarrow D(A_n) = A_n$ as A_n is simple.

Therefore the derived series for S_n gets stuck on A_n, so S_n (nor A_n) is not solvable.

Preservation of solvability

Theorem

Let G be a solvable group.

- *Any subgroup of G is also solvable.*
- *The image of G by any morphism is also solvable.*
- *Any quotient of G is also solvable.*

Proof.

Let $H \leqslant G$ be a subgroup. One checks inductively that $D^n(H) \leqslant D^n(G)$ for all $n \in \mathbb{N}$, so H is solvable.

Let $f : G \longrightarrow \Gamma$ be a group morphism. One checks inductively that $D^n(f(G)) = f(D^n(G))$ for all $n \in \mathbb{N}$, so $f(G)$ is also solvable.

In particular, any quotient of G is solvable. □

Solvable polynomials

Elementary radical extensions

Definition (Elementary radical)

A field extension L/K is elementary radical if there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$ for some $n \in \mathbb{N}$.

The idea is that $L = K(\sqrt[n]{a})$ for some $a = \alpha^n \in K$.
However, this radical notation is subtly wrong, because n-th roots are multi-valued in general. This is the reason why the definition is stated without radicals.

Radical extensions

Definition (Radical)

A field extension L/K is radical if there exists a finite tower of intermediate fields

$$K = E_0 \subseteq E_1 \cdots \subseteq E_r = L$$

with E_{j+1}/E_j elementary radical for all j.

Example

$\mathbb{Q}(\sqrt[23]{\sqrt[7]{12}-9}, \sqrt{5})$ is a radical extension of $\mathbb{Q}$, because

$$\underbrace{\mathbb{Q}}_{\ni 12} \subseteq \underbrace{\mathbb{Q}(\sqrt[7]{12})}_{\ni \sqrt[7]{12}-9} \subseteq \underbrace{\mathbb{Q}(\sqrt[23]{\sqrt[7]{12}-9})}_{\ni 5} \subseteq \mathbb{Q}(\sqrt[23]{\sqrt[7]{12}-9}, \sqrt{5}).$$

Solvable polynomials

Definition (Solvability by radicals)

Let K be a field, and $F(x) \in K[x]$. We say that F is solvable by radicals over K if there exists a radical extension of K in which F has all its roots.

In other words, this means that the roots of F are expressible from K by nested n-th roots and the four field operations.

Galois's theorem

Galois's theorem

Theorem (Galois)

Let K be a field of characteristic 0, and let $F(x) \in K[x]$ be separable. Then F is solvable by radicals over $K \iff \mathrm{Gal}_K(F)$ is a solvable group.

See notes for the proof. The idea is that a chain of elementary radical extensions Galois-corresponds to a normal series with cyclic factors for $\mathrm{Gal}_K(F)$, and vice-versa.

Remark

The only reason why assume F separable is so that $\mathrm{Gal}_K(F)$ makes sense. But in characteristic zero, all fields are perfect, so nonseparable polynomials have repeated factors; by removing these multiplicities, we get another polynomial which is separable and has the same roots as F.

No general radical formula in degree $\geqslant 5$...

Counter-example

Let $F(x) = x^5 - x - 1 \in \mathbb{Q}[x]$.

We have seen that F is separable and has $\mathrm{Gal}_{\mathbb{Q}}(F) = S_5$ which is not solvable. Therefore F is not solvable by radicals over $\mathbb{Q}$.

This means that although F has roots (in $\mathbb{C}$), these roots do not look like $\sqrt[23]{\sqrt[7]{12} - 9} + \sqrt{5}$.

This implies that there cannot exist general formulas to solve by radicals polynomial equations of degree $\geqslant 5$ (consider $F(x)(x-1)(x-2)\cdots$).

… but this is only for the generic case.

Example

Let $n \in \mathbb{N}$ be large.

Then the cyclotomic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$ has degree $\phi(n) \geqslant 5$ and is irreducible;

and yet its Galois group over $\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$ which is Abelian and therefore solvable,

so $\Phi_n(x)$ is solvable by radicals over $\mathbb{Q}$.

Indeed, its roots are of the form $\sqrt[n]{1}$.

Note that this direction of the proof of Galois's theorem is actually constructive, and leads to non-trivial and more satisfying expressions of the roots of $\Phi_n(x)$ by radicals; see the notes for an example.