MA542 Lecture

Timothy Kohl

Boston University

April 18, 2025

We mentioned that abelian groups are solvable, but the converse is false.

For example, $D_3 = \langle x, t \rangle$ is solvable, the one solvable series for D_3 is:

$$\{1\} \leq \langle x \rangle \leq D_3$$

since $\langle x \rangle \triangleleft D_3$ and $\langle x \rangle / \{1\} \cong \langle x \rangle \cong \mathbb{Z}_3$ and $D_3/\langle x \rangle = \{1\langle x \rangle, t\langle x \rangle\} \cong \mathbb{Z}_2$.

In general, all the dihedral groups $D_n = \langle x, t \mid x^n = 1, t^2 = 1; xt = tx^{-1} \rangle$ are solvable, where the solvable series is basically the same

$$\{1\} \leq \langle x \rangle \leq D_n$$

where $\langle x \rangle \triangleleft D_n$ and $\langle x \rangle / \{1\} \cong \langle x \rangle \cong \mathbb{Z}_n$ and $D_n/\langle x \rangle = \{1\langle x \rangle, t\langle x \rangle\} \cong \mathbb{Z}_2$.

There is a direct connection between solvable extensions and solvable groups.

Theorem

Let F be a field of characteristic zero, and let $a \in F$. If E is the splitting field of $x^n - a \in F[x]$ then $Gal(E/F)$ is solvable.

This provides a foundation for the primary result about the relationship between solvability of the extension and that of the Galois group.

But this more general theorem *does* utilize this result.

PROOF: First assume that F contains a primitive n^{th} root of unity ζ.

If b is a zero of $x^n - a$ in E then all the other zeros lie in E too, specifically $\zeta b, \zeta^2 b, \ldots, \zeta^{n-1} b$, ergo $E = F(b)$.

In this case, $Gal(E/F)$ is abelian since if $\phi_1, \phi_2 \in Gal(E/F)$ then $\phi_1(b) = \zeta^{i_1} b$ and $\phi_2(b) = \zeta^{i_2} b$.

As such, $\phi_1 \circ \phi_2(b) = \phi_1(\zeta^{i_2} b) = \zeta^{i_2}(\zeta^{i_1} b) = \zeta^{i_2+i_1} b$ which is the same as $\phi_2 \circ \phi_1(b)$.

PROOF: (continued)
If F does not contain a primitive n^{th} root of unity then since E contains a root b of $x^n - a$ then must contain ζb for ζ a primitive n^{th} root of unity since ζb is a root of $x^n - a$, ergo $\frac{\zeta b}{b} = \zeta \in E$.

So $E \supset F(\zeta) \supseteq F$ where $F(\zeta)$ is a splitting field of $x^n - 1 \in F[x]$.

Hence we may consider $Gal(F(\zeta)/F)$ and observe that it is abelian too!

The reason is that, again, the automorphisms it contains are of the form $\phi_e(b) = \zeta^e b$ and clearly these commute with each other.

Now, E is splitting field of over $F(\zeta)$ of $x^n - a$ and we may observe that $E = F(\zeta)(b)$ for b any root of $x^n - a$ and here too $Gal(E/F(\zeta))$ is abelian.

Moreover, since $F(\zeta)$ is a splitting field over of F then $Gal(E/F)/Gal(E/F(\zeta)) \cong Gal(F(\zeta)/F)$, more to the point, $Gal(E/F(\zeta)) \triangleleft Gal(E/F)$.

So we have a sub-normal series

$$\{e\} \leq Gal(E/F(\zeta)) \leq Gal(E/F)$$

where $Gal(E/F(\zeta))/\{e\} \cong Gal(E/F(\zeta))$ which is abelian, and $Gal(E/F)/Gal(E/F(\zeta)) \cong Gal(F(\zeta)/F)$ which is also abelian.

Ergo $Gal(E/F)$ is solvable. $\square$

Theorem

(Galois) Let F be field of characteristic 0, and let $f(x) \in F[x]$. Suppose that $f(x)$ splits in the extension $F(a_1, a_2, \ldots, a_t)$ with $a_1^{n_1} \in F$ (for some n_1) and $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ for $i = 1, \ldots, t-1$. If E/F is the splitting field of $f(x)$ then $Gal(E/F)$ is a solvable group.

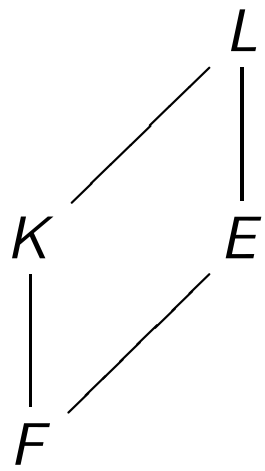
This reflects the goal of viewing a polynomial as being 'solvable by radicals' in that its roots are expressible as a combinations of n^{th} roots of elements, as in the quadratic, cubic, and quartic formulae.

PROOF: Induction on t (where $E \subseteq F(a_1, \ldots, a_t)$)

$(t = 1)$ $F \subseteq E \subseteq F(a_1)$
Let $a = a_1^{n_1}$ and let L be a splitting field for $x^{n_1} - a$ over F.
Then $F \subseteq E \subseteq L$ and both E and L are splitting fields of polynomials over F.
By FTGT we have $Gal(E/F) \cong Gal(L/F)/Gal(L/E)$ where $Gal(L/F)$ is solvable since it's a splitting field of $x^n - a$.
And as $Gal(L/E) \leq Gal(L/F)$ it is solvable, so therefore the quotient $Gal(E/F)$ is as well.

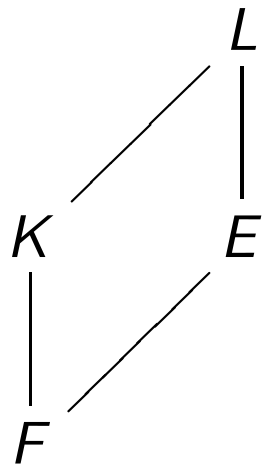
PROOF (continued): $(t > 1)$ Let $a = a^{n_1} \in F$ and let L be a splitting field of $x^{n_1} - a$ over E and let $K \subseteq L$ be the splitting field of $x^{n_1} - a$ over F.

Then L is a splitting field of $(x^{n_1} - a)f(x)$ over F and L is a splitting field of $f(x)$ over K.



i.e. $x^{n_1} - a \in F[x]$ implies $x^{n_1} - a \in E[x]$, and $f(x) \in F[x]$ implies $f(x) \in K[x]$

PROOF: (continued)



Since $F(a_1) \subseteq K$ we have that $f(x)$ splits in $K(a_2, \ldots, a_t)$ so by induction we may assume that $Gal(L/K)$ is solvable and $Gal(K/F)$ is solvable because K is a splitting field for $x^{n_1} - a$), so $Gal(L/F)/Gal(L/K)$ is solvable so $Gal(L/F)$ is solvable (i.e. G/N and N solvable implies G solvable)

So $Gal(E/F) \cong Gal(L/F)/Gal(L/E)$ is solvable.

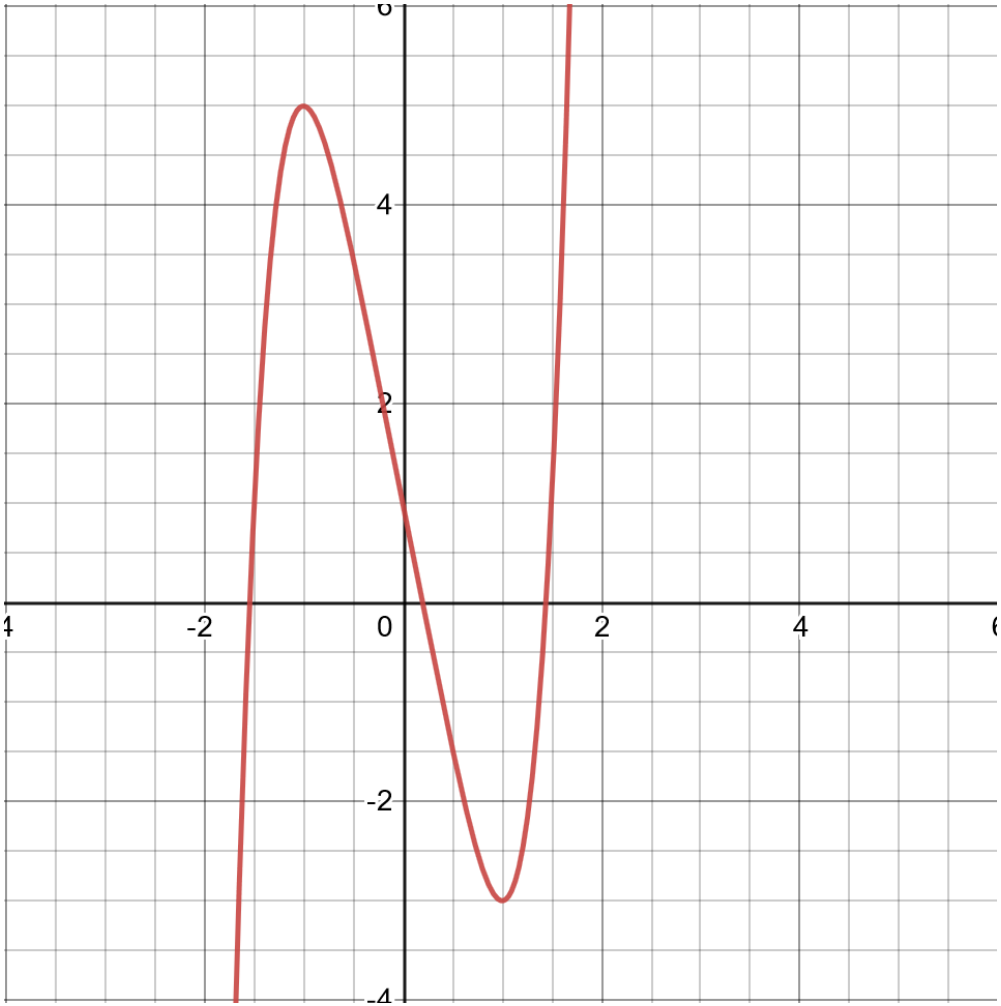
Insolvability of the Quintic

We now demonstrate the existence of a degree 5 polynomial, a quintic, where the splitting field has a non-solvable Galois group.

Let $g(x) = x^5 - 5x + 1$ which is not obviously irreducible, but we can prove it is irreducible using a similar technique like we used to prove the cyclotomic polynomials are irreducible.

If we expand $g(x-1)$ we get $x^5 - 5x^4 + 10x^3 - 10x^2 + 5$ which is readily proven irreducible by Eisenstein's criterion, with $p = 5$, and since $g(x-1)$ is irreducible, then so is $g(x)$ since a factorization of $g(x)$ would imply a factorization of $g(x-1)$.

If we plot this quintic we see that it has 3 real roots, and therefore 2 complex roots.



We could infer this without graphing by looking at $g'(x) = 5x^4 - 5$ which implies 2 extrema, at ± 1, and at these points we find $g(-1) = 5$ and $g(1) = -3$.

As such, we can denote these roots as r_1, r_2, r_3 and z_1, z_2 and we recall a basic fact about roots one learns in algebra, namely that the complex roots come in pairs, which are complex conjugates of each other.

Indeed, a rudimentary argument shows that if z is the root of $f(x) \in \mathbb{R}[x]$ (or $\mathbb{Q}[x]$) then so is $\bar{z}$ since conjuating each of the coefficients leaves the polynomial unchanged.

As such $\bar{z_1} = z_2$, and so $\bar{\bar{z_1}} = z_1 = \bar{z_2}$ and, although obvious, it is important to observe that $\bar{r_i} = r_i$ for $i = 1, 2, 3$.

As there are 5 distinct roots then if E is the splitting field of $g(x) \in \mathbb{Q}[x]$ then $G = Gal(E/\mathbb{Q})$ acts transitively on these 5 roots and is therefore isomorphic to a transitive subgroup of S_5.

Moreover, as G acts transitively on these roots then if r is any one of them then by the theory of group actions (i.e. the orbit stabilizer theorem) we have $[G : G_r] = 5$ where G_r is the subgroup of G fixing r.

But then $|G| = 5|G_r|$ which means $5 \mid |G|$ so that G contains an element of order 5 along with the order 2 element corresponding to conjugation $z_1 \leftrightarrow z_2$, so in terms of cycle structure G contains a 5-cycle and a 2-cycle which means it must contain *all* permutations of the roots, and therefore $G \cong S_5$.

Now, $Gal(E/\mathbb{Q}) \cong S_5$ implies that it is *not* solvable since S_5 is not solvable.

Why? Well the only, non-trivial normal subgroup of S_5 is A_5 where $[S_5 : A_5] = 2$ and A_5 is simple so therefore the only sub-normal series we have is

$$\{I\} \leq A_5 \leq S_5$$

where $S_5/A_5 \cong \mathbb{Z}_2$, but $A_5/\{I\} \cong A_5$ which is *non*-abelian.

As such the splitting field for $g(x) = x^5 - 5x + 1$ is not a solvable extension of $\mathbb{Q}$ and so there are no formulae for the roots involving root extractions.

We note that there are some ways to construct roots to this polynomial, and similar such quintics, but the techniques are **much** harder and involve using identities that are satisfied by certain types of series.