Galois Theory - Week 9 - Solvability by Radicals

Antonio León Villares

May 2023

Contents

Based on the notes by Tom Leinster, Chapter 9

1 Radical Complex Numbers

1.1 Definition: Field of Radicals

A complex number is ***radical*** *if it belongs to* $\mathbb{Q}^{rad}$*, the* ***smallest*** *subfield of* $\mathbb{C}$ *such that* $\forall \alpha \in \mathbb{C}$*, if* $\exists n \geq 1 : \alpha^n \in \mathbb{Q}^{rad}$*, then* $\alpha \in \mathbb{Q}^{rad}$*.*

In other words, $\mathbb{Q}^{rad}$ *is the smallest subfield of* $\mathbb{C}$ *which is closed under the usual arithmetic operations (addition, subtraction, multiplication, division and nth roots).*
(Definition 9.1.2)

This relies on there even existing such a subfield. That is, assuming that there are subfield $X_1, X_2, \ldots$ *satisfying closure under arithmetic operations, does their intersection also satisfy this? Call this intersection* $I = \bigcap_i X_i$*. Then, this is a subfield, since it is an intersection of subfield. If* $\alpha^n \in I$*,* $\alpha^n \in X_i$ *for any* i*. Hence, for any* i*,* $\alpha \in X_i$*, so* $\alpha \in I$*, as required.*

1.2 Definition: Polynomial Solvable by Radicals

A ***non-zero*** $f \in \mathbb{Q}[t]$ *is* ***solvable by radicals*** *if* ***all*** *of its complex roots are* ***radical****.*
(Definition 9.1.5)

1.3 Abelian Galois Groups

1.3.1 Lemma: Galois Group of $t^n - 1$ is Abelian

$\forall n \geq 1$*, the group* $Gal_{\mathbb{Q}}(t^n - 1)$ *is* ***abelian****.*
(Lemma 9.1.6)

Proof. Le t$\omega = e^{2\pi i/n}$. Then, $t^n - 1$ has complex roots

$$1, \omega, \omega^2, \ldots, \omega^{n-1}$$

so $SF_{\mathbb{Q}}(t^n - 1) = \mathbb{Q}(\omega)$.

Now, let $\varphi, \theta \in Gal_{\mathbb{Q}}(t^n - 1)$. φ permutes roots of $t^n - 1$, and so does θ, so:

$$\exists i, j \in \mathbb{Z} \;:\; \varphi(\omega) = \omega^i \quad \theta(\omega) = \omega^j$$

Hence:

$$(\varphi \circ \theta)(\omega) = \omega^{ij} = (\theta \circ \varphi)(\omega)$$

Since $SF_{\mathbb{Q}}(t^n - 1) = \mathbb{Q}(\omega)$, it must then be the case that by:

> *Let M_1, M_2 be extensions of a field K, and let:*
>
> $$\varphi, \psi : M_1 \to M_2$$
>
> *be **homomorphisms over** K.*
> *Let Y be a subset of M_1, such that $M_1 = K(Y)$. Then:*
>
> $$\forall a \in Y,\ \varphi(a) = \psi(a) \implies \varphi = \psi$$
>
> *In other words, knowing the behaviour of φ, ψ on Y is sufficient to understand φ, ψ on all of M_1.*
> *(Lemma 4.3.6)*

$\varphi \circ \theta = \theta \circ \varphi$, so $Gal_{\mathbb{Q}}(t^n - 1)$ is abelian. □

1.3.2 Lemma: Galois Group of $t^n - a$ is Abelian

> *Let K be a **field** and $n \geq 1$. If $t^n - 1$ splits in K, then $\forall a \in K$, $Gal_K(t^n - a)$ is **abelian**.*
> *(Lemma 9.1.8)*

This seems restrictive at first, since for example, $t^n - 1$ doesn't split in $\mathbb{Q}$ or even $\mathbb{R}$ when $n > 2$. For example, $Gal_{\mathbb{Q}}(t^3 - 2) = S_3$ which isn't ableian.. However, this won't matter for later arguments.

Proof. If $a = 0K$, then $Gal_K(t^n - a)$ is trivial. Hence, assume otherwise. Pick a root of $t^n - a$, $\xi \in SF_K(t^n - a)$. If ν is any other root, then:

$$\left(\frac{\xi}{\nu}\right)^n = \frac{a}{a} = 1_K$$

Hence, ξ/ν is a root of $t^n - 1$. Since $t^n - a$ splits in K, then $\xi/\nu \in K$. Since $\xi \in SF_K(t^n - a)$, but $\xi/\nu \in K$, we must have that $SF_K(t^n - a) = K(\xi)$. Then, if $\varphi, \theta \in Gal_K(t^n - a)$, since φ acts by permuting roots, it follows that $\varphi(\xi)/\xi \in K$, so:

$$(\theta \circ \varphi)(\xi) = \theta\left(\frac{\varphi(\xi)}{\xi}\xi\right) = \frac{\varphi(\xi)}{\xi}\theta(\xi) = \frac{\varphi(\xi)\theta(\xi)}{\xi}$$

With a similar argument, it can be shown that:

$$(\varphi \circ \theta)(\xi) = \frac{\varphi(\xi)\theta(\xi)}{\xi}$$

Again using Lemma 4.3.6, since $(\theta \circ \varphi)(\xi) = (\varphi \circ \theta)(\xi)$ and $SF_K(t^n - a) = K(\xi)$, it follows that $\varphi \circ \theta = \theta \circ \varphi$, so $Gal_K(t^n - a)$ is abelian. □

1.3.3 Exercises

1. *[Exercise 9.1.10* **What does the proof of Lemma 9.1.8 tell you about the eigenvectors and eigenvalues of the elements of $Gal_K(t^n - a)$.**

   Notice, we have that:

   $$\varphi(\xi)/\xi \in K \implies \exists k \in K \ : \ \varphi(\xi) = k\xi$$

   In other words, the roots of $t^n - a$ are **eigenvectors** of the elements of the Galois Group; their eigenvalues are elmeents in K.

2 From Solvable Polynomials to Solvable Groups

2.1 Solvable Extensions

2.1.1 Definition: Solvable Field Extension

Let $M : K$ be a ***finite***, ***normal***, ***separable*** *extension. Then, $M.K$ is* ***solvable*** *if there exists $r \geq 0$ and intermediate fields:*

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = M$$

such that $\forall i \in [1, r]$:

- *$L_i : L_{i-1}$ is* ***normal***
- *$Gal(L_i : L_{i-1})$ is* ***abelian***

(Definition 9.2.1)

2.1.2 Example: $t^n - a$ Yields Solvable Extension

Notice, if $a \in \mathbb{Q}, n \geq 1$, then $SF_{\mathbb{Q}}(t^n - a).\mathbb{Q}$ is finite, normal and separable, as it is a splitting field over a field of characteristic 0. We claim that it is solvable.

If $a = 0$, then $SF_{\mathbb{Q}}(t^n - a) = \mathbb{Q}$, and $\mathbb{Q} : \mathbb{Q}$ is solvable.

If $a \neq 0$, let ξ be a complex root, and let $\omega = e^{2\pi i/n}$. The roots of $t^n - a$ are $\xi, \omega\xi, \ldots, \omega^{n-1}\xi$. This implies that $\forall i \in [0, n-1], \omega^i \in SF_{\mathbb{Q}}(t^n - a)$, since $(\omega^i\xi)/\xi = \omega^i$. In particular, $t^n - 1$ splits in $SF_{\mathbb{Q}}(t^n - a)$, so:

$$\mathbb{Q} \subseteq SF_{\mathbb{Q}}(t^n - 1) \subseteq SF_{\mathbb{Q}}(t^n - a)$$

Now, $SF_{\mathbb{Q}}(t^n - 1) : \mathbb{Q}$ is normal, and $Gal_{\mathbb{Q}}(t^n - 1)$ is abelian. Moreover, $SF_{\mathbb{Q}}(t^n - a) : SF_{\mathbb{Q}}(t^n - 1)$ is also normal (it is a splitting field extension of $t^n - a$ over $SF_{\mathbb{Q}}(t^n - 1)$). Moreover, $Gal_K(t^n - a)$ is abelian if $t^n - 1$ splits over K. Using $K = SF_{\mathbb{Q}}(t^n - 1)$ this trivially follows. Hence, $SF_{\mathbb{Q}}(t^n - a) : \mathbb{Q}$ is a solvable extension.

2.1.3 Lemma: Solvable Extension Iff Solvable Galois Group

> *Let $M : K$ ve a **finite**, **normal**, **separable** extension. Then:*
>
> $$M : K \text{ is } \textbf{solvable} \iff Gal(M : K) \text{ is } \textbf{solvable}$$
>
> *(Lemma 9.2.4)*

Proof. We only prove the ($\Longrightarrow$) direction, as that is all we really need, although the ($\Longleftarrow$) direction should be fairly similar.

Recall, a group G is solvable if it contains a subnormal series $G_0 = \{e_G\} \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ of normal subgroups, such that $G_{i+1}(G_i$ is abelian.

Now, suppose $M : K$ is solvable. Then there are intermediate fields:

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = M$$

such that $\forall i \in [1, r]$:

- $L_i : L_{i-1}$ is **normal**
- $Gal(L_i : L_{i-1})$ is **abelian**

By

> *Let $M : L : K$ be **field extensions**. If $M : K$ is **finite** and **normal**, then so is $M : L$.*
> *(Corollary 7.1.6)*

> *Let $M : L : K$ be **field extensions**, and let $M : K$ be **algebraic**. Then:*
>
> $$M : K \text{ is } \textbf{separable} \implies M : L,\ L : K \text{ are } \textbf{separable}$$
>
> *(Lemma 7.2.16)*

each $M : L_j$ is finite, normal and separable. Now, by the Fundamental Theorem of Galois Theory, since $L_i : L_{i-1}$ is normal, $Gal(M : L_i)$ is a normal subgroup of $Gal(M : L_{i-1})$, and

$$\frac{Gal(M : L_{i-1})}{Gal(M : L_i)} \cong Gal(L_i : L_{i-1})$$

By hypothesis, $Gal(L_i : L_{i-1})$ is abelian. Thus, we have a sequence of subgroups:

$$\{e\} = Gal(M : M) \triangleleft \ldots \triangleleft Gal(M : L_1) \triangleleft Gal(M : L_0) = Gal(M : K)$$

where each composition factor is abelian, so $Gal(M : K)$ is solvable. □

2.1.4 Lemma: Properties of Compositum

Let $M : K$ be a ***field extension*** *with intermediate fields L_1, L_2. Then:*

1. *If $L_1 : K, L_2 : K$ are* ***finite*** *and* ***normal****, then so is $L_1L_2 : K$*
2. *If $L_1 : K$ is* ***finite*** *and* ***normal****, then so is $L_1L_2 : L_2$*
3. *$L_1 : K$ is* ***finite*** *and* ***normal*** *with* ***abelian*** *Galois group, then so is $L_1L_2 : L_2$*

(Lemma 9.2.6)

Proof.

1. By normality, $\exists f_1, f_2 \in K[t]$ such that:

$$L_1 = SF_K(f_1) \qquad L_2 = SF_K(f_2)$$

   L_1L_2 is the subfield of M generated by $L_1 \cup L_2$. Hence, it is the subfield of M generated by the roots of f_1 and f_2, so $L_1L_2 = SF_K(f_1f_2)$ is finite and normal over K.

2. Let $L_1 = SF_K(f)$ for some $f \in K[t]$. Then, using

(a) Let:

- *$M : S : K$ be a **field extension***
- $$0_K \neq f \in K[t]$$
- *$Y \subseteq M$*

*Let S be the **splitting field** of f over K. Then, $S(Y)$ is the **splitting field** of f over $K(Y)$:*

$$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$

(b) Let:

- $$0_K \neq f \in K[t]$$
- *L be a **subfield** of $SF_K(f)$ containing K, such that:*

$$SF_K(f) : L : K$$

*Then, $SF_K(f)$ is the **splitting field** of f over L:*

$$SF_K(f) = SF_L(f)$$

(Lemma 6.2.14)

with $S = L_1, Y = L_2$ it follows that:

$$L_1 = SF_K(f) \implies L_1(L_2) = SF_{K(L_2)}(f) \therefore L_1L_2 = SF_{L_2}(f)$$

so L_1L_2 is finite and normal over L_2.

3. $Gal(L_1L_2 : L_2) = Gal_{L_2}(f)$ is isomorphic to a subgroup of $Gal_K(f) = Gal(L : K)$. Hence, if $Gal(L : K)$ is abelian, so is $Gal(L_1L_2 : L_2)$.

□

2.1.5 Lemma: Larger Subfield Containing Finite, Normal and Solvable Extensions

*Let L, M be **subfields** of $\mathbb{C}$, such that $L : \mathbb{Q}, M : \mathbb{Q}$ are **finite**, **normal** and **solvable**. Then, there exists a **subfield** N of $\mathbb{C}$, such that:*

- *$N : \mathbb{Q}$ is **finite**, **normal** and **solvable**.*
- *$L, M \subseteq N$*

(Lemma 9.2.7)

Proof. The proof of this is similar to Lemma 5.3.8 on ruler and compass constructions, and employs Lemma 9.2.6 above.

By solvability of $L : \mathbb{Q}, M : \mathbb{Q}$ we have:

$$\mathbb{Q} = L_0 \subseteq \ldots \subseteq L_r = L \quad \mathbb{Q} = M_0 \subseteq \ldots \subseteq M_s = M$$

where $L_i : L_{i-1}, M_j : M_{j-1}$ are normal and have abelian Galois Groups. We claim that the chain of subfields:

$$\mathbb{Q} = L_0 \subseteq \ldots \subseteq L_r = L = LM_0 \subseteq \ldots \subseteq LM_s = LM$$

is finite, normal and solvable ($L, M \subseteq LM$ automatically).

By Lemma 9.2.6, 2) above, it is definitely finite and normal.

For solvability, we only need to worry about the extensions of the form $LM_j : LM_{j-1}$ (since solvability is immediate for any $L_j : L_{j-1}$). But since $M_j : M_{j-1}$ are finite and normal with abelian Galois Group, by Lemma 9.2.6, 3), it follows that so are $LM_j : LM_{j-1}$, as required. □

2.2 The Field of Solvable Complex Numbers

2.2.1 Definition: Field of Solvable Complex numbers

The field:

$$\mathbb{Q}^{sol} = \{\alpha \in \mathbb{C} \mid \alpha \in L, \textit{where } L \textit{ is some } L \leq \mathbb{C} \\ \textit{which is } \textbf{\textit{finite}}, \textbf{\textit{normal}} \textit{ and } \textbf{\textit{solvable}} \textit{ over } \mathbb{Q}\}$$

It is in fact a ***subfield*** *of* $\mathbb{C}$.
(Lemma 9.2.8)

Proof. This follows immediately from the fact that if $\alpha, \beta \in \mathbb{Q}^{sol}$, then there exist finite, normal and solvable fields L, M such that $\alpha \in L, \beta \in M$, so by 9.2.7 above, LM is also finite, normal and solvable, and contains α, β, from which it follows that $\alpha - \beta \in LM, \alpha\beta, \alpha^{-1}, 0, 1 \in LM$ so these are all in $\mathbb{Q}^{sol}$. □

2.2.2 Lemma: Solvable Field Closed Under nth Roots

Let $\alpha \in \mathbb{C}$ *and* $n \geq 1$. *If* $\alpha^n \in \mathbb{Q}^{sol}$, *then* $\alpha \in \mathbb{Q}^{sol}$.
(Lemma 9.2.9)

Proof. Let $a = \alpha^n \in \mathbb{Q}^{sol}$. Choose a subfield K of $\mathbb{C}$, such that $a \in K$ with $K : \mathbb{Q}$ finite, normal and solvable. We prove this in 2 steps. Firstly, we enlarge K to be a field where $t^n - 1$ splits. Then, we adjoin conjugates of a.

① **Enlarge** K

Let $L = SF_K(t^n - 1)$. Since $K : \mathbb{Q}$ is finite and normal, $\exists f \in K[t]$ such that $K = SF_{\mathbb{Q}}(f)$. Hence, we must have that $L = SF_{\mathbb{Q}}(f(t)(t^n - 1))$, so $L : \mathbb{Q}$ is finite and normal. We must have that $Gal_K(t^n - 1)$ is isomorphic to a subgroup of $Gal_{\mathbb{Q}}(t^n - 1)$, which is abelian. Thus, $L : K$ is a normal extension with an abelian Galois Group. Since $K : \mathbb{Q}$ is solvable by hypothesis, we have a series $\mathbb{Q} \subseteq K \subseteq L$ with normal composition factors and abelian Galois Groups, so $L : \mathbb{Q}$ is solvable. Thus, $L : \mathbb{Q}$ is a subfield of $\mathbb{C}$ containing a, which is finite, normal, solvable and $t^n - 1$ splits in it.

② **Adjoin Conjugates**

Let $m \in \mathbb{Q}[t]$ be the minimal polynomial of a over $\mathbb{Q}$ and put $M = SF_L(m(t^n)) \subseteq \mathbb{C}$. Then, $\alpha \in m$, since $m(\alpha^n) = m(a) = 0$. We show that $M : \mathbb{Q}$ is finite, normal and solvable. $M : \mathbb{Q}$ is finite and normal, as $M = SF_{\mathbb{Q}}(gm(t^n))$, where g is such that $L = SF_{\mathbb{Q}}(g)$, since L is finite and normal. Moreover, $M : L$ is a splitting field extension, so it is also finite and normal. To show that $M : \mathbb{Q}$ is solvable, it is enough to show that $M : L$ is solvable (since $L : \mathbb{Q}$ is solvable, we can just "join" their respective field extensions). Since $L : \mathbb{Q}$ is normal, and $a \in L$, its minimal polynomial m splits in L, say:

$$m(t) = \prod_{i=1}^{r} (t - a_i), \quad a_i \in L$$

Define subfiels $L_0 \subseteq \ldots \subseteq L_r$ of $\mathbb{C}$ by:

$$\begin{aligned} L_0 &= L \\ L_1 &= SF_{L_0}(t^n - a_1) \\ &\vdots \\ L_R &= SF_{L_{r-1}}(t^n - a_r) \end{aligned}$$

Hence:

$$L_i = L\left(\beta \in M \mid \beta^n \in \{a_1, \ldots, a_i\}\right)$$

so in particular $L_r = M$. Now, $L_i : L_{i-1}$ is a splitting field extension, so it is finite and normal. $Gal(L_i : L_{i-1})$ is abelian, since $t^n - 1$ splits in $L \subseteq L_{i-1}$ (and applying Lemma 9.1.8). Hence, $M : L$ will be solvable. Since $\alpha \in M$ and M is finite, normal and solvable, $\alpha \in \mathbb{Q}^{sol}$. ☐

2.2.3 Proposition: Radicals are Subset of Solvables

*Every **radical** number is contained in some **subfield** of $\mathbb{C}$ that is a**finite**, **normal** and **solvable** extension of $\mathbb{Q}$. That is:*

$$\mathbb{Q}^{rad} \subseteq \mathbb{Q}^{sol}$$

(Proposition 9.2.12)

In fact, the above is actually an equality, but the inclusion is all we really need.

By Lemma 9.2.8 and 9.2.9, $\mathbb{Q}^{sol}$ is a subfield of $\mathbb{C}$ such that if $\alpha^n \in \mathbb{Q}^{sol}$ then $\alpha \in \mathbb{Q}^{sol}$. ALl elements of $\mathbb{Q}^{rad}$ satisfy this, by definition.

2.3 Theorem: Polynomials Solvable by Radicals Implies Galois Group Solvable

Let $f \in \mathbb{Q}[t]$ be non-zero. If f is ***solvable by radicals****, then $Gal_{\mathbb{Q}}(f)$ is* ***solvable****.*
(Theorem 9.2.13)

Proof. Assume f is solvable by radicals. Then, its roots $\alpha_!, \dots, \alpha_n \in \mathbb{C}$ are radical, so $\alpha_i \in \mathbb{Q}^{rad} \subseteq \mathbb{Q}^{sol}$. Hence, each root is contained in some subfield of $\mathbb{C}$ that is finite, normal and solvable over $\mathbb{Q}$. By Lemma 9.27, there is a subfield M of $\mathbb{C}$ which if finite, normal an doslvable over $\mathbb{Q}$ which contains $\alpha_1, \dots, \alpha_n$. Then, it follows that:

$$\mathbb{Q}(\alpha_1, \dots, \alpha_n) = SF_{\mathbb{Q}}(f) \subseteq M$$

Now, since $M : \mathbb{Q}$ is solvable, by Lemma 9.2.4, $Gal(M : \mathbb{Q})$ is solvable. Moreover, $SF_{\mathbb{Q}}(f) : \mathbb{Q}$ is a normal extension of $\mathbb{Q}$, so it's Galois Group is a normal subgroup of $Gal(M : \mathbb{Q})$. Since $Gal(M : \mathbb{Q})$ is solvable, $Gal(SF_{\mathbb{Q}}(f) : \mathbb{Q}) = Gal_{\mathbb{Q}}(f)$ is solvable. □

3 Worked Example: Polynomial not Solvable by Radicals

3.1 Preliminary Lemmas

3.1.1 Lemma: Degree of Irreducible Divides Order of Galois Group

Let $f \in K[t]$ be irreducible, with K a field. If $SF_K(f) : K$ is ***separable****, then $\deg(f)$ divides $|Gal_K(f)|$.*
(Lemma 9.3.1)

Proof. Let $\alpha \in SF_K(f)$ be a root of f. By irreducibility, the Tower Law and separability:

$$|Gal_K(f)| = [SF_K(f) : K] = [SF_K(f) : K(\alpha)][K(\alpha) : K] = [SF_K(f) : K(\alpha)] \deg(f)$$

as required.

□

3.1.2 Lemma: Generating the Symmetric Group

For $n \geq 2$, S_n is generated by (12) and $(12\ldots n)$.
(Lemma 9.3.2)

Proof. It is a fact that S_n is generated by adjacent transpositions $(12),(23),\ldots,(n-1\ n)$. It is thus sufficient to show that $(12),(12\ldots n)$ generate these transpositions. But using conjugation over S_n, it follows that if $\sigma = (12), \tau = (12\ldots n)$:

$$\tau^j \sigma \tau^{-j} = (\tau^j(1)\ \tau^j(2)) = (j\ j+1)$$

as required. □

3.1.3 Lemma: Galois Group of Prime Degree Polynomial

*Let p be **prime**, and $f \in \mathbb{Q}[t]$ be such that:*

- $\deg(f) = p$
- *f has exactly $p-2$ real roots*

Then:

$$Gal_{\mathbb{Q}}(f) \cong S_p$$

(Lemma 9.3.3)

Proof. $char(\mathbb{Q} = 0$ and f irreducible, so it is separable and has p distinct roots in $\mathbb{C}$. By

*Let f be a **non-zero polynomial** over a **field** K, with k **distinct roots**:*

$$\alpha_1, \ldots, \alpha_k \in SF_K(f)$$

Then:

$$\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate over } K\}$$

*is a **subgroup** of S_k, **isomorphic** to $Gal_K(f)$.*
(Proposition 6.3.10)

the action of $Gal_{\mathbb{Q}}(f)$ on the roots defines an isomorphism between $Gal_{\mathbb{Q}}(f)$ and a subgroup H of S_p. By Lemma 9.3.1 above, by irreducibility and separability, it follows that $\deg(f) = p$ divides $|Gal_{\mathbb{Q}}(f)| = |H|$.

By Cauchy's Theorem, H has an elment σ of order p. The order of elements in S_n is given by the lowerst common multiple of the cycle orders of elements, so it follows that σ must be a p-cycle. Now, complex conjugation is an automorphism of $SF_{\mathbb{Q}}(f)$ over $\mathbb{Q}$. Since exactly 2 of the roots of f are non-real, complex conjugation transposes them, fixing the rest. Thus, H contains both a p-cycle σ and a transposition τ.

Without loss of generality, let $\tau = (12)$. As a p-cycle, $\exists r \in [1, p-1]$ such that $\sigma^r(1) = 2$. Since p is prime, σ^r must also have order p (again, using lowest common multiple), and so, is a p-cycle. Hence, without loss of generality, $\sigma^r = (12 \dots p)$. Since $(12), (12 \dots p) \in H$, we must have that $H = S_p$, so $Gal_{\mathbb{Q}}(f) \cong S_p$. ☐

3.2 Theorem: Solvability by Radicals of Degree 5 Polynomials

Not every polynomial over $\mathbb{Q}$ of degree 5 is solvable by radicals. (Theorem 9.3.5)

Proof. We claim that $f(t) = t^5 - 6t + 3$ has Galois Group S_5 (by using Lemma 9.3.3 above), which isn't solvable. Then, by Theorem 9.2.13, f won't be solvable by radicals.

By Eisenstein with $p = 3$, f is irreducible. Moreover, $\deg(f) = 5$, which is prime. We need to show that f has exactly 3 real roots. Thinking of f as a function $\mathbb{R} \to \mathbb{R}$, then:

- $\lim_{x \to -\infty} f(x) = -\infty$
- $f(0) > 0$
- $f(1) < 0$
- $\lim_{x \to \infty} f(x) = \infty$

By continuity of f over $\mathbb{R}$, it follows by the Intermediate Value Theorem that f has *at least* 3 real roots (one on $(-\infty, 0)$, one on $(0, 1)$ and one on $(1, \infty)$). Computing the derivative, $f'(x) = 5x^4 - 6$, f' has only 2 real roots ($\pm \sqrt[4]{6/5}$). Now, recall **Rolle's Theorem**:

Let $f : [a, b] \to \mathbb{R}$ be continuous on $[a, b]$, differentiable on (a, b) and with $f(a) = f(b)$. Then, $\exists c \in (a, b)$ such that $f'(c) = 0$.

Since f' only has 2 real roots, there can be at most 3 roots $a_1 < a_2 < a_3$, whereby we must have that $-\sqrt[4]{6/5} \in [a_1, a_2]$ and $\sqrt[4]{6/5} \in [a_2, a_3]$. Hence, f has exactly 3 roots, so f satisfies the conditions of Lemma 9.3.3, so f isn't solvable by radicals. ☐

Non-solvability by radicals can also apply to polynomials of degree 5 with Galois Group A_5, which isn't solvable. For example, $f = t^5 + 20t + 16$.