# 1 Review: solvability by radicals

Let $L \mid K$ be a finite field extension.

The extension $L \mid K$ is *radical* if $L = K(\alpha_1, \ldots, \alpha_k)$ for some elements $\alpha_i \in L$ such that

$$\alpha_1^{n_1} \in K, \qquad \alpha_2^{n_2} \in K(\alpha_1), \qquad \alpha_3^{n_3} \in K(\alpha_1, \alpha_2), \qquad \ldots, \qquad \alpha_k^{n_k} \in K(\alpha_1, \ldots, \alpha_{k-1})$$

for some positive integers $n_1, \ldots, n_k > 0$.

Let $P(x) \in K[x]$ and suppose $J \mid K$ is a splitting extension for $P(x)$.

The polynomial $P(x)$ is *solvable by radicals* if there is an extension $L \mid J$ such that $L \mid K$ is radical.

Informally, a polynomial has this property if all of its roots can be expressed using elements of $K$, the usual field operations in $K$, and $n$th root operators $\sqrt[n]{\cdot}$ for a finite list of values of $n$.

**Theorem.** Assume $\mathrm{char}(K) = 0$. Then the polynomial $P(x) \in K[x]$ is solvable by radicals if and only if the group $\mathrm{Gal}(L \mid K)$ is *solvable* in the sense of having a finite filtration

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = \mathrm{Gal}(L \mid K)$$

with $G_i \lhd G_{i+1}$ and $G_{i+1}/G_i$ abelian for all $i$.

The alternating groups $A_n$ and the symmetric groups $S_n$ are each solvable if and only if $n \in \{1, 2, 3, 4\}$.

# 2 Solving the general cubic equation

This lecture illustrates the preceding theorem for a polynomial of degree three.

Let $K$ be a field and suppose that $\mathrm{char}(K) = 0$. We wish to solve the cubic equation

$$y^3 + ay^2 + by + c = 0$$

where $a, b, c \in K$. Letting $x = y + \frac{a}{3}$, we obtain the equivalent equation

$$x^3 + px + q = 0$$

where

$$p = -\frac{1}{3}a^2 + b \qquad \text{and} \qquad q = \frac{2}{27}a^3 - \frac{1}{3}ab + c.$$

Let $P(x) := x^3 + px + q$. We want to find a formula for the roots of $P(x)$ of the following form.

It should start with the elements $\{p, q\}$ and it should only involve iterations of the following operations:

- multiplication and addition;
- multiplication by elements of $K$; and
- the square root $\sqrt{\cdot}$ and cube root $\sqrt[3]{\cdot}$ operations.

Let $L \mid K$ be a splitting extension for $P(x)$.

Let $\omega \in K(\mu_3)$ be a primitive 3rd root of unity.

By our results on splitting extensions, there is a finite Galois extension $J \mid K$ along with homomorphisms

$$L \mid K \hookrightarrow J \mid K \qquad \text{and} \qquad K(\mu_3) = K(\omega) \mid K \hookrightarrow J \mid K.$$

Let $M = L(\omega)$ be the field generated in $J$ by the images of $L$ and $K(\omega)$ in $J$.

Then we have a commutative diagram of $K$-extensions

$$\begin{array}{ccc} L & \hookrightarrow & M = L(\omega) \\ \uparrow & & \uparrow \\ K & \hookrightarrow & K(\mu_3) = K(\omega) \end{array}$$

The Galois group $\mathrm{Gal}(L \mid K)$ is a subgroup of $S_3$ and therefore solvable.

Our arguments in the last lecture show that $M \mid K$ is radical.

We use this in the calculations below.

Fix a polynomial $Q(x) \in K[x]$. Assume this factors in some splitting extension $L \mid K$ as

$$Q(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Then define

$$\sqrt{\Delta_Q} = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \qquad \text{and} \qquad \Delta_Q = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

A finite subgroup $G$ of $S_n$ is called *transitive* if it has only one orbit in $\{1, \ldots, n\}$.

**Lemma.** In this setup, the following properties hold:

(1) Suppose that $Q(x)$ has no repeated roots.
   Let $\phi : \mathrm{Aut}_K(L) \to S_n$ be the map with $\gamma(\alpha_i) = \alpha_{\phi(\gamma)(i)}$ for all $i \in \{1, \ldots, n\}$.
   Then $\phi$ is an injective group homomorphism.

(2) If $Q(x)$ is irreducible over $K$ and has no repeated roots, then the image of $\phi$ is transitive.

(3) The element $\Delta_Q$ belongs to $K$.

(4) Suppose that $Q(x)$ has no repeated roots.
   Then the image of $\phi$ lies inside $A_n \subseteq S_n$ if and only if $\Delta_Q$ is a nonzero square in $K$.

*Proof.* We consider each part:

(1) When $Q(x)$ has no repeated roots, the map $\phi$ is clearly a group homomorphism.
   It is injective because $L$ is generated by $\alpha_1, \ldots, \alpha_n$.
   Thus if $\gamma \in \mathrm{Aut}_K(L)$ acts as the identity on $\{\alpha_1, \ldots, \alpha_n\}$ then $\gamma = \mathrm{id}_L$.

(2) Assume $Q(x)$ is irreducible over $K$ and has no repeated roots.
   We want to show that $\mathrm{Gal}(L \mid K) = \mathrm{Aut}_K(L)$ acts transitively on the set $\{\alpha_1 \ldots, \alpha_n\}$.
   Since $Q(x)$ is irreducible, it is a scalar multiple of the minimal polynomial of each $\alpha_i$.
   We know from an earlier result that this minimal polynomial is $\prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K), \alpha_i)}(x - \beta)$.
   The desired transitivity therefore follows.

(3) We have $\Delta_Q \in K$ since $\prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$ can be expressed as a polynomial over $\mathbb{Z}$ with
   $$e_k = \textstyle\sum_{1 \le i_1 < i_2 < \ldots i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$
   as variables. (See the lecture notes, or check as an exercise.)
   When we set $x_i = \alpha_i$ each $\pm e_k$ becomes a coefficient of $Q(x)$, so is in $K$.

(4) Consider the expression $\delta(\alpha_1, \ldots, \alpha_n) := \sqrt{\Delta_Q} = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)$.

Then for any $\gamma \in \mathrm{Aut}_K(L)$ we have

$$\gamma(\delta(\alpha_1, \ldots, \alpha_n)) = \delta(\gamma(\alpha_1), \ldots, \gamma(\alpha_n)) = \delta(\alpha_{\phi(\gamma)(1)}, \ldots, \alpha_{\phi(\gamma)(n)}) = \mathrm{sgn}(\phi(\gamma)) \cdot \delta(\alpha_1, \ldots, \alpha_n)$$

(See the lecture notes for the last equality.)

Thus $\delta(\alpha_1, \ldots, \alpha_n)$ is fixed by $\mathrm{Aut}_K(L)$, and hence is in $K$, when the image of $\phi$ lies inside $A_n$.

Now note that $\delta(\alpha_1, \ldots, \alpha_n) \in K$ if and only if $\Delta_Q$ is a nonzero square in $K$.

□

We now consider the sequence of extensions

$$K \hookrightarrow K(\omega) \hookrightarrow K(\omega, \sqrt{\Delta_P}) \hookrightarrow M.$$

Note that $\sqrt{\Delta_P} \in L$.

Note also that $[K(\omega) : K] = |\mathrm{Gal}(K(\omega) \mid K)| \le 2$ since $\mathrm{Gal}(K(\omega) \mid K)$ embeds into $(\mathbb{Z}/3\mathbb{Z})^\times$.

Next, we have $[K(\omega, \sqrt{\Delta_P}) : K(\omega)] \le 2$ by construction.

The field $M$ is a splitting field of $P(x)$ over $K(\omega, \sqrt{\Delta_P})$ by construction.

Thus, using part (4) of the lemma, we see that $\mathrm{Gal}(M \mid K(\omega, \sqrt{\Delta_P}))$ is a subgroup of $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

We conclude that either $\mathrm{Gal}(M \mid K(\omega, \sqrt{\Delta_P}))$ is the trivial group or $\mathrm{Gal}(M \mid K(\omega, \sqrt{\Delta_P})) \cong \mathbb{Z}/3\mathbb{Z}$.

Now let $\alpha_1, \alpha_2, \alpha_3 \in L$ be the three roots of $P(x)$, with multiplicities. Let

$$\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \in M \qquad \text{and} \qquad \gamma = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \in M.$$

Note that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

because negating this sum gives the coefficient of $x^2$ in $P(x)$. In particular, we have

$$\alpha_1 = \frac{1}{3}(\beta + \gamma)$$

because $1 + \omega + \omega^2 = 0$. By similar reasoning

$$\alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma) \qquad \text{and} \qquad \alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma).$$

Now we claim that $\beta^3$ and $\gamma^3$ lie in $K(\omega, \sqrt{\Delta_P})$.

If $\mathrm{Gal}(M \mid K(\omega, \sqrt{\Delta_P}))$ is the trivial group, then $M = K(\omega, \sqrt{\Delta_P})$ so the claim holds.

If $\mathrm{Gal}(M \mid K(\omega, \sqrt{\Delta_P})) \cong \mathbb{Z}/3\mathbb{Z}$, then $P(x)$ is irreducible and the roots have no multiplicities, so the claim follows from by our main theorem on Kummer extensions.

So we see that the minimal polynomials of $\beta^3$ and $\gamma^3$ over $K(\omega)$ are of degree $\le 2$.

In other words, $\beta^3$ and $\gamma^3$ satisfy quadratic equations with coefficients in $K(\omega)$.

In turn, the elements of $K(\omega)$ satisfy quadratic equations with coefficients in $K$.

We may thus express $\alpha_1, \alpha_2$ and $\alpha_3$ by a formula involving only multiplication, addition, $\sqrt{\cdot}$, and $\sqrt[3]{\cdot}$.

We make this explicit.

Using the fact that $1+\omega+\omega^2=0$, we compute

$$\beta\gamma=(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)(\alpha_1+\omega^2\alpha_2+\omega\alpha_3)=\alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_1\alpha_3-\alpha_2\alpha_3.$$

Note also that

$$0=(\alpha_1+\alpha_2+\alpha_3)^2=\alpha_1^2+\alpha_2^2+\alpha_3^2+2\alpha_1\alpha_2+2\alpha_1\alpha_3+2\alpha_2\alpha_3.$$

Thus

$$\beta\gamma=\beta\gamma-(\alpha_1+\alpha_2+\alpha_3)^2=-3(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)=-3p.$$

Similarly, we compute

$$\beta^3+\gamma^3=-27q=27\alpha_1\alpha_2\alpha_3.$$

Thus $\beta^3$ and $\gamma^3$ are the roots of the quadratic equation

$$x^2+27qx-27p^3=0.$$

Putting everything together, we see that the solutions of the equation

$$y^3+ay^2+by+c=0$$

are

$$\beta_1=\frac{1}{3}\sqrt[3]{-\frac{27}{2}q+\frac{1}{2}\sqrt{729q^2+108p^3}}+\frac{1}{3}\sqrt[3]{-\frac{27}{2}q-\frac{1}{2}\sqrt{729q^2+108p^3}}-\frac{1}{3}a,$$

$$\beta_2=\frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q+\frac{1}{2}\sqrt{729q^2+108p^3}}+\frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q-\frac{1}{2}\sqrt{729q^2+108p^3}}-\frac{1}{3}a,$$

$$\beta_3=\frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q+\frac{1}{2}\sqrt{729q^2+108p^3}}+\frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q-\frac{1}{2}\sqrt{729q^2+108p^3}}-\frac{1}{3}a,$$

for some choices of 3rd roots of $-\frac{27}{2}q+\frac{1}{2}\sqrt{729p^2+108p^3}$ and $-\frac{27}{2}q-\frac{1}{2}\sqrt{729p^2+108p^3}$.
(Not all of these choices will give solutions). Recall that here

$$p=-\frac{1}{3}a^2+b \qquad \text{and} \qquad q=\frac{2}{27}a^2-\frac{1}{3}ab+c$$

These formulas are actually valid more generally if $\mathrm{char}(K)\notin\{2,3\}$.