14.7 Solvable and radical extensions.

Question. When can zeros of a polynomial be given by a formula using $+, -, \cdot, /, \sqrt[n]{\cdot}$?

Definition. Let α be algebraic over F. Then α can be *expressed by radicals* if there is a sequence

$$F = K_0 \leq K_1 \leq \cdots \leq K_m = K$$

such that

(1) $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i, n_i \in \mathbb{N}$ for all $i \leq m$ (then K_{i+1} is a *simple radical extension* of K_i and K is a *root extension* of F);

(2) $\alpha \in K$.

$f(x) \in F[x]$ is *solvable by radicals* if all its roots can be expressed by radicals.

Question. Which polynomials are solvable?

Insolvability of quintics.

Assume $\mathrm{ch}F = 0$ (or $\mathrm{ch}F > \deg f(x)$) in the following.

Theorem (Galois). *A separable $f(x) \in F[x]$ is solvable by radicals iff its Galois group is solvable.*

Note. There are polynomials of degree n with Galois group S_n (not solvable for $n \geq 5$), e.g. $x^5 - 6x + 3 \in \mathbb{Q}[x]$. (later)

Recall. A finite group G is solvable iff there exists a subnormal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

with G_{i+1}/G_i cyclic.

For the proof of Galois' Theorem we need

(1) Kummer's Theorem on simple radical extensions

(2) root extensions

Simple radical extensions.

Definition. Galois K/F is <u>cyclic</u> iff $\mathrm{Gal}(K/F)$ is cyclic.

Theorem (Kummer)**.** *Assume* $\mathrm{ch}F \nmid n$ *and* F *contains all* n*-th roots of unity. Then* <u>K/F *is cyclic*</u> *and* $[K:F] \mid n$ *iff* <u>$K = F(\alpha)$ *for some* α *with* $\alpha^n \in F$</u>.

Proof. $\Leftarrow$ $K = F(\alpha)$ with $\alpha^n \in F$ is the splitting field of $x^n - \alpha^n \in F[x]$ since $\zeta_n \in F$.

Hence K/F is Galois and $\sigma \in \mathrm{Gal}(K/F)$ permutes the roots of $x^n - \alpha^n$

$\sigma(\alpha) = \alpha \cdot \zeta_\sigma$ for ζ_σ an n-th root of 1.

Further
$$\varphi : \mathrm{Gal}(K/F) \to \langle \zeta_n \rangle, \quad \sigma \mapsto \zeta_\sigma$$
is a group homomorphism (check!)

$\ker \varphi := \{\sigma \mid \sigma(\alpha) = \alpha \cdot 1\} = 1$

Hence $\mathrm{Gal}(K/F) \hookrightarrow (\mathbb{Z}_n, +)$

$\Rightarrow$ Assume $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ of order $m \mid n$.

Construct α that is not in any proper subfield of K, i.e. not fixed by any power of σ.

For any $\beta \in K$ and ζ an m-th root of 1, let
$$\alpha := \beta + \zeta\sigma(\beta) + \zeta^2\sigma^2(\beta) + \dots + \zeta^{m-1}\sigma^{m-1}(\beta)$$

Then
$$\sigma(\alpha) = \sigma(\beta) + \zeta\sigma^2(\beta) + \dots + \zeta^{m-1}\underbrace{\sigma^m(\beta)}_{\beta} = \alpha\zeta^{-1}$$

Recall Dirichlet's Thm: Distinct automorphisms $1, \sigma, \sigma^2, \dots, \sigma^{m-1}$ are lin independent.

Hence we have $\beta \in K$ for which $\alpha \neq 0$.

$$\sigma(\alpha^n) = \alpha^n \cdot \underbrace{\zeta^{-n}}_{=1} = \alpha^n \in F$$

$$\sigma^k(\alpha) = \alpha \cdot \zeta^{-k} \neq \alpha \quad \text{for } 1 \le k \le m-1$$

Hence α is not in any proper subfield of K, thus $K = F(\alpha)$. $\square$

Root extensions.

Recall. K/F is a root extension if $F = K_0 \leq K_1 \leq \cdots \leq K_m = K$ with $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for $a_i \in K_i$, $n_i \in \mathbb{N}$.

Lemma.

(1) *If K/F and L/F are root extensions, then KL/F is a root extension.*
(2) *Every root extension K/F is contained in a Galois root extension L/F with $F = L_0 \leq L_1 \leq \cdots \leq L_n = L$ and all L_{i+1}/L_i cyclic.*

Proof. 1)

$KL = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_\ell)$

$K(\beta_1) - K(\beta_1, \beta_2) - \cdots$

$K = F(\alpha_1, \dots, \alpha_m)$

$F(\alpha_1, \alpha_2)$

$F(\alpha_1)$

$F - F(\beta_1) \cdots$

$L = F(\beta_1, \beta_2, \dots, \beta_n)$

2) Let L be the Galois closure of K over F.
For $\sigma \in Gal(L/F)$, $\sigma(K)/F$ is a root extension with
$F \leq \sigma(K_1) \leq \cdots \leq \sigma(K_m) = \sigma(K)$.
By 1) $\langle \sigma(K) \mid \sigma \in Gal(L/F) \rangle = L$ is a root extension, Galois.
$F = L_1 \leq \cdots \leq L_k = L$ where $L_{i+1} = L_i(\sqrt[n_i]{a_i})$ for $1 \leq i < k$
Let $E := F(n_i\text{-th roots of } 1 \text{ for } 1 \leq i < k)$
Then E/F is Galois, abelian, a root extension with cyclic factors $E_{i+1} = E_i(\zeta_{n_i})$ for $1 \leq i < k$.

$$\underbrace{F = E_1 \leq \cdots \leq E_k = E}_{\text{cyclotomic extension}} \leq \underbrace{EL_1 \leq EL_2 \leq \cdots \leq EL_k = EL}_{\text{cyclic extensions}}$$

cyclotomic extension ⇒ abelian factors E_{i+1}/E_i that can be refined into cyclic quotients

cyclic extensions by Kummer's Thm

Hence EL/F is Galois root extension with cyclic factors. □

<u>Proof of Galois' Thm.</u>

Let $f(x) \in F[x]$ separable with splitting field K.
⇒ Assume $f(x)$ is solvable by radicals, i.e. all its roots are in a root extension.
By the previous Lemma, K is contained in a Galois root extension L with cyclic factors
$F = L_1 \leq L_2 \leq \cdots \leq L_m = L$
Let $G_i := Gal(L/L_i)$
$Gal(L/F) = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = 1$
and G_i/G_{i+1} is cyclic. Hence $G_1 = Gal(L/F)$ is solvable.

$L \;—\; 1$

$K \;—\; H := Gal(L/K)$

$F \;—\; G_1$

$Gal(K/F) \cong G_1/H$ hence solvable.

$\Leftarrow$ Assume $G = \mathrm{Gal}(K/F)$ is solvable with

$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$

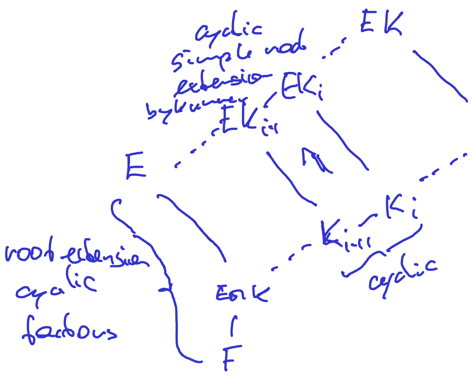
with G_{i+1}/G_i cyclic.

Let $K_i := \mathrm{Fix}(G_i)$

$K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_m = F$

where K_i/K_{i+1} is cyclic of degree n_i.

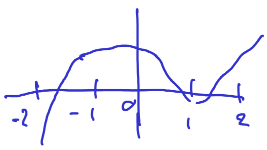
Let $E = F(\xi_{n_1}, \dots, \xi_{n_m})$



∎

Lemma. *Let $f(x) \in \mathbb{Q}[x]$ have prime degree p and splitting field K.*
If $f(x)$ has $p-2$ real roots and 2 non-real roots, then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.

Example. $f(x) = x^5 - 6x + 3$ irreducible by Eisenstein



By Lemma, $f(x)$ has Galois group $\cong S_5$, not solvable, hence zeros of $f(x)$ cannot be expressed by radicals.

Proof. Recall $G := \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_p$

$|G| = [K:\mathbb{Q}]$ is a multiple of p

By Cauchy's Thm G has an element of order p (a p-cycle in S_p)

Complex conjugation acts on K and yields a transposition on the roots of $f(x)$.

So $\underbrace{\langle (12\dots p), (12) \rangle}_{= S_p \text{ since } p \text{ prime.}} \hookrightarrow G$.

∎