Splitting field & Abel-Ruffini (Lecture 8)

Df. Let $L:K$ be a field extension $\varphi: K \to L$ be the embedding $\varphi: K \to L$, and $f \in K[t] \setminus K$. Then f splits over L if $\varphi(f) = c \prod_{j=1}^{d} (t - \alpha_j)$, where $\alpha_j \in L$, $c \in \varphi(K)$. If f splits over L, and $\varphi(K) \subseteq M \subseteq L$ then we say that $M:K$ is a splitting field extension for f if M is the smallest subfield of L containing $\varphi(K)$ over f splits.

L. Let $L:K$ be a splitting field ext. for $f \in K[t] \setminus K$, $\varphi: K \to L$. Let $\alpha_j \in L$ be roots of $\varphi(f)$. Then $L = \varphi(K)(\alpha_1, .., \alpha_n)$.

Pf. We can identify K & $\varphi(K) \Rightarrow$ let $K \subseteq L$ and put $\mathbb{F} = K(\alpha_1, .., \alpha_n) \Rightarrow K - F - L$ and f splits over F. By minimality $L \subseteq \mathbb{F} \Rightarrow L = \mathbb{F}$. ∎

Ex. 1) $\mathbb{C}$ is a splitting field of x^2+1

1') Let $[L:K] = 2 \Rightarrow \forall \alpha \in L \setminus K$, L is a splitting field of μ_α^K ($\deg \mu_\alpha^K = 2 \Rightarrow \mu_\alpha^K = (x-\alpha)(x-\alpha')$ but $K(\alpha, \alpha') = K(\alpha)$ since $\alpha + \alpha' \in K$ by Vieta)

2) $x^3 - 2 \in \mathbb{Q}[x] \Rightarrow \mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$ is a splitting field of x^3-2.

3) $x^n - a \in K[x] \Rightarrow L = K(R, \varepsilon_n)$, R is any root of $x^n = a$ (we need $\operatorname{char} K \nmid n$)

4) $f(x) = x^3 + ax^2 + bx + c$, f is irredicible over K, $\alpha_1, \alpha_2, \alpha_3$ are roots

$$K \overset{3}{—} K(\alpha_1) \begin{array}{l} \nearrow \alpha_2 \in K(\alpha_1) \Rightarrow L = K(\alpha_1) \\ \qquad (\alpha_3 \in K(\alpha_1) \text{ automatically}) \\ \searrow \alpha_2 \notin K(\alpha_1) \Rightarrow L = K(\alpha_1, \alpha_2) \end{array}$$

We have $[K(\alpha_1, \alpha_2) : K] = 6$

In general, we get

L. Let $f \in K[t] \setminus K$ and $L:K$ be a splitting field for f. Then $[L:K] \leq (\deg f)!$

Just consider $K \overset{\leq n}{—} K(\alpha_1) \overset{\leq n-1}{—} K(\alpha_1, \alpha_2) \overset{\leq n-2}{—} \dots \overset{\leq 1}{—} K(\alpha_1, \dots, \alpha_n)$

5) $f = t^4 - 2 \in \mathbb{Q}[t] \Rightarrow \pm\alpha, \pm i\alpha$, where $\alpha = \sqrt[4]{2}$ are roots of $f \Rightarrow L = \mathbb{Q}(\alpha, i)$ is a splitting field. We have $L:K = 8$ $(i \notin \mathbb{R})$

Thm If $f \in K[t] \setminus K$, and $L:K$, $M:K$ are splitting field extensions for f. Then $L \cong M$ (in particular $[L:K] = [M:K]$).

We will prove this result later (the proof requires the concept of algebraic closure) and now let us obtain the first result about solvability by radicals.

Df. Let $L:K$ be a field extension, $R \in L$. Then R is radical over K if $R^n \in K$ for some $n \in \mathbb{N}$. Further $L:K$ is an extension by radicals if $\exists$ a tower of field extensions

$$L_0 = K - L_1 - L_2 - \dots - L = L_m \quad \text{s.t.} \quad L_j = L_{j-1}(R_j)$$

with R_j radical over L_{j-1}, $j = 1, \dots, m$.
Finally, we say $f \in K[t]$ is 'solvable' by radicals if there is a radical extension of K over which f splits.

Thm (Abel - Ruffini) Informally it states that there is no solution by radicals to general equations of degree 5 or higher with arbitrary coefficients (coefficients = indeterminates)

Our basic field is $K = \mathbb{C}(a_1, \dots, a_n)$ where $a_1, \dots, a_n$ are formal variables. Consider the general or generic polynomial eq. of degree n over K:

$$\underbrace{x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n}_{f(x) \in K[x]} = 0, \quad n \geq 5.$$

Let $x_1, \dots, x_n$ be root of f and $L = K(x_1, \dots, x_n)$ be a splitting field for f. We prove that $f \in K[x]$

is not solvable by radicals.

<u>Pf (Ruffini)</u> Suppose that

$$K=\mathbb{C}(a_1,..,a_n)=K_0 - K_1 - K_2 - \dots - K_m = L,$$ with $L = K(x_1,..,x_n)$,

$K_j = K_{j-1}(R_j)$, $R_j^{k_j} \in K_{j-1}$ (i.e. R_j are radicals)

Since a_j are elementary symmetric pol. in $x_1,..,x_n$, we have $K(x_1,..,x_n) = \mathbb{C}(a_1,..,a_n)(x_1,..,x_n)$
$= \mathbb{C}(x_1,..,x_n)$.

Moreover, one can say that $K = \mathbb{C}(a_1,..,a_n) = \mathbb{C}(x_1,..,x_n)^{\mathrm{sym}}$ (the field $\frac{h_1(x_1,..,x_n)}{h_2(x_1,..,x_n)}$, where h_1, h_2 are symmetric).

L.1. Let $R \in L$, $\sigma \in S_n$ and $\sigma(R^k) = R^k$, $k \in \mathbb{Z}^+$. Then $\sigma(R) = \varepsilon R$, where $\varepsilon^{\mathrm{Ord}(\sigma)} = 1$.

<u>Pf.</u> We have $\sigma(R)^k = \sigma(R^k) = R^k \Rightarrow \sigma(R) = \varepsilon R$, where $\varepsilon \in \sqrt[k]{1}$. Further (since $\varepsilon \in \mathbb{C}$ does not depend on $x_1,..,x_n$)

$$\sigma(\sigma(R)) = \sigma(\varepsilon R) = \varepsilon \sigma(R) = \varepsilon^2 R.$$

Similarly, $\sigma^d(R) = \varepsilon^d R$ $\forall d$. Thus for $d = \mathrm{Ord}(\sigma)$ we have $\varepsilon^d R = \sigma^d(R) = R \Rightarrow \varepsilon^{\mathrm{Ord}(\sigma)} = 1$ (if $R=0$, then there is nothing to prove). ∎

Now we use some computations in S_n.

L.2. Let $n \geq 5$ and $\pi = (12345)$, $\rho = (345)$, $\tau = (123)$. If $\pi^k(R) = \rho^k(R) = \tau^k(R) = R$, then $\pi(R) = \rho(R) = \tau(R) = R$.

Pf. By Lemma 1 $\pi(R) = \omega R$, $\omega^5 = 1$
$\tau(R) = \varepsilon R$, $\varepsilon^3 = 1$

$\tau\pi = (13452) \Rightarrow \tau\pi(R) = \tau(\pi(R)) = \omega\varepsilon R$
$\Rightarrow (\omega\varepsilon)^5 = 1 \Rightarrow \varepsilon^5 = 1 \Rightarrow \varepsilon = 1 \Rightarrow \tau(R) = R$

Similarly, $\rho\pi = (12435)$ and the same argument gives us $\rho(R) = R$. Finally, $\tau\rho = \pi$ (obviously) $\Rightarrow \omega = 1 \Rightarrow \pi(R) = R$. ∎

L.0. $x_1, \ldots, x_n$ are algebraically independent over $\mathbb{C}$.

Pf. Let $0 \not\equiv g(x_1, \ldots, x_n) = 0$, where $g(t_1, \ldots, t_n) \in \mathbb{C}[t_1, \ldots, t_n]$
Consider $g_\sigma(t_1, \ldots, t_n) = g(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) \not\equiv 0$, $\sigma \in S_n$
Then $\prod_{\sigma \in S_n} g_\sigma(t_1, \ldots, t_n) = F(t_1 + \ldots + t_n, \ldots, t_1 \ldots t_n)$

elementary symm. pol.

Put $t_i = x_i \Rightarrow LHS = 0 = F(-a_1, a_2, \ldots, (-1)^n a_n)$
$\Rightarrow F \equiv 0$ and this is a contradiction. ∎

Now consider $K_0 - K_1$, $R_1^{k_1} \in K_0 = \mathbb{C}_{sym}(x_1, \ldots, x_n)$.

Thus $\forall \sigma \in S_n$ one has $\sigma(R_1^{k_1}) = R_1^{k_1}$ (this is an element of $K_0 = \mathbb{C}_{sym}(x_1, .., x_n)$). Further, by L.2 π, ρ and τ preserve the whole field $K_1 = K_0(R_1)$, where $R_1^{k_1} \in K_0$ $\Rightarrow$ they preserve $R_2^{k_2} \in K_1$ $\Rightarrow$ by L.2 they preverve R_2. And so on. Thus, π, ρ, τ preserve L. In particular, $\pi(x_1) = x_1$ but $\pi(x_1) = x_2 \neq x_1$. This is a contradiction. ∎

Actually, instead of

$$K = \mathbb{C}(a_1, .., a_n) = K_0 - K_1 - K_2 - \ldots - K_m = \overset{K(x_1,..,x_n)}{\overset{\shortparallel}{L}},$$

$K_j = K_{j-1}(R_j)$, $R_j^{k_j} \in K_{j-1}$ (i.e. R_j are radicals)

we need $K_0 - K_1 - K_2 - \ldots - K_m \supset L$.

Exm $\mathbb{Q} \overset{3}{-} \mathbb{Q}(\cos\frac{2\pi}{9}) \ni \cos\frac{4\pi}{9}, \cos\frac{8\pi}{9}$. conjugated elements

Clearly, the eq. $4x^3 - 3x = -\frac{1}{2}$ is solvable by radicals

If $\exists$ an extension by radicals

$$\mathbb{Q} = K_0 - K_1 - \ldots - K_m = \overset{=L}{\mathbb{Q}(\cos\frac{2\pi}{9})},$$

then obviously, $m = 1 \Rightarrow L = \mathbb{Q}(\sqrt[3]{a})$, $a \in \mathbb{Q}$ $\Rightarrow a > 0$ (exercise: otherwise the degree $\neq 3$) but conjugates of $\sqrt[3]{a}$ are $\sqrt[3]{a} \cdot \varepsilon_3$, $\sqrt[3]{a} \cdot \varepsilon_3^2$ and they do not belong to $\mathbb{Q}(\sqrt[3]{a}) = L$.

In the future such fields L will be called normal!