The Primitive Element Thm. (Lecture 15)

Df. Let $L:K$ be a field extension, $\varphi: K \to L$. Then $L:K$ is a *simple* extension if $\exists\, \theta \in L$ s.t. $L = \varphi(K)(\theta)$.

Exm 1) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{:=M})$. Indeed,

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3}-\sqrt{2} \in M \Rightarrow \sqrt{2}, \sqrt{3} \in M.$$

2) Let α, β be alg. over $K \Rightarrow \exists\, \theta : K(\alpha,\beta) = K(\theta)$

We try to find θ in the following form

$\theta = \alpha + c\beta$, $c \in K$. Clearly, it is enough to prove $\beta \in K(\theta)$. Consider, μ_α^K & μ_β^K. Then

$$\mu_\beta^K(\beta) = \mu_\alpha^K(\theta - c\beta) = 0 \Rightarrow \gcd\left(\mu_\beta^K(x), \mu_\alpha^K(\theta - cx)\right) =: g(x)$$

$\in K(\theta)[x]$. If $g(x) = x - \beta$, then $\beta \in K(\theta)$ and we are done. The 1st polynomial has roots $\underbrace{\beta_1, \dots, \beta_n}_{\kappa_\beta}$, the 2nd: $\alpha_1, \dots, \alpha_m$ and thus we want to find c s.t.

$$\alpha_1 + c\beta_1 - c\beta_i = \theta - c\beta_i = \alpha_j \iff i = j = 1$$

Thus, we want $c \neq \dfrac{\alpha_j - \alpha_1}{\beta_1 - \beta_i}$, $\forall\, i, j$ (excluding $i=j=1$)

Clearly, if $|K| = \infty$, then such c exists.

If $|K| < \infty$, then K^* is a cyclic group and therefore if $[L:K] < \infty$, then we can put $L = K(g)$, where $K^* = \{1, g, g^2, \dots\}$.

Unfortunately, it can be that $g(x) = (x-\beta)^e$, where $e > 1$ due to the existence of inseparable polynomials in positive characteristic.

Thm (the primitive element theorem)

Let $L:K$ be a finite, separable extension, $K \subseteq L$. Then $L:K$ is a simple extension.

Pf. We assume that $L \subseteq \overline{K}$. If $|K| < \infty$, then $|L| = |K|^{[L:K]} \Rightarrow L^* = \langle g \rangle$ and $L = K(g)$.
Now if $|K| = \infty$, then we use induction on $[L:K]$.
Let $\alpha \in L$ be any element of largest degree over K. If $L = K(\alpha)$, then we are done. Otherwise $\exists\ \beta \in L \setminus K(\alpha)$.
Suppose that $[K(\alpha, \beta):K] < [L:K] \Rightarrow$ by induction $K(\alpha, \beta) = K(\gamma)$ for some $\gamma \in L$. Then $[K(\gamma):K] = [K(\alpha, \beta):K] > [K(\alpha):K]$ (recall that $\beta \in L \setminus K(\alpha)$) and this contradicts our maximal assumption. Thus $[K(\alpha, \beta):K] = [L:K]$ and hence $L = K(\alpha, \beta)$.
We know that $L:K$ is separable $\Rightarrow$

we know that $\exists$ ← see Lecture 14 $[L:K]$ distinct K-hom. $\varphi_j : K(\alpha,\beta) \to \overline{K}$. Put

$$f = \prod_{1\le i<j\le n} \left((\varphi_i(\alpha) - \varphi_j(\alpha)) + (\varphi_i(\beta) - \varphi_j(\beta)) t \right)$$

If $f = 0$, then $\varphi_i(\alpha) = \varphi_j(\alpha)$ & $\varphi_i(\beta) = \varphi_j(\beta)$ $\Rightarrow \varphi_i = \varphi_j$ and this is a contradiction.

We have $|K| = \infty \Rightarrow \exists\, c \in K$ s.t. $f(c) \neq 0$.

Put $\theta = \alpha + c\beta$. Then $\varphi_i(\theta) \neq \varphi_j(\theta)$, $i \neq j$.

Indeed, otherwise

$$f(c) = \prod_{1\le i<j\le n} \left(\varphi_i(\alpha + c\beta) - \varphi_j(\alpha + c\beta) \right) = 0$$

and this is a contradiction. Thus φ_j must restrict to distinct K-hom. from $K(\theta) \to \overline{K}$.

As above (see the same Cor. 1 of Lecture 14) we derive that $[K(\theta):K] \geq [L:K]$.

Thus $K(\theta) = L$ as required. ∎

Ex. (Artin) $L:K$ is a finite extension. Then $L:K$ is a simple extension $\Leftrightarrow$ the number of intermidiate fields is finite.

Cor. Let $L:K$ is an algebraic, separable ext. s.t. $\forall \alpha \in L$ one has $\deg \mu_\alpha^K \leq n$. Then $[L:K] \leq n$.

Ex. We want to construct a finite alg (inseparable) extension that is not simple.

First of all, let $K_0 = \mathbb{F}_p(t)$ be our base field. Take any transcendental over K element s. Our first field $M = K_0(s)$ and L be a splitting field extension for the pol. $(x^p - t)(x^p - s) \in M[x]$. So, we have

$$K_0 \overset{\infty}{—} M \ (= K(s)) \overset{?}{—} L$$ (below we obtain $[L:M] = p^2$)

We need to compute $[L:M]$. First consider the pol. $x^p - t$ $=: h(x) \in M[x]$ & M_1 be its splitting field.

L.1. $[M_1 : M] = p$

Pf. Let $h(\alpha) = 0$ ($\alpha \in M_1$) $\Rightarrow t = \alpha^p \Rightarrow$ hence h is inseparable

$(x-\alpha)^p = x^p - \alpha^p = (x-\alpha)^p$, so α has multiplicity p.

Let us check that h is irr. over M.
If $h = f \cdot g \Rightarrow f = (x-\alpha)^\ell$, $g = (x-\alpha)^{p-\ell}$ ($M[x]$ is UFD) $\Rightarrow$ since $\gcd(\ell, p-\ell) = 1$ we can find $a, b \in \mathbb{Z}$ s.t. $a\ell + b(p-\ell) = 1 \Rightarrow x - \alpha = f^a g^b$ $\Rightarrow x - \alpha \in M[x] \Rightarrow \alpha \in M$. It follows that $\exists c, d \in \mathbb{F}_p[s,t]$ with $\alpha = c/d$. Therefore

$t = \alpha^p = \left(\frac{c}{d}\right)^p \Rightarrow c^p = t\, d^p$. This is a contradiction (compare the degrees of LHS/RHS). Thus h is irreducible over $M[x]$ and hence $[M_1 : M] = \deg h = p$. ■

L.2. $[L:M] = p^2$. In particular, $L:M$ is an algebraic extension.

Pf. $M \overset{p}{—} \overset{=M(\alpha)}{M_1} \overset{2}{—} F$ ← the splitting field for $x^p - s$. Let us prove that $[L:M_1] = p$. Indeed, as in the proof of L.1 let $\beta \in L$ s.t. $x^p - s = (x-\beta)^p := H(x)$. If $H(x)$ is reducible over M_1, then as above $\beta \in M_1$ and $\exists\, c, d \in \mathbb{F}_p(\alpha)[s]$ s.t. (recall that $M_1 = M(\alpha)$).

$c^p = s\, d^p$. Comparing $\deg_s$ we obtain a contradiction again and therefore $H(x)$ is irr. over $M_1 \Rightarrow [F : M_1] = p$ (and $F = M_1(\beta)$)

Clearly $F \supseteq L$ and $M_1 \subseteq L \neq M_1 \Rightarrow [L:M] = p^2$ (use the tower law) ■

L.3. $L:M$ is not a simple extension.

Pf. Suppose that $\exists\, \theta \in L$ s.t. $L = M(\theta)$.

Observe that $\forall\, \theta \in L$ one has $\theta^p \in M$.
Indeed, $\alpha, \beta \in L$ and by construction $\alpha^p = t$, $\beta^p = s$. Also, $(x^p - t)(x^p - s) = (x-\alpha)^p (x-\beta)^p$

$$\Rightarrow L = M(\alpha, \beta) \Rightarrow \theta = \frac{q(\alpha,\beta)}{r(\alpha,\beta)}, \quad q, r \in M[z_1, z_2]$$

Then $\theta^p = \dfrac{q^p(\alpha,\beta)}{r^p(\alpha,\beta)} = \dfrac{q(\alpha^p, \beta^p)}{r(\alpha^p, \beta^p)} = \dfrac{q(t,s)}{r(t,s)} \in M$.

Thus, we know that $\theta^p = \delta \in M \Rightarrow$
$\mu_\theta^M \mid (t^p - \delta) \Rightarrow 1 \le [M(\theta) : M] \le p$.

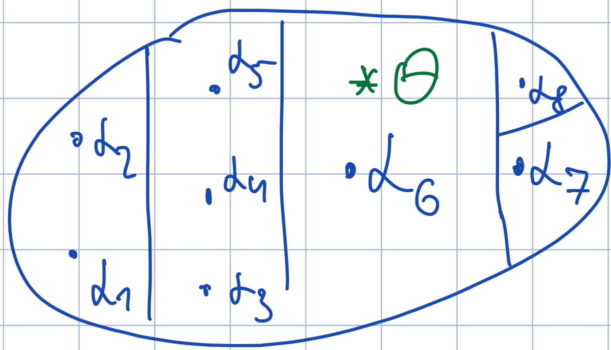
On the other hand, $\underbrace{M - M(\theta) - L}_{p^2}$

$$\Rightarrow [M(\theta) : M] = \begin{cases} p \\ 1 \end{cases}.$$

But $[L : M] = p^2$ and thus $L:M$ cannot be simple. This concludes the proof of L.3 and therefore the constuction is complete. $\blacksquare\ \blacksquare$

We know that if $K - L$ is a normal extension, $\alpha, \beta \in L$ & $\mu_\alpha^K = \mu_\beta^K \Rightarrow \exists\, \tau \in Gal_K(L)$ s.t. $\tau(\alpha) = \beta$ (transitivity).

Now let $f = \mu_1(x) \ldots \mu_s(x)$, μ_i are irr. over K and f be a separable polynomial:



separable

Thm Orbits of $Gal_K(f)$ = conjugate classes over K.

($Gal_K f$ acts on $\{\alpha_1,\dots,\alpha_n\}$)

Pf. If $\mu_1(\alpha_1)=0 \Rightarrow \forall \tau \in Gal_K(f)$ one has $\tau(\mu_1(\alpha_1)) = \mu_1(\tau(\alpha_1))$ (so it is not possible to move α_1 to another conjugate class)

On the other hand, we know that

isomorphism

$K(\alpha_1)\cong K(\alpha_2)$ and moreover $\exists\, \psi: K(\alpha_1)\to K(\alpha_2)$ s.t. $\psi(\alpha_1)=\alpha_2$. Also, we know that $L=K(\alpha_1,\dots,\alpha_n)$ is $K(\theta)$ and hence $\alpha_j = f_j(\theta)$, $f_j\in K[t]$.

If $\theta_1=\theta,\dots,\theta_N$ are conjugates of θ, then

$\alpha_1 = f_1(\theta),\dots,f_1(\theta_N)$ are conj. of α_1

$\alpha_2 = f_2(\theta),\dots,f_2(\theta_N)$ are conj. of α_2

As α_1 & α_2 are conjugated elements, we see that $\alpha_1=f_1(\theta)$, $\alpha_2=f_1(\theta_i)$, $i\in\{1,\dots,N\}$

isomorphism

$\exists\, \varphi: \theta_1\to\theta_i \Rightarrow \varphi(\alpha_1)=\varphi(f_1(\theta)) = f_1(\theta_i)=\alpha_2$ ∎

Cor. $f \in K[t]$ is irreducible over K
$\Longleftrightarrow$ $\mathrm{Gal}_K(f)$ acts transitively on its roots.