The Fundamental Thm. of Galois Theory (2nd part)

Lecture 21

Reminder Let $L:K$ be any extension, $G := \mathrm{Aut}_K L$. Let $I(K,L)$ be the collection of all intermediate fields and $S(G)$ be the family of all subgroups of G.

$$\begin{tikzcd} I(K,L) \arrow[rr, bend left] & & S(G) \arrow[ll, bend left] \end{tikzcd}$$

For any $P \in I(K,L) \longmapsto \overset{:= G_P}{\mathrm{Aut}_P L} \leq G$

For any $H \in S(G) \longmapsto \underset{\in I(K,L)}{L^H} := \{\alpha \in L : \forall h \in H \ h\alpha = \alpha\}$

The Galois correspondence claims that there is a one-to-one correspondence between $I(K,L)$ and $S(G)$. In other words,

Thm.(1st part) Let $L:K$ be a Galois extension and $G = \mathrm{Gal}_K L$. Define $I(K,L)$ and $S(G)$ as above. Then

$$\forall P \in I(K,L) : \ L^{G_P} = P$$
$$\forall H \in S(G) : \ G_{L^H} = H.$$

Also, we know that $P_1 \subseteq P_2 \iff G_{P_1} \geq G_{P_2}$

and $H_1 \leq H_2 \iff L^{H_1} \geq L^{H_2}$ (see Thm. 1 (1,2) of Lecture 19)

(2nd part) $P:K$ is a normal extension $\iff$ $G_P \trianglelefteq G$ and then $\mathrm{Gal}_K P \cong G/G_P$.

Exm. Let f be a separable cubic polynomial with $\mathrm{Gal}_K(f) \cong S_3$ (that is the roots $\alpha_1, \alpha_2, \alpha_3$ of f satisfy $\alpha_1 \notin K(\alpha_2, \alpha_3)$ and so on)

In S_3 we have $A_3 \overset{\cong \mathbb{Z}_3}{}$, $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle)$ (also, let char $K \neq 2$) We know that

$$K(\sqrt{D}) = K((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)) = L^{A_3}$$

Clearly, $\langle(12)\rangle \leftrightarrow K(\alpha_3)$ and so on (indeed, obviously $L^{\langle(12)\rangle} \geq K(\alpha_3)$ but $[K(\alpha_3):K] = 3 \Rightarrow$ $[L^{\langle(12)\rangle}:K] = 3$ or 6 but it cannot be 6 ($\alpha_1 \leftrightarrow \alpha_2$)).

Here $A_3 \trianglelefteq S_3$ and $K - K(\sqrt{D})$ is a normal extension but $K - K(\alpha_i)$ are not normal.

L. $K - P - L$ and $g \in \mathrm{Aut}\, L$. Then $\boxed{G_{gP} = g G_P g^{-1}}$.

Pf. Indeed, $\forall h \in G_{gP} \overset{\text{df}}{\iff} \forall p \in P: hgp = gp$ $\iff g^{-1}hgp = p \iff g^{-1}hg \in G_P \iff h \in g G_P g^{-1}$ ∎

Thus G_{gP} and G_P are conjugated (thus we say that the fields gP and P are conjugated: in particular $K(\alpha_i)$ & $K(\alpha_j)$ are conjugated.

Further, P/K is normal $\Leftrightarrow$ $\forall p \in P$ the field P contains all conjugates of $p \Leftrightarrow \forall g \in G$ $\forall p \in P$ $gp \in P \Leftrightarrow gP \subseteq P$. It follows that $gP = P$ (one can compute $[P:K]$, $[gP:K]$ or just replace $g \to g^{-1} \Rightarrow g^{-1}P \subseteq P \Leftrightarrow P \subseteq gP$)

Thus $\forall g \in G$ one has $gP = P \Leftrightarrow G_P = g G_P g^{-1}$ $\forall g$ by lemma and the 1st part of the Main thm.

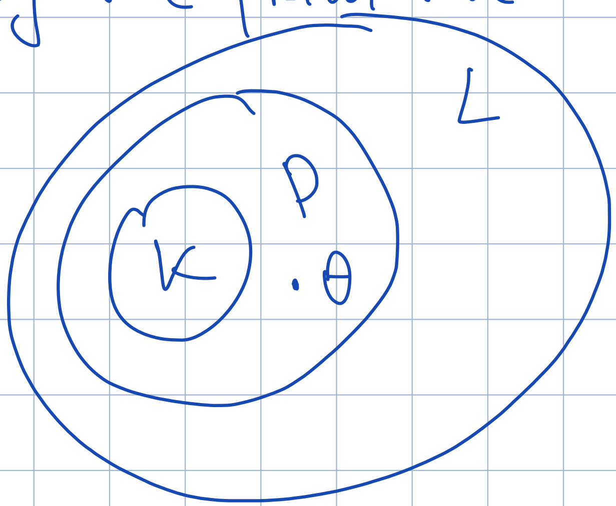
It remains to prove that $\mathrm{Gal}_K P \cong G/G_P$.
By assumption $P:K$ is normal & $L:K$ is Galois $\Rightarrow$ $P:K$ is Galois. Further we know that $\forall g \in G$ one has $gP = P \Rightarrow$ we can consider the restriction

$$G \xrightarrow{\mathrm{Res}_P} \mathrm{Gal}_K P$$
$$g \longmapsto g_P$$

$\mathrm{Ker}\,\mathrm{Res}_P = G_P$ (by definition of G_P)
Let us prove that Res_P is a surjective homomorphism. Thus, we need to prove that

$\forall \varphi \in Gal_K P \overset{?}{\Longrightarrow} \exists\, g \in G$ s.t. $g|_P = \varphi$.

By the primitive element thm. $P = K(\theta)$, $\theta \in P$



$G\cdot\theta = Gal_K P \cdot \theta \overset{\subseteq P}{=}$ conjugates of θ over K

Thus $\exists\, g \in G$ s.t.

$\varphi\cdot\theta = g\cdot\theta \iff \varphi(p) = g(p),\ \forall p \in P$

$\iff \varphi = g|_P$

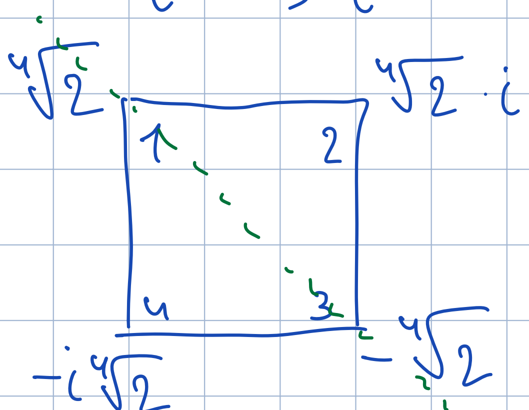
Thus $Gal_K P \cong G/G_P$. ∎

$(Cent((13)(24)))$

Exm. $t^4 - 2 \in \mathbb{Q}[t]$, $L = \mathbb{Q}(\sqrt[4]{2}, i)$, $G \cong D_4$

(see Lecture 18). Let $D_4 = \langle r, s \rangle$

$r: \sqrt[4]{2} \to i\sqrt[4]{2}$, $i \to i$ & $s: \sqrt[4]{2} \mapsto \sqrt[4]{2}$, $i \to -i$ (← complex conjugation)



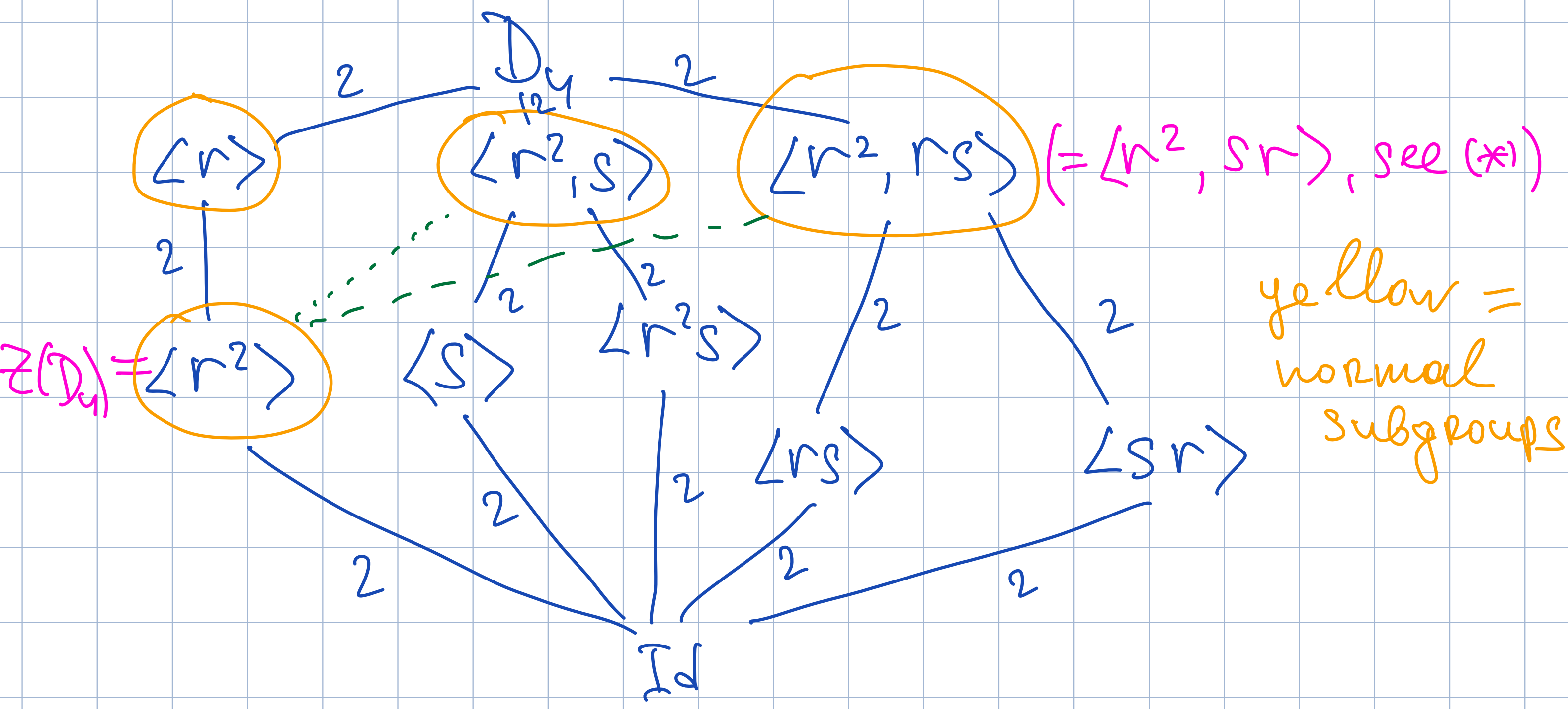
$r: \sqrt[4]{2} \to i\sqrt[4]{2} \to -\sqrt[4]{2} \to -i\sqrt[4]{2}$

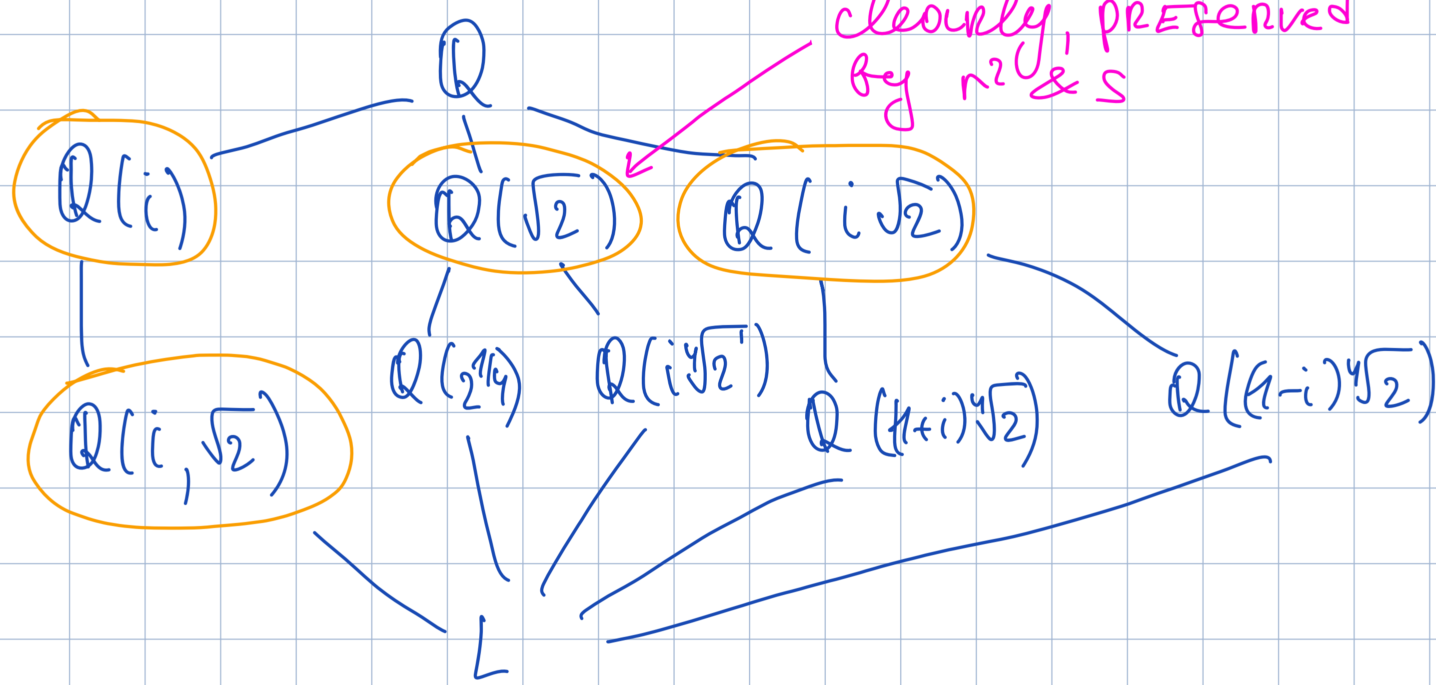
(rotation = cycle of length 4) $= (1234)$

s is a symmetry $= (24)$

One has $rs = sr^3$ $(*)$ ← commutation relation. It follows that $r^2 s = rsr^3 = sr^6 = sr^2$

$\Rightarrow$ the center of D_4 is $Z(D_4) = \langle r^2 \rangle$.





For example, $\mathbb{Q}(i) \subseteq L^{\langle r\rangle}$ but $[\mathbb{Q}(i):\mathbb{Q}]=2$,
$\mathbb{Q} \underset{2}{-} \mathbb{Q}(i) \underset{4}{-} L$ and $[G:\langle r\rangle]=2 \Rightarrow \mathbb{Q}(i)=L^{\langle r\rangle}$,
Further $[G:\langle s\rangle]=4 \Rightarrow L^{\langle s\rangle}=\mathbb{Q}(2^{1/4})$ and
$r^2: \sqrt[4]{2}\to -\sqrt[4]{2} \Rightarrow r^2(\sqrt{2})=\sqrt{2}$. Similarly,
($r^2(i)=i \Rightarrow r^2$ fixes both i & $\sqrt{2}$)
$rs: \sqrt[4]{2}\to i\sqrt[4]{2}$, $i\to -i \Rightarrow rs(i\sqrt{2})=i\sqrt{2}$ & $(1+i)\sqrt[4]{2} \leftrightarrow (1+i)\sqrt[4]{2}$

$sr: \sqrt[4]{2} \to -i\sqrt[4]{2}$, $i \to -i \Rightarrow (1-i)\sqrt[4]{2} \mapsto (1-i)\sqrt[4]{2}$

$r^2 s: \sqrt[4]{2} \to -\sqrt[4]{2}$, $i \to -i \Rightarrow r^2 s(i\sqrt[4]{2}) = i\sqrt[4]{2}$.

Clearly, $\mathbb{Q}(i):\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$, $\mathbb{Q}(i\sqrt{2}):\mathbb{Q}$ and $\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}$ are normal extensions ($\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}((t^2+1)(t^2-2))$)

One has $f = t^4 - 2 = (t \pm \sqrt[4]{2})(t \pm i\sqrt[4]{2})$ and $\langle rs\rangle$, $\langle sr\rangle$ fix some extensions of $\mathbb{Q}(i\sqrt{2})$ and $[L : L^{\langle rs\rangle}] = [L : L^{\langle sr\rangle}] = 2$. For any root α of f its G-orbit is the collection of all conjugates of $\alpha \Rightarrow$ the orbits of $\langle rs\rangle$, $\langle sr\rangle$ are subsets of the conjugates of α $\Rightarrow$ we should consider just divisors of f. E.g.

$(t - \sqrt[4]{2})(t + i\sqrt[4]{2}) = t^2 - t\sqrt[4]{2}(1-i) - i\sqrt{2}$ or

$(t + \sqrt[4]{2})(t + i\sqrt[4]{2}) = t^2 + t\sqrt{2}(1+i) + i\sqrt{2}$.

Remark Let $K \underset{[P:K]}{—} P \underset{[L:P]}{—} L$. Then

$$G \underset{[G:G_P]}{—} G_P \underset{|G_P|}{—} Id$$

In other words, $\forall P \leq G$: $\begin{cases} [P:K] = [G:G_P] \\ [L:P] = |G_P| \end{cases}$

Let $\mathbb{F}_{p^n}$ be a finite field, p be a prime. Then $G = Gal_{\mathbb{F}_p}(\mathbb{F}_{p^n}) \cong \mathbb{Z}_n$. By Lagrange thm. $\forall \Gamma \leq G$ one has $|\Gamma| = d \mid n$ and $\Gamma \trianglelefteq G$ (obviously). Now if K is a subfield of $\mathbb{F}_{p^n}$, then $Gal_{\mathbb{F}_p}(K) \leq G$ (by the fundamental thm.) and $\mathbb{F}_p - K$ is normal (by the fundamental thm. again) $\Rightarrow$ Galois (recall that $L : \mathbb{F}_p$ is algebraic and hence K is separable) $\Rightarrow [K : \mathbb{F}_p] = |Gal_{\mathbb{F}_p}(K)| = d \Rightarrow |K| = p^d$.

Similarly, it is easy to see that $\exists!\, K$ s.t. $|K| = p^d$! Indeed, $\exists!\, \Gamma \leq \mathbb{Z}_n$ s.t. $|\Gamma| = d \mid n$ (namely, $|\Gamma| = \langle \Phi^d \rangle$, where Φ is the Frobenius automorphism) $\Rightarrow$ by the fundamental thm. $\exists!$ subfield K of L s.t. $[K : \mathbb{F}_p] = d \Leftrightarrow |K| = p^d$.

Thus, the fundamental thm. allows us to obtain all basic fact concerning subfields of $\mathbb{F}_{p^n}$.