The Fundamental Thm. of Galois Theory (1st part)

Lecture 20

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.

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

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

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

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

$$L^{G_P} = P \qquad \text{and} \qquad G_{L^H} = H.$$

(here $\forall P \in I(K,L)$ and $\forall H \in S(G)$).

The first statement is $L^{\mathrm{Gal}_P L} = P$
$\Leftrightarrow$ $L:P$ is a Galois extension (see Thm. 2 of the previous lecture). In particular, we see that $L:K$ is a Galois extension. Also, we know (see Corollary of Thm. 4) that

is $K-M-L$ is an extension & $K-L$ is Galois, then $M-L$ is Galois. Thus, we know that

$$\boxed{K-L \text{ Galois} \iff L^{G_P} = P, \quad \forall P \in I(K,L)}$$

Now let $K-L$ be a Galois extension and let us derive that $G_{L^H} = H$. By the primitive element thm. we know that $L = K(\theta)$. Consider the orbit $H\theta$ and the pol.

$$\mu_\theta^{L^H} \mid f(t) := \prod_{\theta' \in H\theta} (t - \theta') \in L^H[t].$$

$\forall h \in H$ one has $hH = H$, so the coeff. of f $\in L^H$

We have $L = K(\theta) = L^H(\theta)$, thus $[L : L^H] = \deg \mu_\theta^{L^H} \leq |H|$.

On the other hand, $H \leq G_{L^H} = \mathrm{Aut}_{L^H} L$

$$= \{\varphi : L \to L \mid \varphi(\alpha) = \alpha, \forall \alpha \in L^H\}$$
$$= \{\varphi : L \to L \mid \varphi(\alpha) = \alpha \text{ s.t. } h(\alpha) = \alpha, \forall h \in H\}$$

Finally, $[L : L^H] = |\mathrm{Gal}_{L^H}(L)| = |G_{L^H}|$ $\leftarrow$ see Thm.3 of the previous lecture. Thus, we have

$$|H| \leq |G_{L^H}| \leq |H| \ \& \ H \subseteq G_{L^H} \Rightarrow H = G_{L^H}.$$

Thus we have proved the following

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

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

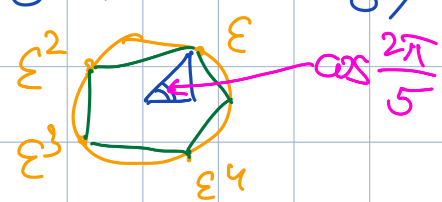
Here $G_P = \mathrm{Aut}_P L$ and $L^H = \{\alpha \in L \mid \forall h \in H: h\alpha = \alpha\}$

Exm 1 Let p be a prime number, $L = \mathbb{Q}(\varepsilon_p)$

$\left(L^{(d)} = \{\alpha \in L : \deg \alpha \mid d\} \leftarrow \text{Gauss periods}\right)$

a) $p=5$: $\mathbb{Q} \overset{2}{\text{—}} \mathbb{Q}(\sqrt{5}) = \mathbb{Q}\left(\cos\frac{2\pi}{5}\right) \overset{2}{\text{—}} \mathbb{Q}(\varepsilon_5)$

$\mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}(\varepsilon_5) \cong \mathbb{Z}_5^* = \langle g \rangle := G$



$g: \varepsilon \to \varepsilon^2 \Rightarrow G = \langle (1243) \rangle < S_4$

The only non-trivial subgroup of G is $\langle g^2 \rangle = H = \{1 \leftrightarrow 4, 2 \leftrightarrow 3\} \Rightarrow H$ is „the complex conjugation". Therefore, one has

$$\begin{tikzcd}
I(K,L): & \mathbb{Q} \arrow[r, dash] \arrow[d, shift right] & \mathbb{Q}(\sqrt{5}) \arrow[r, dash] \arrow[d, shift right] & \mathbb{Q}(\varepsilon_5) \arrow[d, shift right] \\
S(G): & G = \langle g \rangle \arrow[r, dash] \arrow[u, shift right] & \langle g^2 \rangle \arrow[r, dash] \arrow[u, shift right] & \{e\} \arrow[u, shift right]
\end{tikzcd}$$

In particular, $\mathbb{Q}(\sqrt{5})$ is the fixed field of $\langle g^2\rangle$.

b) $p=7 \Rightarrow \mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\overset{=\varepsilon}{\varepsilon_7}) \cong \mathbb{Z}_7^* = \langle g\rangle = G$, $g:\varepsilon\to\varepsilon^3$. The subgroup lattice $S(G)$:

$$\begin{tikzcd}[column sep=small] & \langle g^2\rangle \arrow[dr, dash] & & & & \mathbb{Q}(i\sqrt{7}) \arrow[dr, dash] & \\ \langle g\rangle \arrow[ur, dash] \arrow[dr, dash] & \boxed{S(G)} & e & \leftrightarrows & \mathbb{Q} \arrow[ur, dash] \arrow[dr, dash] & \boxed{I(K,L)} & \mathbb{Q}(\varepsilon) \\ & \langle g^3\rangle \arrow[ur, dash] & & & & \mathbb{Q}(\cos\frac{2\pi}{7}) \arrow[ur, dash] & \end{tikzcd}$$

$g^2:\varepsilon\to\varepsilon^9=\varepsilon^2$ and $g^3:\varepsilon\to\varepsilon^{27}=\varepsilon^{-1}$

Thus $g^3(\varepsilon+\varepsilon^{-1}) = \varepsilon+\varepsilon^{-1} = 2\cos\frac{2\pi}{7}$ and

$g^2(\underbrace{\varepsilon+\varepsilon^2+\varepsilon^4}_{=\,\varepsilon+\varepsilon^{3^2}+\varepsilon^{3^4}}) = \varepsilon+\varepsilon^2+\varepsilon^4=\theta_1$ (this is another Gauss period)

Similarly, $g^2(\underbrace{\varepsilon^3+\varepsilon^5+\varepsilon^6}_{=\,\varepsilon^3+\varepsilon^{3^3}+\varepsilon^{3^5}}) = \varepsilon^3+\varepsilon^5+\varepsilon^6=\theta_2$

Then $\theta_1+\theta_2=-1$ & $\theta_1\theta_2 = \varepsilon^4+\varepsilon^6+1+\varepsilon^5+1+\varepsilon$
$+1+\varepsilon^2+\varepsilon^3=2$

$\Rightarrow \theta_1,\theta_2$ are roots of $t^2+t+2 \Rightarrow$
$\theta_{1,2} = \dfrac{-1\pm i\sqrt{7}}{2}$.

c) Let p be a composite number, e.g. $p=8$.
(then there is no theory of Gauss periods)

$\varepsilon=\varepsilon_8=\dfrac{1+i}{\sqrt{2}} \Rightarrow \mathbb{Q}(\varepsilon_8)=\mathbb{Q}(i,\sqrt{2})$. We have

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(i) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[r, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[r, dash] & \mathbb{Q}(i,\sqrt{2}) \\
 & \mathbb{Q}(i\sqrt{2}) \arrow[ur, dash] &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \langle g_{+-}\rangle \arrow[dr, dash] & \\
V_4 \arrow[ur, dash] \arrow[r, dash] \arrow[dr, dash] & \langle g_{-+}\rangle \arrow[r, dash] & e \\
 & \langle g_{--}\rangle \arrow[ur, dash] &
\end{tikzcd}$$

We know that $G = Gal_{\mathbb{Q}}\, \mathbb{Q}(i,\sqrt{2}) = V_4$. In other words V_4 :

Id	i	$\sqrt{2}$
g_{+-}	i	$-\sqrt{2}$
g_{-+}	$-i$	$\sqrt{2}$
g_{--}	$-i$	$-\sqrt{2}$

$\Rightarrow g_{--}(i\sqrt{2}) = i\sqrt{2}$

<u>Exm. 2.</u> Let $K = \mathbb{F}_2$ and $L = \mathbb{F}_{64}$. Then the intermediate fields are

$$\begin{tikzcd}[column sep=small]
 & \mathbb{F}_8 \arrow[dr, dash] & \\
\mathbb{F}_2 \arrow[ur, dash] \arrow[dr, dash] & \boxed{I(K,L)} & \mathbb{F}_{64} \\
 & \mathbb{F}_4 \arrow[ur, dash] &
\end{tikzcd}$$

$\mathbb{F}_8 = \{\alpha \mid \alpha^8 = \alpha\} = \{\alpha \mid \Phi^3\alpha = \alpha\}$

$\mathbb{F}_{64} = \{\alpha \mid \alpha^{64} = \alpha\}$

$\mathbb{F}_4 = \{\alpha \mid \alpha^4 = \alpha\} = \{\alpha \mid \Phi^2\alpha = \alpha\}$

We know that $G = Gal_{\mathbb{F}_2}(\mathbb{F}_{64}) \cong \mathbb{Z}_6 = \langle \Phi \rangle$, where Φ is the Frobenius automorphism

$\Phi : x \to x^2 \quad \Rightarrow \quad \Phi^2 : x \to x^4 \;\&\; \Phi^3 : x \to x^8$

Thus $\mathbb{F}_8 = \mathbb{F}_{64}^{\langle \Phi^3 \rangle}$ and $\mathbb{F}_4 = \mathbb{F}_{64}^{\langle \Phi^2 \rangle}$.

The subgroup lattice of G is

$$\begin{tikzcd}[column sep=small]
 & \langle \varphi^3 \rangle = \mathbb{Z}_2 \arrow[dr, no head] & & \\
\langle \varphi \rangle = \mathbb{Z}_6 \arrow[ur, no head] \arrow[dr, no head] & & e & S(G) \arrow[l] \\
 & \langle \varphi^2 \rangle = \mathbb{Z}_3 \arrow[ur, no head] & &
\end{tikzcd}$$