Galois theory II

<u>Theorem</u> $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$. So $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$

Proof: Suffices to show that $\Phi_n(x)$ is irreducible over $\mathbb{Z}[x]$

Let $\zeta :=$ a primitive n^{th} root of 1 in a splitting field of $\Phi_n(x)$

<u>NTS</u>: $f(x) := m_{\zeta,\mathbb{Q}}(x)$ the minimal polynomial of ζ over $\mathbb{Q}$ is just $\Phi_n(x)$

Obviously, $f(x) \mid \Phi_n(x)$

Take p a prime <u>not</u> dividing n.

<u>Claim</u>. ζ^p is a zero of $f(x)$.

(This would imply: if $a = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ relatively prime to n, $\zeta^a = (\zeta)^{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}$

So ζ is a zero of $f(x) \Rightarrow \zeta^a$ is a zero of $f(x)$

$\Rightarrow f(x) = \Phi_n(x)$.)

<u>Proof of the claim: Suppose not.</u>

Let $g(x) = m_{\zeta^p,\mathbb{Q}}(x)$ be the minimal polynomial of ζ^p over $\mathbb{Q}$

as $f(x) \neq g(x) \Rightarrow (f(x), g(x)) = (1) \Rightarrow f(x)g(x) \mid \Phi_n(x)$

<u>But</u>: $g(\zeta^p) = 0 \Rightarrow \zeta$ is a zero of $g(x^p)$

$\Rightarrow f(x) \mid g(x^p)$. Write $g(x^p) = f(x)h(x)$ in $\mathbb{Z}[x]$

Take this equation and mod p,

$$\underbrace{\bar{g}(x^p)}_{= \bar{g}(x)^p} = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x]$$

$\Rightarrow \bar{f}(x)$ and $\bar{g}(x)$ have a common factor in $\mathbb{F}_p[x]$

Yet $\bar{f}(x)\cdot\bar{g}(x) \mid \bar{\Phi}_n(x) \mid x^n - 1 \Rightarrow x^n-1$ has repeated factor in $\mathbb{F}_p[x]$

But $(x^n-1,\ nx^{n-1}) = (x^n-1,\ x^{n-1}) = (1)$. No repeated zero! $\divideontimes$

So $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

<u>Cor</u>: For every finite abelian group, there exists a finite Galois extension $K/\mathbb{Q}$ with Galois group G

Proof: Write $G = \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$

For each n_i, find a (distinct) odd prime number p_i s.t. $p_i \equiv 1 \bmod n_i$ (Dirichlet)

Then G is a quotient of $(\mathbb{Z}/p_1)^\times \times \cdots \times (\mathbb{Z}/p_r)^\times$ (say by H)

Then

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{p_1\cdots p_r}) \arrow[dd, dash, "\prod_i (\mathbb{Z}/p_i)^\times"'] \arrow[dr, dash, "H"] & \\
& K = \mathbb{Q}(\zeta_{p_1\cdots p_r})^H \arrow[dl, dash, "G"] \\
\mathbb{Q} &
\end{tikzcd}$$

<u>Example</u>: Find a cyclic extension $\mathbb{Q}$ of order 3.

Write $\zeta = \zeta_7$.

$$\begin{array}{ccccc}
(\mathbb{Z}/7\mathbb{Z})^\times & \xrightarrow{\sim} & Z_6 & \twoheadrightarrow & \mathbb{Z}/3\mathbb{Z} \\
\cup\!| & & \cup\!| & & \\
\{1,-1\} & \leftarrow & \ker = \{0,3\} & &
\end{array}$$

$$\begin{tikzcd}
\mathbb{Q}(\zeta) \arrow[d, dash, "\{1,-1\}"] \\
\mathbb{Q}(?) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Define $\alpha = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)^{\{1,-1\}}$

Compute $\alpha^2 = \zeta^2 + \zeta^{-2} + 2$

$\alpha^3 = \zeta^3 + \zeta^{-3} + 3\zeta + 3\zeta^{-1}$

$\Rightarrow \alpha^3 + \alpha^2 - 2 - 2\alpha = -1.$

<u>Theorem</u> (Kronecker–Weber) Every finite abelian extension $K/\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.

<u>Proof of main theorem of Galois theory</u>

<u>Lemma</u>. For K/F finite Galois, we have

$$\#\mathrm{Gal}(K/F) = [K:F] \qquad (*)$$

Theorem Let K/F be a finite Galois extension with $G = \mathrm{Gal}(K/F)$

Then there is a one-to-one correspondence between

$$\begin{aligned} \{\text{subgroups } H \leq G\} &\longleftrightarrow \{\text{Intermediate field } K/E/F\} \\ H &\longmapsto K^H \\ \mathrm{Gal}(K/E) &\longleftarrow\!\shortmid E \end{aligned}$$

Proof: K/F finite normal $\Rightarrow K/F$ is a splitting field for some $f(x) \in F[x]$

$\Rightarrow K$ is also the splitting field for $f(x)$ over any intermediate field E.

$\Rightarrow \mathrm{Gal}(K/E)$ makes sense and $\#\mathrm{Gal}(K/E) = [K:E]$ by $(*)$

- Given $H \leq G$, need to show $\mathrm{Gal}(K/K^H) = H$

$\forall h \in H$, h fixes $K^H \Rightarrow H \subseteq \mathrm{Gal}(K/K^H)$

So we need to show $\#H \geq \#\mathrm{Gal}(K/K^H) \overset{\text{by }(*)}{=} [K:K^H]$ $\leftarrow$ two proofs $\begin{cases} \text{primitive element theorem} \\ \text{Artin's lemma} \end{cases}$

Proof 1: By primitive element theorem, $K = K^H(\alpha)$ for some α

and $[K:K^H] = \deg m_{\alpha, K^H}(x)$

But consider the polynomial $f(x) = \prod_{h \in H} (x - h(\alpha)) = x^{\#H} + \cdots \in K^H[x]$

has α as a zero.

$\Rightarrow m_{\alpha,K^H}(x) \mid f(x) \Rightarrow \deg m_{\alpha,K^H}(x) \leq \#H$:)

Proof 2 (Artin's lemma) Let $u_1, \cdots, u_{n+1}$ be any $n+1$ elements in K (WTS $u_1, \cdots, u_{n+1}$ are K^H-linearly dependence.)

$$\rightsquigarrow \begin{pmatrix} \sigma_1(u_1) & \cdots & \sigma_1(u_{n+1}) \\ \vdots & & \vdots \\ \sigma_n(u_1) & \cdots & \sigma_n(u_{n+1}) \end{pmatrix}$$

$n \times (n+1)$ matrix with values in K.

$(H = \{\sigma_1, \cdots, \sigma_n\})$

$\Rightarrow$ column vectors $\vec{v}_1, \cdots, \vec{v}_{n+1}$ are K-linearly dependent.

So $\exists\, r$ s.t. $\vec{v}_1, \cdots, \vec{v}_r$ are K-linearly independent, yet $\vec{v}_1, \cdots, \vec{v}_{r+1}$ is not.

$\Rightarrow \vec{v}_{r+1} = \alpha_1 \vec{v}_1 + \cdots + \alpha_r \vec{v}_r \quad (*)$

WTS all $\alpha_i \in K^H$. (then $\Rightarrow$ taking 1^{st} coordinate $u_{r+1} = \alpha_1 u_1 + \cdots + \alpha_r u_r$.)

Applying $\sigma \in H \Rightarrow \sigma(\vec{v}_{r+1}) = \sigma(\alpha_1)\sigma(\vec{v}_1) + \cdots + \sigma(\alpha_r)\sigma(\vec{v}_r)$

But $\sigma \begin{pmatrix} \sigma_1(u_i) \\ \vdots \\ \sigma_n(u_i) \end{pmatrix} = \begin{pmatrix} \sigma\sigma_1(u_i) \\ \vdots \\ \sigma\sigma_n(u_i) \end{pmatrix}$ just permutes the rows.

$$\Rightarrow \vec{v}_{r+1} = \sigma(\alpha_1)\vec{v}_1 + \cdots + \sigma(\alpha_r)\vec{v}_r \quad (**)$$

But $(*)(**)$ must be the same relations $\Rightarrow \forall i \ \sigma(\alpha_i) = \alpha_i$. So $\alpha_i \in F$

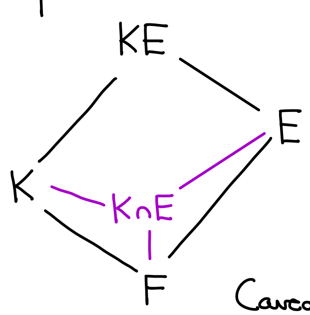
So $u_1, \cdots, u_{n+1}$ are linearly independent $/F \Rightarrow [K : K^H] \leq \# H$.

- Conversely, given an intermediate field E of K/F, need to show that $K^{Gal(K/E)} = E$
  - $*$ $E \subseteq K^{Gal(K/E)}$ as any $h \in Gal(K/E)$ fixes E
  - $*$ But $[K : E] \underset{\substack{\uparrow \\ \text{as } K/E \text{ Galois}}}{=} \# Gal(K/E) \underset{\substack{\uparrow \\ \text{proved above}}}{=} [K : K^{Gal(K/E)}]$

$\Rightarrow E = K^{Gal(K/E)}$

<u>Case of composite field</u> (for Galois extension)

<u>Proposition</u> Consider the following. K/F is finite Galois and



E/F is any extension (not necessarily algebraic)

Then KE/E is Galois and $Gal(KE/E) \simeq Gal(K/K \cap E)$

<u>Cor.</u> $[KE : K \cap E] = [K : K \cap E] \cdot [E : K \cap E]$ if they are finite

<u>Caveat</u>: We have seen earlier that with no Galois assumption that
$$[KE : K \cap E] \geq [K : K \cap E] \cdot [E : K \cap E].$$

But if $K/K \cap E$ is not Galois, this inequality can be strict:

e.g. $\quad \mathbb{Q}(\zeta_3, \sqrt[3]{2})$

$$\begin{tikzcd}[column sep=small] & \cdots \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[3]{2}\zeta_3) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

So what happened? Suppose that $L = KE/F$ is Galois with Galois group $G = \mathrm{Gal}(L/F)$ and that $F = K \cap E$.

Then
$$\begin{tikzcd}[column sep=small] & KE = L \arrow[dl, dash, "H_1"'] \arrow[dr, dash, "H_2"] & \\ K \arrow[dr, dash] & & E \arrow[dl, dash] \\ & F & \end{tikzcd} \quad G$$

Set $H_1 = \mathrm{Gal}(L/K)$, $H_2 = \mathrm{Gal}(L/E) \leqslant G$

$F = K \cap E = L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2 \rangle} \iff \langle H_1, H_2 \rangle = G$

$L = KE \implies H_1 \cap H_2 = \{1\}$

Obviously, $H_1 H_2 \subseteq \langle H_1, H_2 \rangle = G$ but typically not equal as set.

$\implies \# G \geqslant \# H_1 \cdot \# H_2$

$\implies [L:F] \geqslant [L:K] \cdot [L:E]$

$\implies [E:F] \cdot [K:F] \geqslant [L:F]$

But if one of H_i is normal in G, $\langle H_1, H_2 \rangle = H_1 H_2 = G$. The equality holds.

<u>Proof of Proposition</u>.

K/F Galois $\Rightarrow$ K is the splitting field of some separable polynomial $f(x)$ over F

$\Rightarrow KE$ ———————— $f(x)$ over E $\implies$ KE/E is Galois

Moreover, there's a natural homomorphism

$$\Psi : \mathrm{Gal}(KE/E) \longrightarrow \mathrm{Gal}(K/K\cap E)$$
$$\sigma \longmapsto \sigma|_K$$
: <u>note</u>: K is normal$/F \Rightarrow$ stable under σ.

$\ker \Psi = \{ \sigma \in \mathrm{Gal}(KE/E) \text{ s.t. } \sigma|_K = \mathrm{id} \} = \{1\}$

$(\sigma|_E = \mathrm{id},\ \sigma|_K = \mathrm{id} \Rightarrow \sigma|_{KE} = \mathrm{id}.)$

<u>Surjective</u>? KE Let $H := \mathrm{Im}\,\Psi \subseteq \mathrm{Gal}(K/K\cap E)$ subgroup

$$
\begin{tikzcd}
K \arrow[dr, dash] & & E \\
& K^H \arrow[ur, dotted, dash] & \\
& K\cap E \arrow[u, dash] \arrow[uul, dash] \arrow[uur, dash] & \\
& F \arrow[u, dash] &
\end{tikzcd}
$$

Consider $K^H \supseteq K\cap E$

If we can show $K^H \subseteq E$, then $K^H = K\cap E$. Done

<u>Note</u>: $\forall \sigma \in Gal(KE/E)$, $\sigma|_E = id$, $\sigma|_{K^H} = id$

$\Rightarrow \sigma|_{K^H E} = id$

$\Rightarrow K^H E$ is fixed by $Gal(KE/E) \Rightarrow K^H E = E \Rightarrow K^H \subseteq E$. $\square$

<u>Proposition</u> Suppose that we have a tower of extensions, in which K_1 and K_2 are Galois over F

$$
\begin{tikzcd}
& K_1K_2 & \\
K_1 \arrow[ur, dash] & & K_2 \arrow[ul, dash] \\
& K_1\cap K_2 \arrow[ul, dash] \arrow[ur, dash] & \\
& F \arrow[u, dash] &
\end{tikzcd}
$$

Then ① $K_1\cap K_2$ is Galois over F

② K_1K_2 is Galois over F, and

$$Gal(K_1K_2/F) \simeq \{(g_1,g_2) \in Gal(K_1/F)\times Gal(K_2/F),\ g_1|_{K_1\cap K_2} = g_2|_{K_1\cap K_2}\}$$

(In particular, if $K_1\cap K_2 = F$, then $Gal(K_1K_2/F) = Gal(K_1/F)\times Gal(K_2/F)$.)

Proof: ① Need to show $K_1\cap K_2$ is normal $/F$

Suppose that $f(x)\in F[x]$ is an irreducible polynomial that has a zero in $K_1\cap K_2$

Then all zeros of $f(x)$ are in K_1 and in K_2 $\Rightarrow f(x)$ splits in $K_1\cap K_2$.

② K_i = splitting field of separable polynomial $f_i(x)$, $i=1,2$

$\Rightarrow K_1K_2$ = splitting field of $f_1(x)f_2(x)$

So K_1K_2 Galois $/F$

$$\varphi: Gal(K_1K_2/F) \longrightarrow Gal(K_1/F)\times Gal(K_2/F)$$

$$\sigma \longmapsto (\sigma|_{K_1}, \sigma|_{K_2}) \qquad (\sigma \text{ stabilizes each } K_i \text{ b/c } K_i/F \text{ is normal})$$

$\ker\varphi = \{\sigma\in Gal(K_1K_2/F),\ \sigma|_{K_1} = id,\ \sigma|_{K_2} = id\} = \{id\}$

$Im\,\varphi \subseteq \{(\sigma_1,\sigma_2)\in Gal(K_1/F)\times Gal(K_2/F),\ \sigma_1|_{K_1\cap K_2} = \sigma_2|_{K_1\cap K_2}\} =: A$

Now we count: $\underbrace{[K_1K_2 : F]}_{\#Gal(K_1K_2/F)} = [K_1K_2 : K_2][K_2 : F] \overset{\text{previous prop.}}{=} [K_1 : K_1\cap K_2]\cdot[K_2 : F]$

$= [K : K\cap K][K : K\cap K][K\cap K : F]$

$$[K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]$$

$$\|$$

$$\#A = \#\mathrm{Gal}(K_1/K_1 \cap K_2) \cdot \#\mathrm{Gal}(K_2/K_1 \cap K_2) \cdot \#\mathrm{Gal}(K_1 \cap K_2/F) \quad \square$$