6.5.24



# Proof of Galois correspondence

thm 4.2

(1) $L:K$ normal sep $\iff |Gal(L:K)| = [L:K]$

$\iff \phi(\gamma)(K) = K$
Cor 3.9.

let $M \in \mathcal{F}$

(2) We know that $L:M$ is sep and normal
Hence a Galois extension.

Hence $|Gal(L:M)| = [L:M]$ and
by Cor 3.9 $M = Fix(Gal(L:M))$
$= \phi\gamma(M)$.

Now let $H \in \mathcal{G}$, a subgroup of $Gal(L:K) = G$

We know that $H \subset \gamma\phi(H)$ (lemma 3.4)
and
$\phi\gamma\phi(H) = \phi(H)$. (Lemma 3.4)

We know By thm 3.8 that
( $H$ a finite s/gp of $aut(L)$ $L_0 = Fix\ H$
then $[L : L_0] = |H|$ )

Hence $|H| = [L : \phi(H)]$

Therefore $|H| = [L : \phi\gamma\phi(H)] = |\gamma\phi(H)|$
by thm 3.8 again
aplied to $\gamma\phi(H)$

Since $H$ and $\gamma\phi(H)$ are finite groups and $H \subset \gamma\phi(H)$ and they have the same size we have that

$$H = \gamma\phi(H)$$

Hence $\gamma, \phi$ are mutual inverses.

(5) We've seen that when $L:K$ is normal sep. then $L:M$ is also normal sep, Hence Galois

Hence $[L:M] = |Gal(L:M)| = |\gamma(M)|$

It follows that

$$[M:K] = [L:K]/[L:M] = [Gal\ L:K] / |Gal(L:M)|$$

$$= |G| / |\gamma(M)|$$

Before proving (4) and (5) we give a lemma.

**Lemma 5.2** suppose that $L:K$ is an extension, $K \subseteq M \subseteq L$, $\tau : L \to L$ a $K$-autom of $L$.

Then $\gamma(\tau(M)) = \tau(\gamma(M))\tau^{-1}$

ie Galois group of $\tau(M)$ is conjugate of Galois group of $M$ with $\tau$.

**Proof** Let $\tilde{M} := \tau(M)$

Take $\sigma \in \gamma(M)$, $\tilde{x} \in \tilde{M}$

Then $\tilde{x} = \tau(x)$ for some $x \in M$

$$(\tau \sigma \tau^{-1})(\tilde{x}) = \tau\sigma(x) = \tau(x) = \tilde{x}$$

$\downarrow$

$\sigma \in \gamma(M) = Gal(L:M)$ and $x \in M$.

Hence $\tau\sigma\tau^{-1}$ fixes $\tilde{M}$ so

$$\tau\sigma\tau^{-1} \in \gamma(\tilde{M}) \quad \text{and} \quad \tau\gamma(M)\tau^{-1} \subseteq \gamma(\tilde{M})$$

Similarly replacing $M$ by $\tau(M) = \tilde{M}$ and $\tau$ by $\tau^{-1}$ we get

$$\tau^{-1}\gamma(\tilde{M})\tau \subseteq \gamma(M) \Rightarrow \gamma(\tilde{M}) \subseteq \tau\gamma(M)\tau^{-1}$$

Hence $\tau\gamma(M)\tau^{-1} = \gamma(\tau(M))$

$\boxtimes$

Now we can prove parts 4 and 5 of the fund. thm of Galois Theory.

**Proof of 4** ($\Rightarrow$) Suppose $M:K$ is normal $\tau \in Gal(L:K) = G$

Then $\tau|_M$ is a $K$-mon $M \longrightarrow L$

Since $M:K$ is normal by Thm 4.8. $\tau|_M$ is actually a $K$-autom of $M$

Hence $\tau(M) = M$. On the other hand

by Lemma 5-2 $\quad \gamma(\tau(M)) = \tau\,\gamma(M)\,\tau^{-1}$

Since $\tau(M) = M$, this gives

$\gamma(M) = \tau\,\gamma(M)\,\tau^{-1}$ ie $\gamma(M)$ is normal in $G$.

Hence $\gamma(M) \triangleleft G$ as wanted

$(\Leftarrow)$ Suppose conversly $\gamma(M) \triangleleft G$

Let $\sigma$ be any $K$-monom $M \to L$.

<u>w.t.s</u> $\sigma$ is a $K$ autom of $M$ and use Thm 4-8.

Since $L:K$ is normal, By Thm 4-4
$\sigma : M \to L$ can be extended to a
$K$-autom $\tau$ of $L$ such that $\tau|_M = \sigma$.

Since $\gamma(M) \triangleleft G$, $\tau\,\gamma(M)\,\tau^{-1} = \gamma(M)$
On the other hand by Lemma 5-2

$\tau\,\gamma(M)\,\tau^{-1} = \gamma(\tau(M))$

By part 2 since $\gamma$ gives a 1-1 correspondence
$\gamma(\tau(M)) = \gamma(M) \Rightarrow \tau(M) = M$

Then $\sigma(M) = \tau|_M(M) = M$. Hence $\sigma$ is a $K$-autom of $M$

$\blacksquare$

**Proof of 5** Let $\tilde{G} = Gal(M:K)$ where $M:K$ is normal.

Define a map
$$\begin{aligned}\theta : G &\longrightarrow \tilde{G}\\ Gal(L:K) &\longrightarrow Gal(M:K)\\ \sigma &\longmapsto \sigma|_M =: \tau\end{aligned}$$

Since $M:K$ is normal, the $K$-monomorphism

$\tau = \sigma|_M : M \to L$ is actually a $K$-autom of $M$

Hence indeed $\sigma|_M \in Gal(M:K)$

Thm 4.4 says: if $L:K$ finite normal extension

$K \subseteq M \subseteq L$, $\tau$ a $K$-monom $M \to L$

Then $\exists$ a $K$-autom $\sigma : L \to L$ s.t $\sigma|_M = \tau$

Hence $\theta$ is surjective.

Using isomorphism Theorem for groups, we get $G/\ker\theta \cong \tilde{G}$. To prove part 5, we need to

look at $\ker\theta = \{\sigma \in Gal(L:K) \mid \theta(\sigma) = id|_M\}$

$= \{\sigma \in Gal(L:K) \mid \sigma|_M = id|_M\}$

$= \{\sigma \in Gal(L:K) \mid \sigma \text{ fixes } M \text{ pointwise})$

$= Gal(L:M) = \gamma(M)$. Hence $Gal(L:K)/Gal(L:M) \cong Gal(M:K)$ ☒