Fundamental Theorem of Galois Theory

Theorem

Let K/F be a field extension. There exists an inclusion-reversing bijection between all closed intermediate fields in K/F and all closed subgroups of $\mathrm{Aut}(K/F)$.

$$\begin{array}{ccc} K & \mapsto & \mathrm{id} \\ | & & \text{\rotatebox{90}{$\leq$}} \\ L & \mapsto & G(L) \\ | & & \text{\rotatebox{90}{$\leq$}} \\ E & \mapsto & G(E) \\ | & & \text{\rotatebox{90}{$\leq$}} \\ F & \mapsto & G(F) \end{array}$$

Proof

Consider the bijection given by:

$$L \mapsto G(L)$$

By the previous theorem behind the above diagram it is clear that this inclusion-reversing and G(L) is closed.

Consider the inverse:

$$H \mapsto F(H)$$

By the previous theorem, $F(H)$ is also closed.

Assume L is closed. By composition:

$$L \mapsto G(L) \mapsto F(G(L)) = L$$

Assume H is closed. By composition:

$$H \mapsto F(H) \mapsto G(F(H)) = H$$

Note that if there is an intermediate field L that is not closed then $F(G(L)) \supset L$ and the composition chain:

$$L \mapsto G(L) \mapsto F(G(L)) \mapsto E \subset L$$

is broken.

Theorem

Let $F \subseteq E \subseteq L \subseteq K$ be an inclusion of fields such that $[L : E] < \infty$:

$$[G(E) : G(L)] \leq [L : E]$$

Proof

Proof by induction on $n = [L : E]$

Base Case: $n = 1$

$L = E$ and $[G(E) : G(L)] = [L : E] = 1$

Assume $[G(E) : G(L)] \leq [L : E]$ for extension of degree $< n$

Assume $[L : E] = n$

Case 1: There exists a proper extension M such that $E \subset M \subset L$

$$[G(E) : G(L)] = [G(E) : G(M)][G(M) : G(L)] \leq [E : M][M : L] = [E : L]$$

Case 2: No such M exists

Assume $\alpha \in L \setminus E$
$L = E(\alpha)$
Since L/E is finite, α is algebraic
Hence, $[L : E] = [E(\alpha) : E] = \deg(m_{\alpha,E}(x)) = n$

Assume $\varphi, \psi \in G(E)$

$$\begin{aligned} \varphi G(L) = \psi G(L) \quad &\iff \quad \varphi\psi^{-1} \in G(L) \\ &\iff \quad \varphi\psi^{-1}\big|_L = \mathrm{id}_L \\ &\iff \quad (\varphi\psi^{-1})(\alpha) = \alpha \\ &\iff \quad \varphi(\alpha) = \psi(\alpha) \end{aligned}$$

But φ and ψ permute the roots of $m_{\alpha,E}(x)$, so $[G(E) : G(L)]$ is the number of distinct roots of $m_{\alpha,E}(x)$ which equals n

$\therefore [G(E) : G(L)] = [L : E]$

Similarly:

Theorem

Let K/F be an extension of fields and $G = \mathrm{Aut}(K/F)$ with subgroups $1 \leq J \leq H \leq G$ such that $[H : J] < \infty$:

$$[F(J) : F(H)] \leq [H : J]$$

Theorem

Let $F \subseteq E \subseteq L \subseteq L$ be an inclusion of fields such that E is closed and $[L : E] < \infty$:

L is closed and $[G(E) : G(L)] = [L : E]$

Proof

Since E is closed:

$$[L:E] = [L:F(G(E))] \leq [F(G(L)):F(G(E))] \leq [G(E):G(L)] \leq [L:E]$$

Therefore $L = F(G(L))$ and so L is closed, and $[G(E):G(L)] = [L:E]$.

Similarly:

Theorem

Let K/F be an extension of fields and $G = \mathrm{Aut}(K/F)$ with subgroups $1 \leq J \leq H \leq G$ such that J is closed and $[H:J] < \infty$:

H is closed and $[F(J):F(H)] = [H:J]$

Theorem

Let $F \subseteq L \subseteq K$ be an inclusion of groups such that L is stable:

$$G/G(L) \cong G(L/F)$$

Proof

Consider the homomorphism from G to $G(L/F)$ given by:

$$\varphi \mapsto \varphi|_L$$

which is well-defined because L is stable
The kernel of this homomorphism is $G(L)$
Thus, by the FIT, $G/G(L)$ is isomorphic to some subgroup of $G(L/F)$

$$|G/G(L)| = [G:G(L)] = [L:F] = |G(L/F)|$$

Thus, since the extensions are finite, the homomorphism is an isomorphism

$\therefore G/G(L) \cong G(L/F)$

Notation

When K/F is Galois then $G = \mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$

Theorem: Fundamental Theorem of Galois Theory

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

1). There exists a bijection between intermediate field L and subgroups of G.

2). For $F \subseteq E \subseteq L \subseteq K$, $[L:E] = [G(E), G(L)]$.

3). For $1 \leq J \leq H \leq G$, $[H:J] = [F(J):F(H)]$

4). $H \trianglelefteq G \iff L = F(H)$, in which case $G/G(L) \cong G(L/F)$.