proof of fundamental theorem of Galois theory

Canonical name	ProofOfFundamentalTheoremOfGaloisTheory
Date of creation	2013-03-22 14:26:38
Last modified on	2013-03-22 14:26:38
Owner	pbruin (1001)
Last modified by	pbruin (1001)
Numerical id	5
Author	pbruin (1001)
Entry type	Proof
Classification	msc 12F10
Classification	msc 11R32
Classification	msc 11S20
Classification	msc 13B05

The theorem is a consequence of the following lemmas, roughly corresponding to the various assertions in the theorem. We assume L/F to be a finite-dimensional Galois extension of fields with Galois group

$$G = \mathrm{Gal}(L/F).$$

The first two lemmas establish the correspondence between subgroups of G and extension fields of F contained in L.

Lemma 1. *Let K be an extension field of F contained in L. Then L is Galois over K, and $\mathrm{Gal}(L/K)$ is a subgroup of G.*

Proof. Note that L/F is normal and separable because it is a Galois extension; it remains to prove that L/K is also normal and separable. Since L is normal and finite over F, it is the splitting field of a polynomial $f \in F[X]$ over F. Now L is also the splitting field of f over K (because $F \subset K \subset L$), so L/K is normal.

To see that L/K is also separable, suppose $\alpha \in L$, and let $f_F^\alpha \in F[X]$ be its minimal polynomial over F. Then the minimal polynomial f_K^α of α over K divides f_F^α, which has no double roots in its splitting field by the separability of L/F. Therefore f_K^α has no double roots in its splitting field for any $\alpha \in L$, so L is separable over K.

The assertion that $\mathrm{Gal}(L/K)$ is a subgroup of G is clear from the fact that $K \supset F$. □

Lemma 2. *The function ϕ from the set of extension fields of F contained in L to the set of subgroups of G defined by*

$$\phi(K) = \mathrm{Gal}(L/K)$$

is an inclusion-reversing bijection. The inverse is given by

$$\phi^{-1}(H) = L^H,$$

where L^H is the fixed field of H in L.

Proof. The definition of ϕ makes sense because of Lemma **??**. The

$$\phi^{-1} \circ \phi(K) = K \quad \text{and} \quad \phi \circ \phi^{-1}(H) = H$$

for all subgroups $H \subset G$ and all fields K with $F \subset K \subset L$ follow from the properties of the Galois group. The fixed field of $\mathrm{Gal}(L/K)$ is precisely K;

on the other hand, since L^H is the fixed field of H in L, H is the Galois group of L/L^H.

For extensions K and K' of F with $F \subset K \subset K' \subset L$, we have

$$\sigma \in \mathrm{Gal}(L/K') \iff \sigma \in \mathrm{Gal}(L/K),$$

so $\phi(K) \supset \phi(K')$. This shows that ϕ is inclusion-reversing. $\square$

The following lemmas show that normal subextensions of L/F are Galois extensions and that their Galois groups are quotient groups of G.

Lemma 3. *Let H be a subgroup of G. Then the following are equivalent:*

1. *L^H is normal over F.*
2. *$\sigma\left(L^H\right) = L^H$ for all $\sigma \in G$.*
3. *$\sigma H \sigma^{-1} = H$ for all $\sigma \in G$.*

In particular, L^H is normal over F if and only if H is a normal subgroup of G.

Proof. $1 \Rightarrow 2$: Since for all $\sigma \in G$ and $\alpha \in L^H$, $\sigma(\alpha)$ is a zero of the minimal polynomial of α over F, we have $\sigma(\alpha) \in L^H$ by the of L^H/F.

$2 \Rightarrow 3$: For all $\sigma \in G, \tau \in H$ the equality

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

holds for all $x \in L^H$ (from the assumption it follows that $\sigma^{-1}(x) \in L^H$, which is fixed by τ). This implies that

$$\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L/L^H) = H$$

for all $\sigma \in G, \tau \in H$.

$3 \Rightarrow 1$: Let $\alpha \in L^H$, and let f be the minimal polynomial of α over F. Since L/F is normal, f splits into linear factors in $L[X]$. Suppose $\alpha' \in L$ is another zero of f, and let $\sigma \in G$ be such that $\sigma(\alpha') = \alpha$ (such a σ always exists). By assumption, for all $\tau \in H$ we have $\tau' := \sigma\tau\sigma^{-1} \in H$, so that

$$\tau(\alpha') = \sigma^{-1}\tau'\sigma(\alpha') = \sigma^{-1}\tau'(\alpha) = \sigma^{-1}(\alpha) = \alpha'.$$

This shows that α' lies in L^H as well, so f splits in $L^H[X]$. We conclude that L^H is normal over F. $\square$

Lemma 4. *Let H be a normal subgroup of G. Then L^H is a Galois extension of F, and the homomorphism*

$$\begin{array}{rcl} r\colon G & \to & \mathrm{Gal}(L^H/F) \\ \sigma & \mapsto & \sigma|_{L^H} \end{array}$$

induces a natural identification

$$\mathrm{Gal}(L^H/F) \cong G/H.$$

Proof. By Lemma **??**, L^H is normal over F, and because a subextension of a separable extension is separable, L^H/F is a Galois extension.

The map r is well-defined by the implication $1 \Rightarrow 2$ from Lemma **??**. It is surjective since every automorphism of L^H that fixes F can be extended to an automorphism of L (if $L \neq L^H$, for example, we can choose an $\alpha \in L \setminus L^H$ such that $L = L^H(\alpha)$ using the primitive element theorem, and we can extend $\sigma \in \mathrm{Gal}(L^H/F)$ to L by putting $\sigma(\alpha) = \alpha$). The kernel of r is clearly equal to H, so the first isomorphism theorem gives the claimed identification. $\square$