A SIMPLER PROOF OF THE FUNDAMENTAL THEOREM OF GALOIS THEORY

MARTIN BRANDENBURG

Abstract. We give a simple proof of the fundamental theorem of Galois theory which provides a correspondence between the intermediate fields of a finite Galois extension and the subgroups of its Galois group. The proof relies on the combinatorial fact that a field cannot be written as a union of finitely many proper subfields.

1. Introduction

The fundamental theorem of finite Galois theory states that for every finite Galois, i.e. normal and separable extension $L/K$ the maps $E \mapsto \text{Aut}_E(L)$ and $L^H \hookrightarrow H$ establish a bijection

$$\{\text{intermediate fields of } L/K\} \cong \{\text{subgroups of } \text{Aut}_K(L)\}.$$ 

This theorem can be separated in two parts:

1. For every intermediate field $E$ of $L/K$ the trivial inclusion $E \subseteq L^{\text{Aut}_E(L)}$ is an equality.
2. For every subgroup $H$ of $\text{Aut}_K(L)$ the trivial inclusion $H \subseteq \text{Aut}_{L^H}(L)$ is an equality.

There are several standard proofs which can be found in textbooks on algebra, for example [2, Thm. 16], [4, Thm. V.§33.4], [8, Thm. 14.14], [1, Thm. VII.6.9]. This note is the result of an attempt to prove (1) and (2) as directly as possible from the definitions. In particular, we will not prove (1) and (2) by comparing the degrees resp. orders of both sides. We will not use the linear independence of characters either. Splitting fields are not even mentioned once.

Instead, (1) will be derived rather directly from the definitions and basic facts about algebraic extensions, whereas (2) will be derived rather easily from a combinatorial result, namely that a field cannot be written as a union of finitely many proper subfields. The same result has been used by Geck [9] to give a very short proof of the well-known equivalent characterizations of Galois extensions, which in turn leads to a short proof of the fundamental theorem. Other quick proofs have been found by DeMeyer [5] and Dress [7]. Dress’s approach is very conceptual as it uses general facts about group actions on sets and vector spaces.

This note does not assume prior knowledge about Galois theory. We only assume basic field theory and develop in detail all the ingredients here which are necessary to state and prove the fundamental theorem of Galois theory. As such, this note can also be used as an introduction to Galois theory. We will, however, omit most results which are not necessary for the theorem.

Acknowledgments. I would like to thank Peter Müller for pointing me to Geck’s paper [9].

2. Preliminaries

For basic field theory we refer to [1, sect. VII.1, VI.2.1]. A field extension is, by (modern) definition, a homomorphism of fields. It is automatically injective. We assume the notions of finite and algebraic extensions and their homomorphisms, the degree of a field extension, the multiplicativity formula for degrees, minimal polynomials as well as algebraic closures. For a
field extension $L/K$ and an algebraic element $a \in L$ we have $K(a) = K[a] \cong K[T]/(f)$, where $f \in K[T]$ is the minimal polynomial of $a$ over $K$. This is all we need.

For extensions $L/K$, $M/K$ we denote by $\text{Hom}_K(L, M)$ the set of $K$-homomorphisms $L \to M$. We denote by $\text{Aut}_K(L)$ the group of $K$-automorphisms of $L$.

**Lemma 2.1.** Let $L/K$, $M/K$ be extensions. Let $a \in L$ be algebraic over $K$ with minimal polynomial $f \in K[T]$. Then we have a bijection

$$\text{Hom}_K(K(a), M) \cong \{m \in M : f(m) = 0\}$$

given by $\sigma \mapsto \sigma(a)$. In particular, $\text{Hom}_K(K(a), M)$ has at most $\deg(f) = [K(a) : K]$ elements.

*Proof.* This follows from $K(a) \cong K[T]/(f)$ as well as the universal properties of quotient algebras and polynomial algebras:

$$\text{Hom}_K(K(a), M) \cong \text{Hom}_K(K[T]/(f), M)$$

$$\cong \{\sigma \in \text{Hom}_K(K[T], M) : \sigma(f) = 0\}$$

$$\cong \{m \in M : \text{ev}_m(f) = 0\}$$

(where $\text{ev}_m : K[T] \to M, T \mapsto m$)

$$= \{m \in M : f(m) = 0\} \quad \Box$$

**Lemma 2.2.** Let $L/K$ be a finite extension. Let $M/K$ be any extension. Then $\text{Hom}_K(L, M)$ has at most $[L : K]$ elements.

*Proof.* We need to show that the given homomorphism $K \to M$ admits at most $[L : K]$ extensions to $L$. We proceed by induction on $[L : K]$. The case $[L : K] = 1$ is easy. Now assume $[L : K] > 1$ and pick some $a \in L \setminus K$. Because of Lemma 2.1 there are at most $[K(a) : K]$ extensions of $K \to M$ to $K(a)$. We have $[L : K(a)] < [L : K]$. By induction hypothesis, each extension $K(a) \to M$ has at most $[L : K(a)]$ extensions to $L$. Therefore, there are at most $[L : K(a)] \cdot [K(a) : K] = [L : K]$ extensions of $K \to M$ to $L$.

*Remark 2.4.* The assumption that $M$ is algebraically closed is much too strong: It suffices that $L/K$ has a generating set such that the minimal polynomial of every generator has a root in $M$. Moreover, in the case of a finite extension, which we are mainly interested in, Zorn’s Lemma is not necessary to prove Lemma 2.3. Here, an induction on the degree does the job.

**Lemma 2.3.** Let $L/K$ be an algebraic extension. Let $M$ be an algebraically closed field. Then every homomorphism $\sigma : K \to M$ admits an extension $\tau : L \to M$.

*Proof.* Consider the set of pairs $(E, \tau)$, where $K \subseteq E \subseteq L$ is an intermediate field and $\tau : E \to M$ is a homomorphism extending $\sigma$. We define $(E, \tau) \leq (E', \tau')$ by $E \subseteq E'$ and $\tau|_E = \tau'$. This defines a partial order in which every chain has an upper bound – simply take the union. Thus, by Zorn’s Lemma there is a maximal pair $(E, \tau)$, and we need to prove $E = L$. Let $a \in L$ with minimal polynomial $f \in E[T]$ over $E$. By means of $\tau : E \to M$ we can see $M$ as an extension of $E$. Then the image of $f$ in $M[T]$ has a root in $M$, since $M$ is algebraically closed. By Lemma 2.1 we can therefore extend $\tau$ to a homomorphism $E(a) \to M$. Since $(E, \tau)$ is maximal, this shows $E(a) = E$, so that $a \in E$. \[\Box\]

**Lemma 2.5.** Let $L/K$ be an algebraic extension. Then $\text{Hom}_K(L, L) = \text{Aut}_K(L)$.

*Proof.* Let $\sigma : L \to L$ be a $K$-homomorphism. Of course, $\sigma$ is injective. In order to show that $\sigma$ is surjective, let $a \in L$ and let $f \in K[T]$ be its minimal polynomial. Let $N \subseteq L$ be the set
of roots of $f$ in $L$. Then $\sigma(N) \subseteq N$, so that $\sigma$ restricts to an injective map $N \to N$. Since $N$ is finite, it has to be surjective. In particular, $a \in N$ has a preimage. \hfill $\Box$

3. Combinatorial results

It is a well-known fact that a vector space cannot be the union of two proper subspaces. The following combinatorial results are variants of this fact and are contained in [3]. We include the proofs for the convenience of the reader.

**Lemma 3.1.** A vector space over an infinite field cannot be written as the union of finitely many proper subspaces.

*Proof.* Let $K$ be an infinite field and $V$ be a vector space over $K$ which can be written as $V = V_1 \cup \cdots \cup V_n$ with proper subspaces $V_1, \ldots, V_n$. We use induction on $n$. The cases $n = 0, 1$ are trivial. Let’s assume $n \geq 2$. By induction hypothesis there is some $v \in V \setminus (V_2 \cup \cdots \cup V_n)$.

Then $v \in V_1$. Choose some $w \in V \setminus V_1$. For every $\lambda \in K^\times$ we have $v + \lambda w \notin V_1$, and these are infinitely many vectors. Thus, there is some $V_j$ with $1 < j \leq n$ which contains infinitely many of these vectors. Subtracting two of them yields $(v + \lambda w) - (v + \lambda' w) = (\lambda - \lambda')w$, so that $w \in V_j$ and thus $v = (v + \lambda w) - \lambda w \in V_j$, which is a contradiction. \hfill $\Box$

It is worth mentioning that Lemma 3.1 can be used to prove the primitive element theorem [6, Thm. 5.4.11].

**Lemma 3.2.** Let $G$ be an infinite group. Let $G_1, \ldots, G_n$ be finitely many subgroups of $G$ with $G = \bigcup_{1 \leq i \leq n} G_i$ (as sets) such that $G \neq \bigcup_{1 \leq i \leq n, i \neq j} G_i$ for all $j$. Then their intersection $\bigcap_{1 \leq i \leq n} G_i$ is infinite.

*Proof.* By induction on $k$ we will prove that there are pairwise distinct indices $i_1, \ldots, i_k$ such that $G_{i_1} \cap \cdots \cap G_{i_k}$ is infinite; the case $k = n$ then finishes the proof. As for the case $k = 1$, since $G$ is infinite at least one $G_i$ has to be infinite as well. Now let $k < n$ and assume that the claim is proven for $k$. By assumption we have $G \neq G_{i_1} \cup \cdots \cup G_{i_k}$. Pick some $b \in G$ with $b \notin G_{i_1} \cup \cdots \cup G_{i_k}$. For every element $a$ of the infinite group $G_{i_1} \cap \cdots \cap G_{i_k}$ we have $ab \notin G_{i_1} \cup \cdots \cup G_{i_k}$, which yields an index $j \neq i_1, \ldots, i_k$ with $ab \in G_j$. So there must be some index $i_{k+1} \neq i_1, \ldots, i_k$ such that the set $S := \{a \in G_{i_1} \cap \cdots \cap G_{i_k} : ab \in G_{i_{k+1}}\}$ is infinite. For all $a, a' \in S$ we then have $aa'^{-1} = (ab)(a'b)^{-1} \in G_{i_{k+1}}$, on the other hand also $aa'^{-1} \in G_{i_1} \cap \cdots \cap G_{i_k}$. Therefore $SS^{-1} \subseteq G_{i_1} \cap \cdots \cap G_{i_k} \cap G_{i_{k+1}}$ is infinite. \hfill $\Box$

**Lemma 3.3.** A field cannot be written as the union of finitely many proper subfields.

*Proof.* Assume $L$ is a field such that $L = L_1 \cup \cdots \cup L_n$ with proper subfields $L_1, \ldots, L_n$. If $L$ is finite, then $L^\times$ is cyclic. Choose a generator of $L^\times$. It lies in some $L_i$, so that $L = L_i$, contradiction. Now assume that $L$ is infinite. We proceed by induction on $n$. The case $n = 0$ is trivial. Let $n \geq 1$ and assume the claim is true for $n - 1$. By induction hypothesis $L \neq \bigcup_{1 \leq i \leq n, i \neq j} L_i$ for all indices $j$. Thus, Lemma 3.2 applied to the additive groups implies that the intersection $K := L_1 \cap \cdots \cap L_n$ is infinite. Now we may regard $L$ as a vector space over $K$ and $L_i$ as subspaces of $L$. Then Lemma 3.1 gives the desired contradiction. \hfill $\Box$

**Remark 3.4.** For what follows, actually a weaker form of Lemma 3.3 is sufficient, namely that for a finite extension $L/K$ the field $L$ is not the union of finitely many proper intermediate fields. But this follows immediately from Lemma 3.1 if $K$ is infinite, and for finite fields $K
the field $L$ is also finite, so that $L^\times$ is cyclic and we are done. This shortens the proof, but we did not choose this path here since it would restrict Proposition 4.2 below to finite extensions.

4. Classification of subgroups

Definition 4.1. Let $L/K$ be an extension of fields and $H \subseteq \text{Aut}_K(L)$ be a subgroup. We define the fixed field as

$$L^H := \{ a \in L : \forall \sigma \in H \ (\sigma(a) = a) \}.$$ 

This is clearly an intermediate field of $L/K$.

We can rephrase the definition using group actions: In fact, the group $\text{Aut}_K(L)$ acts on $L$ in a natural way, and $L^H$ is nothing but the field of fixed points of this action when restricted to the subgroup $H$.

We have the obvious relationship $H \subseteq \text{Aut}_{L^H}(L)$. In some cases, the converse is also true:

Proposition 4.2. Let $L/K$ be an extension and $H \subseteq \text{Aut}_K(L)$ be a finite subgroup. Then

$$H = \text{Aut}_{L^H}(L).$$

Proof. Let $\tau \in \text{Aut}_{L^H}(L)$. We need to prove $\tau \in H$. First, we claim that

$$L = \bigcup_{\sigma \in H} \{ \sigma = \tau \},$$

where $\{ \sigma = \tau \}$ is a short notation of the subfield $\{ a \in L : \sigma(a) = \tau(a) \}$, the equalizer of $\sigma, \tau$.

Let $a \in L$. In order to use the assumption that $\tau$ fixes elements of $L^H$, we need to somehow come up with elements of $L^H$. Consider the polynomial

$$p := \prod_{\sigma \in H} (T - \sigma(a)) \in L[T].$$

Of course, this is only well-defined since $H$ is finite, and we have $p(a) = 0$. The natural action of $H$ on $L$ extends to an action on $L[T]$. The polynomial $p$ is clearly fixed by this action since the action just permutes the linear factors. Hence, we have

$$p \in L[T]^H = L^H[T].$$

Thus, $\tilde{\tau} : L[T] \to L[T]$ fixes $p$, i.e. $\tilde{\tau}(p) = p$. Since $\tau(a)$ is a root of $\tilde{\tau}(p) = p$, there is some $\sigma \in H$ with $\sigma(a) = \tau(a)$, so that $a \in \{ \sigma = \tau \}$. This proves our claim.

Now, each equalizer $\{ \sigma = \tau \}$ is a subfield of $L$. Thus, Lemma 3.3 implies that there is some $\sigma \in H$ with $L = \{ \sigma = \tau \}$, which just means $\sigma = \tau$. \qed

5. Separable extensions

Definition 5.1. Let $\overline{K}$ be an algebraic closure of $K$ and $L/K$ be an algebraic extension. We call $a \in L$ separable over $K$ if its minimal polynomial $f \in K[T]$ has only simple roots in $\overline{K}$. The extension $L/K$ is called separable if every element of $L$ is separable over $K$.

Lemma 5.2. Let $L/E/K$ be two algebraic extensions. If $L/K$ is separable, then $L/E$ and $E/K$ are separable as well.

Proof. The claim for $E/K$ is trivial. The claim for $L/E$ follows from the observation that the minimal polynomial of an element of $L$ over $E$ divides the minimal polynomial over $K$. \qed
Proposition 5.3. If $L/K$ is finite separable, then $\text{Hom}_K(L, \overline{K})$ has exactly $[L : K]$ elements.

Proof. We can just recycle the proof of Lemma 2.2 (which showed inequality). In the induction step we only need to observe 1) that $K \to \overline{K}$ admits exactly $[K(a) : K]$ extensions to $K(a)$ because $a$ is separable, and 2) that $L/K(a)$ is separable by Lemma 5.2.

Remark 5.4. Actually, a finite extension $L/K$ is separable if and only if $\text{Hom}_K(L, \overline{K})$ has $[L : K]$ elements [1, Lem. VII.4.24]. This is crucial for the theory of separable extensions.

Lemma 5.5. Let $L/K$ be a separable extension and $a \in L$ be an element. Assume that for all $K$-homomorphisms $\sigma, \tau : L \to \overline{K}$ we have $\sigma(a) = \tau(a)$. Then $a \in K$.

Proof. Because every $K$-homomorphism $K(a) \to \overline{K}$ extends to $L$ by Lemma 2.3, we may assume $L = K(a)$. Because of Lemma 2.1 the assumption means that the minimal polynomial of $a$ has exactly one root in $\overline{K}$. On the other hand, it has only simple roots, since $a$ is separable. Hence, it must be a linear polynomial, meaning $a \in K$. □

6. Normal extensions

Recall that a right action of a group $G$ on a set $X$ is called transitive if $X$ is non-empty and for all $x, y \in X$ there is some $g \in G$ with $y = xg$. Equivalently, $X$ has exactly one $G$-orbit.

Definition 6.1. An algebraic extension $L/K$ is called normal if the natural right action of $\text{Aut}_K(L)$ on the set $\text{Hom}_K(L, \overline{K})$ is transitive.

Remark that $\text{Hom}_K(L, \overline{K})$ is non-empty by Lemma 2.3. So the definition means that for all $K$-homomorphisms $\sigma, \tau : L \to \overline{K}$ there is some $K$-automorphism $\varphi : L \to L$ with $\tau = \sigma \circ \varphi$. Here, $\varphi$ is unique since $\sigma$ is injective. Thus, if we fix a $K$-homomorphism $\sigma : L \to \overline{K}$, this property means that the map

$$\text{Aut}_K(L) \xrightarrow{2.5} \text{Hom}_K(L, L) \to \text{Hom}_K(L, \overline{K}), \varphi \mapsto \sigma \circ \varphi$$

is bijective. Also, for the existence of $\varphi$ above it is clearly enough to check $\text{im}(\tau) \subseteq \text{im}(\sigma)$. This observation together with $E = \overline{K}$ already implies the next result.

Lemma 6.2. Let $L/E/K$ be two algebraic extensions. If $L/K$ is normal, then $L/E$ is normal as well. □

Proposition 6.3. Let $L/K$ be a normal separable extension and $E$ be an intermediate field of $L/K$. Then

$$E = L^{\text{Aut}_E(L)}.$$  

Proof. By Lemmas 5.2 and 6.2 the extension $L/E$ is normal and separable, so that it suffices to treat the special case $E = K$. Let $a \in L^{\text{Aut}_K(L)}$. For all $K$-homomorphisms $\sigma, \tau : L \to \overline{K}$ there is some $\varphi \in \text{Aut}_K(L)$ with $\tau = \sigma \circ \varphi$. We get $\tau(a) = \sigma(\varphi(a)) = \sigma(a)$. Thus, Lemma 5.5 implies $a \in K$. □

For the sake of completeness, we include the equivalence between Definition 6.1 and a more common definition of a normal extension.

Lemma 6.4. An algebraic extension $L/K$ is normal if and only if every irreducible polynomial $f \in K[T]$ which has a root in $L$ splits completely over $L$, i.e. is a product of linear factors.
Proof. Choose some \( K \)-homomorphism \( \sigma : L \to \overline{K} \). The splitting property means that for every \( a \in L \) its minimal polynomial splits completely over \( L \). Equivalently, its roots in \( \overline{K} \) are all contained in \( \text{im}(\sigma) \). By Lemma 2.1 and Lemma 2.3 these roots are \( \tau(a) \) for \( \tau \in \text{Hom}_K(L, \overline{K}) \). So the condition is just \( \text{im}(\tau) \subseteq \text{im}(\sigma) \) for all \( \tau \in \text{Hom}_K(L, \overline{K}) \). \( \square \)

7. Fundamental theorem of Galois theory

We are now able to combine the results from the previous sections.

**Definition 7.1.** A Galois extension is a normal separable algebraic extension.

**Remark 7.2.** Notice that for a Galois extension \( L/K \) and an intermediate field \( E \) the extension \( L/E \) is also Galois by Lemmas 5.2 and 6.2.

**Theorem 7.3.** Let \( L/K \) be a finite Galois extension. Then \( \text{Aut}_K(L) \) is a finite group of order \( [L : K] \), called the Galois group of \( L/K \).

**Proof.** Since \( L/K \) is normal, we have \( \text{Aut}_K(L) \cong \text{Hom}_K(L, \overline{K}) \), and since \( L/K \) is separable, \( \text{Hom}_K(L, \overline{K}) \) has exactly \( [L : K] \) elements by Proposition 5.3. \( \square \)

Let us briefly mention that the proof of Proposition 5.3 can actually be used to compute Galois groups in examples. We are now ready to prove the main theorem.

**Theorem 7.4** (Fundamental theorem of Galois theory). Let \( L/K \) be a finite Galois extension.

1. The maps \( E \mapsto \text{Aut}_E(L) \) and \( L^H \leftarrow H \) are inverse to each other and hence establish a bijection
   \[ \{ \text{intermediate fields of } L/K \} \cong \{ \text{subgroups of } \text{Aut}_K(L) \} . \]

2. These maps are inclusion-reversing in the sense
   - \( E \subseteq E' \implies \text{Aut}_{E'}(L) \subseteq \text{Aut}_E(L) \)
   - \( H \subseteq H' \implies L^{H'} \subseteq L^H \)
   and hence provide an anti-isomorphism of partial orders.

3. The degree of an intermediate field \( E \) is the index of the corresponding subgroup:
   \[ [E : K] = [\text{Aut}_K(L) : \text{Aut}_E(L)] \]

4. For intermediate fields \( E, E' \) and subgroups \( H, H' \) the following relationships hold:
   - \( \text{Aut}_{E \cap E'}(L) = \langle \text{Aut}_E(L), \text{Aut}_{E'}(L) \rangle \)
   - \( \text{Aut}_{E \cdot E'}(L) = \text{Aut}_E(L) \cap \text{Aut}_{E'}(L) \)
   - \( L^{H \cap H'} = L^H \cdot L^{H'} \)
   - \( L^{H \cdot H'} = L^H \cap L^{H'} \)
   Here, \( E \cdot E' \) denotes the compositum of \( E \) and \( E' \).

5. For an intermediate field \( E \) the extension \( E/K \) is normal (and hence a Galois extension) if and only if \( \text{Aut}_E(L) \) is a normal subgroup of \( \text{Aut}_K(L) \). In this case, we have
   \[ \text{Aut}_K(L)/\text{Aut}_E(L) \cong \text{Aut}_K(E) . \]
(6) The bijection from (1) restricts to a bijection
\[ \{ \text{normal intermediate fields of } L/K \} \cong \{ \text{normal subgroups of } \text{Aut}_K(L) \}. \]

Proof. (1) For an intermediate field \( E \) of \( L/K \) we have \( E = L^{\text{Aut}_E(L)} \) by Proposition 6.3. For a subgroup \( H \) of \( \text{Aut}_K(L) \) we have \( H = \text{Aut}_{L,H}(L) \) by Proposition 4.2, which is applicable since \( H \) is finite by Lemma 2.2.

(2) The verification of these inclusions is trivial.

(3) By Remark 7.2 and Theorem 7.3 we have
\[ [\text{Aut}_K(L) : \text{Aut}_E(L)] = \text{ord}(\text{Aut}_K(L))/\text{ord}(\text{Aut}_E(L)) = [L : K]/[L : E] = [E : K]. \]

(4) This follows from (2) as follows: The usual definition of a supremum as the least upper bound works in every partial order. Similarly for an infimum. In the partial order of subgroups of a group we have \( \text{sup}(H, H') = \langle H, H' \rangle \) and \( \text{inf}(H, H') = H \cap H' \). In the partial order of intermediate fields of an extension we have \( \text{sup}(E, E') = E \cdot E' \) as well as \( \text{inf}(E, E') = E \cap E' \).

Now we may use the general and easy fact that an anti-isomorphism of partial orders transforms suprema into infima and vice versa.

(5) Let \( E/K \) be normal. Fix a \( K \)-homomorphism \( L \to \overline{K} \). Because of Lemma 2.3 the restriction map \( \text{Hom}_K(L, \overline{K}) \to \text{Hom}_K(E, \overline{K}) \) is surjective, and since \( L/K \) and \( E/K \) are normal, it identifies with a restriction map \( \text{Aut}_K(L) \to \text{Aut}_K(E) \). This is clearly a homomorphism of groups whose kernel is \( \text{Aut}_E(L) \). Thus, \( \text{Aut}_E(L) \) is a normal subgroup with \( \text{Aut}_K(L)/\text{Aut}_E(L) \cong \text{Aut}_K(E) \).

For the other direction assume that \( H \) is a normal subgroup of \( \text{Aut}_K(L) \). To prove that \( L^H \) is normal over \( K \), choose two \( K \)-homomorphisms \( \sigma, \tau : L^H \to \overline{K} \). By Lemma 2.3 there are extensions \( \sigma', \tau' \) to \( L \). Since \( L/K \) is normal, we have \( \sigma' = \tau' \circ \varphi \) for some \( \varphi : L \to L \). We claim \( \varphi(L^H) \subseteq L^H \). In fact, for every \( a \in L^H \) and \( \psi \in H \) we have \( \varphi^{-1} \psi \varphi \in H \) (since \( H \) is normal), hence \( (\varphi^{-1} \psi \varphi)(a) = a \), i.e. \( \psi(\varphi(a)) = \varphi(a) \). Now, from \( \varphi(L^H) \subseteq L^H \) we deduce
\[ \sigma(L^H) = \sigma'(L^H) = \tau'(\varphi(L^H)) \subseteq \tau'(L^H) = \tau(L^H). \]

(6) This follows from (1) and (5).

Remark 7.5. Both Theorem 7.3 and Theorem 7.4(1) actually characterize Galois extensions by [1, Thm. VII.6.9].

References

[1] Aluffi, P. Algebra: Chapter 0, Grad. Stud. Math. Vol. 104, 2009
[2] Artin, E. Galois theory, Notre Dame Math. Lect. 2, ND Press, 1972
[3] Białynicki-Birula, A., Browkin, J., Schinzel, A., On the representation of fields as finite unions of subfields. Colloq. Math. 7, 31–32, 1959
[4] Bourbaki, N. Algebra II. Chapters 4–7, Springer, 1981
[5] De Meyer, F., Another Proof of the Fundamental Theorem of Galois Theory, Am. Math. Mon. 74 (7), 720–724, 1968
[6] Douady, R., Douady, A., Algebra and Galois theories, Springer, 2020
[7] Dress, A.W.M., One More Shortcut to Galois Theory, Adv. Math. 110 (1), 129–140, 1995
[8] Dummit, D.S., Foote, R.M. Abstract algebra, Prentice Hall, 1990
[9] Geck, M., On the Characterization of Galois Extensions, Am. Math. Mon. 121 (7), 637–639, 2014