Galois Theory Like You've Never Seen Before

Dhruv Goel

September 2025

Abstract

The standard proof of the fundamental theorem of (finite) Galois theory, as found in, say, [2] or [5], uses two key ideas from field theory, namely those of normality and separability. The goal of this article is to expand on an alternative approach to this theorem, due to Bavula [1], which avoids the notions of normality and separability entirely, and uses instead only one result from the theory of central simple algebras over a field: the Double Centralizer Theorem. The key new insight is to establish a correspondence between the lattices of intermediate subfields and subgroups of the Galois group by introducing a third lattice of algebras that is isomorphic to both of the them. A delightful feature of this approach, other than its simplicity and elegance, is it makes abundantly clear at what (unique) point the Galois hypothesis–interpreted here as saying the field extension is "maximally symmetric"–comes into play.

Contents

1 Introduction

Let L/K be a field extension, and let $G := \mathrm{Aut}_K(L)$ be the group of field automorphisms of L that fix K pointwise.[1] The first key result and definition we recall is

Lemma/Definition 1.1 (Finite Galois Extensions)**.** In the above setting, if L/K is a *finite* extension of degree $[L : K] := \dim_K L$, then G is a finite group whose cardinality $\#G$ satisfies

$$\#G \leq [L : K].$$

The extension L/K is said to be *Galois* if equality holds in the above, i.e., $\#G = [L : K]$. In this case we call the group G the *Galois group* of L/K and denote it by $\mathrm{Gal}(L/K)$.

In other words, a finite Galois extension is a maximally symmetric finite field extension.[2] The above inequality follows from Dedekind's Lemma on the linear independence of automorphisms. Dedekind's Lemma is recalled in §2, and we use it to prove Lemma/Definition 1.1 in §3. Given this definition, we are ready to state

Theorem 1.2 (Fundamental Theorem of Galois Theory)**.** Let L/K be a finite field extension with $G := \mathrm{Aut}_K(L)$. Let $\mathscr{F}$ denote the lattice of intermediate subfields F of the extension L/K, and let $\mathscr{G}$ denote the lattice of subgroups H of G.

(a) There are morphisms of posets

$$\mathscr{F}^\vee \leftrightarrow \mathscr{G}$$

given by the operations $F \mapsto \mathrm{Aut}_F(L)$ and $H \mapsto L^H$. When L/K is Galois, these operations are inverse bijections. In this case, for any $F \in \mathscr{F}$, the extension L/F is Galois as well, so that $\mathrm{Aut}_F(L)$ can be written as $\mathrm{Gal}(L/F)$ and

$$[L : F] = \#\,\mathrm{Gal}(L/F).$$

(b) In (a), if L/K is Galois and the intermediate field F corresponds to the subgroup H, then F/K is Galois iff $H \trianglelefteq G$, i.e., the subgroup H of G is normal. In this case there is a natural restriction morphism $G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ which fits into a short exact sequence of groups

$$0 \to H \to G \to \mathrm{Gal}(F/K) \to 0,$$

so that $G/H \xrightarrow{\sim}_{\mathsf{Grp}} \mathrm{Gal}(F/K)$.

Remark 1.3.

(a) The $(-)^\vee$ denotes the dual lattice; this amounts to saying that the bijection in (a) is in inclusion-reversing. The additional structure captured by the lattice formulation of the statement, which is not essential and actually follows from the classical formulation, is that the bijection in part (a) preserves joins and meets, i.e., that for any two subgroups $H, H' \leq G$, we have $L^{H \cap H'} = L^H L^{H'}$ and $L^{HH'} = L^H \cap L^{H'}$

[1] This coincides with the the group $\mathrm{Aut}_{K\text{-}\mathsf{Alg}}(L)$ of the automorphisms of L considered as a K-algebra.

[2] For the relationship between this definition and another equivalent one–that L/K is Galois iff $L^G = K$–see Corollary 5.2. Indeed, the equivalence between these two definitions is a direct consequence of our approach to the fundamental theorem. A third definition is also possible, in which an extension L/K is said to be Galois iff it is normal and separable; a fourth as well, in which an extension L/K is Galois iff it is the splitting field of a collection of separable polynomials. Either of these last three definitions is more useful when studying infinite Galois theory, but for our present purposes (in the context of our approach to finite Galois theory without using the notions of normality or separability), the equivalence of these definitions can be considered a coincidence and not an essential feature. However, I suspect also that there is a way to extend the present proof to the setting of infinite Galois theory by introducing appropriate topologies; in this setting, the correct definition (still avoiding normality and separability) could be some analog of Corollary 3.3.

(b) Given part (a) and the existence of a morphism $G \to \mathrm{Gal}(F/K)$ as in (b), the existence of the following short exact sequence–or what amounts to the same thing, the surjectivity of the map $G \to \mathrm{Gal}(F/K)$–follows immediately from size considerations and the multiplicativity of the degree in towers of field extensions.

The standard proof of this fundamental theorem (Theorem 1.2), as found in, say, [2] or [5], uses two notions from field theory: that of normality and separability. The goal of this paper is to give an alternative proof, following [1], that does not invoke these notions at all; all the heavy lifting in this case is done by essentially one result from the theory of central simple algebras, namely the Double Centralizer Theorem (Theorem 4.6).

The rest of this article is organized as follows. In the next section (§2), we review Dedekind's lemma on the linear independence of field automorphisms, and in the following section (§3), we use it to provide a reinterpretation of the Galois condition in terms of endomorphism algebras. In §4, we review the definition of central simple algebras and state (and give references to proofs of) the fundamental theorem needed–the Double Centralizer Theorem. In the final section (§5), we then present the new proof of the fundamental theorem with this approach.

2 Dedekind's Lemma

In this section, we review Dedekind's lemma on the linear independence of field automorphisms. In fact, the same (standard) proof can be used to prove the slightly strong result of

Lemma 2.1. Let R and S be commutative rings, with S is a nonzero integral domain. Any set of ring homomorphisms $R \to S$ is linearly independent over S in $\mathrm{Hom}_{\mathsf{Ab}}(R, S)$. In other words, given $n \in \mathbb{Z}_{\geq 1}$ and pairwise distinct ring homomorphisms $g_1, \ldots, g_n : R \to S$, if for some $\lambda_1, \ldots, \lambda_n \in S$ we have

$$\sum_{i=1}^{n} \lambda_i g_i = 0 \tag{1}$$

as abelian group morphisms $R \to S$, then $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Proof. We induct on n, with $n = 1$ being clear by evaluating at 1. Suppose $n \geq 2$. Since the g_i are ring homomorphisms, we also have for any $\lambda \in R$ that

$$\sum_{i=1}^{n} \lambda_i g_i(\lambda) \cdot g_i = 0. \tag{2}$$

Since $g_1 \neq g_n$, there is a $\lambda \in R$ such that $g_1(\lambda) \neq g_n(\lambda)$. For this value of λ, if we multiply (1) by $g_n(\lambda)$ and subtract it from (2), we get also

$$\sum_{i=1}^{n-1} \lambda_i \left(g_i(\lambda) - g_n(\lambda)\right) g_i = 0.$$

By the inductive hypothesis, all coefficients are zero; in particular, $\lambda_1(g_1(\lambda) - g_n(\lambda)) = 0$. Since S is a domain and $g_1(\lambda) - g_n(\lambda) \neq 0$ by our choice of λ, we must have $\lambda_1 = 0$. Plugging this in (1) and using the inductive hypothesis one more time finishes the proof. ∎

Remark 2.2. For a counterexample when S is not a domain, take $R = S = \mathbb{C}[\varepsilon]/(\varepsilon^2)$, take $n = 2$, the first map f_1 to be the identity, and the second map f_2 to be the $\mathbb{C}$-algebra homomorphism sending x to 0. Then $\varepsilon \cdot f - \varepsilon \cdot g = 0$ in $\mathrm{Hom}_{\mathsf{Ab}}(R, S)$.

Given a field L and a group G, we define a *(linear) character* of G in L to be a group homomorphism $\chi : G \to L^\times$. In this language, the classical version of Dedekind's Lemma is about linear independence of characters as follows.

Corollary 2.3 (Dedekind's Lemma)**.** Let L be a field.

(a) Given any group G, distinct linear characters $G \to L^\times$ are linearly independent over L.
(b) Distinct field automorphisms of L are linearly independent over L.

Proof.

(a) Take $R := \mathbb{Z}[G]$ and $S = L$ in Lemma 2.1, noting that specifying a character $G \to L^\times$ is the same thing as specifying a ring homomorphism $R \to L$.[3]
(b) Take $G = L^\times$ in (a).

■

Remark 2.4. The more general formulation of this classical lemma may seem unnecessary, but I believe that this exposition with minimal hypotheses actually clarifies the result. Besides, this result is also directly useful in modular representation theory (see, e.g., [7, Corollary 6.8]).

3 Reinterpreting the Galois Condition

We will now use Dedekind's Lemma (Corollary 2.3(b)) to prove the result of Lemma/Definition 1.1 and to reinterpret the Galois condition in terms of algebras. For that, let's first quickly review the definition of algebras over a field.

Let K be a field. In general, by an *algebra over* K, or a K*-algebra*, we mean a possibly noncommutative but associative unital ring E equipped with a unital ring homomorphism $K \to E$ such that the image of K lies in the center $\mathrm{Z}(E)$ of E. Given such a K-algebra E, the ring homomorphism $K \to E$ is automatically injective (since K is a field) and maps K bijectively to a subring of the center $\mathrm{Z}(E)$, which is a commutative ring. The definitions of a K-subalgebra $A \subset E$ and of a K-algebra homomorphism $E \to E'$ are clear, and left to the reader. Our main source of algebras in this article will come from

Example 3.1. Given a field K and a vector space V over K, let $E := \mathrm{End}_{K\text{-}\mathsf{Vect}}(V)$. Then E is naturally a K-algebra; this algebra is called the *endomorphism algebra* of the vector space V.

Now suppose that L/K is a field extension, and let $G := \mathrm{Aut}_K(L)$ be as above. Let $E := \mathrm{End}_{K\text{-}\mathsf{Vect}}(L)$ denote the endomorphism algebra of the underlying vector space of L. There are two kinds of elements of E that we understand really well:

(a) There is a natural K-algebra homomorphism $\mu : L \to E$ which takes a $\lambda \in L$ to the K-linear endomorphism $\mu(\lambda) : L \to L$ given by left multiplication by λ. Since L is a field, the map μ is injective, so that L can be identified with the K-subalgebra $\mu(L)$ of E.
(b) Every element of G gives rise to a K-linear endomorphism of L, i.e., there is a natural homomorphism $\iota : G \to E^\times$ which is again evidently injective.[4]

In fact, we can combine these two kinds of endomorphisms; to do this, we first make

[3] In other words, the group algebra functor $\mathbb{Z}[-] : \mathsf{Grp} \to \mathsf{Ring}$ is left adjoint to the group-of-units functor $(-)^\times : \mathsf{Ring} \to \mathsf{Grp}$.

[4] However, it is never surjective (except in the very trivial case of $K = L = \mathbb{F}_2$): $G = \mathrm{Aut}_K(L)$ is only a subgroup of $E^\times = \mathrm{Aut}_{K\text{-}\mathsf{Vect}}(L)$. Indeed, it is very easy to come up with K-linear automorphisms of L that are not field automorphisms.

Definition 3.2. In the above setting, define the *crossed product algebra* $L \rtimes G$ to be the K-algebra with underlying K-vector space

$$L^{\oplus G} = \bigoplus_{g \in G} L\mathrm{e}_g$$

and multiplication defined by the formula

$$\lambda\, \mathrm{e}_g \otimes \lambda'\, \mathrm{e}_{g'} \mapsto \big(\lambda g(\lambda')\big)\, \mathrm{e}_{gg'}$$

for $\lambda, \mu \in L$ and $g, h \in G$. The K-algebra structure comes from the homomorphism $K \to L \rtimes G$ given by the inclusion $K \hookrightarrow L \cong L\mathrm{e}_1 \subset L \rtimes G$, where $1 \in G$ is the identity.

One can check very directly that this defines an associative unital ring, but this also follows immediately from the following discussion. First note that $L \rtimes G$ is evidently a left L-vector space, and by construction, there is a natural K-algebra homomorphism $L \rtimes G \to E$ given by $\lambda\, \mathrm{e}_g \mapsto \mu(\lambda) \cdot \iota(g)$; indeed, the K-algebra structure $L \rtimes G$ is *defined* to make this map a homomorphism.[5] Now Dedekind's Lemma (Corollary 2.3(b)) implies in particular that

$$\text{the } K\text{-algebra homomorphism } L \rtimes G \to E \text{ is injective.} \tag{3}$$

In particular, $L \rtimes G$ can be considered as a K-subalgebra of E, and we will make this implicit identification in all that follows. It is also for this reason that we will also denote e_g by g for $g \in G$, and drop both μ and ι from the notation, identifying everything with their images in E. Finally, note that G acts on E by conjugation; this action preserves $L \subset L \rtimes G \subset E$, and indeed recovers the tautological action of G on L by automorphisms.

Now suppose that L/K is a *finite* extension. In this case, the algebras $L \rtimes G$ and E are both finite dimensional over K. Indeed, we have that

$$\dim_K L \rtimes G = [L : K] \cdot \dim_L L \rtimes G = [L : K] \cdot \#G,$$

whereas

$$\dim_K E = [L : K]^2.$$

Combining this dimension count with the observation (3) immediately gives us the result of Lemma/Definition 1.1, and also proves

Corollary 3.3. In the above notation, the finite extension L/K of fields is Galois iff the natural map $L \rtimes G \to E$ is an isomorphism.

It is this reinterpretation of the Galois condition that we will use in the rest of the paper.

Example 3.4. For the Galois extension $\mathbb{C}/\mathbb{R}$, the isomorphism $\mathbb{C} \rtimes \mathbb{Z}/2 \xrightarrow{\sim} \mathrm{End}_{\mathbb{R}\text{-}\mathsf{Vect}}(\mathbb{C})$ amounts to the statement that every $\mathbb{R}$-linear map $f : \mathbb{C} \to \mathbb{C}$ can be uniquely written as the sum of a $\mathbb{C}$-linear and a $\mathbb{C}$-antlinear map, a fact (the higher-dimensional analog of) which is very familiar to complex geometers. Indeed, any $\mathbb{R}$-linear map f can be written as

$$f = \frac{f + \bar{f}}{2} + \frac{f - \bar{f}}{2},$$

where the first summand is $\mathbb{C}$-linear and the second $\mathbb{C}$-antilinear.

[5] This is even a left L-linear map when E is given the structure of an L-vector space by using the K-algebra homomorphism μ.

Example 3.5. The previous example may suggest that degree two Galois extensions might behave strangely in characteristic two, but at least in terms of Galois theory there is no difference. For instance, it is again true that any $\mathbb{F}_2$-linear endomorphism of $\mathbb{F}_4 \cong \mathbb{F}_2[\omega] = \mathbb{F}_2[x]/(x^2+x+1)$ is a unique linear combination of $1_{\mathbb{F}_4}$ and the Frobenius automorphism $\sigma : \mathbb{F}_4 \to \mathbb{F}_4$ taking $\omega \mapsto \omega^2$.

We end this section by making a general observation we will use below. Given a field K, an algebra E over it, and a subalgebra $A \subset E$, we define the *centralizer* (also called *commutant*) $\mathrm{C}_E(A)$ *of* A *in* E to be the K-subalgebra of E consisting of those elements which commute with all elements of A, i.e.,

$$\mathrm{C}_E(A) := \{e \in E : (\forall\, a \in A)\, ae = ea\}.$$

Therefore, for example, we have $\mathrm{Z}(E) = \mathrm{C}_E(E)$. Note that this operation is inclusion-reversing: if $A \subset B \subset E$ are K-subalgebras, then $\mathrm{C}_E(A) \supset \mathrm{C}_E(B) \supset \mathrm{Z}(E)$; ultimately, this is the reason for the inclusion-reversing nature of the Galois correspondence in our approach to it. The key observation we will need, and the first indication that something interesting is happening, is

Lemma 3.6. Let L/K be a field extension, and let $E := \mathrm{End}_{K\text{-}\mathsf{Vect}}(L)$ be the endomorphism algebra of the underlying K-vector space of L. Consider L as a K-subalgebra of E as in §3. For any intermediate extension F (i.e., field F with $K \subset F \subset L$), considered as a K-subalgebra of E via $F \subset L \subset E$, we have

$$\mathrm{C}_E(F) = \mathrm{End}_{F\text{-}\mathsf{Vect}}(L).$$

In particular, $\mathrm{C}_E(L) = L$.

Proof. Trivial unraveling of the definitions, and left to the reader. ∎

Convention 3.7. In the rest of this article, we will require all our algebras E over our field K to be finite dimensional over K.

4 Central Simple Algebras

Given a finite dimensional vector space V over a field K, the endomorphism algebra $E = \mathrm{End}_{K\text{-}\mathsf{Vect}}(V)$ is a *central simple algebra*, and it is this property that will be central to our proof of the Fundamental Theorem of Galois Theory. Let us recount this story here.

Definition 4.1. Let K be a field and E be an algebra over K. We say that E is a *central simple algebra* over K iff it is both

(a) *central*, i.e., the map $K \to \mathrm{Z}(E)$ coming from the structure of E is an isomorphism, and
(b) *simple*, i.e., it has no nonzero proper two-sided ideals.

Remark 4.2. Central simple algebras are also known as *Azumaya algebras*; see [6, §1.5.1], where one can also find several equivalent definitions to the one given above.

In this article, we will need only two results which we will not prove fully. The first of these is

Theorem 4.3. A finite-dimensional algebra over a field is simple iff it admits a finite-dimensional faithful simple module, in which case this module is unique up to isomorphism.

This is a essentially a consequence of the Artin-Wedderburn Theorem; see [3, Chapters 1-2] or [4, Theorem 5.48] for the general theory. Here we give the short proof of the first statement found in [1, Lemma 2.4], which is all we need.

Proof of the first statement. Let K be a field and E a K-algebra. If E is simple, then all nontrivial E-modules are faithful. In particular, E itself, say, by the left regular action is a faithful simple module, which is finite-dimensional if E is. Conversely, suppose M is a faithful simple E-module, and let $\mathrm{Rad}(E)$ denote the Jacobson radical of E ([4, Def. 5.38]). Since M is simple, $\mathrm{Rad}(E) \cdot M = 0$; since M is faithful, $\mathrm{Rad}(E) = 0$. In particular, E is semisimple ([4, Lemma 5.39]), and hence by the Artin-Wedderburn Theorem ([4, Theorem 5.48]), E is a finite direct product of simple finite-dimensional algebras (i.e., matrix algebras over skewfield extensions of K). In particular, we understand all the simple modules over E. If E is semisimple but not simple, then no simple E-module can be faithful; but we've asserted the existence of one such module, namely M, and hence E must be simple. ■

Example 4.4. Let V be a finite dimensional vector space over K. The K-algebra $E := \mathrm{End}_{K\text{-}\mathsf{Vect}}(V)$ of K-linear endomorphisms of K is a central simple algebra over K. Indeed, a choice of basis of V yields an isomorphism of E with a square matrix algebra over K, and then centrality and simplicity amount to trivial checks about matrices, left to the reader. Alternatively, centrality is clear by basic linear algebra, and by Remark 4.2(b), it only remains to note that V is a faithful simple module for E. In fact, Theorem 4.3, shows us that in this case every K-subalgebra $A \subset E$ is simple, a fact we shall need in what follows.

These are, however, far from the only central simple algebras over a field. The simplest non-matrix-algebra example I know is

Example 4.5. When $K = \mathbb{R}$, the $\mathbb{R}$-algebra $E = \mathbb{H}$ of Hamiltonian quaternions is a central simple algebra over $\mathbb{R}$ that is *not* isomorphic to a matrix algebra over $\mathbb{R}$ (check!).

In general, central simple algebras over a field K are classified by its Brauer group $\mathrm{Br}(K) \cong \mathrm{H}^2(K, \mathbb{G}_m)$; since this is irrelevant to our current exposition, we redirect the interested reader to [4] or [6]. The theory of central simple algebras over a field is rich and vast, with many applications to number theory (local class field theory) and arithmetic geometry (rationality questions); however, the only other result from it we shall need is

Theorem 4.6 (Double Centralizer Theorem)**.** Let K be a field and E a central simple algebra over K. If $A \subset E$ is a simple K-subalgebra, then so is the centralizer $\mathrm{C}_E(A)$, and we have

$$A = \mathrm{C}_E(\mathrm{C}_E(A)).$$

Further, we have

$$\dim_K A \cdot \dim_K \mathrm{C}_E(A) = \dim_K E.$$

Proof. See [3, Theorem 3.15(d)] or [4, Theorem 6.26]. ■

5 Proof of the Fundamental Theorem

We are now ready to prove the Fundamental Theorem of Galois Theory (Theorem 1.2) using the Double Centralizer Theorem (Theorem 4.6).

The first part of the Fundamental Theorem is a consequence of

Theorem 5.1. Let L/K be a finite extension of fields with $G := \mathrm{Aut}_K(L)$. Let $\mathscr{F}$ and $\mathscr{G}$ be as in 1.2. Let $\mathscr{A}$ denote the lattice of intermediate K-subalgebras A between L and E.

(a) There is an isomorphism of lattices
$$\mathscr{F}^\vee \leftrightarrow \mathscr{A}$$
given by the operations $F \mapsto \mathrm{C}_E(F) = \mathrm{End}_{F\text{-}\mathsf{Vect}}(L)$ and $A \mapsto \mathrm{C}_E(A)$.

(b) There are morphisms of posets
$$\mathscr{A} \leftrightarrow \mathscr{G}$$
given by $A \mapsto A \cap G$ and $H \mapsto L \rtimes H$. For any $H \in \mathscr{G}$, we have $(L \rtimes H) \cap G = H$. For any $A \in \mathscr{A}$, we have $L \rtimes (A \cap G) \subset A$, and further, *if* L/K is Galois, then equality holds. In particular, if L/K is Galois, then these morphisms give inverse isomorphisms of lattices.

In particular, for any extension L/K, the lattice $\mathscr{G}$ embeds into $\mathscr{F}^\vee$ via this composition, and it is maps surjectively (and hence isomorphically) if L/K is Galois.

(c) The compositions of the poset morphisms in (a) and (b) are the morphisms in 1.2(a).

(d) If L/K is Galois, then for any $F \in \mathscr{F}$, so the extension L/F is also Galois.

Proof.

(a) If $F \in \mathscr{F}$, then $F \subset L \subset E$ implies $\mathrm{C}_E(F) \supset \mathrm{C}_E(L) = L$, so that $\mathrm{C}_E(F) \in \mathscr{A}$. Conversely, if $A \in \mathscr{A}$, then $L \subset A \subset E$ implies $L = \mathrm{C}_E(L) \supset \mathrm{C}_E(A)$, and a K-subalgebra of L is automatically a field.[6] That these operations are mutual inverses follows from the Double Centralizer Theorem (Theorem 4.6), after we recall that every K-subalgebra of E is simple, as explained in Example 4.4.

(b) That these are morphisms of posets is clear. Given $H \in \mathscr{G}$, the inclusion $H \subset (L \rtimes H) \cap G$ is obvious, and the other inclusion follows from Dedekind's Lemma (Lemma 2.1(b)). Given $A \in \mathscr{A}$, the inclusion $L \rtimes (A \cap G) \subset A$ follows from the fact that A contains L and is a K-algebra. It remains to show that *when L/K is Galois*, we have the other inclusion as well. For this, note that when L/K is Galois, $E = L \rtimes G$ (Corollary 3.3), and so it remains to show that for any $A \in \mathscr{A}$, if $\sum_{g \in G} \lambda_g g \in A$ with $\lambda_g \in L$, then in fact each g such that $\lambda_g \neq 0$ is in A. This is easily done by induction on the number $n \in \mathbb{Z}_{\geq 0}$ of nonzero λ_g. The proof of this statement is very reminiscent of the proof of Lemma 2.
When $n = 0$, there is nothing to show, and when $n = 1$, the result is clear because $L \subset A$. Suppose now that $n \geq 2$ and we have shown the result for $n - 1$. Label to write the given sum as $\sum_{i=1}^n \lambda_i g_i$ with the g_i all pairwise distinct and λ_i all nonzero. Since $g_1 \neq g_n$, there is a $\lambda \in L$ such that $g_1(\lambda) \neq g_n(\lambda)$. Since $L \subset A$ and A is an algebra,
$$A \ni \left(\sum_{i=1}^n \lambda_i g_i\right) \cdot \lambda = \sum_{i=1}^n \lambda_i g_i(\lambda) g_i$$
as well. But also
$$A \ni g_n(\lambda) \cdot \left(\sum_{i=1}^n \lambda_i g_i\right) = \sum_{i=1}^n \lambda_i g_n(\lambda) g_i.$$
Subtracting the two yields
$$\sum_{i=1}^{n-1} \lambda_i (g_i(\lambda) - g_n(\lambda)) g_i \in A.$$
Since L is a domain, we have $\lambda_1(g_1(\lambda) - g_n(\lambda)) \neq 0$. Therefore, by induction, we get that $g_1 \in A$. Then also $\lambda_1 g_1 \in A$, and so again subtracting we conclude $\sum_{i=2}^n \lambda_i g_i \in A$. One more application of the inductive hypothesis then tells us that each g_i is in A as needed.

[6] Indeed, a domain that is finite dimensional over some field is automatically a field.

(c) For any $F \in \mathscr{F}$, we have $\mathrm{C}_E(F) \cap G = \mathrm{End}_{F\text{-}\mathsf{Vect}}(L) \cap G = \mathrm{Aut}_F(L)$. Similarly, for any $H \leq G$, we have that $\mathrm{C}_E(L \rtimes H) = \{\lambda \in L : (\forall h \in H)\, h\lambda = \lambda h\} = L^H$.
(d) If F corresponds to $H = \mathrm{Aut}_F(L)$, then (a), (b), and (c) combine to tell us that the natural map $L \rtimes H \to \mathrm{C}_E(F)$ is an isomorphism; we are then done by Lemma 3.6 coupled with Corollary 3.3.

■

This theorem also gives us a way to relate our definition of a Galois extension to another common definition found in the literature.

Corollary 5.2. Let L/K be a finite extension of fields and $G := \mathrm{Aut}_K(L)$. Then L/K is Galois (i.e., $\#G = [L : K]$) if and only if the subfield $L^G \subset L$ of L fixed pointwise by all elements of G is K.

Proof. For any finite L/K with $G = \mathrm{Aut}_K(L)$ and $E = \mathrm{End}_{K\text{-}\mathsf{Vect}}(L)$, since $L \rtimes G \subset E$, we have that

$$L^G = \mathrm{C}_E(L \rtimes G) \supset \mathrm{C}_E(E) = \mathrm{Z}(E) = K.$$

Therefore, $L^G = K$ iff $\mathrm{C}_E(L \rtimes G) = \mathrm{C}_E(E)$, which by the Double Centralizer Theorem (Theorem 4.6) happens iff $L \rtimes G = E$, so we are done by Corollary 3.3. ■

To prove the rest of the Fundamental Theorem, it remains to show

Theorem 5.3. Let L/K be a finite Galois extension of fields with $G = \mathrm{Gal}(L/K)$. In the above notation and under the correspondences of Theorem 5.1, let the field $F \in \mathscr{F}$, the algebra $A \in \mathscr{A}$, and the subgroup $H \in \mathscr{G}$ all correspond to each other, so that $A = L \rtimes H = \mathrm{C}_E(F)$. The following conditions are equivalent.

(a) The subgroup $H \leq G$ is normal.
(b) The subalgebra $A \subset E$ is stable under conjugation by G.
(c) The subalgebra $F \subset E$ is stable under conjugation by G.
(d) The subfield $F \subset L$ is stable under the action of G on L.
(e) The extension F/K is Galois.

In this case, (d) gives a natural restriction morphism $G \to \mathrm{Gal}(F/K)$, and this morphism is surjective with kernel H.

Proof.

(a) $\Leftrightarrow$ (b) For $g \in G$, we have $g(L \rtimes H)g^{-1} = L \rtimes gHg^{-1}$ and so $gAg^{-1} \cap G = g(A \cap G)g^{-1}$.
(b) $\Leftrightarrow$ (c) For $g \in G$, we have $\mathrm{C}_E(gAg^{-1}) = g^{-1}\mathrm{C}_E(A)g$.
(c) $\Leftrightarrow$ (d) The group G acts on L by automorphisms via conjugation in E.
(d) $\Rightarrow$ (e) The hypothesis implies there is a homomorphism $G \to \mathrm{Aut}_K(F)$ with kernel H. Therefore,

$$\#\,\mathrm{Aut}_K(F) \geq \#G/\#H = [L : K]/[L : F] = [F : K],$$

so F/K is Galois by Lemma/Definition 1.1.
(e) $\Rightarrow$ (d) Let $Q := \mathrm{Aut}_K(F)$. By Corollary 5.2, $F^Q = K$, so for any $\lambda \in F$, we have $p(x) := \prod_{\lambda' \in Q \cdot \lambda}(x - \lambda') \in F^Q[x] = K[x]$. In particular, for any $g \in G$, the element $g(\lambda)$ is a root of $g(p(x)) = p(x)$ as well; but all roots of $p(x)$ lie in F, so $g(\lambda) \in F$.

■

References

[1] Bavula, V. V. The Galois Theory (a ring theoretic approach). https://arxiv.org/pdf/2509.01284, 2025.

[2] Dummit, D. S., and Foote, R. M. *Abstract Algebra*, third ed. Wiley, 2003.

[3] Farb, B., and Dennis, R. K. *Noncommutative Algebra*, vol. 144 of *Graduate Texts in Mathematics*. Springer, 1993.

[4] Guillot, P. *A Gentle Course in Local Class Field Theory*. Cambridge University Press, 2018.

[5] Morandi, P. *Fields and Galois Theory*, vol. 167 of *Graduate Texts in Mathematics*. Springer, 1996.

[6] Poonen, B. *Rational Points on Varieties*, vol. 186 of *Graduate Studies in Mathematics*. American Mathematical Society, 2010.

[7] Pound, E. Modular Representation Theory (Lectures by Stuart Martin). Available at https://ep455.user.srcf.net/pdfs/MRTnotes.pdf.