SYMMETRIES OF THE NON-CANONICAL

An Exposition of the Galois Correspondence

SEBASTIAN CORRY

June 24, 2025

PREFACE

Fields are awfully non-canonical objects. Every field has an algebraic closure, and any two algebraic closures thereof are isomorphic, but not uniquely. Likewise, every polynomial has a splitting field, and any two splitting fields thereof are isomorphic, but not uniquely. When faced with the non-canonical, the best we can do is account for its symmetries and how our choices are reflected in them. For fields, the aggregate of these considerations is called *Galois theory*.

The first three parts of these notes discuss the category of fields (1), algebraic extensions (2), and separable extensions (3). The fourth section proves Grothendieck's Galois correspondence for finite separable field extensions (the connected case); it proceeds to specialize this result to the classical fundamental theorem of Galois theory (4).

I have documented the sources I consulted when writing these notes in the bibliography. I, of course, do not claim any ideas or proofs presented here as original.

Prerequisites: Familiarity with (finite) group theory, the rudiments of commutative algebra, and basic category theory, *i.e.* the notions of category, functor, equivalence, etc.

Notation: We denote hom-sets in the category of k-algebras by $\hom_k$, in the category of sets by hom, and in the category of G-sets by $\hom_G$. For a field extension, we use the symbols $k \to E$ and E/k interchangeably.

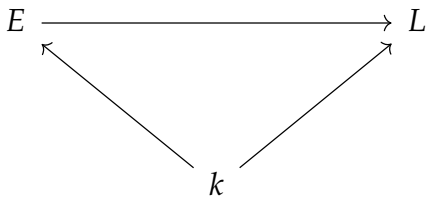
1. Field Extensions

Theorem 1.1. A field is a non-zero simple commutative ring.

Proof. Suppose k is a field, and consider the zero ideal $(0) \subseteq k$. Any non-zero $x \in k$ is a unit, so $(0, x) = k$. It follows that (0) is a maximal ideal and, in turn, that there are no other proper ideals.

Conversely, suppose $k \neq 0$ is simple. If $x \in k$ is non-zero, then the ideal (x) is likewise non-zero, hence $(x) = k$ by simplicity; thus, x is a unit and k a field. □

Let's enjoy simple and non-trivial pleasures and restrict our attention from commutative rings to the full subcategory of fields. Among fields, the kernel of a morphism $k \to E$ is an ideal of k and proper at that since 1 goes to 1. We are imagining simple rings, so this kernel is necessarily trivial and the morphism injective. Colloquially, this means that fields relate to each other by inclusion; a morphism thereof is thus called a *(field) extension*. Sometimes, when the map is implicitly understood, we suppress it and alternatively write E/k; other times, simply E suffices. Given extensions E and L of k, a *k-morphism* from E to L is a morphism of fields for which the following diagram commutes:



Classically, these matters are discussed concretely. Given an extension E/k, we can isomorphically identify k with its image in E. In doing so, a field extension E/k becomes a field E containing k as a subfield, and a k-morphism becomes a morphism fixing each element of k. We avoid making these identifications on the nose, for the exigencies of rigor would demand frequent and distracting digressions on mundane minutiae. However, the intuition of inclusion is of sufficient psychological merit that it justifies a small abuse of language: we will often refer to an element α of E as lying in k, when what we really mean is that α lies in the image of k; for example, for two extensions E and L of k, to restrict a k-morphism $\varphi : E \to L$ to k is to compose it with the morphism E/k.

All happy families are alike; all nice objects are like vector spaces. And an extension E/k is after all quite nice, for it is, among other things, a k-algebra. By linear algebra, it has some dimension—a cardinal $[E : k]$—called the *degree* of E over k.

Theorem 1.2 (Tower Theorem)**.** Let $k \to E \to L$ be a tower of field extensions. If $\{\alpha_i\}_i$ and $\{\beta_j\}_j$ are bases for E over k and L over E respectively, then $\{\alpha_i\beta_j\}_{i,j}$ is a basis for L over k. In particular,

$$[L : k] = [L : E][E : k].$$

Proof. Fix any element $x \in L$. Then $x = \sum_j \xi_j \beta_j$ for some ξ_j's in E, all but finitely-many of which vanish. Each $\xi_j = \sum_i \eta_{ij} \alpha_i$ for some η_{ij}'s in k which, like the ξ_j's, are almost all zero. Therefore,

$$x = \sum_{i,j} \eta_{ij} \alpha_i \beta_j,$$

and $\{\alpha_i \beta_j\}_{i,j}$ spans L over k.

As for linear independence, suppose

$$\sum_{i,j} \eta_{ij} \alpha_i \beta_j = 0$$

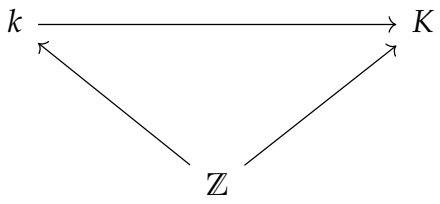
for some η_{ij}'s in k, almost all of which are zero. By the linear independence of the β_j's,

$$\sum_i \eta_{ij} \alpha_i = 0$$

for each j. Therefore, $\eta_{ij} = 0$ for all i and j by the linear independence of the α_i's. □

The prototypical example of a field is that of the rational numbers, $\mathbb{Q}$. Finite (meaning finite-degree) extensions of $\mathbb{Q}$ are called *number fields* and are the primary objects of study in algebraic number theory. Other celebrities include the fields of real and complex numbers, $\mathbb{R}$ and $\mathbb{C}$; in aggregate, these form a tower $\mathbb{Q} \to \mathbb{R} \to \mathbb{C}$. A cardinality argument shows that the degree of $\mathbb{R}$ over $\mathbb{Q}$ is infinite; in these sorts of cases, rather than worrying about transfinite particularities, we will suggestively write $[\mathbb{R} : \mathbb{Q}] = \infty$. In contrast, the phrase "complex plane" encodes the entirely elementary observation that $[\mathbb{C} : \mathbb{R}] = 2$.

It should be said that fields can make for rather poor company when taken all together—it is wiser to admit them in cliques. The reason for this is that the category of fields is partitioned by primes: Among commutative rings, each field K admits a unique morphism $\mathbb{Z} \to K$. The kernel is a prime ideal and, since $\mathbb{Z}$ is a principal ideal domain, it is generated by a unique integer equal to 0 or a prime p, the *characteristic* of K. Quotienting by this kernel and subsequently taking the field of fractions—in short, taking the residue field at the kernel—yields a morphism $F \to K$, where $F = \mathbb{Q}$ or $F = \mathbb{F}_p = \mathbb{Z}/(p)$. Suppose we have another morphism of fields $k \to K$. Then, by uniqueness, the diagram



commutes, hence

$$\ker(\mathbb{Z} \to k) = \ker(\mathbb{Z} \to K),$$

and passage to residue fields produces a morphism $F \to k$. The whole apparatus arranges itself into a tower $F \to k \to K$; in concrete terms, F is K's smallest subfield, the *prime field* of K. Two fields have the same prime field if and only if they have the same characteristic, and if we restrict our attention to fields of a fixed characteristic, we obtain a full subcategory with initial object the corresponding prime field.

At this point, a coarser break presents itself: There are fields of characteristic zero, and there are fields of positive characteristic. And there is the age-old question: What happens in characteristic $p > 0$? Consider a field k with prime field $\mathbb{F}_p$, *i.e.* an extension $k/\mathbb{F}_p$. Given two elements $x, y \in k$, by the binomial theorem,

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{n-i}.$$

For $1 \leqslant i \leqslant p-1$, the prime p divides $\binom{p}{i}$, hence this coefficient, computed in the $\mathbb{F}_p$-algebra k, vanishes. Therefore,

$$(x+y)^p = x^p + y^p.$$

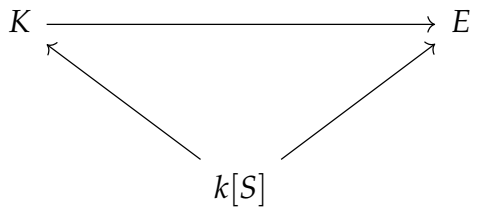
In other words, the map $\sigma_k : k \to k, x \mapsto x^p$ is an endomorphism, the *Frobenius endomorphism* of k. We follow the convention that the Frobenius endomorphism of a characteristic zero field is the identity.

2. ALGEBRAICITY

THE category of k-algebras admits a forgetful functor sending each algebra E to its underlying set $U(E)$, and this functor has a left-adjoint sending a set S to the ring $k[S]$ of polynomials in the elements of S. In other words, there is a canonical bijection

$$\hom_k(k[S], E) \cong \hom(S, U(E))$$

given by restriction to S (see [3, p. 109]). In particular, when S is a subset of $U(E)$, there is a unique k-morphism from $k[S]$ to E sending each element of S to itself. The kernel is a prime ideal whose residue field, denoted $k(S)$, we call the *extension of k generated by S*. In keeping with typical notation, we usually write $k(x_1, \ldots, x_n)$ in place of $k(\{x_1, \ldots, x_n\})$. This nomenclature is justified by the concrete interpretation: By its construction, there is a natural k-morphism from $k(S)$ into E, so we may imagine the former as a subfield of the latter in a manner congruent with the embedding of k into E. Any subfield K of E containing k is naturally a k-algebra and, if it contains S as well, then there is a canonical k-morphism $k[S] \to K$. By uniqueness, the diagram



commutes, from which it follows that the morphisms from $k[S]$ to K and to E have the same kernel. This yields a k-morphism $k(S) \to K$ harmonious with the inclusion of $k(S)$ into E, in that the latter is the composition of the tower $k(S) \to K \to E$. It follows that $k(S)$ is the smallest subfield of E containing k and S.

Theorem 2.1. Let E/k be an extension. For any $S, T \subseteq U(E)$, there is a canonical k-isomorphism

$$k(S)(T) \cong k(S \cup T).$$

Proof. Consider each side's isomorphic image in E. Both are the smallest subfield containing k, S, and T and are thus one and the same. □

Adjoining elements is our main method for building (intermediary) extensions. For example, fixing the extension $\mathbb{C}/\mathbb{Q}$, we can adjoin i and the positive 4th root of 2 to get a tower of extensions

$$\mathbb{Q} \to \mathbb{Q}(2^{1/4}) \to \mathbb{Q}(2^{1/4})(i) \cong \mathbb{Q}(2^{1/4}, i) \to \mathbb{C}.$$

The same approach allows us to analyze the elements of an extension E/k. Taking a point $* = \{X\}$, the free-forgetful adjunction provides a correspondence

$$U(E) \cong \hom(*, U(E)) \cong \hom_k(k[X], E),$$

wherein each element $\alpha \in E$ corresponds to a unique morphism $k[X] \to E$ sending X to α, *i.e.* evaluation at α. If the kernel of this morphism is trivial, then $k(\alpha) \cong k(X)$ and α is *transcendental* over k. If it is non-trivial, then it is generated by a unique monic irreducible polynomial $f \in k[X]$ called the *minimal polynomial* of α over k. Then $k(\alpha) \cong k[X]/(f)$—α is identified with X—and α is *algebraic* over k. An extension E/k is *algebraic* if every element of E is algebraic over k and *transcendental* otherwise.

Importantly, all finite extensions are algebraic. Indeed, let E/k be an extension of finite degree n, and fix any $\alpha \in E$. Then the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent over k, and any choice of non-trivial relation of these powers provides a non-zero polynomial vanishing at α.

Theorem 2.2. Let E/k be a field extension. If $\alpha \in E$ is algebraic over k with minimal polynomial f of degree n, then the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $k(\alpha)$ over k. In particular, $[k(\alpha) : k] = \deg(f)$.

Proof. The first thing to understand is the name "minimal polynomial." By the definition of f, if $g(\alpha) = 0$, then $g \in (f)$, so f divides g in $k[X]$. To specify a linear relation of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is to provide a polynomial $g \in k[X]$ of degree strictly less than n with $g(\alpha) = 0$. Then f divides g and $\deg(g) < \deg(f)$, so $g = 0$. It follows that the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent over k.

Recall that $k(\alpha) \cong k[X]/(f)$ via an isomorphism identifying α with X. Therefore, each element of $k(\alpha)$ is of the form $g(\alpha)$ for some $g \in k[X]$. Let $y \in k(\alpha)$ be arbitrary, and choose such a suitable g. Performing Euclidean division, we have $g = qf + r$, where $r \in k[X]$ has degree strictly less than n. Then

$$y = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha).$$

This exhibits y as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ over k. It follows that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $k(\alpha)$. □

Consequently, adjoining finitely-many algebraic elements to a field yields a finite extension. Of course, these elements have to come from some ambient field. Often, however, we find ourselves working with naught but a base field k and a polynomial $f \in k[X]$ we very much would like to vanish. When f is non-constant,

the ideal (f) is contained in a maximal ideal $\mathfrak{m}$, and we have a field extension $k \to k[X]/\mathfrak{m}$. The image α of X in the quotient is a root of f. In other words, every non-constant polynomial over k has a root in an extension of k. Furthermore, if f is monic and irreducible, then $\mathfrak{m} = (f)$ and f is the minimal polynomial of α.

Theorem 2.3. Let $k \to E \to L$ be a tower of extensions. If L/E and E/k are algebraic, then so is L/k.

Proof. Fix any $\alpha \in L$. Since L/E is algebraic, α has some minimal polynomial f with coefficients $a_0, \ldots, a_n \in E$. Each of these is algebraic over k, so adjoining them yields a tower of finite extensions

$$k \to k(a_0, \ldots, a_n) \to k(a_0, \ldots, a_n, \alpha).$$

It follows from the tower theorem that α is algebraic over k. □

Recall the tower constructed above:

$$\mathbb{Q} \to \mathbb{Q}(2^{1/4}) \to \mathbb{Q}(2^{1/4}, i) \to \mathbb{C}.$$

The algebraicity of the extension $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$ can be inferred either from its finiteness—in particular,

$$[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

—or from the algebraicity of each intermediary extension. A comfortable application of the tower theorem give us a basis

$$\{1, 2^{1/4}, 2^{1/2}, 2^{3/4}, i, 2^{1/4}i, 2^{1/2}i, 2^{3/4}i\}$$

for $\mathbb{Q}(2^{1/4}, i)$ over $\mathbb{Q}$. We can consider further steps, some ever-ascending tower

$$\mathbb{Q} \to \mathbb{Q}(2^{1/4}) \to \mathbb{Q}(2^{1/4}, i) \to \cdots \to \mathbb{C}.$$

And it very well may be that each step is algebraic and thus as comprehensible as those already taken, but this is not at all guaranteed. To see this, note that there are certainly no more algebraic elements of $\mathbb{C}$ than polynomials in $\mathbb{Q}[X]$. Letting $\mathbb{Q}[X]_{<n}$ be the set of of rational polynomials of degree less than n, we see that

$$\mathbb{Q}[X] = \bigcup_{n \geqslant 1} \mathbb{Q}[X]_{<n},$$

As each of these constituents is equinumerous with the set $\mathbb{Q}^n$, thus countable, $\mathbb{C}$ possesses at most countably-many algebraic elements, which stand as exceptional points in an uncountable whole.

Algebraicity is a kind of foothold: In all cases, focusing on an algebraic element yields a finite extension whose structure is summarized by a single polynomial. In contrast, transcendental elements have too fine a nature for our present methods to grab hold—only the analytic has purchase. If we ascend along the algebraic, what lies at the summit?

An *algebraic closure* of k is an algebraic extension $\overline{k}/k$ for which every algebraic E/k admits a k-morphism $E \to \overline{k}$. Note that this embedding need not be unique, so algebraic closures are not quite terminal objects. A field is *algebraically-closed* if it is an algebraic closure of itself, *i.e.* if the identity morphism $k \to k$ is an algebraic closure.

Theorem 2.4. A field k is algebraically-closed if and only if every algebraic extension $k \to E$ is an isomorphism.

Proof. Suppose k is algebraically-closed, and let E/k be an algebraic extension. Since k/k is an algebraic closure, there is a k-morphism $E \to k$, meaning the composition

$$k \to E \to k$$

is the identity. By the tower theorem,

$$[k : E][E : k] = [k : k] = 1,$$

hence $[E : k] = 1$ and $k \to E$ is surjective, hence an isomorphism.

Conversely, if every algebraic E/k corresponds to an isomorphism $\varphi : k \to E$, then $\varphi^{-1} : E \to k$ is the desired k-morphism. □

In other words, one knows they have reached the peak of the mountain when they can ascend no further.

Theorem 2.5. Every field k admits an algebraic extension $\overline{k}/k$ such that $\overline{k}$ is algebraically-closed.

Proof. Let S be the set of all monic irreducibles in $k[X]$, and let $X_S = \{X_f\}$ be a set of indeterminates indexed by the elements of S. Consider the ideal $\mathfrak{a}$ of $k[X_S]$ generated by all elements of the form $f(X_f)$ with $f \in S$. To see that $\mathfrak{a}$ is a proper ideal, assume $1 \in \mathfrak{a}$, so there are $f_1, \ldots, f_n \in S$ with corresponding $c_1, \ldots, c_n \in k[X_S]$ such that

$$1 = \sum_{i=1}^{n} c_i f_i(X_{f_i})$$

We can form a finite tower of extensions

$$k \to k(\alpha_1) \to \cdots \to k(\alpha_1, \ldots, \alpha_n) = E,$$

where each α_i is a root of f_i. Using the free-forgetful adjunction, there is a unique morphism $k[X_S] \to E$ sending each X_{f_i} to α_i and every other X_f to 0. Applying this morphism to the equation above, we get $1 = 0$ in E, a contradiction. Therefore, $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{m}$. Quotienting yields a field extension

$$k \to k_1 = k[X_S]/\mathfrak{m}$$

in which every irreducible in $k[X]$ has a root.

Let S_1 be the set of all monic irreducibles over k_1, and repeat the construction above with k_1 in place of k and S_1 in place of S. This yields an extension $k_1 \to k_2$ in which every irreducible in $k_1[X]$ has a root. Continuing in this manner, we obtain a tower of extensions

$$k = k_0 \to k_1 \to k_2 \to \cdots.$$

Let $K = \varinjlim k_i$, so each k_i admits a morphism $k_i \to K$. Importantly, we have an extension K/k. Let $\overline{k}$ be the set of all elements of K algebraic over k. Clearly, k is contained in $\overline{k}$, and for any $\alpha, \beta \in \overline{k}$, we have finite extensions

$$k \to k(\alpha) \to k(\alpha, \beta),$$

so $k(\alpha, \beta)/k$ is algebraic and, importantly, contained in $\overline{k}$. Therefore, $\overline{k}/k$ is an (algebraic) field extension.

Furthermore, $\overline{k}$ is algebraically-closed. Indeed, let $E/\overline{k}$ be algebraic, and fix any $\alpha \in E$ with minimal polynomial $f \in \overline{k}[X]$. The polynomial f has coefficients $a_0, \ldots, a_n \in \overline{k}$. For sufficiently large N, the a_i's all lie in k_N, so f, being monic and irreducible, has a root in $k_{N+1} \subseteq \overline{k}$. But f is irreducible, so this means that $\deg(f) = 1$, hence α lies in the image of $\overline{k}$ in E. It follows that $\overline{k} \to E$ is surjective, hence an isomorphism. □

Theorem 2.6. An algebraic extension $\overline{k}/k$ is an algebraic closure if and only if $\overline{k}$ is algebraically-closed. Consequently, any two algebraic closures of k are k-isomorphic.

Proof. Suppose $\overline{k}/k$ is an algebraic closure, and choose an algebraic extension K/k such that K is algebraically-closed. Since $\overline{k}$ is an algebraic closure, there is a k-morphism $K \to \overline{k}$. For each $\alpha \in \overline{k}$, the minimal polynomial $f \in k[X]$ of α can be viewed as an element of $K[X]$ via K/k, and since $K \to \overline{k}$ is a k-morphism, evaluation at α sends $f \in K[X]$ to 0. Therefore, the extension $K/\overline{k}$ is algebraic. But K is algebraically-closed, so $\overline{k} \to K$ is an isomorphism.

Conversely, suppose $\overline{k}$ is algebraically-closed. Let L/k be algebraic, and consider the set Σ of all k-morphisms $E \to \overline{k}$ with $k \subseteq E \subseteq L$; for example, $\overline{k}/k \in \Sigma$. Define a partial ordering on Σ as follows: write

$$E \leqslant E'$$

if $E \subseteq E'$ and the morphism $E' \to \overline{k}$ restricts to $E \to \overline{k}$. Let $\{E_i\}_i$ be a non-empty chain in Σ with directed union $E = \bigcup_i E_i$. Then E is a field, $k \subseteq E \subseteq L$, and E inherits an embedding $E \to \overline{k}$ from the E_i, so E is an upper bound for our chain in Σ. By Zorn's lemma, Σ has a maximal element M.

Fix any $\alpha \in L$, and let f be the minimal polynomial of α over M. Via the extension $\overline{k}/M$, we may view f as a polynomial in $\overline{k}[X]$. Choose an algebraic extension of $\overline{k}$ in which f has a root. Since $\overline{k}$ is algebraically-closed, this extension is trivial, hence the field $\overline{k}$ contains a root α' of f. Consider the morphism $M[X] \to \overline{k}$ evaluating at α'. The kernel of this morphism is (f) so, quotienting and utilizing the canonical k-isomorphism $M(\alpha) \cong M[X]/(f)$, we obtain a k-morphism $M(\alpha) \to \overline{k}$. Then $M(\alpha) \geqslant M$, so $M(\alpha) = M$ and $\alpha \in M$ by maximality. It follows that $M = L$, hence $\overline{k}/k$ is an algebraic closure. $\square$

3. SEPARABILITY

AMONG fields, we are burdened by choice. At the end of the last section, we proved that every field has an algebraic closure, and already we feel at the tip of our tongue the tendency towards the definite, the desire to say "*the* algebraic closure." Unfortunately, while any two algebraic closures of k are k-isomorphic, they are not uniquely so. Fixing an algebraic closure $\overline{k}/k$, our problem of identifying algebraic closures generalizes to that of embedding algebraic extensions in $\overline{k}$—this is always possible, but rarely can it be done in a unique manner.

We are interested in the set of k-morphisms $\hom_k(E, \overline{k})$ and, in particular, determining when it is a singleton. In the simple case $E = k(\alpha)$, this set is an old friend: Denoting by f the minimal polynomial of α, each k-morphism $k(\alpha) \to \overline{k}$ sends α to a root of f in $\overline{k}$ and, in fact, is determined by this value. In the other direction, to each root α' of f in our algebraic closure, there is a k-morphism $k(\alpha) \to \overline{k}$ sending α to α'—it appears as a quotient of the k-morphism evaluating at α'. In short, $\hom_k(E, \overline{k})$ is in one-to-one correspondence with the roots of f in $\overline{k}$.

Consequently, a simple extension $k(\alpha)$ embeds canonically if and only if the minimal polynomial of α has but one root in $\overline{k}$. Certainly this is the case when $\alpha \in k$. For a more exotic example, consider the field $\mathbb{F}_p(t)$ obtained by adjoining an indeterminate to a finite prime field. Over this field, $X^p - t$ is irreducible—indeed, in an algebraic closure,

$$X^p - t = (X - t^{1/p})^p,$$

so if this polynomial were reducible, we would have $t^{m/p} \in \mathbb{F}_p(t)$ for some $1 \leqslant m < p$, a contradiction—and we can form the non-trivial extension $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$, which admits only one $\mathbb{F}_p(t)$-morphism into any algebraic closure $\overline{\mathbb{F}_p(t)}$.

Such considerations prompt us to distinguish the cardinality of $\hom_k(E, \overline{k})$; we dub it the *separability degree* of E over k and denote it by $[E : k]_s$. That this value is independent of our choice of algebraic closure can be verified by casting any isomorphism between algebraic closures into the functor $\hom_k(E, -)$.

Theorem 3.1 (Tower Theorem, redux)**.** Let $k \to E \to L$ be a tower of algebraic field extensions. Then

$$[L : k]_s = [L : E]_s [E : k]_s.$$

Proof. Let $\{\varphi_i\}_i = \hom_k(E, \overline{k})$, so there are $[E : k]_s$ distinct φ_i's in total. For each i, the extension φ_i is an algebraic closure, since it's algebraic—each element of $\overline{k}$ is the root of a polynomial over k, hence over E via E/k—and $\overline{k}$ is algebraically-closed. Therefore, if we let $X_i = \hom_E(L, \varphi_i)$ for each i, then $|X_i| = [L : E]_s$ for all i.

Suppose $X_i \cap X_j$ is non-empty; choosing $\psi \in X_i \cap X_j$, we see that φ_i and φ_j are each the restriction of ψ to E, hence $i = j$. Therefore, the X_i's are pairwise disjoint and

$$\left| \bigcup_i X_i \right| = \sum_i |X_i| = [L : E]_s [E : k]_s,$$

and we are done. □

In the simple case $k(\alpha)/k$, the separability degree is the number of roots of the minimal polynomial f of α in our algebraic closure. Therefore,

$$[k(\alpha) : k]_s \leqslant \deg(f) = [k(\alpha) : k].$$

An algebraic element α of E/k is *separable* over k if equality holds above. Clearly, $\alpha \in E$ is separable over k if and only if its minimal polynomial $f \in k[X]$ has no multiple roots in $\overline{k}$. We call such polynomials *separable* as well, so a separable element is an algebraic element with separable minimal polynomial.

Theorem 3.2. A polynomial $f \in k[X]$ is separable if and only if it is coprime to its (formal) derivative in $k[X]$.

Proof. Suppose f is separable, and let $\alpha \in \overline{k}$ be a root of f. Then $f(X) = (X - \alpha)q(X)$ for some $q \in \overline{k}[X]$, and $q(\alpha) \neq 0$ since f has no multiple roots. We compute

$$f'(X) = q(X) + (X - \alpha)q'(X),$$

from which it follows that $f'(\alpha) \neq 0$, hence f and f' share no roots in $\overline{k}$. Therefore, f and f' are coprime, for a non-trivial common divisor $h \in k[X]$ would entail a common root in $\overline{k}$.

Conversely, suppose f and f' are coprime in $k[X]$. Then there are polynomials $s, t \in k[X]$ with $sf + tf' = 1$. This identity remains true when lifted to $\overline{k}[X]$ via the extension $\overline{k}/k$, so f and f' are coprime over $\overline{k}$. Now assume f is inseparable, *i.e.* $f(X) = (X - \alpha)^2 q(X)$ for some $\alpha \in \overline{k}$ and $q \in \overline{k}[X]$. Then

$$f'(X) = (X - \alpha)(2q(X) + (X - \alpha)q'(X)),$$

and we have a contradiction. □

The most pertinent consequence of this is that every irreducible polynomial over a characteristic-zero field k is separable. Indeed, if $f \in k[X]$ is irreducible, then f has positive degree, hence $f' \neq 0$; were there a non-trivial common divisor h of f and f' then, by the irreducibility of f, we would have $h = f$, hence $f' = 0$

since $\deg(f') < \deg(f)$, a contradiction. Consequently, there are no non-trivial, uniquely-embedding extensions of k.

Theorem 3.3. Let E/k be an algebraic extension, p the characteristic of k. If $\alpha \in E$, there is a power $q = p^n$ of p such that α^q is separable over k.

Proof. In light of the preceding discussion, we may assume $p > 0$. If α is separable over k, $q = 1$ suffices; assume, then, that α is inseparable, and let $f \in k[X]$ be its minimal polynomial. Then f is inseparable, so f and f' have a non-trivial common divisor and, since f is irreducible, this divisor is none other than f itself. Since $\deg(f') < \deg(f)$, this tells us that $f' = 0$. Writing $f(X) = \sum_{i=0}^{n} a_i X^i$, we have

$$\sum_{i=1}^{n} i a_i X^{i-1} = 0,$$

so $a_i = 0$ for all i not divisible by p. It follows that f is a polynomial in X^p, *i.e.* $f(X) = g(X^p)$ for some $g \in k[X]$. Choose $n \geqslant 1$ to be maximal such that there is $g \in k[X]$ with $f(X) = g(X^q)$, where $q = p^n$. Then g is separable—otherwise, the same argument as above would allow us to choose n even larger—and inherits irreducibility from f. It follows that g is the minimal polynomial of α^q, and the latter is separable over k. □

An algebraic extension E/k is *purely inseparable* if the only separable elements of E are those lying in k. From the previous theorem, E/k is purely inseparable if and only if to each $\alpha \in E$, there corresponds a power q of the characteristic such that $\alpha^q \in k$. Thus, we say that $\alpha \in E$ is *purely inseparable* over k if $\alpha^q \in k$ for some such q. The key point is that an extension embeds canonically into an algebraic closure if and only if it is purely inseparable.

Of course, we are often interested in extensions that are not purely inseparable—for example, any non-trivial extension of characteristic-zero fields. In light of this, we shift our focus to the other extreme, forgoing canonicity and considering those algebraic extensions E/k for which every element of E is separable over k; we call these *separable*.

Theorem 3.4. Let $k \to K \to E \to L$ be a tower of algebraic extensions. If L/k is separable, then so is E/K.

Proof. Fix any $\alpha \in E$. Then α, lying in L, is separable over k. Let f and g be the minimal polynomials of f over k and K respectively. Via the extension K/k, we may view f as a polynomial in $K[X]$; as f vanishes at α, there is some $h \in K[X]$ for which $f = gh$. Observe, then, that

$$f' = gh' + g'h.$$

Any common divisor of g and g' is therefore a common divisor f and f', which are coprime; it follows that g and g' are coprime, and α is separable over K. □

Theorem 3.5. If E/k is a finite extension, then

$$[E : k]_s \leqslant [E : k],$$

with equality holding precisely when E/k is separable.

Proof. Since E/k is finite, we can write it as the composition of a tower

$$k \to k(\alpha_1) \to \cdots \to k(\alpha_1, \ldots, \alpha_n) = E$$

for some $\alpha_1, \ldots, \alpha_n \in E$. Let $k_i = k(\alpha_1, \ldots, \alpha_i)$ and $k_0 = k$, so for each $1 \leqslant i \leqslant n$, the extension $k_i = k_{i-1}(\alpha_i)$ and

$$[k_i : k_{i-1}]_s \leqslant [k_i : k_{i-1}].$$

By the tower theorems,

$$[E : k]_s = \prod_{i=1}^{n} [k_i : k_{i-1}]_s \leqslant \prod_{i=1}^{n} [k_i : k_{i-1}] = [E : k]. \tag{1}$$

If equality holds, then for any $\alpha \in E$, the tower theorem yields

$$[E : k(\alpha)]_s [k(\alpha) : k]_s = [E : k]_s = [E : k],$$

and we have

$$[k(\alpha) : k] \geqslant [k(\alpha) : k]_s = \frac{[E : k]}{[E : k(\alpha)]_s} \geqslant \frac{[E : k]}{[E : k(\alpha)]} = [k(\alpha) : k],$$

hence $[k(\alpha) : k]_s = [k(\alpha) : k]$, and α is separable over k.

Conversely, suppose E/k is separable. Then, for each $1 \leqslant i \leqslant n$, the extension k_i/k_{i-1} is separable, hence

$$[k_i : k_{i-1}]_s = [k_i : k_{i-1}],$$

from which equality in (1) is trivial. □

Theorem 3.6. If E/k is a separable extension, and if $[E : k]$ is infinite, then so is $[E : k]_s$.

Proof. Since E/k is infinite, there is an infinite tower of finite extensions

$$k_0 \to k_1 \to k_2 \to \cdots$$

with $k_0 = k$, $k_i = k_{i-1}(\alpha_i)$ for some $\alpha_i \in E$, and $[k_i : k_{i-1}] \geqslant 2$ for all $i \geqslant 1$. Since E/k is separable, so is each k_i/k_{i-1}. For all $N \geqslant 1$, we have

$$[E : k]_s \geqslant \prod_{i=1}^{N} [k_i : k_{i-1}]_s = \prod_{i=1}^{N} [k_i : k_{i-1}] \geqslant 2^N.$$

Therefore, $[E : k]_s$ is infinite. □

For any algebraic extension E/k, let E_s be the set of all separable elements of E. Clearly, $k \subseteq E_s$. For any $\alpha, \beta \in E_s$, there is a tower

$$k \to k(\alpha) \to k(\alpha, \beta).$$

Since α and β are separable over k—consequently, β is separable over $k(\alpha)$—we have that

$$\begin{aligned} [k(\alpha, \beta) : k]_s &= [k(\alpha, \beta) : k(\alpha)]_s [k(\alpha) : k]_s \\ &= [k(\alpha, \beta) : k(\alpha)][k(\alpha) : k] = [k(\alpha, \beta) : k], \end{aligned}$$

so $k(\alpha, \beta)/k$ is separable. In particular, $k(\alpha, \beta) \subseteq E_s$, and E_s is a field. Thus, E/k induces a separable extension E_s/k called the *separable closure* of k in E.

Theorem 3.7. A k-morphism $\varphi : E \to L$ of algebraic extensions is determined by its restriction to E_s.

Proof. Suppose we have two k-morphisms $\varphi, \psi : E \rightrightarrows L$ that agree on E_s. Fix any inseparable element $\alpha \in E$. There is some $q = p^n$, where p is the characteristic of k, such that α^q is separable over k. Now, for any $\beta \in E$, we have that $\beta^q = \sigma_E^n(\beta)$, where σ_E is the Frobenius endomorphism of E. Therefore,

$$\sigma_E^n \varphi(\alpha) = \varphi(\alpha^q) = \psi(\alpha^q) = \sigma_E^n \psi(\alpha).$$

But σ_E^n, being a morphism of fields, is necessarily injective, so this shows that $\varphi(\alpha) = \psi(\alpha)$; the author refers to this technique of repeatedly applying the Frobenius endomorphism as *Frobenating*. □

Consequently, restriction yields a bijection $\hom_k(E, \bar{k}) \cong \hom_k(E_s, \bar{k})$. In other words, when considering the various embeddings of an algebraic extension into an algebraic closure, nothing is lost by assuming separability.

4. Galois Theory

We are interested in the non-canonical: Algebraic extensions that do not embed uniquely into algebraic closures. From the previous section, we know that we can replace the term "algebraic" with "separable" in its first appearance; what about the second? If $\overline{k}/k$ is an algebraic closure and E/k an algebraic extension, there is a k-morphism $E \to \overline{k}$. If E is, in fact, separable, then this morphism sends the elements of E to separable elements of $\overline{k}$. Thus, we actually have a k-morphism $E \to \overline{k}_s$.

In other words, $\overline{k}_s/k$ is a separable extension to which every other separable E/k admits a k-morphism. Extension Ω/k with this property are called *separable closures*. Working in analogy to section 2, a field k is *separably-closed* if the identity morphism $k \to k$ is a separable closure. Predictably, k is separably-closed if and only if every separable extension $k \to E$ is an isomorphism; an extension Ω/k is a separable closure if and only if it is separable and Ω is separably-closed; and any two separable closures of k are k-isomorphic.

We encounter the same problem with separable closures as we did with the algebraic: We cannot canonically identify them; we cannot say "*the* separable closure." This failure of canonicity is a consequence of the the (potential) existence of distinct k-isomorphisms $\Omega \rightrightarrows \Omega'$ between two separable closures; any such troublesome pair yields a non-trivial k-automorphism of Ω via the diagram

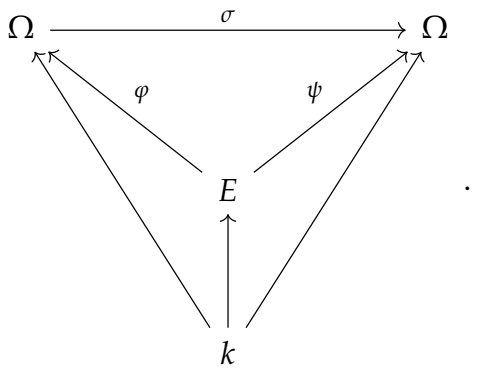
$$\Omega \;\substack{\longleftarrow \\ \longrightarrow}\; \Omega' \ .$$

This prompts us to consider the group $\mathscr{G}_k = \mathrm{Aut}(\Omega/k)$ of k-automorphisms of Ω, the *absolute Galois group* of k. Some justification is needed for our usage of definite article: If Ω and Ω' are separable closures of k, fixing any k-isomorphism φ between the two induces an isomorphism between the automorphism groups sending $\sigma \in \mathrm{Aut}(\Omega/k)$ to $\varphi\sigma\varphi^{-1} \in \mathrm{Aut}(\Omega'/k)$. This shows that $\mathscr{G}_k$ is well-defined up to inner automorphism.

Now, if k is separably-closed, the identity $\mathrm{id} : k \to k$ is a separable closure, so for any other separable closure Ω/k and k-isomorphism $\varphi : k \to \Omega$, the extension Ω/k is one and the same with $\varphi \circ \mathrm{id} = \varphi$, and thus separable closures of k are unique up to *unique* isomorphism, and $\mathscr{G}_k$ is trivial. The converse is an immediate consequence of the next theorem. Since every extension of a characteristic-zero field is separable, and since the complex numbers $\mathbb{C}$ are algebraically-closed, $\mathbb{C}_S = \mathbb{C}$ is separably-closed and $\mathscr{G}_{\mathbb{C}}$ is trivial. However, fields are not separably-closed in general and neither are their absolute Galois groups.

Theorem 4.1. Let E/k be an separable extension. The group $\mathscr{G}_k$ acts transitively on $\hom_k(E, \Omega)$ by left composition.

Proof. Each $\varphi \in \hom_k(E, \Omega)$ is an separable extension of the form Ω/E, and Ω is separably-closed, hence each φ is a separable closure of Ω. It follows that for any $\varphi, \psi \in \hom_k(E, \Omega)$, there is an E-morphism $\sigma : \Omega \to \Omega$ such that the following diagram commutes:



Then $\sigma \in \mathscr{G}_k$ sends φ to ψ, so $\mathscr{G}$'s action on $\hom_k(E, \Omega)$ is transitive. □

Thus, to each finite separable extension E/k, there corresponds a finite transitive $\mathscr{G}_k$-set $\mathscr{F}(E) = \hom_k(E, \Omega)$. We call the contravariant functor $\mathscr{F}(-)$ the *fiber functor*, and the set $\mathscr{F}(E)$ the *fiber* over E.

Fix a finite separable extension E/k. Each φ in the fiber of E has a stabilizer $\mathscr{G}_\varphi = \mathrm{Aut}(\varphi)$ in $\mathscr{G}_k$. Note that this group is an absolute Galois group of E and is thus determined up to inner automorphism; it follows that the conjugates of $\mathscr{G}_\varphi$ are precisely the subgroups of the form $\mathscr{G}_\psi$ for $\psi \in \mathscr{F}(E)$. Therefore, if any one of the $\mathscr{G}_\varphi$ is normal, then they all agree, and we may unambiguously refer to the subgroup $\mathscr{G}_E$; we say that E/k is *Galois*. More generally, algebraic—but not necessarily separable—extensions satisfying an analogous condition are called *normal*. Since we are only considering separable extensions, we use the two terms interchangeably.

The *Galois group* of a Galois extension E/k is the quotient $\mathrm{Gal}(E/k) = \mathscr{G}_k/\mathscr{G}_E$. Since $\mathscr{G}_E$ is the stabilizer of any $\varphi \in \mathscr{F}(E)$ under the (transitive) action of the $\mathscr{G}_k$, we have

$$|\mathrm{Gal}(E/k)| = (\mathscr{G}_k : \mathscr{G}_E) = |\mathscr{F}(E)| = [E : k]_s.$$

Thus, when E/k is finite, $|\mathrm{Gal}(E/k)| = [E : k]$.

For a subgroup H of $\mathscr{G}_k$, let Ω^H be the set of all elements of Ω fixed by the action of H; it is easily seen that Ω^H is a subfield of Ω containing k, so we have an induced separable extension Ω^H/k.

Theorem 4.2. Let E/k be a finite Galois extension, $N = \mathscr{G}_E$. Each φ in the fiber of E is a k-isomorphism $E \cong \Omega^N$, and N is the set of all k-automorphisms of Ω fixing Ω^N.

Proof. Fix a k-morphism $\varphi : E \to \Omega$. Since E/k is Galois, the subgroup $\mathrm{Aut}(\varphi) = N$. Clearly, $\varphi(E) \subseteq \Omega^N$, so φ induces an extension Ω^N/k. Letting $H = \mathrm{Aut}(\iota)$, where $\iota : \Omega^N \to \Omega$ is the canonical inclusion, we have that $N \subseteq H$. Then

$$\begin{aligned}[\Omega^N : k] \geqslant [E : k] &= |\mathrm{Gal}(E/k)| \\ &= (\mathscr{G}_k : N) \\ &\geqslant (\mathscr{G}_k : H) = [\Omega^N : k]_s = [\Omega^N : k],\end{aligned}$$

so $[\Omega^N : k] = [E : k]$ and $\Omega^N = \varphi(E)$.

By definition, every element of N fixes all of Ω^N. Conversely, let σ be an element of $\mathscr{G}_k$ fixing Ω^N. By the preceding paragraph, the Ω^N is the image of φ, so σ fixes φ; that is, $\sigma \in \mathrm{Aut}(\varphi) = N$, and we are done. □

Theorem 4.3. For a Galois extension E/k, the Galois group $\mathrm{Gal}(E/k) \cong \mathrm{Aut}(E/k)$.

Proof. Let $N = \mathscr{G}_E$. In light of the previous result, we can choose a k-isomorphism $E \cong \Omega^N$, which induces a group isomorphism $\mathrm{Aut}(E/k) \cong \mathrm{Aut}(\Omega^N/k)$. For any $\sigma \in \mathscr{G}_k$, $x \in \Omega^N$, and $\tau \in N$, we have $\tau\sigma(x) = \sigma(y)$ for some $y \in \Omega$, hence $\sigma^{-1}\tau\sigma(x) = y$. Now, since N is normal, $\sigma^{-1}\tau\sigma \in N$ and $y = x$. It follows that $\tau\sigma(x) = \sigma(x)$, so $\sigma(x) \in \Omega^N$. Thus, we have a morphism of groups $\Phi : \mathscr{G}_k \to \mathrm{Aut}(\Omega^N/k)$ sending each automorphism to its restriction to Ω^N. Each $\sigma' \in \mathrm{Aut}(\Omega^N/k)$ induces a separable closure $\Omega^N \to \Omega$; since the standard inclusion $\iota : \Omega^N \to \Omega$ is a separable closure, there is an Ω^N-automorphism σ of Ω—in particular, a k-automorphism—such that $\sigma \circ \iota = \sigma'$. But this left-hand side is just $\Phi(\sigma)$, so Φ is surjective. By the previous result, $\Phi(\sigma)$ is the identity if and only if $\sigma \in N = \mathscr{G}_E$, so Φ factors to yield an isomorphism

$$\mathrm{Gal}(E/k) = \mathscr{G}_k/\mathscr{G}_E \cong \mathrm{Aut}(\Omega^N/k),$$

and we are done. □

Theorem 4.4. Every finite separable extension of k admits a k-morphism into a finite Galois extension.

Proof. Let E/k be finite and separable. Define $N = \bigcap_\varphi \mathscr{G}_\varphi$, where φ ranges over the fiber of E. Then N is normal—it is the intersection of all the conjugates of any $\mathscr{G}_\varphi$—and Ω^N/k is separable. Let $\iota : \Omega^N \to \Omega$ be the canonical inclusion, and suppose $\sigma \in \mathscr{G}_k$ fixes ι, *i.e.* σ fixes Ω^N. Clearly, if $\varphi \in \mathscr{F}(E)$, then N fixes every element in the image of φ, so said image in contained in Ω^N and is thus fixed by σ as well. It follows that $\sigma \in \mathscr{G}_\varphi$ for all $\varphi \in \mathscr{F}(E)$, hence $\sigma \in N$ and $\mathrm{Aut}(\iota) \subseteq N$. The reverse inclusion is trivial, so Ω^N/k is Galois; any choice of $\varphi \in \mathscr{F}(E)$ provides the desired k-morphism.

All that remains is to show that Ω^N/k is finite. For each $\varphi \in \mathscr{F}(E)$, the group $\mathscr{G}_\varphi$ is the stabilizer of the action of $\mathscr{G}_k$ on the fiber of E, which is finite since E/k is, and thus has finite index. Therefore, N is a finite intersection of groups of finite index, so has finite index itself. Finally,

$$[\Omega^N : k] = [\Omega^N : k]_s = (\mathscr{G}_k : N)$$

is finite. □

Theorem 4.5. For a finite group G of automorphisms of a field E, $\mathrm{Aut}(E/E^G) = G$.

The following proof is adapted from [2, p. 36].

Proof. Let $k = E^G$, $G = \{\sigma_1, \ldots, \sigma_n\}$, and consider any distinct $x_1, \ldots, x_N \in E$ with $N > n$. Let T be the linear transformation from $E^N \to E^n$ with matrix $(\sigma_i(x_j))$ with respect to the standard bases. Since $N > n$, the kernel of T is non-trivial. Choose non-zero $(y_1, \ldots, y_N) \in \ker(T)$ such that a minimum number of the y_i's are non-zero. Without loss of generality, we may assume $y_1 \neq 0$; up to a scalar (e.g., y_1^{-1}), we may also assume that $y_1 \in k$. Now, suppose that there is some y_m not in k; there corresponds a σ_i with $\sigma_i(y_m) \neq y_m$. Since left multiplication by σ_i permutes G, *i.e.* $\sigma_i\sigma_j = \sigma_{\tau(j)}$ for some fixed permutation τ of $\{1, \ldots, n\}$, and since

$$\sigma_i \sum_{j=1}^{N} \sigma_r(x_j)y_j = \sum_{j=1}^{N} \sigma_i\sigma_r(x_j)\sigma_i(y_j) = \sum_{j=1}^{N} \sigma_{\tau(r)}(x_j)\sigma_i(y_j) = 0$$

for each $1 \leqslant r \leqslant n$, we have another element

$$(\sigma_i(y_1), \ldots, \sigma(y_N)) = (y_1, \sigma_i(y_2), \ldots, \sigma_i(y_N))$$

of the kernel of T. Subtracting the two, we see that

$$(0, y_2 - \sigma_i(y_2), \ldots, y_N - \sigma_i(y_N)) \in \ker(T).$$

But this element is non-zero, since $y_m - \sigma_i(y_m) \neq 0$, and has fewer non-zero elements than $(y_1, \ldots, y_N)$, a contradiction. Therefore, $y_i \in k$ for all $1 \leqslant i \leqslant N$. It follows that

$$0 = \sum_{j=1}^{N} \sigma_1(x_j)y_j = \sigma_1 \sum_{j=1}^{N} y_j x_j,$$

hence $\sum_{j=1}^{N} y_j x_j = 0$ and the x_j's are linearly dependent over k. Consequently, $[E : k] \leqslant n = |G|$.

Clearly, $G \leqslant \mathrm{Aut}(E/k)$. Fix an algebraic closure $\bar{k}$ of k. Since E/k is finite, it is algebraic and thus admits a k-morphism $\iota : E \to \bar{k}$. Each $\sigma \in \mathrm{Aut}(E/k)$ induces another such k-morphism $\iota \circ \sigma$, and if $\iota \circ \sigma = \iota \circ \tau$, then $\iota \circ \sigma\tau^{-1} = \iota$, hence $\sigma\tau^{-1}$ fixes E and $\sigma = \tau$. Therefore,

$$[E : k] \leqslant |G| \leqslant |\mathrm{Aut}(E/k)| \leqslant [E : k]_s \leqslant [E : k],$$

hence $G = \mathrm{Aut}(E/k)$. □

Theorem 4.6 (Galois Correspondence)**.** The fiber functor $\mathscr{F}(-)$ is an anti-equivalence between the categories of finite separable extensions of k and finite transitive $\mathscr{G}_k$-sets.

Proof. It is sufficient to show that $\mathscr{F}(-)$ is fully faithful and essentially surjective. Beginning with the latter, let X be a finite transitive $\mathscr{G}_k$-set. We want to show that X is isomorphic to some $\mathscr{F}(E)$. Let $S \leqslant \mathscr{G}_k$ be the stabilizer of a point $* \in X$. The index of S is the cardinality of the orbit of $*$; since the action of $\mathscr{G}_k$ on X is transitive, $(\mathscr{G}_k : S) = |X|$ is finite. Consider the separable extension Ω^S/k, and let $H = \mathrm{Aut}(\Omega/\Omega^S)$ by the group of Ω^S-automorphisms of Ω. Clearly, $S \subseteq H$, so H has finite index. Now, $\mathscr{G}_k$ acts transitively on the set $\hom_k(\Omega^S, \Omega)$, and H is the stabilizer of the canonical inclusion $\iota : \Omega^S \to \Omega$ under this action, hence

$$[\Omega^S : k]_s = |\hom_k(\Omega^S, \Omega)| = (\mathscr{G}_k : H)$$

is finite; separability then implies Ω^S/k is finite.

Consequently, we can choose a finite Galois extension Ω^N containing Ω^S, where N is a normal subgroup of $\mathscr{G}_k$; in fact, N is a (normal) subgroup of H. Then Ω^N is invariant under the action of $\mathscr{G}_k$, so we may restriction the action to this subfield. An element of $\mathscr{G}_k$ fixes Ω^N if and only if its an element of N by **Theorem 4.2.**, so this action factors through $\mathscr{G}_k/N = \mathrm{Gal}(\Omega^N/k)$, and since Ω^N/k is finite, so is the quotient. Observe that

$$(\Omega^N)^{SN/N} = (\Omega^N)^{SN} = \Omega^S = \Omega^H = (\Omega^N)^{H/N}.$$

By the preceding theorem, $SN/N = H/N$. But the inclusion $SN/N \to H/N$ is just the morphism of groups induced by the inclusion $S \to H$ when quotienting H by N, since $SN/N \cong S/(S \cap N)$, so this, in fact, shows that this inclusion is surjective; concretely, $S = H$.

What remains to be shown is that $\mathscr{F}(\Omega^S) \cong X$. We know that $X \cong \mathscr{G}_k/S$ as $\mathscr{G}_k$-sets, so it is sufficient to show that $\mathscr{F}(\Omega^S) \cong \mathscr{G}_k/S$ as well. Define $\Phi : \mathscr{G}_k \to \mathscr{F}(\Omega^S), \sigma \mapsto \sigma \circ \iota$. Note that $\Phi(\sigma) = \Phi(\tau)$ if and only if $\sigma^{-1}\tau$ fixes Ω^S, *i.e.* $\sigma^{-1}\tau \in S$. Therefore, Φ factors to yield an isomorphism of $\mathscr{G}_k$-sets $\mathscr{G}_k/S \cong \mathscr{F}(\Omega^S)$, and the fiber functor is essentially surjective.

Shifting now to full-faithfulness, we want to show that the fiber functor induces a bijection $\hom_k(E, L) \cong \hom_{\mathscr{G}_k}(\mathscr{F}(L), \mathscr{F}(E))$ for any two finite separable extensions E and L of k. Fix a map of $\mathscr{G}_k$-sets $f : \mathscr{F}(L) \to \mathscr{F}(E)$. If $\varphi \in \hom_k(E, L)$ satisfies $\mathscr{F}(\varphi) = f$, then

$$* \circ \varphi = \mathscr{F}(\varphi)(*) = f(*)$$

for each point $* \in \mathscr{F}(L)$. In fact, since the action of $\mathscr{G}_k$ is transitive, f is determined by its value on any one such point; fixing $*$, we have $\mathscr{F}(\varphi) = f$ if and only if $* \circ \varphi = f(*)$, and φ, should it exist, is unique.

If σ is in the stabilizer S_* of $*$, then

$$\sigma f(*) = f(\sigma *) = f(*),$$

so σ is in the stabilizer $S_{f(*)}$ of $f(*)$ as well. Therefore, taking fixed fields, we see that

$$f(*)(E) \subseteq \Omega^{S_{f(*)}} \subseteq \Omega^{S_*}.$$

Now, by the preceding discussion, we know that Ω^{S_*} is a finite, separable extension of k with $\mathscr{F}(\Omega^{S_*}) \cong \mathscr{F}(L)$. In particular, Ω^{S_*} and L have the same separability degree over k, hence the same degree. Clearly, $*(L)$ is contained in Ω^{S_*}; by the tower theorem,

$$[\Omega^{S_*} : L] = \frac{[\Omega^{S_*} : k]}{[L : k]} = 1,$$

so this shows that $\Omega^{S_*} = *(L)$. Thus, letting $*^{-1} : *(L) \to L$ denote the inverse to L—which exists since $*$, being a morphism of fields, is injective—we have a k-morphism $\varphi = *^{-1} \circ f(*)$ from E to L. Then

$$* \circ \varphi = * \circ *^{-1} \circ f(*) = f(*),$$

and we are done. □

Let L/k be a Galois extension and $k \subseteq E \subseteq L$ an intermediary subfield. We claim that L/E is Galois. Indeed, if Ω is a separable closure of k, then any choice of k-morphism $\iota : E \to \Omega$ is a separable closure of E, and we have $\mathscr{G}_E = \mathrm{Aut}(\iota) \leqslant \mathscr{G}_k$. Since L/E is separable, we may fix an E-morphism $\varphi : L \to \Omega$; then φ is, in particular, a k-morphism and

$$\mathscr{G}_L = \mathrm{Aut}(\varphi) \leqslant \mathrm{Aut}(\iota) = \mathscr{G}_E.$$

Since $\mathscr{G}_L$ is normal in $\mathscr{G}_k$, it is normal in $\mathscr{G}_E$, and L/E is normal. Notice, then, that if we apply the fiber functor to the tower $k \subseteq E \subseteq L$, we get a diagram

$$\begin{array}{ccccc} L & & \mathscr{F}(L) & \ni & * \\ \uparrow & & \downarrow & & \downarrow \\ E & \rightsquigarrow & \mathscr{F}(E) & \ni & *' \\ \uparrow & & \downarrow & & \downarrow \\ k & & \mathscr{F}(k) & \ni & *'' \end{array},$$

where $*$ is any point in the fiber of L/k. Taking stabilizers, we see that

$$S_* \leqslant S_{*'} \leqslant S_{*''}.$$

Now, since L/k is Galois, $S_* = \mathrm{Aut}(\Omega/L)$; similarly, $S_{*''} = \mathscr{G}_k$. Finally, since $*' : E \to \Omega$ is a separable closure, $S_{*'} = \mathrm{Aut}(*')$ is an absolute Galois group $\mathscr{G}_E$ of E. Consequently, we can quotient by S_* to obtain a tower of subgroups:

$$\begin{array}{ccc} \mathrm{Aut}(\Omega/L) & & 1 \\ \downarrow & & \downarrow \\ \mathscr{G}_E & \rightsquigarrow & \mathrm{Gal}(L/E) \\ \downarrow & & \downarrow \\ \mathscr{G}_k & & \mathrm{Gal}(L/k) \end{array}$$

Thus, to each intermediary subfield E of L/k, there corresponds a subgroup $\mathrm{Gal}(L/E)$ of $\mathrm{Gal}(L/k)$.

Theorem 4.7 (Fundamental Theorem of Galois Theory)**.** Let L/k be a Galois extension. The map $E \mapsto \mathrm{Gal}(L/E)$ induces a contravariant, normality-preserving

correspondence between the poset of intermediary subfields of L/k and that of subgroups of $\mathrm{Gal}(L/k)$ with inverse $H \mapsto L^H$. In particular, for intermediary subfields $K \subseteq E$ of L/k,

$$[E : K] = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E));$$

symmetrically, for subgroups $H \leqslant G$ of $\mathrm{Gal}(L/k)$,

$$(G : H) = [E^H : E^G].$$

Proof. Evidently, for intermediary subfields $k \subseteq K \subseteq E \subseteq L$, we have that

$$\mathrm{Gal}(L/E) \leqslant \mathrm{Gal}(L/K).$$

For any subgroup H of $\mathrm{Gal}(L/k)$, we have $\mathrm{Gal}(L/L^H) = \mathrm{Aut}(L/L^H) = H$. In particular, for $H = \mathrm{Gal}(L/E)$, it is clear that $E \subseteq L^H$, and we have

$$[L : L^H] = |H| = [L : E],$$

hence

$$[L^H : E] = \frac{[L : E]}{[L : L^H]} = 1$$

and $L^H = E$. It follows that the map $E \mapsto \mathrm{Gal}(L/E)$ between the lattices of intermediary subfields of L/k and subgroups of $\mathrm{Gal}(L/k)$ is bijective and order-reversing.

Suppose an intermediary field E is normal over k. Then since

$$\mathrm{Gal}(L/E) = \mathrm{Aut}(\Omega/E)/\mathrm{Aut}(\Omega/L),$$

the normality of $\mathrm{Aut}(\Omega/E)$ in $\mathscr{G}_k$ implies the normality of $\mathrm{Gal}(L/E)$ in $\mathrm{Gal}(L/k) = \mathscr{G}_k/\mathrm{Aut}(\Omega/L)$. Symmetrically, suppose N is a normal subgroup of $\mathrm{Gal}(L/k)$. Then

$$N = \mathrm{Gal}(L/L^N) = \mathrm{Aut}(\varphi)/\mathrm{Aut}(\Omega/L)$$

for any k-morphism $\varphi : L^N \to \Omega$, so $\mathrm{Aut}(\varphi)$ is normal in $\mathscr{G}_k$; it follows that L^N/k is normal.

Lastly, for subgroups $H \leqslant G$ of $\mathrm{Gal}(L/k)$,

$$|G| = |\mathrm{Gal}(L/L^G)| = [L : L^G] \text{ and } |H| = |\mathrm{Gal}(L/L^H)| = [L : L^H],$$

so

$$(G : H) = \frac{|G|}{|H|} = \frac{[L : L^G]}{[L : L^H]} = [L^H : L^G].$$

Likewise, for intermediary subfields $K \subseteq E$ of L/k,

$$(\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)) = [L^{\mathrm{Gal}(L/E)} : L^{\mathrm{Gal}(L/K)}] = [E : K],$$

and we are done. □

BIBLIOGRAPHY

[1] Serge Lang. *Algebra*. 3rd edition. Springer New York, NY, 2005.

[2] J. S. Milne. *Fields and Galois Theory*. Ann Arbor, MI: Kea Books, 2022.

[3] Steve Shatz and Jean Gallier. *Algebra*. 2023.

[4] Tamás Szamuely. *Galois Groups and Fundamental Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.