GALOIS THEORY: THE PROOFS, THE WHOLE PROOFS, AND NOTHING BUT THE PROOFS

MARK DICKINSON

Contents

I've adopted a slightly different method of proof from the textbook for many of the Galois theory results. For your reference, here's a summary of the main results and their proofs, without any of that pesky history and motivation—or distracting examples—to get in the way. Just the proofs[1]. Almost all of the hard work lies in three main theorems: Corollary 7.9 (a splitting field of a separable polynomial is Galois), Theorem 8.1 (linear independence of characters), and Theorem 9.1 (the degree of K over K^H is bounded by the order of H).

1. Notation and conventions

For groups H and G, we write $H < G$ to mean that H is a (not necessarily proper) subgroup of G. Similarly, for sets S and T, we write $S \subset T$ to indicate that S is a (not necessarily proper) subset of T.

2. Field extensions

Definition 2.1. A *field extension* K/F is a triple (F, K, i) consisting of fields F and K together with a field homomorphism $i : F \to K$. When there is no danger of confusion F will be identified with its image $i(F)$ under i, and so regarded as a subfield of K.

Definition 2.2. A field extension K/F is *finite* if K is finite-dimensional as a vector space over F. The *degree* $[K : F]$ of a finite extension K/F is the dimension of K as a vector space over F.

[1] and the occasional definition or two. Not to mention the theorems, lemmas and so forth.

Proposition 2.3 (Tower Law)**.** *Suppose that K/E and E/F are field extensions. Then K/F is finite if and only if K/E and E/F are finite, and in this case*

$$[K : F] = [K : E][E : F].$$

Proof. If K/F is finite then any basis for K as a vector space over F spans K as a vector space over E, hence contains a basis for K over E, so K/E is finite. Similarly, any basis for E/F gives a subset of K linearly independent over F, which can be completed to a basis of K/F. Hence E/F is also finite.

Conversely, suppose that K/E and E/F are finite, and let S be a basis for K as a vector space over E and T a basis for E as a vector space over F. We'll show that the $[K : E][E : F]$ elements ts for s in S and t in T are distinct, and that they provide a basis for K as vector space over F.

Suppose that v is an element of K. Since S spans K over E,

$$v = \sum_{s \in S} \lambda_s s$$

for some elements λ_s in E. Since T spans E over F, for every s in S there is a relation

$$\lambda_s = \sum_{t \in T} \mu_{s,t} t$$

for some elements $\mu_{s,t}$ of F. Substituting gives

$$v = \sum_{s \in S} \sum_{t \in T} \mu_{s,t} ts,$$

hence the elements ts span K as a vector space over F.

Now suppose that there are elements $\mu_{s,t}$ of F such that

$$\sum_{s \in S} \sum_{t \in T} \mu_{s,t} ts = 0.$$

Letting $\lambda_s = \sum_{t \in T} \mu_{s,t} t$ for each s in S, we can rewrite this as

$$\sum_{s \in S} \lambda_s s = 0.$$

Since each λ_s is in E and the elements of S are linearly independent over E, it follows that $\lambda_s = 0$ for each s, hence

$$\sum_{t \in T} \mu_{s,t} t = 0$$

for each s in S. Since the elements of T are linearly independent over F, it follows that $\mu_{s,t} = 0$ for all s in S and t in T. Hence the elements ts are distinct and linearly independendent over F. So $TS = \{ts \mid s \in S, t \in T\}$ gives a basis for K over F, and it follows that $[K : F] = |TS| = |T||S| = [K : E][E : F]$ as required. □

Lemma 2.4. *Suppose that K/F is a field extension and that E is a subset of K that contains F and is closed under addition and multiplication. If E is finite-dimensional as a vector space over F then E is a field.*

Proof. Since E is closed under addition and multiplication, and contains F, it follows that it is a vector space over F. For each nonzero α in E, multiplication by α gives an injective F-linear map from E to itself. Since any injective linear map from a finite-dimensional vector space to itself is automatically surjective,

multiplication by α must be surjective. In particular, 1 is in the image, so $1 = \alpha\beta$ for some β in E. Hence α has an inverse in E. Since this is true for arbitrary nonzero α, E is a field. □

Definition 2.5. Suppose that K/F is a field extension and that S is a subset of K. Then we write $F(S)$ for the intersection of all subfields of K containing both F and S, and call it the field *generated by S over F*. If α is an element of K then we write $F(\alpha)$ for the field $F(\{\alpha\})$ generated by F and α. An extension K/F is a *simple extension* if $K = F(\alpha)$ for some α in K.

Definition 2.6. Suppose that K is a field, and that E_1 and E_2 are subfields of K. The *compositum* or *composite* E_1E_2 of E_1 and E_2 is the intersection of all subfields of K containing both E_1 and E_2. So in the notation of Definition 2.5, $E_1E_2 = E_1(E_2) = E_2(E_1)$.

Corollary 2.7. *Suppose that K/F is an extension, and that E_1 and E_2 are subfields of K containing F. If E_1/F and E_2/F are finite then E_1E_2/F is finite, and $[E_1E_2 : F] \leq [E_1 : F][E_2 : F]$.*

Proof. Choose a basis S for E_1 over F, and consider the subset E of K consisting of linear combinations of the elements of S with coefficients in E_2:

$$E = \Big\{ \sum_{s\in S} \lambda_s s \;\Big|\; \lambda_s \in E_2 \Big\}.$$

Since 1 is in E_1 and S spans E_1 over F, there are elements ϵ_s of F such that

$$1 = \sum_{s\in S} \epsilon_s s.$$

Hence for any x in E_2,

$$x = \sum_{s\in S} (x\epsilon_s)s$$

is an element of E. Since E_1 is closed under multiplication, for every t and u in S there are elements $\mu_s^{t,u}$ of F such that

$$tu = \sum_{s\in S} \mu_s^{t,u} s.$$

Hence for elements $x = \sum_{s\in S} \lambda_s s$ and $y = \sum_{s\in S} \nu_s s$ of E,

$$x + y = \sum_{s\in S} (\lambda_s + \nu_s)s$$

is in E and

$$\begin{aligned} xy = \sum_{t\in S, u\in S} \lambda_t\nu_u tu &= \sum_{t\in S, u\in S} \lambda_t\nu_u \Big(\sum_{s\in S} \mu_s^{t,u} s \Big) \\ &= \sum_{s\in S} \Big(\sum_{t\in S, u\in S} \lambda_t\nu_u\mu_s^{t,u} \Big) s \end{aligned}$$

is an element of E. So E contains E_2 and is closed under addition and multiplication. Furthermore, S spans E as a vector space over E_2, so E is finite-dimensional over E_2, of dimension at most $|S| = [E_1 : F]$. Hence by Lemma 2.4, E is a subfield of K. Since E contains both E_1 and E_2, and is generated by elements of E_1E_2, $E = E_1E_2$. By the Tower Law, E_1E_2/F is finite, and $[E_1E_2 : F] = [E_1E_2 : E_2][E_2 : F] \leq [E_1 : F][E_2 : F]$ as required. □

3. Algebraic extensions

Throughout this section, K/F will be a field extension and α will denote an element of K.

Notation 3.1. Let $f = \sum_{0 \le i \le d} a_i x^i$ be a polynomial in $F[x]$. Then we write $f(\alpha)$ for the element

$$f(\alpha) = \sum_{0 \le i \le d} a_i \alpha^i$$

of K.

It follows directly from the definitions that for f and g in $F[x]$ and α in K, $(f \pm g)(\alpha) = f(\alpha) \pm g(\alpha)$, $(fg)(\alpha) = f(\alpha)g(\alpha)$ and $a(\alpha) = a$ for any a in F (where a is interpreted as the constant polynomial a on the left-hand side).

Remark 3.2. While the notation above resembles the usual one for application of a function f to an argument α, it's important not to forget that a polynomial is not, strictly speaking, a function from F to F. For example, when $F = \mathbf{F}_p$ is the finite field with p elements, the polynomials $f = x^p$ and $g = x$ in $F[x]$ are distinct, even though as functions on F they're identical: $f(\alpha) = g(\alpha)$ for all α in F.

Definition 3.3. Let f be a nonzero polynomial in $F[x]$. The element α of K is a *root* of f if $f(\alpha) = 0$ in K.

Proposition 3.4. *With the notation of the previous definition, α is a root of F if and only if there is a factorization $f = (x - \alpha)g$ in $K[x]$ for some nonzero polynomial g in $K[x]$.*

Proof. Apply the Division Algorithm (in $K[x]$) to f and $(x - \alpha)$ to $K[x]$ to obtain $f = (x-\alpha)q+r$ for some polynomial q in $K[x]$ and some constant r in K. Applying both sides to α, $0 = f(\alpha) = r(\alpha)$, hence $r = 0$ and so $f = (x-\alpha)q$ gives the required factorization. The converse is obvious. □

Definition 3.5. An element α of K is *algebraic* over F if α is the root of some nonzero polynomial f in $F[x]$. An extension K/F is *algebraic* if every element α of K is algebraic over F.

Proposition 3.6. *If α is an algebraic element of K, then there is a unique monic irreducible polynomial m such that $m(\alpha) = 0$. Furthermore, for any polynomial f in $F[x]$, m divides f if and only if α is a root of f.*

Proof. Since α is algebraic there is a nonzero polynomial f such that $f(\alpha) = 0$. By rescaling f if necessary, we may assume that f is monic. Now choose a monic polynomial m of smallest degree such that $m(\alpha) = 0$. Then m is irreducible: it's clearly nonconstant, and if $m = gh$ for some polynomials g and h of smaller degree then $m(\alpha) = g(\alpha)h(\alpha)$, so either $g(\alpha) = 0$ or $h(\alpha) = 0$, contradicting the choice of m.

Now suppose that f is any polynomial in $F[x]$. It's clear that if $m|f$ then $f(\alpha) = 0$. Conversely, suppose that $f(\alpha) = 0$ let $g = \gcd(f, m)$. Since g is a linear combination of f and m, $g(\alpha) = 0$. But then $\deg(g) \ge \deg(m)$, by the choice of m. Since $g|m$, and both g and m are monic, it follows that $g = m$, hence that $m|f$.

It remains to show uniqueness of m. But if m' is a monic irreducible polynomial such that $m'(\alpha) = 0$ then $m|m'$. Hence $m = m'$, by irreducibility of m'. □

Definition 3.7. The unique irreducible monic polynomial m in $F[x]$ such that $m(\alpha) = 0$, whose existence is guaranteed by Proposition 3.6, is the *minimal polynomial* of α. The *degree* $\deg(\alpha)$ of α is $\deg(m)$. Note that $\deg(\alpha)$ is always a positive integer.

Lemma 3.8. *Suppose that α is an element of K, algebraic over F of degree d. Then every element of the simple extension $F(\alpha)$ can be represented uniquely in the form $\sum_{0\le i<d} a_i\alpha^i$, where the coefficients a_i are elements of F.*

Proof. Consider the 'evaluate at α' map $\phi : F[x] \to K$ defined by $\phi(f) = f(\alpha)$. Let E be the image of this map. We will first show that the image E of ϕ is precisely $F(\alpha)$, and then show that every element of E can be represented in the given form.

It follows directly from the definitions that E is a subset of $F(\alpha)$ that is closed under addition and multiplication and contains F. To show that E is equal to $F(\alpha)$, it suffices to show that every nonzero element of E has an inverse in E; then E is a subfield of K containing both F and $\alpha = \phi(x)$, and hence contains $F(\alpha)$ by Definition 2.5. Suppose that $f(\alpha)$ is a nonzero element of the image of ϕ. Then by Proposition 3.6, f is not divisible by the minimal polynomial m of α in $F[x]$. Hence f is relatively prime to m, so there are polynomials a and b such that $af + bm = 1$ in $F[x]$. But then $1 = a(\alpha)f(\alpha)+b(\alpha)m(\alpha) = a(\alpha)f(\alpha)$ in K and $a(\alpha)$ is an inverse for $f(\alpha)$.

Now we show that every element $f(\alpha)$ of E has the given form. For any polynomial r, $f(\alpha) = r(\alpha)$ if and only if $(f - r)(\alpha) = 0$, which is true if and only if $f - r$ is divisible by m by Proposition 3.6. But by the Division Algorithm applied to f and m, there is a unique polynomial r such that $f - r$ is divisible by m and $r = \sum_{0\le i<d} a_i x^i$ for some a_i in F. Hence there are unique coefficients a_i in F such that $f(\alpha) = \sum_{0\le i<d} a_i\alpha^i$. □

Corollary 3.9. *Suppose that K/F is a field extension and that α is an element of K. Suppose that α is algebraic over F, of degree d. Then the extension $F(\alpha)/F$ is finite, of degree d.*

Proof. By Lemma 3.8, the set of elements $\{\alpha^i \mid 0 \le i < d\}$ gives a basis for $F(\alpha)$ as a vector space over F. □

Proposition 3.10. *The following are equivalent, for an element α of a field extension K/F.*

1. *α is algebraic.*
2. *The extension $F(\alpha)/F$ is finite.*
3. *There is a subfield E of K containing α such that E/F is finite.*

Proof. That (1) implies (2) follows from Corollary 3.9 The implication (2) implies (3) is immediate: just take $E = F(\alpha)$. To show that (3) implies (1), suppose that $[E : F] = d$. Then the $d+1$ elements α^i, $0 \le i \le d$ of E must be linearly dependent over F. Hence there's a relation $\sum_{0\le i\le d} a_i\alpha^i = 0$ for some a_i in F, not all zero, and then α is a root of the nonzero polynomial $f = \sum_{0\le i\le d} a_i x^i$. □

Corollary 3.11. *Any finite extension is algebraic.*

Proof. This follows immediately from Proposition 3.10 and Definition 3.5. □

Corollary 3.12. *Suppose that K/F is a field extension. Then the subset of K consisting of all elements that are algebraic over F is a subfield of K.*

Proof. Suppose that α and β are elements of K that are algebraic over F. Then $F(\alpha)$ and $F(\beta)$ are finite over F by Proposition 3.10. Thus the compositum $F(\alpha)F(\beta) = F(\{\alpha, \beta\})$ is finite over F by Corollary 2.7. Since this compositum is a field containing both α and β, it contains $\alpha \pm \beta$, $\alpha\beta$ and (provided $\beta \neq 0$) α/β; hence all these elements are algebraic by Proposition 3.10 again. □

Proposition 3.13. *Suppose that K/E and E/F are field extensions. Then K/F is algebraic if and only if both K/E and E/F are algebraic.*

Proof. If K/F is algebraic then every element of E is an element of K, and hence is algebraic over F. So E/F is algebraic. Furthermore, any element α of K is the root of some nonzero polynomial f in $F[x]$; regarding f as a nonzero polynomial in $E[x]$ we find that K/E is algebraic.

For the other direction, suppose that K/E and E/F are algebraic. Let α be an element of K. Since K/E is algebraic there is a polynomial f in $E[x]$ such that $f(\alpha) = 0$. Let c_i, $0 \leq i \leq d$ be the coefficients of this polynomial. Since E/F is algebraic, each extension $F(c_i)/F$ is finite by Proposition 3.10. Hence the compositum $F(c_0, \ldots, c_d)/F$ is finite, by repeated application of Corollary 2.7. Now α is algebraic over $F(c_0, \ldots, c_d)$, hence $F(c_0, \ldots, c_d; \alpha)$ is finite over $F(c_0, \ldots, c_d)$ by Proposition 3.10, and so by the Tower Law it's finite over F. So α is algebraic over F by Proposition 3.10. □

4. Splitting fields

Definition 4.1. Let F be a field and f a nonzero polynomial in $F[x]$. The polynomial f *splits completely* in $F[x]$ if it can be written as a nonzero constant times a product of linear polynomials in $F[x]$.

Suppose that K is an extension field of F. Then K is a *splitting field* for f over F if f splits completely in $K[x]$ and the roots of f generate K over F.

Lemma 4.2. *Suppose that F is a field, and that m is an irreducible polynomial in $F[x]$. Then there is an extension E/F such that m has a root α in E and $E = F(\alpha)$.*

Proof. The relation $\sim$ defined on $F[x]$ by

$$f \sim g \iff m|(f - g)$$

is easily seen to be an equivalence relation. Let E be the set of equivalence classes in $F[x]$ under this equivalence relation, and define addition and multiplication on E by the formulas

$$[f] + [g] = [f + g]; \quad [f][g] = [fg]$$

where $[f]$ denotes the equivalence class of f. It's straightforward to check that these operations are well-defined, and that all field axioms are satisfied, with the possible exception of the existence of inverses. We now show that E is a field: suppose that $[f]$ is a nonzero element of E. Then m does not divide f, so m and f are relatively prime. Hence there are polynomials a and b in $F[x]$ such that $am+bf = 1$. But then $[b][f] = [a][m]+[b][f] = [am+bf] = [1] = 1_E$, so $[b]$ is an inverse for $[f]$ in E. Write α for the element $[x]$ of E. Then $0_E = [m] = [m(x)] = m([x]) = m(\alpha)$, hence α is

a root of m in E. Similarly, for any element $[f]$ of E, $[f] = [f(x)] = f([x]) = f(\alpha)$, so E is generated by F and α. Hence $E = F(\alpha)$. □

Theorem 4.3. *Let F be a field and f a nonzero polynomial in $F[x]$. Then there is a splitting field K for f over F.*

Proof. We prove this by induction on the degree of f. If $\deg(f) = 0$ then F is already a splitting field for f. So suppose that $\deg(f) > 0$ and that splitting fields exist for all polynomials of smaller degree. Let p be an irreducible factor of f. By Lemma 4.2, there is an extension E/F such that p has a root α in E and $E = F(\alpha)$. Then we can write $f = (x - \alpha)g$ in $E[x]$. By the induction hypothesis there is a splitting field K for g over E. Then f splits completely in $K[x]$, and K is generated over F by α and the roots of g, hence by the roots of f. So K is a splitting field for f over F. □

5. Normality

Definition 5.1. An algebraic extension K/F is *normal* if every irreducible polynomial f in $F[x]$ that has a root in K splits completely in $K[x]$.

Proposition 5.2. *The following conditions are equivalent, for an algebraic extension K/F.*

1. *K/F is normal.*
2. *For every element α of K, the minimal polynomial of α over F splits completely in $K[x]$.*
3. *For every element α of K, there is some polynomial f in $F[x]$ such that $f(\alpha) = 0$ and f splits completely in $K[x]$.*

Proof. (1) implies (2): For any element α of K, the minimal polynomial of α is an irreducible polynomial in $F[x]$ that has a root α in K, and hence splits completely. (2) implies (3): just take f to be the minimal polynomial of α. (3) implies (1): Suppose that f is an irreducible polynomial in $F[x]$ and that α is a root of f in K. Let g be a polynomial such that $g(\alpha) = 0$ and g splits completely in $K[x]$. Then since f and g share a root, $\gcd(f, g)$ is nontrivial. Hence $\gcd(f, g) = f$ by irreducibility of f, so $f|g$ and f must also split completely in $K[x]$. □

6. Separability

Definition 6.1. Let F be a field and $f = \sum_{0 \le i \le d} a_i x^i$ a polynomial in $F[x]$. The *derivative* of f is the polynomial

$$Df = \sum_{1 \le i \le d} i a_i x^{i-1}$$

in $F[x]$.

Proposition 6.2. *For polynomials f and g in $F[x]$ and a constant a in F, $D(1) = 0$, $D(f \pm g) = Df \pm Dg$, $D(af) = a\,Df$, $Dx = 1$, and $D(fg) = f\,Dg + Df\,g$.*

Proof. All of these except the product rule can be proved by first establishing it in the case $f = x$, then giving a proof by induction on the degree of f. □

Definition 6.3. Suppose that F is a field. A nonzero polynomial f in $F[x]$ is *separable* if f and its derivative Df are relatively prime in $F[x]$. Otherwise, f is *inseparable*.[2]

Definition 6.4. Suppose that K/F is an extension and that f is a nonzero polynomial in $F[x]$. Say that α in K is a *multiple root* of f if $f = (x-\alpha)^2 g$ for some polynomial g in $K[x]$.

Proposition 6.5. *Suppose that F is a field and f a separable polynomial in $F[x]$. Then f has no multiple roots in any extension E/F. Conversely, if f splits completely in an extension E/F and f has no multiple roots in E then f is separable.*

Proof. Suppose, for a contradiction, that $f = (x-\alpha)^2 g$ for some α in E and g in $E[x]$. Then $Df = (x-\alpha)(2g + (x-\alpha)Dg)$, hence $f(\alpha) = Df(\alpha) = 0$. It follows that both f and Df are divisible by the minimal polynomial m of α over $F[x]$, hence are not relatively prime.

For the converse, suppose that f splits completely in E/F and f has no multiple roots in E. Let $g = \gcd(f, Df)$; note that since g is a divisor of f, it splits completely in $E[x]$. So if f and Df are not relatively prime then g has a root α in E. Then $f(\alpha) = Df(\alpha) = 0$. So $f = (x-\alpha)h$ for some polynomial h in $E[x]$. But then $Df = h + (x-\alpha)Dh$, so $0 = Df(\alpha) = h(\alpha)$. Hence $h = (x-\alpha)h'$ for some h' in $E[x]$. Then $f = (x-\alpha)^2 h'$, contradicting the assumption that f has no multiple roots. Hence f and Df are relatively prime. □

Proposition 6.6. *If f is separable and $g|f$ then g is separable.*

Proof. Write $f = gh$. Then $Df = g\,Dh + Dg\,h$. So if g and Dg have a common irreducible factor p then so do f and Df. □

Definition 6.7. Let K/F be an extension. An algebraic element α of K is *separable* over F if there is a separable polynomial f in $F[x]$ such that $f(\alpha) = 0$. An algebraic extension K/F is *separable* if every element α of K is separable over F.

Proposition 6.8. *Suppose that K/F is an extension and that α is an algebraic element of K. Then α is separable if and only if its minimal polynomial is separable.*

Proof. Suppose that α is the root of a separable polynomial f in $F[x]$. Since $f(\alpha) = 0$, the minimal polynomial m of α divides f. Hence m is separable by Proposition 6.6. The other direction is immediate. □

7. Galois extensions

Definition 7.1. Suppose that E/F and K/F are extensions of a common base field F. Say that a field homomorphism $\phi : E \to K$ *fixes* F if $\phi(x) = x$ for all x in F. We also call a homomorphism from E to K that fixes F an *F-homomorphism*.

Definition 7.2. Suppose that K is a field. An *automorphism of K* is a field homomorphism $\phi : K \to K$ for which there is an *inverse* ψ with $\phi \circ \psi = \psi \circ \phi = \mathrm{id}_K$. (Equivalently, it's a homomorphism from K to K which is a bijection on the underlying sets.) We write $\mathrm{Aut}(K)$ for the group of automorphisms of K under composition.

[2]This definition, although it's the one adopted by Dummit and Foote, is slightly unorthodox: the more usual definition is that a polynomial g is separable if and only if f and Df are relatively prime for every irreducible factor f of g.

Now suppose that K/F is an extension of fields. Then an *automorphism of K over F* is an automorphism of K that fixes F. We write $\mathrm{Aut}(K/F)$ for the subgroup of $\mathrm{Aut}(K)$ whose elements fix F:

$$\mathrm{Aut}(K/F) = \{\phi \in \mathrm{Aut}(K) \mid \phi(x) = x \text{ for all } x \text{ in } F\} < \mathrm{Aut}(K).$$

Definition 7.3. Say that a field extension K/F is *Galois* if K/F is finite and $|\mathrm{Aut}(K/F)| = [K : F]$. It's common to write $\mathrm{Gal}(K/F)$ for the automorphism group $\mathrm{Aut}(K/F)$ when K/F is a Galois extension.

Lemma 7.4. *Suppose that E/F and K/F are extensions of a base field F, and that $\phi : E \to K$ is a field homomorphism that fixes F. Then for any polynomial f in $F[x]$ and element α of E, $\phi(f(\alpha)) = f(\phi(\alpha))$.*

Proof. The evaluation of α builds up $f(\alpha)$ from α and the coefficients of f by addition and multiplication. The result then follows from the observation that ϕ respects addition and multiplication and fixes all coefficients of f. □

Proposition 7.5. *Suppose that E/F is a simple algebraic extension: $E = F(\alpha)$ for some α in F. Let m be the minimal polynomial of α over F. Suppose that K/F is another extension. Then every homomorphism $E \to K$ that fixes F takes α to a root of m in K. Conversely, for each root β of m in K there is a unique homomorphism $\phi : E \to K$ that fixes F and maps α to β.*

Proof. Suppose that $\phi : E \to K$ is a homomorphism that fixes every element of F. Then $m(\phi(\alpha)) = \phi(m(\alpha)) = \phi(0) = 0$, hence $\phi(\alpha)$ is a root of m.

For the second part, we define a map as follows. Every element of the simple extension $E = F(\alpha)$ has the form $f(\alpha)$ for some polynomial f in $F[x]$. For any element $f(\alpha)$ of E, $\phi(f(\alpha)) = f(\phi(\alpha)) = f(\beta)$, so ϕ is uniquely determined, if it exists. To show existence, we define a map $\phi : E \to K$ by $\phi(f(\alpha)) = f(beta)$. This is well-defined: if $f(\alpha) = g(\alpha)$ then $(f - g)(\alpha) = 0$, hence m divides $f - g$, so $f(\beta) - g(\beta) = 0$ and $f(\beta) = g(\beta)$. It's also clearly a homomorphism that preserves F since for example $\phi(f(\alpha)g(\alpha)) = \phi((fg)(\alpha)) = (fg)(\beta) = f(\beta)g(\beta) = \phi(f(\alpha))\phi(g(\alpha))$. □

Theorem 7.6. *Suppose that E/F is a finite extension and let S be a subset of E that generates E over F. Suppose further that K/F is an extension such that the minimal polynomial of any α in S splits completely in $K[x]$. Then there is a field homomorphism from E to K that fixes F. If every element of S is separable, then there are exactly $[E : F]$ such homomorphisms.*

Proof. We give a proof by induction on $[E : F]$. If $[E : F] = 1$ then $E = F$ and the result is trivial. Suppose that $[E : F] > 1$ and the result has already been proved for all extension of smaller degree. Since E is generated by S over F, there is an element α of S not contained in F. Let $m = m_\alpha$ be its minimal polynomial.

Each homomorphism $E \to K$ that fixes F restricts to a homomorphism $F(\alpha) \to K$ fixing F. By Proposition 7.5 these homomorphisms are in one-to-one correspondence with roots of m_α in K; since m_α splits completely in $K[x]$ by assumption, there is at least one such homomorphism, and if α is separable then the number of these homomorphisms is exactly $\deg(m_\alpha)$, which is equal to $[F(\alpha) : F]$ by Corollary 3.9.

Now given a homomorphism $\phi : F(\alpha) \to K$, we can consider K as an extension of $F(\alpha)$ via the map ϕ. By the induction hypothesis there is a map $E \to K$ that

fixes $F(\alpha)$, and hence F. Furthermore if every element of S is separable then by the induction hypothesis there are exactly $[K : F(\alpha)]$ such maps for each of the $[F(\alpha) : F]$ choices for ϕ, and so by the Tower Law there are exactly $[K : F(\alpha)][F(\alpha) : F] = [K : F]$ maps $E \to K$ that fix F, as claimed. □

Corollary 7.7. *Suppose that F is a field, f a nonzero polynomial in $F[x]$. Then any splitting field for f over F is normal.*

Proof. Let K be a splitting field for f over F, let α be an element of K, and let m be its minimal polynomial. Let H be a splitting field for m over K, and suppose that β is any root of m in H. Then there is a homomorphism $\phi : F(\alpha) \to F(\beta)$ taking α to β, and since both $F(\alpha)$ and $F(\beta)$ are finite, of degree $\deg(m)$ over F, this homomorphism is an isomorphism. Now K is a splitting field for f over $F(\alpha)$, while $K(\beta) \subset H$ is a splitting field for f over $F(\beta)$.

□

Corollary 7.8. *Suppose that F is a field, f a nonzero polynomial in $F[x]$. Then any two splitting fields for f over F are isomorphic.*

Proof. Suppose that E/F and K/F are both splitting fields for f over F. Let S be the set of roots of f in E, and apply the theorem with this S. □

Corollary 7.9. *Suppose that K/F is the splitting field of a separable polynomial f in $F[x]$. Then K/F is Galois.*

Proof. By the previous theorem, applied with $E = K$ and S the set of roots of f in K, there are exactly $[K : F]$ automorphisms of K fixing F. □

8. Linear independence of characters

Theorem 8.1. *Let E and K be fields. Then any set S of field homomorphisms $s : E \to K$ is* linearly independent *over K. More precisely, suppose that there exist elements λ_s of K for each s in S such that all but finitely many of the λ_s are zero and*

$$\sum_{s \in S} \lambda_s s(x) = 0$$

for all x in E. Then $\lambda_s = 0$ for all s in S.

Note that the set of all functions from E to K is naturally a vector space over K, with addition and scalar multiplication defined pointwise. Linear independence in the above sense is the usual notion of linear independence in this vector space over K.

Proof. Suppose, for a contradiction, that the elements s are not linearly independent. Then there is a relation

$$\sum_{s \in S} \lambda_s s(x) = 0 \quad \text{for all } x \text{ in } E \tag{1}$$

for some coefficients λ_s in K, not all zero. Choose such a relation with the minimal number of nonzero coefficients λ_s. Substituting 1 for x in (1) and using $s(1) = 1$ gives $\sum_{s \in S} \lambda_s = 0$, so there must be at least two elements of S, t and u say, for which the corresponding coefficients λ_t and λ_s are nonzero. Since t and u are

distinct, there is an element y of E such that $t(y) \neq u(y)$. Substituting yx for x in (1) and using $s(yx) = s(y)s(x)$ gives

$$\sum_{s \in S} \lambda_s s(y)s(x) = 0 \quad \text{for all } x \text{ in } E. \tag{2}$$

Taking $t(y)$ times (1) minus (2) gives

$$\sum_{s \in S} \lambda_s (t(y) - s(y))s(x) = 0 \quad \text{for all } x \text{ in } E. \tag{3}$$

But $\lambda_s(t(y) - s(y))$ is zero whenever λ_s is zero, and it's also zero for $s = t$. Since it's nonzero for $s = u$ (3) gives a shorter relation, a contradiction to the original choice of relation. Hence the elements s are linearly independent. □

Corollary 8.2. *Suppose that E/F and K/F are field extensions, and that $[E : F]$ is finite. Then there are at most $[E : F]$ distinct field homomorphisms from E to K that fix F.*

Proof. The set of F-linear maps ϕ from E to K is a vector space of dimension $[E : F]$ over K. By Theorem 8.1, the set of maps from E to K that fix F is linearly independent in this vector space, and hence there are at most $[E : F]$ such maps. □

Corollary 8.3. *For any finite extension K/F, $|\operatorname{Aut}(K/F)| \leq [K : F]$.*

Proof. Apply Corollary 8.2 with $E = K$. □

Corollary 8.4. *If K/F is Galois then $\operatorname{Aut}(K/F)$ is a finite subgroup of $\operatorname{Aut}(K)$ and $K^{\operatorname{Aut}(K/F)} = F$.*

Proof. Let $E = K^{\operatorname{Aut}(K/F)}$. Then

$$\begin{aligned}
[K : F] &= |\operatorname{Aut}(K/F)| && \text{by definition of Galois} \\
&= |\operatorname{Aut}(K/E)| && \text{since every element of } \operatorname{Aut}(K/F) \text{ fixes } E \\
&\leq [K : E] && \text{by Theorem 8.1} \\
&= [K : F]/[E : F] && \text{by the Tower Law} \\
&\leq [K : F]
\end{aligned}$$

Hence all inequalities are equalities and $[E : F] = 1$, so $E = F$. □

Proposition 8.5. *Let K/F be a Galois extension. Then for any subfield E of K, K/E is a Galois extension. Furthermore, E/F is Galois if and only if $\sigma(E) \subset E$ for all σ in $\operatorname{Aut}(K/F)$, and in this case $\operatorname{Aut}(K/E)$ is a normal subgroup of $\operatorname{Aut}(K/F)$ and $\operatorname{Aut}(E/F)$ is isomorphic to the quotient group $\operatorname{Aut}(K/F)/\operatorname{Aut}(K/E)$.*

Proof. Let $G = \operatorname{Aut}(K/F)$, and let X be the set of field homomorphisms from E to K that fix F. Let i be the element of X given by the inclusion map $E \to K$. Define an action of G on X by composition of functions: $g \cdot s = g \circ s$ for g in G and s in X. The stabilizer of i is exactly $\operatorname{Aut}(K/E)$. Let $\operatorname{orb}_G(i)$ be the orbit of i

under the action of G.

$$\begin{aligned}
[K:F] &= |G| && \text{by definition of Galois}\\
&= |\operatorname{Aut}(K/E)||\operatorname{orb}_G(i)| && \text{by the orbit-stabilizer formula}\\
&\leq |\operatorname{Aut}(K/E)||X| && \text{since } \operatorname{orb}_G(i) \text{ is a subset of } X\\
&\leq [K:E][E:F] && \text{by Corollary 8.3 and Corollary 8.2}\\
&= [K:F] && \text{by the Tower Law.}
\end{aligned}$$

Hence all inequalities are equalities. In particular, $|\operatorname{Aut}(K/E)| = [K:E]$ and hence K/E is Galois. Furthermore, there must be exactly $[E:F]$ elements of X.

The function $\operatorname{Aut}(E/F) \to X$ given by $h \mapsto i \circ h$ is easily seen to be injective. If E/F is Galois then $\operatorname{Aut}(E/F)$ and X both have exactly $[E:F]$ elements, and hence this map is also surjective. It follows that for any s in $\operatorname{Aut}(K/F)$, the restriction of s to E has the form $i \circ h$ for some h in $\operatorname{Aut}(E/F)$, and hence $s(E) = i(h(E)) = i(E) = E$.

Conversely, suppose that $s(E) = E$ for all s in $\operatorname{Aut}(K/F)$. Then restriction gives a group homomorphism $\operatorname{Aut}(K/F) \to \operatorname{Aut}(E/F)$, whose kernel is precisely $\operatorname{Aut}(K/E)$. By the first isomorphism theorem for groups, the quotient group $\operatorname{Aut}(K/F)/\operatorname{Aut}(K/E)$ is isomorphic to a subgroup of $\operatorname{Aut}(E/F)$. But

$$\begin{aligned}
|\operatorname{Aut}(K/F)/\operatorname{Aut}(K/E)| &= |\operatorname{Aut}(K/F)|/|\operatorname{Aut}(K/E)| && \text{by Lagrange's Theorem}\\
&= [K:F]/[K:E]\\
&= [E:F] && \text{by the Tower Law.}
\end{aligned}$$

Since $|\operatorname{Aut}(E/F)| \leq [E:F]$ by Corollary 8.3, it follows that $|\operatorname{Aut}(E/F)| = [E:F]$, E/F is Galois, and $\operatorname{Aut}(E/F)$ is isomorphic to $\operatorname{Aut}(K/F)/\operatorname{Aut}(E/F)$. □

Theorem 8.6. *For a finite extension K/F, the following conditions are equivalent.*

1. *K/F is Galois.*
2. *$K^{\operatorname{Aut}(K/F)} = F$.*
3. *K/F is normal and separable.*
4. *K is a splitting field for a separable polynomial f in $F[x]$.*

Proof. Corollary 7.9 states that (4) implies (1), while Corollary 8.4 gives us (1) implies (2). We now show that (2) implies (3). Assume that $K^{\operatorname{Aut}(K/F)} = F$, and let α be an element of K. Consider the action of $\operatorname{Aut}(K/F)$ on K given by $g \cdot x = g(x)$, and let X be the orbit of α under this action. Now define a polynomial f in $K[x]$ by

$$f = \prod_{\beta \in X} (x - \beta).$$

Any element g of the group $\operatorname{Aut}(K/F)$ permutes the elements of X, hence if $g(f)$ denotes the result of applying g to the coefficients of f, then

$$g(f) = \prod_{\beta \in X} (x - g(\beta)) = f.$$

So the coefficients of f lie in the fixed field of $\operatorname{Aut}(K/F)$; by assumption this fixed field is F. Hence f is an element of $F[x]$. Now f is a monic polynomial in $F[x]$ such that $f(\alpha) = 0$, f splits completely in $K[x]$ and all roots of f in K are distinct. Since we can find such an f for any α, it follows that K/F is both separable and normal.

Finally, we show that (3) implies (4). Suppose that K/F is normal and separable. Let B be a basis for K as a vector space over F. Then for each b in B, the minimal polynomial m_b of b in $F[x]$ splits completely in $K[x]$ (since K/F is normal) and has distinct roots in K (since K/F is separable). Let f be the product of all distinct polynomials m_b arising this way. Then f splits completely in $K[x]$ and the set of roots of F in K contains B, hence generates K over F. So K is a splitting field for f over F. Finally, f has distinct roots in K: any multiple root would have to be a root of more than one of the polynomials m_b, but if m_b and m_c share a root then $\gcd(m_b, m_c)$ is nontrivial, and hence $\gcd(m_b, m_C) = m_b = m_c$ by irreducibility of m_b and m_c. □

9. Fixed fields

Theorem 9.1. *Suppose that K is a field and H is a finite subgroup of $\mathrm{Aut}(K)$. Then K/K^H is finite and $[K : K^H] \leq |H|$.*

Proof. Let B be a finite subset of K that's linearly independent over K^H. We'll show that the corresponding maps $g \mapsto g(b)$ from H to K are linearly independent. Since the space of maps $H \to K$ is a finite-dimensional vector space over K, of dimension $|H|$, it follows that $[K : K^H] \leq |H|$.

Suppose, for a contradiction, that there is a nontrivial relation

$$\sum_{b \in B} \lambda_b g(b) = 0 \quad \text{for all } g \text{ in } H \tag{4}$$

with not all of the λ_b nonzero; say $\lambda_c \neq 0$ for some c in B. Choose a relation with the minimal number of nonzero λ_b. Substituting the identity element of H for g in (4) gives $\sum_{b \in B} \lambda_b b = 0$, and dividing by λ_c gives $\sum_{b \in B} \lambda_b/\lambda_c b = 0$. Since the elements of B are linearly independent over K^H it follows that there's at least one d in B such that λ_d/λ_c is not in K^H. Choose h such that $h(\lambda_d/\lambda_c) \neq \lambda_d/\lambda_c$. Now substituting $h^{-1}g$ for g in (4), and applying h to the result, gives

$$\sum_{b \in B} h(\lambda_b) g(b) = 0 \quad \text{for all } g \text{ in } G. \tag{5}$$

Now taking $h(\lambda_c)$ times (4) and subtracting λ_c times (5) gives

$$\sum_{b \in B} (\lambda_b h(\lambda_c) - \lambda_c h(\lambda_b)) g(b) = 0 \quad \text{for all } g \text{ in } G. \tag{6}$$

The $b = c$ term of this sum vanishes, so this relation has fewer nonzero entries than the original one. However, the $b = d$ term does not vanish, since $\lambda_d h(\lambda_c) - \lambda_c h(\lambda_d) \neq 0$. So this is a shorter relation, again contradicting the choice of the relation. □

Corollary 9.2. *Suppose that K is a field and H is a finite subgroup of $\mathrm{Aut}(K)$. Then $H = \mathrm{Aut}(K/K^H)$ and K/K^H is Galois.*

Proof. Since $H < \mathrm{Aut}(K/K^H)$, it's enough to show that $|H| = |\mathrm{Aut}(K/K^H)|$. But

$$\begin{aligned} |\mathrm{Aut}(K/K^H)| &\leq [K : K^H] && \text{by Corollary 8.3} \\ &\leq |H| && \text{by Theorem 9.1} \end{aligned}$$

Hence $|H| = |\mathrm{Aut}(K/K^H)$, and $H = \mathrm{Aut}(K/K^H)$. Furthermore, $|\mathrm{Aut}(K/K^H)| = [K : K^H]$, so K/K^H is a Galois extension. □

10. The Fundamental Theorem

Fix a field K, and let $G = \mathrm{Aut}(K)$. Let $\mathcal{F}$ be the set of subfields of K. Let $\mathcal{G}$ be the set of subgroups of G. Define maps $\alpha : \mathcal{F} \to \mathcal{G}$ and $\beta : \mathcal{G} \to \mathcal{F}$ by

$$\alpha(E) = \mathrm{Aut}(K/E)$$

and

$$\beta(H) = K^H.$$

The sets $\mathcal{F}$ and $\mathcal{G}$ have important additional structure. Both sets are posets, the set $\mathcal{F}$ with respect to the subset relation $\subset$, and the set $\mathcal{G}$ with respect to the subgroup relation $<$. Moreover, both sets are lattices: any pair of fields E_1 and E_2 has a meet $E_1 \cap E_2$ and a join E_1E_2, and similarly any pair of subgroups H_1 and H_2 has a meet $H_1 \cap H_2$ and a join $\langle H_1, H_2\rangle$. Finally, both sets enjoy a natural action of the group G: suppose that σ is an element of G. Then for any subfield E of K $\sigma(E) = \{\sigma(x) \,|\, x \in E\}$ is a subfield of E, while for any subgroup H of G, $\sigma H \sigma^{-1}$ is also a subgroup of G.

Proposition 10.1. *The following hold, for any field E in $\mathcal{F}$ and any group H in $\mathcal{G}$.*

1. *For any E in $\mathcal{F}$ and H in $\mathcal{G}$, $H < \alpha(E)$ if and only if $E \subset \beta(H)$.*
2. *For any inclusion $E_1 \subset E_2$ of fields in $\mathcal{F}$, $\alpha(E_2) < \alpha(E_1)$.*
3. *For any inclusion $H_1 < H_2$ of groups in $\mathcal{G}$, $\beta(H_2) \subset \beta(H_1)$.*
4. *$H < \alpha\beta(H)$, with equality if and only if $H = \alpha(E)$ for some E in $\mathcal{F}$.*
5. *$E \subset \beta\alpha(E)$, with equality if and only if $E = \beta(H)$ for some H in $\mathcal{G}$.*
6. *The maps α and β are G-invariant:*

$$\alpha(\sigma E) = \sigma\alpha(E)\sigma^{-1}$$

and

$$\beta(\sigma H \sigma^{-1}) = \sigma(\beta(H)).$$

7. *For any two fields E_1 and E_2, $\alpha(E_1E_2) = \alpha(E_1) \cap \alpha(E_2)$.*
8. *For any two subgroups H_1 and H_2, $\beta(\langle H_1, H_2\rangle) = \beta(H_1) \cap \beta(H_2)$.*

Proof. The first three properties follow directly from the definitions of α and β. Substituting $E = \beta(H)$ in (1) and observing that $\beta(H) < \beta(H)$ is always true, the first part of (4) follows. Similarly, the first part of (5) follows on substituting $H = \alpha(E)$ in (1). Applying β to both sides of (4) and using (3) gives $\beta\alpha\beta(H) < \beta(H)$, while substituting $E = \beta(H)$ in (5) gives $\beta(H) < \beta\alpha\beta(H)$. Combining these two inequalities gives $\beta(H) = \beta\alpha\beta(H)$, which proves the second part of (5); the proof of the second part of (4) is entirely analogous.

For the proof of (6), simply unravelling the definitions shows that $\sigma\alpha(E)\sigma^{-1} < \alpha(\sigma E)$, and that $\sigma^{-1}\alpha(E)\sigma < \alpha(E)$. Conjugating the latter relation gives $\alpha(E) < \sigma\alpha(E)\sigma^{-1}$, and hence the first half of (6). The second half is similar.

To prove (7), let H be an arbitrary subgroup of G. Then by (1), $H < \alpha(E_1E_2)$ if and only $E_1E_2 < \beta(H)$. But this condition is equivalent to $E_1 < \beta(H)$ and $E_2 < \beta(H)$, hence to the condition that $H < \alpha(E_1)$ and $H < \alpha(E_2)$, or equivalently that $H < \alpha(E_1) \cap \alpha(E_2)$. So $H < \alpha(E_1E_2)$ if and only if $H < \alpha(E_1) \cap \alpha(E_2)$. Applying this with $H = \alpha(E_1E_2)$ and $H = \alpha(E_1) \cap \alpha(E_2)$ gives (7). The proof of (8) is analogous. □

Note that the maps α and β above are *not* necessarily inverse to one another. But properties (4) and (5) suggest that if we restrict attention to the fields in $\mathcal{F}$

arising as fixed fields, and the groups in $\mathcal{G}$ arising as automorphism groups—that is, those E in the image of β and H in the image of α respectively, then α and β do in fact give a bijection

$$\{E \in \mathcal{F} \mid E = \beta(H) \text{ for some } H\} \longleftrightarrow \{H \in \mathcal{G} \mid H = \alpha(E) \text{ for some } E\}$$

between these two subsets.

Now fix a subfield F of K. If E is a subfield of K containing F then $\alpha(E)$ is contained in $\alpha(F) = \mathrm{Aut}(K/F)$, by property (2) above. Conversely, if H is a subgroup of G contained in $\mathrm{Aut}(K/F)$ then $\beta(H)$ contains F, by property (1). Thus we can restrict the correspondence above one further step to give a correspondence

$$\left\{ E \in \mathcal{F} \middle| \begin{array}{l} E = \beta(H) \text{ for some } H \\ F \subset E \end{array} \right\} \longleftrightarrow \left\{ H \in \mathcal{G} \middle| \begin{array}{l} H = \alpha(E) \text{ for some } E \\ H < \mathrm{Aut}(K/F) \end{array} \right\}$$

So far in this section, we've used very little of the theory from the previous sections of this document, and none of the major theorems. That's about to change. We now assume that K/F is Galois, so that K/F is finite and $|\mathrm{Aut}(K/F)| = [K : F]$. We'll use earlier results to simplify the description of the correspondence given above.

Let E be any subfield of K containing F. Then K/E is Galois by Proposition 8.5, and hence $K^{\mathrm{Aut}(K/E)} = E$ by Corollary 8.4. But this can be rewritten as $\beta\alpha(E) = E$, and hence E is in the image of β.

Let H be any subgroup of $\mathrm{Aut}(K/F)$. Then H is finite, so $H = \mathrm{Aut}(K/K^H)$ by Corollary 9.2. This says exactly that $H = \alpha\beta(H)$, hence H is contained in the image of α. Thus the correspondence above becomes a correspondence between all subfields of K containing F, and all subgroups of $\mathrm{Aut}(K/F)$.

Finally, if K/F is Galois then for any subfield E of K containing F, E/F is Galois if and only if $\sigma(E) = E$ for all σ in $\mathrm{Aut}(K/F)$, by Proposition 8.5. Since the correspondence respects G-actions, E/F is Galois if and only if $\sigma\alpha(E)\sigma^{-1} = \alpha(E)$ for all σ in $\mathrm{Aut}(K/F)$, which is precisely the condition for $\alpha(E)$ to be a normal subgroup of $\mathrm{Aut}(K/F)$. We summarize all of the above as follows.

Theorem 10.2 (Fundamental Theorem of Galois Theory)**.** *Suppose that K/F is a Galois extension and let $G = \mathrm{Aut}(K/F)$. Let $\mathcal{F}$ be the set of fields E such that $K \subset E \subset F$, and let $\mathcal{G}$ be the set of subgroups of G. Then the maps $\alpha : \mathcal{F} \to \mathcal{G}$ and $\beta : \mathcal{G} \to \mathcal{F}$ defined by $\alpha(E) = \mathrm{Aut}(K/E)$ and $\beta(H) = K^H$ give a well-defined bijective correspondence between $\mathcal{F}$ and $\mathcal{G}$. This correspondence enjoys the following properties:*

1. *It's inclusion reversing: if E_1 and E_2 correspond to H_1 and H_2 respectively, then $E_1 \subset E_2$ if and only if $H_2 < H_1$.*
2. *If E corresponds to H then $[K : E] = |H|$ and $[E : F] = |G : H|$.*
3. *For any E in $\mathcal{F}$, K/E is a Galois extension.*
4. *Suppose that E corresponds to H. Then E/F is a Galois extension if and only if H is normal in G; in this case, the Galois group of E over F is $\mathrm{Aut}(E/F) \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/E)$.*
5. *If E_1 and E_2 correspond to H_1 and H_2 respectively, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$, while the composite field E_1E_2 corresponds to $H_1 \cap H_2$.*