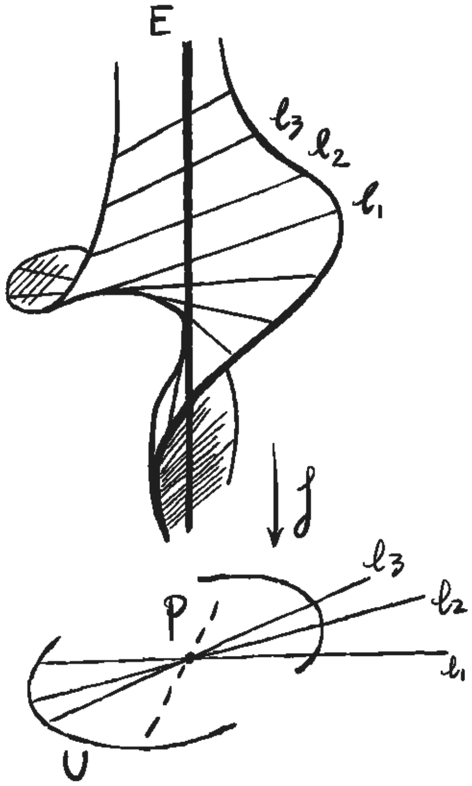
Algebra

Xiaolong Pan

December 31, 2023



Contents

Chapter 1

Field Theory

1.1 Field extensions

We first deal with several basic notions in field theory, mostly inspired by easy linear algebra considerations. The keywords here are finite, simple, finitely generated, algebraic.

1.1.1 Basic definitions of field extensions

The study of fields is (of course) the study of the category **Fld** of fields, with ring homomorphisms as morphisms. The task is to understand what fields are and above all what they are in relation to one another. The place to start is a reminder from elementary ring theory: every ring homomorphisms from a field to a nonzero ring is injective. Indeed, the kernel of a ring homomorphism to a nonzero ring is a proper ideal (because a homomorphism maps 1 to 1 by definition and $1 \neq 0$ in nonzero rings), and the only proper ideal in a field is (0). In particular, every ring homomorphism of fields is injective (fields are nonzero rings by definition!); every morphism in **Fld** is a monomorphism.

The coarsest invariant of a field K is its **characteristic**. We have a unique ring homomorphisms $\iota : \mathbb{Z} \to K$ (recall that $\mathbb{Z}$ is initial in **Ring**: 1 must go to 1 by definition of homomorphism, and this fixes the value of $\iota(n)$ for all $n \in \mathbb{Z}$); the characteristic of K, $\operatorname{char}(K)$, is defined to be the nonnegative generator of the ideal $\ker \iota$; that is, $\operatorname{char}(K) = 0$ if ι is injective, and $\operatorname{char}(K) = p > 0$ if $\ker \iota = (p) \neq (0)$. Since $\iota(\mathbb{Z})$ must be an integral domain, (p) is a prime ideal in $\mathbb{Z}$. Therefore, the characteristic of a field is either 0 or a prime number.

Definition 1.1.1.1. A field E containing a field K is called an **extension field of K** (or simply an **extension** of K, and we speak of an extension E/K). The dimension of E as an K-vector space is called the **degree of E over K**, and is denote by $[E : K]$. We say that E is **finite** over K when it has finite degree over K.

Example 1.1.1.2 (Example of field extensions).

(a) The field of complex numbers $\mathbb{C}$ has degree 2 over $\mathbb{R}$, so $\mathbb{R} \subseteq \mathbb{C}$ is a extension of degree 2.

(b) The field of real numbers $\mathbb{R}$ has infinite degree over $\mathbb{Q}$: the field $\mathbb{Q}$ is countable, and so every finite-dimensional $\mathbb{Q}$-vector space is also countable, but a famous argument of Cantor shows that $\mathbb{R}$ is not countable.

(c) The field of Gaussian numbers
$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$
has degree 2 over $\mathbb{Q}$.

(d) The field $K(X)$ has infinite degree over K; in fact, even its subspace $K[X]$ has infinite dimension over K.

Let K be a subfield of a field E, and let S be a subset of E. The intersection of all the subfields of E containing K and S is obviously the smallest subfield of E containing both K and S. We call it the **subfield of E generated by K and S** (or **generated over K by S**), and we denote it $K(S)$. It is the field of fractions of the ring $K[S]$ in E because this is a subfield of E containing K and S and contained in every other such field. When $S = \{\alpha_1, \ldots, \alpha_n\}$, we write $K(\alpha_1, \ldots, \alpha_n)$ for $K(S)$. Thus, $F[\alpha_1, \ldots, \alpha_n]$ consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in K, and $K(\alpha_1, \ldots, \alpha_n)$ consists of all elements of E that can be expressed as a quotient of two such polynomials.

Let E and F be subfields of a field L. The intersection of the subfields of L containing both E and F is obviously the smallest subfield of L containing both E and F. We call it the **composite** of E and F in L, and we denote it by $E \cdot F$. It can also be described as the subfield of L generated over E by F, or the subfield generated over F by E:

$$E \cdot F = E(F) = F(E).$$

More generally, the composite $\bigvee E_i$ of a family $\mathcal{E} = \{E_i : i \in I\}$ of fields, all of which are contained in a single field L, is the smallest subfield of L containing all members of the family.

A **monomial** over a family $\mathcal{E} = \{E_i : i \in I\}$ of fields with $E_i \subseteq L$ is simply a product of a finite number of elements from the union $\bigcup_i E_i$. The set of all finite sums of monomials over $\mathcal{E}$ is the smallest subring R of L containing each field E_i and the set of all quotients of elements of R (the quotient field of R) is the composite $\bigvee E_i$. Thus, each element of $\bigvee E_i$ involves only a finite number of elements from the union $\bigcup_i E_i$ and is therefore contained in a composite of a finite number of fields from the family $\mathcal{E}$.

The collection of all subfields of a field L forms a complete lattice (under set inclusion), with meet being intersection and join being composite. The bottom element is the prime subfield of L and the top element is L itself.

1.1.1.1 Distinguished extensions We will have much to say about towers of fields of the form $K \subseteq E \subseteq F$. Let us refer to such a tower as a **2-tower**, where E is the intermediate field, $K \subseteq E$ is the lower step, $E \subseteq F$ is the upper step and $K \subseteq F$ is the full extension.

Following Lang, we will say that a class $\mathcal{C}$ of field extensions is **distinguished** provided that it has the following properties

(1) (**The Tower Property**) For any 2-tower $K \subseteq E \subseteq F$, the full extension is in $\mathcal{C}$ if and only if the upper and lower steps are in $\mathcal{C}$. In symbols,

$$(K \subseteq F) \in \mathcal{C} \Leftrightarrow (K \subseteq E) \in \mathcal{C} \text{ and } (E \subseteq F) \in \mathcal{C}.$$

(2) (**The Lifting Property**) The class $\mathcal{C}$ is closed under lifting by an arbitrary field, that is,

$$(K \subseteq E) \in \mathcal{C} \text{ and } K \subseteq F \Rightarrow (F \subseteq EF) \in \mathcal{C}.$$

provided, of course, that EF is defined. The tower $F \subseteq EF$ is the **lifting** of $K \subseteq E$ by F.

(3) (**Closure under finite composites**) If EF is defined, then

$$(K \subseteq E) \in \mathcal{C} \text{ and } (K \subseteq F) \in \mathcal{C} \Rightarrow (K \subseteq EF) \in \mathcal{C}.$$

Note that if $\mathcal{C}$ satisfies (1) and (2), then it also satisfies (3). This follows from the fact that $K \subseteq EF$ can be decomposed into $K \subseteq F \subseteq EF$, and the first step is in $\mathcal{C}$, the second step is in $\mathcal{C}$ since it is the lifting of $K \subseteq E$ by F, and so the full extension is in $\mathcal{C}$. Therefore, to show a class $\mathcal{C}$ is distinguished, we noly need to check the properties (1) and (2).

If a class $\mathcal{C}$ of extensions has the property that

$$(K \subseteq E_i) \in \mathcal{C} \Rightarrow (K \subseteq \bigvee E_i) \in \mathcal{C}$$

for any family $\{E_i\}$ of fields (provided, as always, that the composite is defined), we say that $\mathcal{C}$ is **closed under arbitrary composites**. This property does not follow from closure under finite composites.

Here is a list of the common types of extensions and their distinguishedness. We will verify these statements in due course.

1.1.2 Simple, finite, and algebraic extensions

1.1.2.1 Simple extensions

Definition 1.1.2.1. A field extension E/K is **simple** if there exists an element $\alpha \in K$ such that $E = K(\alpha)$.

Distinguished	Nondistinguished
Algebraic extensions	Simple extensions
Finite extensions	Transcendental extensions
Finitely generated extensions	Normal extensions
Separable extensions	
Purely ineparable extensions	

Let $f(X) \in K[X]$ be a monic polynomial of degree n, and let $(f(X))$ be the ideal generated by f. Consider the quotient ring $K[X]/(f(X))$, and write α for the image of X in $K[X]/(f(X))$. The map $g(X) \mapsto g(\alpha)$ is a homomorphism from $K[X]$ to $K[\alpha]$ sending $f(X)$ to 0, so we have $f(X) = 0$. Moreover, the division algorithm shows that each element g of $K[X]/(f(X))$ is represented by a unique polynomial r of degree $< n$. Hence each element of $K[X]$ can be expressed uniquely as a sum

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in K.$$

If in addition $f(X)$ is irreducible, then every nonzero in $K[\alpha]$ has an inverse, so $K[\alpha]$ becomes a field which extends K. From these observations, we conclude:

Proposition 1.1.2.2. *For a monic irreducible polynomial $f(X)$ of degree n in $K[X]$,*

$$E = K[X]/(f(X))$$

is a field of degree n over K.

It turns out that every simple extension is of the form mentioned above. To be precise, we have the following result.

Proposition 1.1.2.3. *Let $K \subseteq K(\alpha)$ be a simple extension. Consider the evaluation map $\epsilon : K[X] \to K(\alpha)$, defined by $f(X) \mapsto f(\alpha)$. Then we have the following:*

(i) *ϵ is injective if and only if $K(\alpha)/K$ is an infinite extension. In this case, $K(\alpha)$ is isomorphic to the field of rational functions $K(X)$.*

(ii) *ϵ is not injective if and only if $K(\alpha)$ is finite. In this case there exists a unique monic irreducible nonconstant polynomial $p(X) \in K[X]$ of degree $n = [K(\alpha) : K]$ such that*

$$K(\alpha) \cong \frac{K[X]}{(p(X))}$$

Via this isomorphism, α corresponds to the coset of x. The polynomial $p(X)$ is the monic polynomial of smallest degree in $K[X]$ such that $p(\alpha) = 0$ in $K(\alpha)$, it is called the ***minimal polynomial*** *of α over K.*

Proof. By the first isomorphism theorem, the image of $\epsilon : K[X] \to K(\alpha)$ is isomorphic to $K[X]/\ker\epsilon$. Since $K(\alpha)$ is an integral domain, so is $K[X]/\ker\epsilon$; hence $\ker(\epsilon)$ is a prime ideal in $K[X]$.

Assume $\ker\epsilon = 0$; that is, ϵ is an injective map from the integral domain $K[X]$ to the field $K(\alpha)$. By the universal property of fields of fractions, ϵ extends to a unique homomorphism

$$K(X) \to K(\alpha).$$

The (isomorphic) image of $K(X)$ in $K(\alpha)$ is a field containing K and α; hence it equals $K(\alpha)$ by definition of simple extension.

Since ϵ is injective, the powers $1, \alpha, \alpha^2, \cdots$ (that is, the images $\epsilon(X^i)$) are all distinct and linearly independent over K (because the powers $1, X, X^2, \cdots$ are linearly independent over K); therefore the extension $K \subseteq K(\alpha)$ is infinite in this case.

If $\ker\epsilon \neq 0$, then $\ker\epsilon = (p(X))$ for a unique monic irreducible nonconstant polynomial $p(X)$, which has smallest degree among all nonzero polynomials in $\ker\epsilon$. As $(p(X))$ is then maximal in $K[X]$, the image of ϵ is a subfield of $K(\alpha)$ containing $\alpha = \epsilon(X)$. By definition of simple extension, $K(\alpha)$ is the image of ϵ; that is, the induced homomorphism

$$\frac{K[X]}{(f(X))} \to K(\alpha)$$

is an isomorphism. In this case $[K(\alpha) : K] = \deg p(X)$, and in particular the extension is finite, as claimed. □

Example 1.1.2.4. Consider the extension $\mathbb{Q} \subseteq \mathbb{R}$. The polynomial $X^2 - 2 \in \mathbb{Q}[X]$ has roots in $\mathbb{R}$; therefore, there exists a homomorphism (hence a field extension)

$$\epsilon : \frac{\mathbb{Q}[X]}{(X^2 - 2)} \to \mathbb{R}$$

such that the image of (the coset of) x is a root α of $X^2 - 2$. Proposition 1.1.2.3 simply identifies the image of this homomorphism with $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

This is hopefully crystal clear; however, note that even this simple example shows that the induced morphism ϵ is not unique: because there are more than one root of $X^2 - 2$ in $\mathbb{R}$. Concretely, there are two possible choices for $\alpha : \alpha = +\sqrt{2}$ and $\alpha = -\sqrt{2}$. The choice of α determines the evaluation map ϵ and therefore the specific realization of $\mathbb{Q}[X]/(X^2 - 2)$ as a subfield of R.

Definition 1.1.2.5. Let E/K be a field extension. The **group of automorphisms** of the extension, denoted $\mathrm{Aut}_K(E)$, is the group of field automorphisms $\sigma : E \to E$ such that $\sigma|_K = \mathrm{id}_K$.

Corollary 1.1.2.6. *Let $K \subseteq E = K(\alpha)$ be a simple finite extension, and let $p(X)$ be the minimal polynomial of α over K. Then $|\mathrm{Aut}_K(E)|$ equals the number of distinct roots of $p(X)$ in K; in particular,*

$$|\mathrm{Aut}_K(E)| \leq [E : K]$$

with equality if and only if $p(X)$ factors over K as a product of distinct linear polynomials.

The class of simple extensions has all of the properties required of distinguished extensions except that the lower and upper steps being simple does not imply that the full extension is simple. That is, if each step in a 2-tower is simple

$$K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta).$$

this does not imply that the full extension is simple.

Example 1.1.2.7. Let u and v be independent variables and let p be a prime. In the tower

$$\mathbb{F}_p(u^p, v^p) \subseteq \mathbb{F}_p(u, v^p) \subseteq \mathbb{F}_p(u, v)$$

each step is simple but the full extension is not. We will prove this in due time.

On the other hand, if the full extension is simple: $K \subseteq K \subseteq K(\alpha)$, then the upper step is $K \subseteq K(\alpha)$, which is simple. Also, the lower step is simple, but the nontrivial proof requires us to consider the algebraic and transcendental cases separately. Here we give a proof about the algebraic case.

Proposition 1.1.2.8. *A finite extension E/K is simple if and only if the number of distinct intermediate fields $K \subseteq K \subseteq E$ is finite.*

Proof. Assume $E = K(\alpha)$ is simple and algebraic, and let $q(X)$ be the minimal polynomial of α over K. Embed E in an algebraic closure $\overline{K}$ of K. If K is an intermediate field, then $E = K(\alpha)$ is also a simple, algebraic extension; denote by $q_K(X)$ the minimal polynomial of α over K. Since $q_K(X) \in K[X]$ for all K and $q_K(\alpha) = 0$, we know that each $q_K(X)$ is a factor of $q_K(X)$. We claim that K is in fact determined by $q_K(X)$. Since $q_K(X)$ has finitely many factors in K, this proves that there are only finitely many intermediate fields, that is, the only if part of the statement.

To verigy our claim, let K_0 be the field generated by the coefficients of $q_K(X)$. Then q_K has coefficients in K_0 and is irreducible over K_0 since it is irreducible over K. Hence the degree of α over K_0 is the same as the degree of α over K, and this implies $K = K_0$.

Assume that there is only a finite number of fields, intermediate between K and E. Let $\alpha, \beta \in E$. As c ranges over elements of K, we can only have a finite number of fields of type $K(c\alpha + \beta)$. Hence there exist elements $c_1, c_2 \in K$ with $c_1 \neq c_2$ such that

$$K(c_1\alpha + \beta) = K(c_2\alpha + \beta)$$

Note that $c_1\alpha + \beta$ and $c_2\alpha + \beta$ are in the same field, whence so is $(c_1 - c_2)\alpha$, and hence so is α. Thus β is also in that field, and we see that $K(\alpha, \beta)$ can be generated by one element.

Proceeding inductively, if $E = K(\alpha_1, \ldots, \alpha_n)$ then there will exist elements $c_1, \ldots, c_n \in K$ such that

$$E = K(c_1\alpha_1 + \cdots + c_n\alpha_n).$$

This proves our claim. □

In view of the previous theorem, it is clear that if $K \subseteq E \subseteq K(\alpha)$, where α is *algebraic*, then the lower step $K \subseteq E$ is also simple. (Note that $K \subseteq E$ is a finite extension and therefore finitely generated by the elements of a basis for E over K, whose elements are algebraic over K.)

1.1.2.2 Finite and algebraic extensions Now we consider more complicated cases. The finite extension and algebraic extension defined below will be of our main consideration.

Definition 1.1.2.9. Let E/K be a field extension, and let $\alpha \in E$. Then α is **algebraic** over K of degree n if $n = [K(\alpha) : K]$ is finite; α is **transcendantal** over K otherwise. The extension E/K is **algebraic** if every $\alpha \in E$ is algebraic over K.

By Proposition 1.1.2.3, $\alpha \in E$ is algebraic over K if and only if there exists a nonzero polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$. The minimal polynomial of α is the monic polynomial of smallest degree satisfying this condition; as we have seen, it is necessarily irreducible. Also note that if α is algebraic over K, then every element of $K(\alpha)$ may in fact be written as a polynomial with coefficients in K.

It is clear that a finite extension must be algebraic.

Proposition 1.1.2.10. *Let E/K be a finite extension. Then every $\alpha \in E$ is algebraic over K, with degree less than $[E : K]$.*

Proof. Since $K \subseteq K(\alpha) \subseteq E$, the dimension of $K(\alpha)$ as a K-vector space is bounded by $\dim_K E = [E : K]$. □

Concretely, if E/K is finite and $\alpha \in E$, then the powers $1, \alpha, \alpha^2, \dots$ are necessarily *linearly dependent*; and any nontrivial linear dependence relation among them provides us with a nonzero polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$.

The literal converse of the claim that finite extensions are algebraic is not true; we will see an example in a moment. However, something along these lines holds; understanding the situation requires a more careful look at finiteness conditions.

First of all, compositions of finite extensions are finite extensions, and the degree behaves nicely with respect to this operation:

Proposition 1.1.2.11 (Multiplicativity of Degrees). *Consider fields $K \subseteq E \subseteq F$. Then F/K is of finite degree if and only if F/E and E/K are both of finite degree, in which case*

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

Proof. If F is finite over K, then it is certainly finite over E; moreover, E, being a subspace of a finite-dimensional K-vector space, is also finite-dimensional.

Thus, assume that F/E and E/K are of finite degree, and let $\{e_1, \dots, e_m\}$ be a basis for E as an K-vector space and let $\{f_1, \dots, f_n\}$ be a basis for F as an E-vector space. To complete the proof of the proposition, it suffices to show that $\{e_i f_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for F over K, because then F will be finite over K of the predicted degree.

First, $\{e_i f_j\}$ spans F: let $\gamma \in F$, then because $\{f_j\}$ spans F as an E-vector space, we have

$$\gamma = \sum_j \alpha_j f_j$$

for some $\alpha_j \in E$. Because $\{e_i\}$ spans E as an K-vector space, for each j there exist $a_{ij} \in K$ such that

$$\alpha_j = \sum_i a_{ij} e_i.$$

On putting these together, we find that

$$\gamma = \sum_{i,j} a_{ij} e_i f_j.$$

Second, $\{e_i f_j\}$ is linearly independent. A linear relation $\sum_{ij} a_{ij} e_i f_j = 0$, $a_{ij} \in K$, can be rewritten into $\sum_j (\sum_i a_{ij} e_i) f_j = 0$. The linear independence of the f_j's now shows that $\sum_i a_{ij} e_i = 0$ for each j, and the linear independence of the e_i's shows that each $a_{ij} = 0$. □

As in the case of groups, we draw the immediate (but powerful) consequence, reminiscent of Lagrange's theorem:

Corollary 1.1.2.12. *Let L/K be a finite extension, and let E be an intermediate field (that is, $K \subseteq E \subseteq L$). Then both $[L : E]$ and $[E : K]$ divide $[L : K]$.*

Example 1.1.2.13. Let E/K be a field extension, and let $\alpha \in E$ be an algebraic element over K, of odd order. Then we claim that α may be written as a polynomial in α^2, with coefficients in K. Indeed, $K(\alpha^2)$ is intermediate between K and $K(\alpha)$:

$$K \subseteq K(\alpha^2) \subseteq K(\alpha)$$

Let $d = [K(\alpha) : K(\alpha^2)]$. Since α satisfies the polynomial $X^2 - \alpha^2 \in K(\alpha^2)[X]$, we get $d \leq 2$. On the other hand, d divides $[K(\alpha) : K]$ by Corollary 1.1.2.12, and $[K(\alpha) : K]$ is odd, so $d \neq 2$. Therefore $d = 1$, proving $K(\alpha) = K(\alpha^2)$, and in particular $\alpha \in K(\alpha^2)$, which is the claim.

Here is something else that should evoke fond memories for the reader. An algebra is **finite** over the base ring if it is finitely generated as a *module*, that is, if it admits an onto homomorphism (of modules) from a finitely generated free module; a commutative algebra is of **finite type** if it admits an onto homomorphism (of algebras) from a polynomial ring in finitely many variables.

Something along the same lines is going to occur here. First, it is easy to see that an extension E/K is finite if and only if $\dim_K E$ is finite, that is, if and only if E is a finite K-algebra. The other finiteness condition takes the following form.

Definition 1.1.2.14. A field extension E/K is **finitely generated** if there exist $\alpha_1, \ldots, \alpha_n \in K$ such that

$$E = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Coming back to the issue of finite vs. algebraic, these two notions do coincide for finitely generated extensions.

Proposition 1.1.2.15. *Let $K \subseteq E = K(\alpha_1, \ldots, \alpha_n)$ be a finitely generated field extension. Then the following are equivalent:*

(i) *E/K is a finite extension.*

(ii) *E/K is an algebraic extension.*

(iii) *Each α_i is algebraic over K.*

If these conditions are satisfied, then

$$[E : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

Proof. Proposition 1.1.2.10 show that (i) ⇒ (ii), (ii) ⇒ (iii) tivially, so we prove the implication (iii) ⇒ (i). Assume that each α_i is algebraic over K, and let d_i be the degree of α_i over K. By definition, $K \subseteq K(\alpha_i)$ is finite, of degree d_i. Since each extension

$$K(\alpha_1, \ldots, \alpha_{i-1}) \subseteq K(\alpha_1, \ldots, \alpha_i)$$

is finite, of degree $\leq d_i$, Applying Corollary 1.1.2.12 to the composition of extensions

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n) = E$$

proves that E/K is finite and $[E : K] \leq d_1 \cdots d_n$, as needed. □

While rather straightforward, Proposition 1.1.2.15 has always seemed remarkable to us: it says (in particular) that if α and β are algebraic over a field K, then so are $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ and any other rational function of α and β. One immediate consequence of this observation is that the set of algebraic elements of any extension forms a field:

Corollary 1.1.2.16. *Let E/K be a field extension. Let*

$$\overline{K} = \{\alpha \in E : \alpha \textit{ is algebraic over } K\}.$$

Then $\overline{K}$ is a field.

Example 1.1.2.17. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the set of complex numbers that are algebraic over $\mathbb{Q}$; then $\overline{\mathbb{Q}}$ is a field, and the extension $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is (tautologically) algebraic. Note that $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is not a finite extension, because in it there are elements of arbitrarily high degree over $\mathbb{Q}$: indeed, there exist irreducible polynomials in $\mathbb{Q}[X]$ of arbitrarily high degree.

Corollary 1.1.2.18. *If E is algebraic over K, then every subring of E containing K is a field.*

Proof. Let A be a ring with $K \subseteq A \subseteq E$. If $\alpha \in A$, then $K[\alpha] \subseteq A$. But $K[\alpha]$ is a field because α is algebraic, and so A contains α^{-1}. This implies A is a field. □

Another consequence of Proposition 1.1.2.15 is the important fact that compositions of algebraic extensions are algebraic (whether finitely generated or not):

Corollary 1.1.2.19. *Let $K \subseteq E \subseteq F$ be field extensions. Then F/K is algebraic if and only if both F/E and E/K are algebraic.*

Proof. If F/K is algebraic, then every element of F is algebraic over K, hence over E, and every element of E is algebraic over K; thus F/K and E/K are algebraic.

Conversely, assume F/E and E/K are both algebraic, and let $\alpha \in F$. Since α is algebraic over E, there exists a polynomial

$$f(X) = X^n + e_{n-1}X^{n-1} + \cdots + e_0 \in E[X]$$

such that $f(\alpha) = 0$. This implies that α is already algebraic over the subfield $K(e_0, \ldots, e_{n-1})$; therefore,

$$K(e_0, \ldots, e_{n-1}) \subseteq K(e_0, \ldots, e_{n-1}, \alpha)$$

is a finite extension. On the other hand, since each e_i is in E and therefore algebraic over K, the extension

$$K \subseteq K(e_0, \ldots, e_{n-1})$$

is finite by Proposition 1.1.2.15. By Proposition 1.1.2.11 the extension

$$K \subseteq K(e_0, \ldots, e_{n-1}, \alpha)$$

is finite. This implies that α is algebraic over K. □

Theorem 1.1.2.20. *Let E be an extension of K and X a subset of E such that $E = K(X)$ and every element of X is algebraic over K. Then E is an algebraic extension of K. If X is a finite set, then E is a finite extension of K.*

Proof. If $\beta \in E$, then $\beta \in K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in X$. By Proposition 1.1.2.15, since $K(\alpha_1, \ldots, \alpha_n)$ is finitely generated, we conclude that it is finite. Hence by Proposition 1.1.2.10 β is algebraic over K. □

We will essentially deal only with finitely generated extensions, and Proposition 1.1.2.15 will simplify our work considerably. Also, since finitely generated extensions are compositions of simple extensions, the reader should expect that we will give a careful look at automorphisms of such extensions.

It may in fact come as a surprise that, in many cases, finitely generated extensions turn out to be simple to begin with; we will prove a precise statement to this effect in due time. The reader already has enough tools to contemplate easy (but interesting) examples, such as the following. This should serve as an encouragement to look at many more.

Example 1.1.2.21. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a finite extension, of degree at most 4, thus any five elements in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must be linearly dependent over $\mathbb{Q}$. We consider the powers of $(\sqrt{2} + \sqrt{3})$:

$$1, \quad (\sqrt{2}+\sqrt{3}), \quad (\sqrt{2}+\sqrt{3})^2, \quad (\sqrt{2}+\sqrt{3})^3, \quad (\sqrt{2}+\sqrt{3})^4.$$

These elements must be linearly dependent, and we find

$$q_0 + q_1(\sqrt{2}+\sqrt{3}) + q_2(\sqrt{2}+\sqrt{3})^2 + q_3(\sqrt{2}+\sqrt{3})^3 + (\sqrt{2}+\sqrt{3})^4 = 0$$

is satisfied when $q_0 = 1, q_1 = 0, q_2 = -10, q_3 = 0$: that is, $(\sqrt{2}+\sqrt{3})$ is the root of

$$f(X) = X^4 - 10X^2 + 1.$$

It follows that $\sqrt{2}+\sqrt{3}$ has degree 4 over $\mathbb{Q}$, therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Consider the composition of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

By Corollary 1.1.2.12, we have

$$4 = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}],$$

thus we conclude that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3})]$, and it follows that

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Staring now at the composition

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}),$$

Corollary 1.1.2.12 tells us that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. That is, a side-effect of the computation carried out above is that the polynomial $t^2 - 3$ must be irreducible over $\mathbb{Q}(\sqrt{2})$.

The fact that the other roots of the minimal polynomial of $\sqrt{2}+\sqrt{3}$ looked so much like $\sqrt{2}+\sqrt{3}$ is not surprising. Indeed, since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a simple extension, we know that there is an automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ fixing $\mathbb{Q}(\sqrt{2})$ and swappint $\sqrt{3}$ and $-\sqrt{3}$. Similarly, there is an automorphism fixing $\mathbb{Q}(\sqrt{3})$ and swapping $\sqrt{2}$ and $-\sqrt{2}$. These automorphisms must act on the set of roots of $f(X)$: applying them and their composition to $\sqrt{2}+\sqrt{3}$ produces the other three roots of $f(X)$.

In fact, at this point we know that $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ must consist of 4 elements and has at least two elements of order 2 (both automorphisms found above have order 2). This is enough to conclude that G is not a cyclic group, and hence it must be isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.1.3 Algebraic closure

Recall that a field K is **algebraically closed** if all irreducible polynomials in $K[X]$ have degree 1, that is, if every polynomial in $K[X]$ factors completely as a product of linear terms. Equivalently every maximal ideal in $K[X]$ is of the form $(X - c)$, for $c \in K$. The following lemma is immediate from the definition.

Lemma 1.1.3.1. *For a field K, the following are equivalent:*

- *K is algebraically closed.*
- *K has no nontrivial algebraic extensions.*
- *If L is any extension of K and $\alpha \in L$ is algebraic over K, then $\alpha \in K$.*

Definition 1.1.3.2. An **algebraic closure** of a field K is an algebraic extension $K \subseteq \Omega$ such that Ω is algebraically closed.

We can now easily establish the existence of algebraic closures.

Theorem 1.1.3.3. *Let K be a field. Then there is an extension Ω of K that is algebraically closed.*

Proof. The following proof is due to Emil Artin. The first step is to construct an extension field K_1 of K, with the property that all nonconstant polynomials in $K[X]$ have a root in K_1.

To do this, consider a set $\mathscr{T} = \{t_f\}$ in bijection with the set of nonconstant monic polynomials $f(X) \in K[X]$, and let $K[\mathscr{T}]$ be the corresponding polynomial ring in all the indeterminates t_f. Let $I \subseteq K[\mathscr{T}]$ be the ideal generated by all polynomials $f(t_f)$. Then I is a proper ideal. Indeed, otherwise we could write

$$1 = \sum_{i=1}^{n} a_i f_i(t_{f_i}) \tag{1.1.3.1}$$

where $a_i \in K[\mathscr{T}]$. We claim that this cannot be done: indeed, we can construct an extension E/K where the polynomials $f_1, \dots, f_n$ have roots $\alpha_1, \dots, \alpha_n$, respectively; view (1.1.3.1) as an identity in $F[\mathscr{T}]$, and plug in $t_{f_i} = \alpha_i$, obtaining

$$1 = \sum_{i=1}^{n} a_i f(\alpha_i) = \sum_{i=1}^{n} a_i \cdot 0 = 0$$

which is nonsense.

Since I is proper, it is contained in a maximal ideal $\mathfrak{m}$ containing I. Thus, we obtain a field extension

$$K \subseteq K_1 := K[\mathscr{T}]/\mathfrak{m}.$$

By construction every nonconstant monic (and hence every nonconstant) polynomial $f(X)$ has a root in K_1, namely the coset of t_f.

Using the same technique, we may define a tower of field extensions

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

such that each nonconstant polynomial $f(X) \in K_i[X]$ has a root in K_{i+1}. The union $\Omega = \bigcup_i K_i$ is an extension field of K. Moreover, any polynomial $f(X) \in \Omega[X]$ has all of its coefficients in K_i for some i and so has a root in K_i, hence in Ω. It follows that every polynomial in $\Omega[X]$ splits over Ω. Hence Ω is algebraically closed. □

We can now easily establish the existence of algebraic closures.

Theorem 1.1.3.4. *Let $K \subseteq L$ be a field extension where L is algebraically closed. Let*

$$\overline{K} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then $\overline{K}$ is the only algebraic closure of K that is contained in L. Thus, any field has an algebraic closure.

Proof. By Corollary 1.1.2.16, $\overline{K}$ is a field, and the extension $K \subseteq \overline{K}$ is tautologically algebraic. To verify that $\overline{K}$ is algebraically closed, let α be algebraic over $\overline{K}$; then

$$K \subseteq \overline{K} \subseteq \overline{K}(\alpha)$$

is a composition of algebraic extensions, so $\overline{K} \subseteq \overline{K}(\alpha)$ is algebraic, and in particular α is algebraic over K. But then $\alpha \in \overline{K}$, by definition of the latter. It follows that $\overline{K}$ is algebraically closed, by Lemma 1.1.3.1.

As to uniqueness, if $K \subseteq E \subseteq L$ with E an algebraic closure of K, then since $K \subseteq E$ is algebraic, we have $E \subseteq \overline{K}$. But if the inclusion is proper, then there is an $\alpha \in \overline{K} \setminus E$. It follows that $\min(\alpha, E)$ does not split over E, a contradiction to the fact that E is algebraically closed. Hence $\overline{K} = E$. The final statement comes from Theorem 1.1.3.3. □

We will show a bit later that all algebraic closures of a field K are isomorphic, which is one reason why the notation $\overline{K}$ is (at least partially) justified.

Here is a characterization of algebraic closures.

Proposition 1.1.3.5. *Let $K \subseteq E$ be a field extension. The following are equivalent.*

(i) *E is an algebraic closure of K.*

(ii) *E is a maximal algebraic extension of K, that is, $K \subseteq E$ is algebraic, and if $E \subseteq F$ is algebraic then $F = E$.*

(iii) *E is a minimal algebraically closed extension of K, that is, if $K \subseteq E' \subseteq E$ where E' is algebraically closed, then $E' = E$.*

(iv) *$K \subseteq E$ is algebraic and every nonconstant polynomial in $K[X]$ splits over E.*

Proof. To see that (i) implies (ii), suppose that E is an algebraic closure of K. Then E/K is algebraic by definition. If $E \subseteq F$ is another algebraic extension, then by Lemma 1.1.3.1 we have $F = E$. Therefore E is a maximal algebraic extension of K. Conversely, let E be a maximal algebraic extension of K and let $f(X) \in E[X]$. Let L be the splitting field for $f(X)$ over E. Then $K \subseteq E \subseteq L$ is an algebraic tower, since L is generated over E by the finite set of roots of $f(X)$. Hence, the maximality of E implies that $E = L$, and so $f(X)$ splits in E, which says that E is algebraically closed and therefore an algebraic closure of K.

To see that (i) implies (iii), suppose that E is an algebraic closure of K and $K \subseteq E' \subseteq E$, where E' is algebraically closed. Since $E' \subseteq E$ is algebraic, it follows that $E' = E$, by Lemma 1.1.3.1. Conversely, suppose that E is a minimal algebraically closed extension of K. Let $\overline{K}$ be the algebraic closure of K in E. Thus, $K \subseteq \overline{K} \subseteq E$, with $K \subseteq \overline{K}$ algebraic. By hypothesis, since $\overline{K}$ is algebraic closed, we conclude $\overline{K} = E$, so E is an algebraic closure of K.

Finally, it is clear that (i) implies (iv). If (iv) holds, then E/K is algebraic and if $K \subseteq E \subseteq L$ is algebraic, then let $\alpha \in L \setminus E$ have minimal polynomial $f(X)$ over K. This polynomial splits over E and so $\alpha \in E$, which implies that $E = L$, whence E is a maximal algebraic extension of K and so (ii) holds. □

1.1.4 Embeddings and their extensions

Homomorphisms between fields play a key role in the theory. Since a field has no nontrivial ideals, any homomorphism between fields is actually an embedding. In this part we study the general properties of embedding of fields and the extension of embeddings.

Let $\sigma : K \to L$ be an embedding of K into L and let E be an extension of K. An embedding $\bar{\sigma} : E \to L$ for which $\bar{\sigma}|_K = \sigma$ is called an **extension** of σ to E. An embedding of E that extends the identity map on K is called an **embedding over K**, or **K-embedding**. The set of all embeddings of K into L is denoted by $\mathrm{Hom}(K, L)$; the set of all embeddings of E into L that extend σ is denoted by $\mathrm{Hom}_\sigma(E, L)$ and the set of all embeddings over F is denoted by $\mathrm{Hom}_K(E, L)$.

Embeddings play a central role in Galois theory, and it is important to know when a given embedding $\sigma : K \to L$ can be extended to a larger field E, and how many such embeddings are possible. We will discuss the former issue here, and the latter issue in the next section.

First we establish some basic properties of embeddings. If $f(X) = \sum_i a_i X^i \in K[X]$ and if $\sigma : K \to E$ is an embedding, the polynomial $\sum_i \sigma(a_i)X^i$ is denoted by $f^\sigma(X)$.

Proposition 1.1.4.1 (Properties of embeddings).

(i) ***(Embeddings preserve factorizations and roots)*** *If $\sigma : K \to L$ is an embedding and $f(X)$, $p(X)$, $q(X)$ are polynomials in $K[X]$, then $f(X) = p(X)q(X)$ if and only if $f^\sigma(X) = p^\sigma(X)q^\sigma(X)$. Also, $\alpha \in K$ is a root of $f(X)$ if and only if $\sigma(\alpha)$ is a root of $f^\sigma(X)$.*

(ii) ***(Embeddings preserve the lattice structure)*** *If $\sigma : F \to L$ is an embedding and $\{E_i : i \in I\}$ is a family of subfields of F, then*

$$\sigma\Big(\bigcap_i E_i\Big) = \bigcap_i \sigma(E_i), \quad \sigma\Big(\bigvee_i E_i\Big) = \bigvee_i \sigma(E_i).$$

(iii) ***(Embeddings preserve adjoining)*** *If $\sigma : E \to F$ is an embedding and if $K \subseteq E$ and $S \subseteq E$, then*

$$\sigma(K(S)) = \sigma(K)(\sigma(S)).$$

(iv) ***(Embeddings preserve being algebraic)*** *Let $\sigma : K \to L$ is an embedding and let E/K be an algebraic extension. If $\bar{\sigma} : E \to L$ is an extension of σ, then $\sigma(K) \subseteq \bar{\sigma}(E)$ is algebraic.*

(v) ***(Embeddings preserve algebraic closures)*** *Let $\sigma : K \to L$ and let E be an algebraic closure of K. If $\bar{\sigma} : E \to L$ is an extension of σ, then $\bar{\sigma}(E)$ is an algebraic closure of $\sigma(K)$.*

Proof. Part (i) is easy to prove, and part (ii) follows from the following observation

$$\begin{aligned}\sigma\Big(\bigvee E_i\Big) &= \bigcap\{\sigma(H) : E_i \subseteq H \subseteq F \text{ for all } i \in I\} \\ &= \bigcap\{H' : \sigma(E_i) \subseteq H' \subseteq \sigma(F) \text{ for all } i \in I\} = \bigvee \sigma(E_i).\end{aligned}$$

Also, part (iii) follows from (ii).

For (iv), let $\alpha \in E$, then α is algebraic over K, so there is a polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$. By (i) we know that $\bar{\sigma}(\alpha)$ is a root of $f^{\bar{\sigma}}$, so it is algebraic over $\sigma(K)$, since α is arbitrary, this implies $\bar{\sigma}(E)$ is algebraic over $\sigma(K)$. Finally we prove (v). Since E/K is algebraic, by (iv) the extension $\bar{\sigma}(E)$ is algebraic over $\sigma(K)$. Let f^σ be a polynomial in $\sigma(K)[X]$. Then $f(X) \in K[X]$ so $f(X)$ split in E, since E is algebraic closed. It follows that f^σ split in $\bar{\sigma}(E)$, in view of (i), and therefore $\bar{\sigma}(E)$ is an algebraic closure of $\sigma(K)$, by Proposition 1.1.3.5. □

Even though the next result has a simple proof, the result is of major importance.

Theorem 1.1.4.2. *If $K \subseteq E$ is algebraic and $\sigma : E \to E$ is a K-embedding, then σ is an automorphism. In other words,*

$$\mathrm{Hom}_K(E, E) = \mathrm{Aut}_K(E).$$

Proof. Let $\alpha \in E$ and let R be the set of roots of the minimal polynomial of α that lie in E. Then $\sigma|_R$ is an injection on R and so is bijective. Therefore there is a $\beta \in S$ for which $\sigma(\beta) = \alpha$. Hence, σ is surjective and thus an automorphism of E. □

Now we proceed the construction of extension of embeddings. We first consider simple extensions. Suppose that $\sigma : K \to L$, where L is algebraically closed. Let α be algebraic over K. We can easily extend σ to $K(\alpha)$, using the minimal polynomial of α over K.

Proposition 1.1.4.3. *Let $K \subseteq E$ and let $\alpha \in E$ be algebraic over K with minimal polynomial $f(X)$. Let $\sigma : K \to L$ be an embedding, where L is algebraically closed.*

(i) *If β is any root of f^σ in L, then σ can be extended to an embedding $\bar{\sigma} : K(\alpha) \to L$ for which $\bar{\sigma}(\alpha) = \beta$. Moreover, any extension of σ to $K(\alpha)$ must have this form.*

(ii) *The number of extensions of σ to $K(\alpha)$ is equal to the number of distinct roots of $f(X)$ in L.*

Proof. The key point is that any extension $\bar{\sigma}$ of σ is completely determined by its value on α and this value must be a root β of $f^\sigma(X)$. In fact, we must have

$$\bar{\sigma}(f(\alpha)) = f^\sigma(\beta)$$

for any $f \in K[X]$. This prove (i), and (ii) follows from (i). □

The simple case above, together with Zorn's lemma, is just what we need to prove that if $\sigma : K \to L$, with L algebraically closed and if E/K is algebraic, then there is at least one extension of σ to E.

Theorem 1.1.4.4. *Let $K \subseteq E$ be an algebraic extension. Then any embedding $\sigma : K \to L$, where L is algebraically closed, can be extended to an embedding $\bar{\sigma} : E \to L$. Moreover, if $\alpha \in E$, $f(X) = \min(\alpha, K)$, and β is a root of $f^\sigma(X)$, then we can choose $\bar{\sigma}$ so that $\bar{\sigma}(\alpha) = \beta$.*

Proof. Consider the set $\mathcal{E}$ of homomorphisms $\tau \in \mathrm{Hom}_\sigma(K, L)$ such that $\tau(\alpha) = \beta$, where K is an intermediate field; $\mathcal{E}$ is nonempty, since the extension $\sigma_\beta : K(\alpha) \subseteq L$ defined by $\sigma_\beta(\alpha) = \beta$ gives an element of $\mathcal{E}$. We give a poset structure to $\mathcal{E}$ by defining

$$\tau \preceq \tau'$$

if $K \subseteq K' \subseteq E$ and τ' restricts to τ on K. If $\mathcal{K} = \{\tau_i : K_i \to L\}$ is a chain in $\mathcal{E}$, the map $\tau : \bigcup K_i \to L$ defined by the condition $\tau|_{K_i} = \tau_i$ is an upper bound for $\mathcal{K}$ in $\mathcal{E}$. Zorn's lemma implies the existence of a maximal extension $\tau : K \to L$. We contend that $K = E$, for if not, there is an element $\gamma \in E \setminus K$. But γ is algebraic over K and so we may extend τ to $K(\gamma)$, contradicting the maximality. □

As a corollary, we can establish the essential uniqueness of algebraic closures.

Theorem 1.1.4.5. *Every field K admits an algebraic closure $K \subseteq \bar{K}$; this extension is unique up to isomorphism.*

Proof. We only need to show the second point. Let L_1 and L_2 be algebraic closures of K. The identity map $\mathrm{id} : K \to K$ can be extended to an embedding $\tau : L_1 \to L_2$. Since L_1 is algebraically closed so is $\sigma(L_1)$ (Proposition 1.1.4.1). But L_2 is an algebraic extension of $\sigma(L_1)$ and so $\sigma(L_1) = L_2$. Hence, σ is an isomorphism. □

To conclude, we introduce the independence of embedding and prove a very useful result. We choose a somewhat more general setting, however. A **monoid** is a nonempty set M with an associative binary operation and an identity element. If M and N are monoids, a homomorphism of M into N is a map $\varphi : M \to N$ such that $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ and $\varphi(1) = 1$.

Definition 1.1.4.6. Let M be a monoid and let K be a field. A homomorphism $\chi : M \to K^\times$, where $K^\times$ is the multiplicative group of all nonzero elements of K, is called a **character** of M in K.

Note that an embedding $\sigma : E \to L$ of fields is a character, when restricted to $E^\times$.

Theorem 1.1.4.7 (E. Artin). *Any set $\mathcal{T}$ of distinct characters of M in K is linearly independent over K.*

Proof. Suppose that we have a nontrivial relation

$$\sum_{i=1}^{n} a_i \chi_i = 0$$

for some $\chi_i \in \mathcal{T}$ and $a_i \in K$. Look among all such nontrivial linear combinations of the χ_i's for one with the fewest number of nonzero coefficients and, by relabeling if necessary, assume that these coefficients are $a_1, \ldots, a_r$. Thus,

$$a_1\chi_1(g) + \cdots + a_r\chi_r(g) = 0 \tag{1.1.4.1}$$

for all $g \in M$ and this is the "shortest" such nontrivial equation (hence $a_i \neq 0$ for all i). Note that since $\chi_i(g) \in K^\times$, we have $\chi_i(g) \neq 0$ for all $g \in M$. Hence, $r > 1$.

Let us find a shorter relation. Since χ_1 is a character, $\chi_1(f) \neq 0$ for all $f \in M$. Multiplying by $\chi_1(f)$ gives

$$a_1\chi_1(f)\chi_1(g) + a_2\chi_1(f)\chi_2(g) + \cdots + a_r\chi_1(f)\chi_r(g) = 0.$$

On the other hand, replacing g by fg in (1.1.4.1) gives

$$a_1\chi_1(f)\chi_1(g) + a_2\chi_2(f)\chi_2(g) + \cdots + a_r\chi_r(f)\chi_r(g) = 0.$$

Subtracting the two equations cancels the first term, and we get

$$a_2[\chi_1(f) - \chi_2(f)]\chi_2(g) + \cdots + a_r[\chi_1(f) - \chi_r(f)]\chi_r(g) = 0.$$

Now, since $\chi_1 \neq r$, there is an $f \in M$ for which $\chi_1(f) - \chi_r(f) \neq 0$ and we have a shorter nontrivial relation of the form (1.1.4.1). This contradiction proves the theorem. □

Corollary 1.1.4.8 (Dedekind independence theorem). *Let E and F be fields. Any set of distinct embeddings of E into F is linearly independent over F.*

1.1.5 Splitting fields and normal extensions

we have constructed the algebraic closure $\overline{K}$ of any given field K: every polynomial in $K[X]$ factors as a product of linear terms (that is, *splits*) in $\overline{K}[X]$, and $\overline{K}$ is the smallest extension of K satisfying this property.

Here is an analogous, but more modest, requirement: given a subset $\mathcal{F} \subseteq K[X]$ of polynomials, construct an extension E/K such that every polynomial in $\mathcal{F}$ splits as a product of linear terms over E, and require E to be as small as possible with this property. We then call E the *splitting field* for $\mathcal{F}$. To be precise, we make the following definition.

Definition 1.1.5.1. Let K be a field, and let $\mathcal{F}$ be a family of polynomials in $K[X]$. The **splitting field** for $\mathcal{F}$ over K is an extension E of K such that each polynomial in $\mathcal{F}$ splits in E and that E is generated by the set of all roots of the polynomials in $\mathcal{F}$.

The next theorem says that splitting fields not only exist, but are essentially unique.

Theorem 1.1.5.2. *Let $\mathcal{F}$ be a family of polynomials over K.*

(i) *In any algebraic closure $\overline{K}$ of K, there is a unique splitting field for $\mathcal{F}$.*

(ii) *If $K \subseteq E_1 \subseteq L_1$ and $K \subseteq E_2 \subseteq L_2$ are algebraic, where E_1 is the splitting field for $\mathcal{F}$ in L_1 and E_2 is the splitting field for $\mathcal{F}$ in L_2, then any embedding $\sigma : L_1 \to L_2$ over K maps E_1 onto E_2.*

(iii) *Any two splitting fields for $\mathcal{F}$ are isomorphic over K.*

Proof. For part (i), if $\mathcal{F}$ is a family of polynomials over K, then every member of $\mathcal{F}$ splits in $\overline{K}$ and so $\overline{K}$ contains the field E generated over K by the roots in $\overline{K}$ of the polynomials in $\mathcal{F}$, that is, $\overline{K}$ contains a splitting field for $\mathcal{F}$. It is clear that this splitting field is unique in $\overline{K}$, because any splitting field in $\overline{K}$ must be generated, in $\overline{K}$, by the roots of all polynomials in $\mathcal{F}$.

For part (ii), if R is the family of roots of $\mathcal{F}$ contained in L_1 then $E_1 = K(R)$ and so

$$\sigma(E_1) = \sigma(K(R)) = K(\sigma(R)).$$

But $\sigma(R)$ is precisely the set of roots of $\mathcal{F}$ in L_2 and so $K(\sigma(R))$ is the splitting field for $\mathcal{F}$ in L_2, that is, $\sigma(E_1) = E_2$. Part (iii) follows immediately from part (ii). □

Example 1.1.5.3. The splitting field of $X^8 - 1$ over $\mathbb{Q}$ is generated by $\zeta := e^{2\pi i}/8$: indeed, the roots of $X^8 - 1$ are all the 8-th roots of 1, and all of them are powers of ζ. In fact, ζ is a root of the polynomial $X^4 + 1$, which is irreducible over $\mathbb{Q}$; therefore $E = \mathbb{Q}(\zeta)$ is already the splitting field of $X^4 + 1$. The degree of E over $\mathbb{Q}$ is

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4.$$

To understand this splitting field better, note that $i = \zeta^2$ is in E, and so is $\sqrt{2} = \zeta + \bar{\zeta} = \zeta + \zeta^{-1}$; thus E contains $\mathbb{Q}(i, \sqrt{2})$. Conversely, $\zeta = \frac{\sqrt{2}}{2}(1 + i) \in \mathbb{Q}(i, \sqrt{2})$. Therefore, the splitting field of $X^4 + 1$ is $\mathbb{Q}(i, \sqrt{2})$. Analyzing $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2})$ shows that its group of automorphisms over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 1.1.5.4. The polynomial $X^4 - 1$ factors over $\mathbb{Q}$:

$$X^4 - 1 = (X^2 + 1)(X + 1)(X - 1)$$

and it follows that the splitting field is the same as for $X^2 + 1$, that is, just $\mathbb{Q}(i)$.

Example 1.1.5.5. Now consider the polynomial $X^4 + 2$ over $\mathbb{Q}$. The overoptimistic reader may now hope that the difference between the splitting fields of $X^4 + 1$ vs. $X^4 - 1$ over $\mathbb{Q}$ is just due to the fact that the first polynomial is irreducible over $\mathbb{Q}$ and the second is not. This example will nip any such guess in the bud. With notation as above, the roots of $X^4 + 2$ are

$$\sqrt[4]{2}\zeta, \quad \sqrt[4]{2}\zeta^3, \quad \sqrt[4]{2}\zeta^5, \quad \sqrt[4]{2}\zeta^7$$

Therefore, with $E = \mathbb{Q}(\sqrt[4]{2}\zeta, \sqrt[4]{2}\zeta^3, \sqrt[4]{2}\zeta^5, \sqrt[4]{2}\zeta^7)$ the splitting field of $X^4 + 2$,

$$E \subseteq \mathbb{Q}(\zeta, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2}).$$

On the other hand,

$$\sqrt{2} = \frac{(\sqrt[4]{2}\zeta)^3}{\sqrt[4]{2}\zeta^3}, \quad i = \frac{(\sqrt[4]{2})^2}{\sqrt{2}}, \quad \zeta = \frac{\sqrt{2}}{2}(1 + i), \quad \sqrt[4]{2} = \frac{\sqrt[4]{2}\zeta}{\zeta}.$$

Therefore, $\mathbb{Q}(i, \sqrt[4]{2}) \subseteq E$, and the conclusion is that the splitting field of $X^4 + 2$ equals $E = \mathbb{Q}(i, \sqrt[4]{2})$. A simple degree computation shows $[E : \mathbb{Q}] = 8$ and in particular the splitting field of $X^4 + 2$ is certainly not isomorphic to the splitting field of $X^4 + 1$.

Example 1.1.5.6. Consider the polynomial $X^6 + X^3 + 1$ over $\mathbb{Q}$. Let $\omega := (-1 + \sqrt{3}i)/2$. The solutions of $X^2 + X + 1$ are ω, ω^2, so the solutions of $X^6 + X^3 + 1$ are

$$\sqrt[3]{\omega}, \quad \omega\sqrt[3]{\omega}, \quad \omega^2\sqrt[3]{\omega}, \quad \sqrt[3]{\omega^2}, \quad \omega\sqrt[3]{\omega^2}, \quad \omega^2\sqrt[3]{\omega^2}.$$

So the splitting field of $X^6 + X^3 + 1$ is $\mathbb{Q}(\omega^{1/3})$, which has degree 9 over $\mathbb{Q}$.

Splitting fields will play an important role in the rest of the story. They are even more special than they may appear to be at first: it turns out that not only do they split the given polynomial, but they also automatically split any irreducible polynomial which dares touch them with a root. To make this property crystal clear, we introduce the following terminology.

Suppose that $K \subseteq E \subseteq \overline{K}$ is algebraic and that $\sigma : E \to \overline{K}$ is an embedding over K of E into the algebraic closure $\overline{K}$. Then E is said to be ***σ*-invariant** if $\sigma(E) \subseteq E$. However, since E/K is algebraic, any embedding of E into itself is an automorphism of E (Theorem 1.1.4.2) and so E is σ-invariant if and only if $\sigma(E) = E$, that is, if and only if σ is an automorphism of E.

If the field E is σ-invariant for all embeddings $\sigma : E \to \overline{K}$ over K, then it is not hard to see that any irreducible polynomial $f(X)$ over K that has one root α in E must split over K. For if β is also a root of $f(X)$ in $\overline{K}$, then there is an embedding $\sigma \in \operatorname{Hom}_K(E, \overline{K})$ for which $\sigma(\alpha) = \beta$. Hence, the σ-invariance of E implies that $\beta \in E$. Put another way, we can say that E is the splitting field for the family

$$\min(E, K) := \{\min(\alpha, K) : \alpha \in E\}.$$

We now formulate the observation above into the following theorem.

Theorem 1.1.5.7. *Let $K \subseteq E \subseteq \overline{K}$, where $\overline{K}$ is an algebraic closure of K. The following are equivalent.*

(i) *E is a splitting field for a family $\mathcal{F}$ of polynomials over K.*

(ii) *E is invariant under every embedding $\sigma : E \to \overline{K}$ over K.*

(iii) *Every irreducible polynomial over E having one root in E splits in E.*

Proof. We have already see the implications (ii) ⇒ (iii) ⇒ (i). Now we prove (i) ⇒ (ii). Suppose that E is a splitting field of a family $\mathcal{F}$ of polynomials over K. Thus, $E = K(R)$, where R is the set of roots of the polynomials in $\overline{K}$. But any embedding $\sigma : E \to \overline{K}$ over K sends roots to roots and so sends R to itself. Hence,

$$\sigma(E) = \sigma(K(R)) = K(\sigma(R)) = K(R) = E.$$

Since σ is an embedding of E into itself over K and $K \subseteq E$ is algebraic, it follows that σ is an automorphism of E. Thus the claim follows. □

Definition 1.1.5.8. An algebraic extension $K \subseteq E$ that satisfies any (and hence all) of the conditions in the previous theorem is said to be a **normal extension**. We also say that E is **normal** over K and write $K \lhd E$.

Corollary 1.1.5.9. *If E/K is a finite normal extension, then E is the splitting field of a finite family of irreducible polynomials.*

Proof. Let $E = K(\alpha_1, \dots, \alpha_n)$. Since E/K is normal, each minimal polynomial $\min(\alpha_i, K)$ splits in E. Clearly, E is generated by the roots of the finite family $\mathcal{F} = \{\min(\alpha_i, K) : i = 1, \dots, n\}$ and so E is the splitting field of $\mathcal{F}$. □

Note that the extension $K \subseteq \overline{K}$ is normal, since any nonconstant polynomial $f(X) \in K[X]$ splits in $\overline{K}$.

Example 1.1.5.10. If a complex root of an irreducible polynomial $p(X) \in \mathbb{Q}[X]$ may be expressed as a polynomial in i and $\sqrt[4]{2}$ with rational coefficients, then all roots of $p(X)$ may be expressed likewise in terms of i and $\sqrt[4]{2}$. Indeed, we have checked that $\mathbb{Q}(i, \sqrt[4]{2})$ is a splitting field over $\mathbb{Q}$; hence it is a normal extension of $\mathbb{Q}$.

Example 1.1.5.11. Let E/K be a degree 2 extension. Let $\alpha \in E \setminus K$, then the minimal polynomial of α over K must have degree 2, and therefore $E = K(\alpha)$. It follows that $\alpha^2 \in K$, and so $X^2 - \alpha^2$ is a polynomial in $K[X]$. Clearly this is the minimal polynomial of α. Since it splits in E, it follows that E is normal over K.

1.1.5.1 Normal extensions are not distinguished

As it happens, the class of normal extensions is not distinguished, but it does enjoy some of the associated properties.

Example 1.1.5.12. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal since $\mathbb{Q}(\sqrt[4]{2})$ contains exactly two of the four roots of the irreducible polynomial $X^4 - 2$. On the other hand,

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

has each step of degree 2 and therefore each step is normal.

Here is what we can say on the positive side.

Proposition 1.1.5.13 (Properties of normal extensions).

- *(a) (**Full extension normal implies upper step normal**) Let $K \subseteq E \subseteq F$. If F is normal over K then F is normal over E.*
- *(b) (**Lifting of a normal extension is normal**) If E is normal over K and $K \subseteq F$, then EF is normal over F.*
- *(c) (**Arbitrary composites and intersections of normal are normal**) If $\{E_i\}$ is a family of fields, and each E_i is normal over K, then $\bigvee E_i$ and $\bigcap E_i$ are both normal over K.*

Proof. Part (a) follows from the fact that a splitting field for a family of polynomials over K is also a splitting field for the same family of polynomials over E.

For (b), let E be a splitting field for a family $\mathcal{F}$ of polynomials over K and let R be the set of roots in E of all polynomials in $\mathcal{F}$. Then $E = K(R)$. Hence, $EF = F(K(R)) = F(R)$, which shows that EF is a splitting field for the family $\mathcal{F}$, thought of as a family of polynomials over F. Hence, EF is normal over F.

For (c), let $\sigma : \bigvee E_i \to \overline{K}$ be an embedding over K. Then σ is an embedding when restricted to each E_i and so $\sigma(E_i) = E_i$, whence

$$\sigma\Big(\bigvee E_i\Big) = \bigvee \sigma(E_i) = \bigvee E_i,$$

and so σ is an automorphism of $\bigvee E_i$. Similarly, if $\sigma : \bigcap E_i \to \overline{K}$ over K, then

$$\sigma\Big(\bigcap E_i) = \bigcap \sigma(E_i) = \bigcap E_i.$$

This proves the claim. □

1.1.5.2 Normal closures If the extension E/K is not normal, then there is a smallest extension N of E (in a given algebraic closure $\overline{K}$) for which N is normal over K. Perhaps the simplest way to see this is to observe that $K \subseteq \overline{K}$ is normal and the intersection of normal extensions is normal, so

$$N = \bigcap \{F \subseteq \overline{K} : F \text{ contains } E \text{ and the extension } F/K \text{ is normal}\}.$$

Definition 1.1.5.14. Let $K \subseteq E \subseteq \overline{K}$. The **normal closure** of E over K in $\overline{K}$ is the smallest subfield of $\overline{K}$ containing E for which F/K is normal. The normal closure is denoted by $\langle E/K \rangle$.

Theorem 1.1.5.15. *Let $K \subseteq E \subseteq \overline{K}$ be algebraic extensions, with normal closure $N = \langle E/K \rangle$.*

(b) N is the composition of the image of E under $\mathrm{Hom}_K(E, \overline{K})$.

(c) N is the splitting field in $\overline{K}$ of the family $\min(E, K)$.

(d) If $E = K(S)$, where $S \subseteq E$, then N is the splitting field in $\overline{K}$ of the family $\min(S, K)$.

(e) If E/K is finite, then N/K is also finite.

Proof. Let N' be the composition field in (a). If $\sigma \in \mathrm{Hom}_K(E, \overline{K})$ then σ can be extended to a K-embedding of N to $\overline{K}$, denoted by $\bar{\sigma}$. Since N normal, we have $\bar{\sigma}(N) = N$, and thus

$$\sigma(E) = \bar{\sigma}(E) \subseteq \bar{\sigma}(N) = N.$$

This shows $N' \subseteq N$. Conversely, we show that N'/K is normal, so that $N \subseteq N'$.

Let $\tau : N' \to \overline{K}$ be an K-embedding. Then by Theorem 1.1.4.4 τ extends to an automorphism φ of $\overline{K}$. Both of the inclusions of N' into $\overline{K}$ are K-embeddings, so φ must be a K-automorphism. Now for $\sigma \in \mathrm{Hom}_K(E, \overline{K})$, we see $\varphi \circ \sigma \in \mathrm{Hom}_K(E, \overline{K})$, therefore

$$\varphi(N') = \varphi\Big(\bigvee_{\sigma \in \mathrm{Hom}_K(E,\overline{K})} \sigma(E)\Big) = \bigvee_{\sigma \in \mathrm{Hom}_K(E,\overline{K})} \varphi(\sigma(E)) \subseteq N'.$$

Since φ coincides with τ on N', it follows that $\tau(N') = N'$ and thus N' is normal. This completes the proof of (a). The rest part are easy. □

1.1.6 Separable extensions and linearly disjointness

Our intuition may lead us to think that if a polynomial factors as a product of linear factors and we are not *purposely* repeating one of the factors (as in $(X-1)^2(X-2)$), then these will be *distinct*. For example, surely irreducible polynomials necessarily split as products of distinct factors in an algebraic closure, right? Wrong.

Example 1.1.6.1. Let p be a prime, and consider the field $\mathbb{F}_p(X)$ of rational functions over $\mathbb{F}_p$. Then the polynomial

$$X^p - t \in \mathbb{F}_p(t)[X]$$

is irreducible: by Eisenstein's criterion it is irreducible in $\mathbb{F}_p[t][X]$ (since (t) is prime in $\mathbb{F}_p[t]$), hence in $\mathbb{F}_p(t)[X]$ by **??**. Let α be a root of this polynomial in an extension L of $\mathbb{F}_p(X)$ (for example L could be the algebraic closure of $\mathbb{F}_p(X)$, or more modestly a splitting field for the polynomial). Then

$$X^p - t = (X - \alpha)^p$$

in $L[X]$; that is, α has multiplicity p as a root of $f(X)$.

In other words, the minimal polynomial over $\mathbb{F}_p(X)$ of $\alpha \in L$ vanishes p times at α, and there is nothing to do about this: no smaller power of $(X - \alpha)$ than $(X - \alpha)^p = X^p - t$ has coefficients in $\mathbb{F}_p(X)$ (a smaller power would give a nontrivial factor of $X^p - t$, and $X^p - t$ is irreducible).

We have always found this example difficult to visualize, because of intuition developed in characteristic 0, and as we will see, no such pathology can occur in characteristic 0.

1.1.6.1 Separable polynomials

Definition 1.1.6.2. Let K be a field. A polynomial $f(X) \in K[X]$ is **separable** if it has no multiple factors over its splitting field; $f(X)$ is **inseparable** if it has multiple factors over its splitting field.

The first, somewhat surprising, observation about separability is that we can in fact detect it without leaving the field of coefficients of $f(X)$. This fact uses a notion borrowed from calculus: for a polynomial

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

we denote by $f'(X)$ the derivative

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Of course this is a purely formal operation; no limiting process is at work over arbitrary fields. Still, all expected properties of derivatives hold, as the reader should check: for example, $(fg)' = f'g + fg'$ as usual.

Proposition 1.1.6.3. *Let K be a field, and let $f(X) \in K[X]$. Then $f(X)$ is separable if and only if $f(X)$ and $f'(X)$ are relatively prime.*

Proof. Over a splitting field E for $f(X)$, we have

$$f(X) = (X - \alpha_1)^{e_1}(X - \alpha_2)^{e_2} \cdots (X - \alpha_n)^{e_n}$$

where the α_i's are distinct. It is easy to see that $f(X)$ and $f'(X)$ have no nontrivial common factors over E if and only if $e_i = 1$ for all i. □

By definition, $f(X)$ and $f'(X)$ are relatively prime precisely when the greatest common divisor of $f(X)$ and $f'(X)$ is 1. Note that if E/K, the gcd of $f(X)$ and $f'(X)$ is the same whether it is considered in $K[X]$ or in $E[X]$: for example because it can be computed by applying the Euclidean algorithm, and this proceeds in exactly the same way whether it is performed in $K[X]$ or in $E[X]$.

For example, the polynomial $X^p - t$ may be seen to be inseparable without invoking splitting fields: the derivative of $X^p - t$ equals $pX^{p-1} = 0$ in characteristic p, and $\gcd(X^p - t, 0) = X^p - t \neq 1$. This example captures one of the key features of inseparability:

Corollary 1.1.6.4. *Let K be a field, and let $f(X) \in K[X]$ be an irreducible polynomial. Then $f(X)$ is separable if and only if $f'(X) \neq 0$.*

Proof. Since $\deg(f'(X)) < \deg(f(X))$ and f is irreducible, it follows that $f(X)$ and $f'(X)$ are relatively prime if and only if $f'(X) = 0$. □

Corollary 1.1.6.5. *All irreducible polynomials over a field of characteristic* 0 *are separable.*

In fact, Corollary 1.1.6.4 gives us a precise picture of what inseparable irreducible polynomials must look like. If

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

is irreducible and inseparable, then the characteristic of the field must be a positive prime p, and by Corollary 1.1.6.4 we must have

$$f'(X) = \sum_{i=0}^{n} i a_i X^{i-1} = 0.$$

That is, $ia_i = 0$ for all i. Now $ia_i = 0$ is automatic if i is a multiple of p, and it implies $a_i = 0$ for all the indices i which are not multiples of p. Therefore, the only nonvanishing coefficients in $f(X)$ must be those corresponding to indices which are multiples of p:

$$f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \cdots,$$

therefore, $f(X)$ must in fact be a polynomial in X^p.

Corollary 1.1.6.6. *Let* $\mathrm{char}(K) = p$*. An irreducible polynomial* $f(X)$ *over* K *is inseparable if and only if* $f(X)$ *has the form*

$$f(X) = g(X^{p^d})$$

where $d > 0$ *and* $g(X)$ *is a nonconstant polynomial. In this case, the integer* d *can be chosen so that* $g(X)$ *is separable, in which case every root of* $f(X)$ *has multiplicity* p^d*. In this case, the number* d *is called the* ***radical exponent*** *of* $f(X)$*.*

Proof. As we mentioned, if $f(X)$ is inseparable then $f'(X) = 0$, which implies that $f(X) = q(X^p)$ for some polynomial $q(X)$. If $q(X)$ has no multiple roots, we are done. If not, then we may repeat the argument with the irreducible polynomial $q(X)$, eventually obtaining the equation $f(X) = g(X^{p^d})$, where $g(X)$ is separable.

For the converse, suppose that $f(X) = g(X^{p^d})$ for some $d > 0$. Let K be a field in which $f(X)$ and $g(X)$ split. Thus,

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_K)$$

for $\alpha_i \in K$, and so

$$f(X) = (X^{p^d} - \alpha_1) \cdots (X^{p^d} - \alpha_k).$$

Since $f(X)$ splits in K, there exist roots $\beta_i \in K$ for each of the factors $(X^{p^d} - \alpha_i)$, and so $\beta_i^{p^d} = \alpha_i$. Hence,

$$f(X) = (X^{p^d} - \beta_1^{p^d}) \cdots (X^{p^d} - \beta_k^{p^d}) = (X - \beta_1)^{p^d} \cdots (X - \beta_k)^{p^d}.$$

This shows that $f(X)$ is inseparable. Finally, if $f(X) = g(X^{p^d})$, where $g(X)$ is separable, then the α_i's above are distinct and so are the β_i's. Hence, each root of $f(X)$ has multiplicity p^d. □

1.1.6.2 Separable extensions The terminology examined in the previous part now extends to the language of field extensions.

Definition 1.1.6.7. If E/K is an extension and $\alpha \in K$, we say that α is **separable over** K if the minimal polynomial of α over K is separable; otherwise, it is inseparable. Also, the **radical exponent** of α over K is the radical exponent of $\min(\alpha, K)$. An algebraic field extension E/K is **separable** if every $\alpha \in K$ is separable over K.

In particular, algebraic extensions of $\mathbb{Q}$ (or any field of characteristic zero) and of every finite field are necessarily separable.

Before proceeding, we record a useful lemma. If E is a field and $S \subseteq E$ then S^n denotes the set $\{s^n : s \in S\}$.

Lemma 1.1.6.8. *Let* E/K *be algebraic with* $\mathrm{char}(K) = p \neq 0$ *and let* $S \subseteq E$*.*

(i) $K(S) = K(S^{p^n})$ *holds for some* $n \geq 1$ *if and only if it holds for all* $n \geq 1$*.*

(ii) $K = K^{p^n}$ *holds for some* $n \geq 1$ *if and only if it holds for all* $n \geq 1$*.*

Proof. For part (i), suppose that $K(S) = K(S^{p^n})$ holds for some $n \geq 1$. Since

$$K(S) = K(S^{p^n}) \subseteq K(S^p) \subseteq K(S).$$

it follows that $K(S^p) = K(S)$. Now, since $[K(S)]^p = K^p(S^p)$, we have for any $n \geq 1$,

$$[K(S)]^{p^n} = K^{p^n}(S^{p^n})$$

and so

$$K(S^{p^n}) = K(K^{p^n}(S^{p^n})) = K([K(S)]^{p^n}) = K([K(S^p)]^{p^n}) = K(K^{p^n}(S^{p^{n+1}})) = K(S^{p^{n+1}}).$$

Hence, $K(S) = K(S^{p^n})$ for all $n \geq 1$. The converse part is obvious.

For part (ii), we observe that $K^{p^n} \subseteq K^p \subseteq K$ and so $K = K^{p^n}$ holds for some $n \geq 1$ if and only if $K = K^p$, which holds if and only if $K = K^{p^n}$ for all $n \geq 1$. □

According to Proposition 1.1.4.3, the number of extensions of an embedding $\sigma : K \to L$ to $K(\alpha)$, where L is algebraically closed, is equal to the number of distinct roots of $\min(\alpha, K)$. Hence, as we remarked earlier, the size of $\mathrm{Hom}_\sigma(K(\alpha), K)$ does not depend on either σ or L. The same is true for extensions of σ to any algebraic extension.

Theorem 1.1.6.9. *If E/K is algebraic and $\sigma : K \to L$, where L is algebraically closed, then the cardinality of $\mathrm{Hom}_\sigma(E, L)$ depends only on the extension E/K and not on σ or L. In other words, if $\tau : K \to L'$, with L' algebraically closed, then*

$$|\mathrm{Hom}_\sigma(E, L)| = |\mathrm{Hom}_\tau(E, L')|$$

as cardinal numbers.

Proof. Since for any $\bar\sigma \in \mathrm{Hom}_\sigma(E, L)$, the image $\bar\sigma(E)$ is contained in an algebraic closure of $\sigma(K)$, we may assume that L is an algebraic closure of $\sigma(K)$, and similarly, that L' is an algebraic closure of $\tau(K)$.

Since $\tau \circ \sigma^{-1} : \sigma(K) \to \tau(K)$ is an isomorphism and $K \subseteq L$ is algebraic, the map $\tau \circ \sigma^{-1}$ can be extended to an embedding of L into L'. Since $\bar\sigma(K) \subseteq L$ is algebraic, so is its image under λ, which is $\tau(K) \subseteq L'$, and since $\lambda(L)$ is algebraically closed, we have $\lambda(L) = L'$, implying that λ is an isomorphism.

$$\begin{tikzcd}
L' & & L \arrow[ll, "\lambda=\overline{\tau\circ\sigma^{-1}}"'] \\
& E \arrow[ul, "\lambda\circ\bar\sigma"] \arrow[ur, "\bar\sigma"'] & \\
\tau(K) \arrow[uu] & K \arrow[l, "\tau"'] \arrow[r, "\sigma"] \arrow[u] & \sigma(K) \arrow[uu]
\end{tikzcd}$$

Now, if $\bar\sigma \in \mathrm{Hom}_\sigma(E, L)$, then the map $\lambda \circ \bar\sigma$ is an embedding of E into L' extending τ on K. This defines a function from $\mathrm{Hom}_\sigma(E, L)$ to $\mathrm{Hom}_\tau(E, L')$ given by $\bar\sigma = \lambda \circ \bar\sigma$. Moreover, if $\tau, \mu \in \mathrm{Hom}_\sigma(E, L)$ are distinct, then there is a $\beta \in E$ for which $\tau(\beta) \neq \mu(\beta)$ and since λ is injective, $\lambda(\tau(\beta)) = \lambda(\mu(\beta))$, which implies that the map $\bar\sigma \mapsto \lambda \circ \bar\sigma$ is injective. Hence,

$$|\mathrm{Hom}_\sigma(E, L)| \leq |\mathrm{Hom}_\tau(E, L')|.$$

By a symmetric argument, we have the reverse inequality and so equality holds. □

In view of Theorem 1.1.6.9, we may make the following definition.

Definition 1.1.6.10. Let E/K be algebraic and let $\sigma : K \to L$, where L is algebraically closed. The cardinality of the set $\mathrm{Hom}_\sigma(E, L)$ is called the **separable degree** of E over K and is denoted by $[E : K]_s$.

This new terminology allows us to rephrase the situation for simple extensions.

Theorem 1.1.6.11 (Separable degree of simple extensions). *Let E/K and let $\alpha \in E$ be algebraic over K, with minimal polynomial $f(X)$. Then*

(a) If α is separable then

$$[K(\alpha) : K]_s = [K(\alpha) : K].$$

(b) If α is inseparable with radical exponent d, then

$$[K(\alpha) : K]_s = \frac{1}{p^d}[K(\alpha) : K],$$

and then extension $K(\alpha^{p^d})$ is separable over K.

Proof. This comes from Proposition 1.1.4.3 and Corollary 1.1.6.6. □

We would like to recast separability of simple and finite extensions entirely in the light of separable degree. First of all, we need to establish that the separable degree is multiplicative.

Theorem 1.1.6.12. *Let $K \subseteq E \subseteq F$ be algebraic extensions. Then*

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

Proof. Let $\iota : K \to \overline{F}$ be the canonical inclusion map. Then the set $\operatorname{Hom}_\iota(E, \overline{F})$ consists of extensions of ι to an embedding $\bar{\iota} : E \to \overline{F}$ and has cardinality $[E : K]_s$. Each extension $\sigma \in \operatorname{Hom}_\iota(E, \overline{F})$ is an embedding of E into $\overline{F}$ and can be further extended to an embedding of F into $\overline{F}$. Since the resulting extensions, of which there are $[F : E]_s[E : K]_s$, are distinct extensions of ι to E, we have

$$[F : K]_s \geq [F : E]_s[E : K]_s.$$

On the other hand, if $\sigma \in \operatorname{Hom}_\iota(F, \overline{F})$ then $\sigma|_E$ is the extension of E to $\overline{F}$, hence an element of $\operatorname{Hom}_\iota(E, \overline{F})$. Since σ is an extension of $\sigma|_E$ to F, we see that σ is obtained by a double extension of $\iota : K \to \overline{F}$ and so equality holds in the inequality above. □

Proposition 1.1.6.13 (Separability of simple extensions). *Let E/K be algebraic, with* $\operatorname{char}(K) = p \neq 0$. *The following are equivalent.*

(i) *α is separable over K.*

(ii) *$K(\alpha)$ is a separable extension over K.*

(iii) *$[K(\alpha) : K]_s = [K(\alpha) : K]$.*

(iv) *There is a positive integer n for which $K(\alpha) = K(\alpha^{p^n})$, in which case $K(\alpha) = K(\alpha^{p^n})$ for all n.*

If α is inseparable with radical exponent d, then

$$[K(\alpha) : K]_s = \frac{1}{p^d}[K(\alpha) : K].$$

Proof. By Theorem 1.1.6.11 we now that (i) $\Leftrightarrow$ (iii). Let α be separable and $\beta \in K(\alpha)$, then we have the tower

$$K \subseteq K(\beta) \subseteq K(\alpha).$$

The separable degree and the ordinary (vector space) degree are multiplicative and, at least for simple extensions, the separable degree does not exceed the ordinary degree. Hence, $[K(\alpha) : K]_s = [K(\alpha) : K]$ implies that the same is true for each step in the tower, and so $[K(\beta) : K]_s = [K(\beta) : K]$, which means β is separable over K.

Now we prove (i) $\Rightarrow$ (iv). Assume that α is separable. Note that α is a root of the polynomial $f(X) = X^p - \alpha^p = (X - \alpha)^p$ over $K(\alpha^p)$, and so $\min(\alpha, K(\alpha^p))$ divides $(X - \alpha)^p$. Since α is separable over K, it is also separable over $K(\alpha^p)$, which the implies

$$\min(\alpha, K(\alpha^p)) = x - \alpha.$$

Hence $\alpha \in K(\alpha^p)$. By Lemma 1.1.6.8 we conclude that (iii) holds.

Conversely, assume that $K(\alpha^{p^n}) = K(\alpha)$ for all $n \geq 1$. Let d be the radical exponent of α, then $K(\alpha^{p^d}) = K(\alpha)$. But $K(\alpha^{p^d})$ is a separable extension, therefore α is separable. This completes the proof. □

Proposition 1.1.6.14 (Separability of finite extensions). *Let E/K be a finite extension. Then $[E : K]_s \leq [E : K]$, and the following are equivalent:*

(i) *$E = K(\alpha_1, \ldots, \alpha_r)$, where each α_i is separable over K.*

(ii) *E/K is separable.*

(iii) *$[E : K] = [E : K]_s$.*

(iv) *If $E = K(S)$ for a finite set $S \subseteq E$, then $K(S) = K(S^{p^n})$ for some $n \geq 1$, in which case $K(S) = K(S^{p^n})$ for all $n \geq 1$.*

If E/K is not separable, then

$$[E : K]_s = \frac{1}{p^e}[E : K]$$

for some integer $e \geq 1$.

Proof. Since E is finite over K, it is finitely generated. Let $F = K(\alpha_1, \dots, \alpha_r)$. Then using Theorem 1.1.6.11, Theorem 1.1.6.12, and Proposition 1.1.2.15,

$$\begin{aligned}[E : K]_s &= [K(\alpha_1, \dots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \dots, \alpha_{r-1})]_s \cdots [K(\alpha_1) : K]_s \\ &\leq [K(\alpha_1, \dots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \dots, \alpha_{r-1})] \cdots [K(\alpha_1) : K] = [E : K].\end{aligned}$$

This proves the stated inequality.

First we show (i)⇒(iii). If each α_i is separable over K, then it is separable over the field $K(\alpha_1, \dots, \alpha_{i-1})$, so the inequality above is an equality. For (iii)⇒(ii), assume $[E : K]_s = [E : K]$, and let $\alpha \in E$. We have $K \subseteq K(\alpha) \subseteq E$; hence by Theorem 1.1.6.12

$$[E : K(\alpha)]_s [K(\alpha) : K]_s = [E : K]_s = [E : K] = [E : K(\alpha)][K(\alpha) : K].$$

Since both separable degrees are less than or equal to their plain counterparts, the equality implies

$$[K(\alpha) : K]_s = [K(\alpha) : K]$$

proving that α is separable, by Theorem 1.1.6.11. Therefore the extension E/K is separable. Now if $[E : K]_s = [E : K]$ and $E = K(\alpha_1, \dots, \alpha_n)$, then the inequality becomes an equality, and so each α_i is separable over K, so (i) holds.

Finnaly, we prove (ii) ⇔ (iv). Let $E = K(S)$ where S is a finite set. If E is separable, then any $\alpha \in E$ is separable over K and so

$$K(\alpha) = K(\alpha^{p^n}) \subseteq K(S^{p^n}).$$

for any $n \geq 1$. Thus, $K(S) = K(S^{p^n})$, for any $n \geq 1$. Conversely, if $K(S^{p^n}) = K(S)$ for some $n \geq 1$, then Lemma 1.1.6.8 implies that $K(S) = K(S^{p^n})$ for all $n \geq 1$. Since S is a finite set, we can take p^n to be the maximum of the numbers p^d, where d varies over all radical exponents of the elements of S, in which case each α^{p^d} is separable, and so $K(S^{p^n})$ is separable. Since $K(S) = K(S^{p^d})$, it is also separable. □

Finally, we consider the separability of algebraic extensions.

Proposition 1.1.6.15 (Separability of algebraic extensions). *Let E/K be algebraic and* $\operatorname{char}(K) = p \neq 0$.

(a) E is separable if and only if it is generated by separable elements over K.

(b) If E is separable and $E = K(S)$, then $K(S) = K(S^{p^n})$ for all $n \geq 1$.

Proof. For part (a), if E/K is separable then E is generated by itself over K. For the converse, assume that $E = K(S)$ where each $\alpha \in S$ is separable over K and let $\beta \in E$. Then $\beta \in K(S_0)$ for some finite subset $S_0 \subseteq S$. Since $K(S_0)$ is finitely generated and algebraic, it is finite. Thus, Proposition 1.1.6.14 implies that $K(S_0)$ is separable. Hence β is separable over K and so E is separable. As to part (b), we have for any $\alpha \in S$ $n \geq 1$

$$K(\alpha) = K(\alpha^{p^n}) \subseteq K(S^{p^n})$$

which implies that $K(S) \subseteq K(S^{p^n})$ and so $K(S) = K(S^{p^n})$. □

Using our characterization of separable extensions, we may now establish that the class of separable extensions is distinguished.

Proposition 1.1.6.16. *The class of separable extensions is distinguished and is also closed under the taking of arbitrary composites.*

Proof. For the tower property, if the full extension in $K \subseteq E \subseteq F$ is separable, then by definition so is $K \subseteq E$. As for the extension $E \subseteq F$, for any $\alpha \in F$, we have

$$\min(\alpha, K) \mid \min(\alpha, E),$$

and so α separable over K implies α separable over E, hence $E \subseteq F$ is separable. Conversely, suppose now that $K \subseteq E$ and $E \subseteq F$ are separable and let $\alpha \in F$. Let $S \subseteq E$ be the set of coefficients of $\min(\alpha, E)$. Then $\min(\alpha, E) = \min(\alpha, K(S))$ and so α is separable over $K(S)$. It follows that each step in the tower $K \subseteq K(S) \subseteq K(S, \alpha)$ is finite and separable, implying that α is separable over K. Hence, F is separable.

For the lifting property, let $K \subseteq E$ be separable and let $K \subseteq F$. Since every element of E is separable over K, it is also separable over the larger field F. Hence $EF = F(E)$ is separably generated and is therefore separable (Proposition 1.1.6.15).

The fact that separable extensions are closed under the taking of arbitrary composites follows from the finitary property of arbitrary composites. That is, each element of an arbitrary composite involves elements from only a finite number of the fields in the composite and so is an element of a finite composite, which is separable. □

1.1.6.3 Perfect fields It is intersecting to consider certain condition on fields that guarantees the inseparability of its extensions. We make the following definition.

Definition 1.1.6.17. A field K is **perfect** if every irreducible polynomial over K is separable.

The following property of perfect fields is immediate from definition.

Proposition 1.1.6.18. *A field K is perfect if and only if every algebraic extension of K is separable over K.*

Proof. It is clear from the definitions that if K is perfect then any algebraic extension of K is separable. Conversely, suppose that every algebraic extension of K is separable. If $f(X) \in K[X]$ is irreducible and α is a root of $f(X)$ in some extension of K, then $K \subseteq K(\alpha)$ is algebraic and so α is separable over K, that is, $f(X)$ is separable. Thus, K is perfect. □

It is clear that fields with characteristic zero must be perfect. Also, we will prove later that finite fields are all perfect. Therefore if K is not a perfect field, it must be infinite and have nonzero characteristic.

Definition 1.1.6.19. Let K be a field of characteristic $p > 0$. The **Frobenius homomorphism** is the map $\sigma : K \to K$ defined by $x \mapsto x^p$.

The Frobenius homomorphism may not look like a homomorphism of rings, but it is. It must be injective, as is every nontrivial ring homomorphism from a field; but it is not necessarily surjective. In fact, it is surjective if and only if the field is perfect.

Proposition 1.1.6.20. *Let K be a field with characteristic $p > 0$. The following are equivalent.*

(i) *K is perfect.*

(ii) *$K = K^{p^n}$ for some $n \geq 1$.*

(iii) *The Frobenius homomorphism is an automorphism for K.*

Proof. Suppose K is perfect. Let $\alpha \in K$ and consider the polynomial $f(X) = X^p - \alpha$. If β is a root of $f(X)$ in a splitting field then $\beta^p = \alpha$ and so

$$f(X) = X^p - \beta^p = (X - \beta)^p$$

Now, if $g(X) = (X - \beta)^e$ is an irreducible factor of $f(X)$ over K, then it must be separable and so $e = 1$. Thus $\beta \in K$, that is, $\alpha = \beta^p \in K^p$ and so $K \subseteq K^p$. Since the reverse inclusion is manifest, we have $K = K^p$. Then (ii) follows from Lemma 1.1.6.8.

Now assume that (ii) holds. Then Lemma 1.1.6.8 implies that $K = K^p$. Suppose that $f(X) \in K[X]$ is irreducible. If $f(X)$ is not separable, then

$$f(X) = g(X^p) = \sum_i a_i (X^p)^i = \sum_i b_i^p (X^i)^p = \sum_i (b_i X^i)^p$$

contradicting the fact that $f(X)$ is irreducible. Hence, every irreducible polynomial is separable and so K is perfect. Thus, (ii) implies (i). Since the Frobenius map is a monomorphism, statement (ii), which says that σ^n is surjective, is equivalent to statement (iii). □

Example 1.1.6.21. Let p be a prime. Then the field $\mathbb{F}_p$ is finite and hence perfect. However, if t is an independent variable, then the field $\mathbb{F}_p(t)$ is not perfect, as we have seen in Example 1.1.6.1.

While it is true that any algebraic extension of a perfect field is perfect, not all subfields of a perfect field need be perfect.

Proposition 1.1.6.22. *Let $K \subseteq E$ be an algebraic extension.*

(a) *If K is perfect then E is also perfect.*

(b) *If E/K is finite and E is perfect, then K is perfect.*

Proof. Part (a) follows from Proposition 1.1.6.18 and the fact that every algebraic extension of E is an algebraic extension of K.

For part (ii), let $p = \mathrm{char}(K)$ and suppose first that $K \subseteq E$ is simple. Thus, $E = K(\alpha)$ is perfect and α is algebraic over K. Since $K(\alpha)$ is perfect, we have $K(\alpha) = [K(\alpha)]^p = K^p(\alpha^p)$. Consider the tower

$$K^p \subseteq K \subseteq K(\alpha) = K^p(\alpha^p).$$

If $f(X) = \sum_i a_i X^i$ is the minimal polynomial of α over K, then

$$0 = \Big(\sum_i a_i \alpha^i\Big)^p = \sum_i a_i^p \alpha^{pi}$$

and so $[K^p(\alpha^p) : K^p] \leq [K(\alpha) : K] = 1$. It follows that in the tower above, $[K : K^p] = 1$, that is, $K = K^p$, whence K is perfect. Since E is finitely generated by algebraic elements, the result follows by repetition of the previous argument. □

Note that we cannot drop the finiteness condition in part (b) of the previous theorem since, for example, the extension $K \subseteq \overline{K}$ is algebraic and $\overline{K}$ is perfect for any field K, even if K is not.

1.1.6.4 Purely inseparability

The antithesis of a separable element is a purely inseparable element.

Definition 1.1.6.23. An element α algebraic over K is **purely inseparable** over K if its minimal polynomial has the form $(X - \alpha)^n$ for some $n \geq 1$. An algebraic extension E/K is **purely inseparable** if every element of E is purely inseparable over K.

It is clear that for a purely inseparable element E, an element $\alpha \in K$ is separable if and only if $\min(\alpha, K) = x - \alpha$; that is, $\alpha \in K$. In particular, for extensions of fields of characteristic 0 or finite fields, there are no "interesting" purely inseparable elements.

Lemma 1.1.6.24. *Let E/K be a purely inseparable extension with $p = \mathrm{char}(K) \neq 0$. If $\alpha \in E$ is inseparable over K and d is the radical exponent of α, then the minimal polynomial of α over K is $(X - \alpha)^{p^d}$.*

Proof. By definition, $\min(\alpha, K) = (X - \alpha)^n$ for some $n \geq 1$. For $\alpha \notin K$. Since the coefficient of X^{n-1} in $(X - \alpha)^n$ is $-n\alpha$, it follows that n must be a multiple of p, that is,

$$\min(\alpha, K) = (X - \alpha)^{mp^e}.$$

But $\min(\alpha, K) = g(X^{p^d})$, hence $e \geq d$ and we can write

$$\min(\alpha, K) = (X^{p^d} - \alpha^{p^d})^{mp^{e-d}}.$$

which implies that $g(X) = (X - \alpha^{p^d})^{mp^{e-d}}$, which is separable if and only if $m = 1$ and $e = d$. Thus,

$$\min(\alpha, K) = (X - \alpha)^{p^d}$$

where d is the radical exponent of α over K. □

Example 1.1.6.25. Let $\mathrm{char}(K) = p$. If t is transcendental over K, then t is purely inseparable over $K(t^p)$, since its minimal polynomial over $K(t^p)$ is $X^p - t^p = (X - t)^p$.

Example 1.1.6.26. Here we present an example of an element that is neither separable nor purely inseparable over a field K. Let $\mathrm{char}(K) = p$ and let $\alpha \in K$ be nonzero. Let t be transcendental over K and let

$$s = \frac{t^{p^2}}{t^p + \alpha}.$$

According to Proposition 1.4.2.2, $K(s) \subseteq K(t)$ is algebraic and has degree equal to p^2, and the monic polynomial

$$p(X) = X^{p^2} - sX^p - s\alpha$$

is the minimal polynomial for t over $K(s)$. Since $p(X) = q(X^p)$, we deduce that t is not separable over $K(s)$. On the other hand, if t were purely inseparable over $K(s)$, we would have

$$X^{p^2} - sX^p - s\alpha = (X - t)^{p^2} = X^{p^2} - t^{p^2}$$

which would imply that $s = 0$, which is not the case. Hence, t is neither separable nor purely inseparable over $K(s)$.

Definition 1.1.6.27. Let E/K be a finite extension. Since $[E:K]_s \mid [E:K]$, we may write

$$[E:K] = [E:K]_i [E:K]_s$$

where $[E:K]_i$ is the **inseparable degree** of E over K.

Note that while the separable degree is defined for arbitrary extensions, the inseparable degree is defined only for finite extensions.

Now we assemble some properties of the inseparable degree.

Proposition 1.1.6.28. *Let $K \subseteq E \subseteq F$ be a finite extensions with* $\operatorname{char}(K) = p \neq 0$.

(a) $[F:K]_i = [F:E]_i[E:K]_i$.

(b) E/K is separable if and only if $[E:K]_i = 1$.

(c) If $\alpha \in E$ then $[K(\alpha):K] = p^d$, where d is the radical exponent of α over K.

(d) $\alpha \in E$ is purely inseparable if and only if $[K(\alpha):K]_s = 1$, if and only if $[K(\alpha):K]_i = [K(\alpha):K]$.

(e) $[E:K]_i$ is a power of p.

Proof. The first three statements are clear. Also, (d) follows from the fact that α is purely inseparable if and only if its minimal polynomial has only one distinct root. But this is equivalent to saying that $\operatorname{Hom}_K(K(\alpha), \overline{K})$ has cardinality 1. Finally, (e) follows from the fact that E/K is finitely generated and the inseparable degree is multiplicative. □

We next characterize purely inseparable elements.

Proposition 1.1.6.29 (Purely inseparable elements). *Let* $\operatorname{char}(K) = p \neq 0$. *Let α be algebraic over K, with radical exponent d and let $f(X) = \min(\alpha, K)$. The following are equivalent.*

(i) *α is purely inseparable over K.*

(ii) *$K \subseteq K(\alpha)$ is a purely inseparable extension.*

(iii) *$\alpha^{p^n} \in K$ for some $n \geq 1$.*

Proof. If (i) holds and $\beta \in K(\alpha)$, then in the tower $K \subseteq K(\beta) \subseteq K(\alpha)$ the inseparable degree of the full extension is equal to the degree, and so the same holds for the lower step. Hence, β is purely inseparable over K and (ii) holds. Clearly, (ii) implies (i).

If (i) holds, then $\min(\alpha, K) = X^{p^d} - \alpha^{p^d}$, which implies (iii). If (iii) holds, then $\min(\alpha, K) = X^{p^n} = \alpha^{p^n}$ and, as we have seen, α is purely inseparable. □

One may translate our results into the following remark. Let α be element in E, then we have the following tower of extensions:

$$K(\alpha) \supseteq K(\alpha^p) \supseteq \cdots \supseteq K(\alpha^{p^n}) \supseteq \cdots \supseteq K.$$

Then Theorem 1.1.6.11 says that if α is separable, then this tower is trivial, with the field all being $K(\alpha)$; and if α is inseparable, then this tower is descending. Now Proposition 1.1.6.29 tells us α is purely inseparability condition if and only if this twoer arrives at K. Note that Example 1.1.6.26 shows that there are cases where the tower is descending but never arrives at K.

The following result is the analogue of Proposition 1.1.6.15.

Proposition 1.1.6.30 (Purely inseparable extensions). *Let E/K be algebraic. The following are equivalent.*

(i) *E is **purely inseparably generated**; that is, generated by purely inseparable elements.*

(ii) *E/K is **degreewise purely inseparable**, that is, $[E:K]_s = 1$.*

(iii) *E/K is a purely inseparable extension.*

Proof. To prove that (i) implies (ii), suppose that $E = K(I)$, where all elements of I are purely inseparable over K. Let $\sigma : K \to L$ be an embedding to an algebraic closed field L. Then any $\tau \in \operatorname{Hom}_\sigma(E, L)$ is uniquely determined by its values on the elements of I. But if $\alpha \in I$ then $\tau(\alpha)$ is a root of the minimal polynomial $\min(\alpha, K) = (X - \alpha)^n$ and so $\tau(\alpha) = \alpha$. Hence τ must be the identity and therefore $[E : K]_s = 1$.

To show that (ii) implies (iii), let $\alpha \in E$ and suppose that β is a root of $\min(\alpha, K)$ in $\overline{K}$. Then by Theorem 1.1.4.4 the identity on K can be extended to an embedding $\sigma : E \to \overline{K}$, for which $\sigma(\alpha) = \beta$. Since $[E : K]_s = 1$, we must have $\sigma = \mathrm{id}$ and so $\beta = \alpha$. Thus, $\min(\alpha, K)$ has only one distinct root in $\overline{K}$ and so E is purely inseparable. It is clear that (iii) implies (i). □

Similarly to separable extensions, We can show that the class of purely inseparable extensions is distinguished.

Proposition 1.1.6.31. *The class of purely inseparable extensions is distinguished. It is also closed under the taking of arbitrary composites.*

Proof. Let $K \subseteq E \subseteq F$ be finite extensions. Since pure inseparability is equivalent to degreewise pure inseparability and $[F : K]_i = 1$ if and only if $[E : K]_i = 1$ and $[F : E]_i = 1$, it is clear that the tower property holds. For lifting, suppose that $K \subseteq E$ is purely inseparable and $K \subseteq F$. Since every element of E is purely inseparable over K, it is also purely inseparable over the larger field F. Hence $EF = F(E)$ is purely inseparably generated and therefore purely inseparable.

The fact that purely inseparable extensions are closed under the taking of arbitrary composites follows from the finitary property of arbitrary composites, as in the separable case. □

1.1.6.5 Separable and purely inseparable closures

Let $K \subseteq E$ be an extension. Recall that the algebraic closure of K in E is the set $\overline{K}$ of all elements of E that are algebraic over E. The fact that $\overline{K}$ is a field is a consequence of the fact that an extension that is generated by algebraic elements is algebraic.

We can do exactly the same analysis for separable and purely inseparable elements. To wit, if $\alpha, \beta \in E$ are separable over K, then $K(\alpha, \beta)$ is separable over K. It follows that $\alpha \pm \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$ are separable over K. Hence, the set of all elements of E that are separable over K is a subfield of E. A similar statement holds for separable and purely inseparable elements.

Definition 1.1.6.32. Let E/K be algebraic. The field

$$K^{\mathrm{sep}} = \{\alpha \in E : \alpha \text{ is separable over } K\}$$

is called the **separable closure** of K in E. The field

$$K^{\mathrm{isep}} = \{\alpha \in E : \alpha \text{ is purely inseparable over } K\}$$

is called the **purely inseparable closure** of K in E.

The separable closure allows us to decompose an arbitrary algebraic extension into separable and purely inseparable parts.

Proposition 1.1.6.33. *Let E/K be algebraic.*

(a) In the tower $K \subseteq K^{\mathrm{sep}} \subseteq E$, the first step is separable and the second step is purely inseparable.

(b) Any automorphism σ of E over K is uniquely determined by its restriction to K^{sep}.

Proof. For (a), if $\alpha \in E \setminus K$ has radical exponent d, then α^{p^d} has a separable minimal polynomial and is therefore in K^{sep}. Thus, Proposition 1.1.6.29 implies that α is purely inseparable over K^{sep}. For (b), let α be purely inseparable over K, then any automorphism σ of E must send α to a root of $\min(\alpha, K) = (X - \alpha)^n$, and so $\sigma|_{K^{\mathrm{isep}}}$ is the identify. □

Corollary 1.1.6.34. *Let E/K be finite, then $[E : K]_s = [K^{\mathrm{sep}} : K]$ and $[E : K]_i = [E : K^{\mathrm{isep}}]$.*

Proof. The first equality follows from part (b) of Proposition 1.1.6.33, and the second follows from the definition of $[E : K]_i$. □

Corollary 1.1.6.35. *If E/K is normal, then K^{sep}/K is also normal.*

Proof. Let σ be an embedding of K^{sep} in $\overline{K}$ over K and extend σ to an embedding of E. Then σ is an automorphism of E by Theorem 1.1.4.2. Furthermore, $\sigma(K^{\text{sep}})$ is separable over K, hence is contained in K^{sep}. Hence $\sigma(K^{\text{sep}}) = K^{\text{sep}}$, as contended. □

Proposition 1.1.6.33 shows that any algebraic extension can be decomposed into a separable extension followed by a purely inseparable extension. In general, the reverse is not possible: an algebraic extension can not be decomposed into a purely inseparable extension followed by a separable extension. This is because, although $K \subseteq K^{\text{isep}}$ is purely inseparable, the elements of $E \setminus K^{\text{isep}}$ need not be separable over K^{isep}; they are simply not purely inseparable over K. However, we do have a characterization for the extension $K^{\text{isep}} \subseteq E$ to be separable. For this we need a lemma.

Lemma 1.1.6.36. *Let E, F be two finite extensions of K, and assume that E/K is separable, F/K is purely inseparable. Assume E, F are subfields of a common field. Then*

$$[EF : F] = [E : K] = [EF : K]_s, \quad [EF : E] = [F : K] = [EF : K]_i.$$

Proof. In fact, we have the following picture:

$$\begin{tikzcd}
 & EF & \\
E \arrow[ur, dash, "\text{p isep}"] & & F \arrow[ul, dash, "\text{sep}"'] \\
 & K \arrow[ul, dash, "\text{sep}"] \arrow[ur, dash, "\text{p isep}"'] &
\end{tikzcd}$$

Since separable and purely inseparable extensions are distinguished, the extension EF/E is purely insepara and EF/F is separable. Therefore, by Proposition 1.1.6.15 and Proposition 1.1.6.30, we have

$$[EF : K]_s = [EF : F]_s[F : K]_s = [EF : F]_s = [EF : F],$$

and the claim for inseparable degree can be proved similarly. □

Proposition 1.1.6.37. *Let E/K be an algebraic extension. Then the extension E/K^{isep} is separable if and only if we have $E = K^{\text{sep}}K^{\text{isep}}$.*

Proof. Consider the following diagram of extensions

$$\begin{tikzcd}
 & E & \\
 & K^{\text{sep}}K^{\text{isep}} \arrow[u, dash] & \\
K^{\text{sep}} \arrow[ur, dash, "\text{p isep}"] & & K^{\text{isep}} \arrow[ul, dash, "\text{sep}"'] \\
 & K \arrow[ul, dash, "\text{sep}"] \arrow[ur, dash, "\text{p isep}"'] &
\end{tikzcd}$$

We already know that E/K^{sep} is purely inseparable, and so $E/K^{\text{sep}}K^{\text{isep}}$ is also purely inseparable. If E/K^{isep} is separable, then $E/K^{\text{sep}}K^{\text{isep}}$ is also separable, hence we get $E = K^{\text{sep}}K^{\text{isep}}$. The converse is trivial from the diagram above. □

We can obtain further results in the setting of Proposition 1.1.6.37 when E/K is a normal extension, which includes the case $E = \overline{K}$. Let $G = \text{Aut}_K(E)$ be the set of all automorphisms of E over K. Since E is normal, G is also the set of all embeddings of E into $\overline{K}$ over K. We define the **fixed field** of G in E by

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Proposition 1.1.6.38. *Let E be normal over K, G its group of automorphisms over K, and E^G the fixed field of G. Then $E^G = K^{\text{isep}}$, the extension E/K^{isep} is separable, and we have $E = K^{\text{sep}}K^{\text{isep}}$.*

Proof. Let $\alpha \in E^G$. If $\beta \in \overline{K}$ is conjugate to α then there exists an embedding $\sigma : E \to \overline{K}$ over K for which $\sigma(\alpha) = \beta$. But $\sigma(\alpha) = \alpha$ by the definition of E^G, and so $\beta = \alpha$. Hence the minimal polynomial of α has only one root and $\alpha \in K^{\text{isep}}$. On the other hand, if $\alpha \in K^{\text{isep}}$ then any $\sigma \in G$ must map σ to itself (Proposition 1.1.6.33). Hence $\alpha \in E^G$. This proves that $E^G = K^{\text{isep}}$.

Now let $\alpha \in E$ and $f(X) = \min(\alpha, E^G)$. Let $g(X) = \prod(X - r_i)$ where $R = \{r_1, \ldots, r_n\}$ is the set of *distinct* roots of $f(X)$ in E. Since any $\sigma \in G$ is a permutation of R, we deduce that $g^\sigma(X) = g(X)$ and so the coefficients of $g(X)$ lie in E^G. Hence $f(X) = g(X)$ and α is separable over E^G. □

1.1.6.6 Existence of primitive elements We wish now to describe conditions under which a finite extension is simple. The most famous result along these lines is the theorem of the primitive element, which states that a finite separable extension is simple.

Theorem 1.1.6.39 (Theorem of the primitive element).

(a) Any extension of the form

$$K \subseteq K(\alpha_1, \ldots, \alpha_n, \beta)$$

where α_i is separable over K and β is algebraic over K is a simple extension. Moreover, if K is infinite, this extension has infinitely many primitive elements, of the form $c_1\alpha_1 + \cdots + c_n\alpha_n + \beta$, where $c_1, \ldots, c_n \in K$.

(b) For any finite extension $K \subseteq E$, there exists a $\beta \in E$ such that

$$[K(\beta) : K] = [E : K]_s.$$

If K is infinite, there exist infinitely many such elements β.

(c) If $K \subseteq E$ is finite and separable, say

$$E = K(\alpha_1, \ldots, \alpha_n)$$

where α_i is separable over K, then $K \subseteq E$ is simple. If K is infinite, there exist infinitely many primitive elements for E over K of the form $c_1\alpha_1 + \cdots + c_n\alpha_n$, where $c_i \in K$.

(d) If K has characteristic 0 or if K is a finite field then any finite extension of K is simple.

Proof. If K is a finite field, then so is E, since $[E : K]$ is finite. Hence $E^\times = \langle\beta\rangle$ is cyclic and $K \subseteq E = K(\beta)$ is simple. Let us now assume that K is an infinite field.

For (a), we show that if $E = K(\alpha, \beta)$, with α separable over K and β algebraic over K, then $E = K(\gamma)$, where γ is algebraic over K. The argument can be repeated to obtain a primitive element in the more general case.

Let $f(X) = \min(\alpha, K)$, $g(X) = \min(\beta, K)$, and suppose that the roots of $f(X)$ are $\alpha_1 = \alpha, \ldots, \alpha_s$ and the roots of $g(X)$ are $\beta_1 = \beta, \ldots, \beta_t$. Since $f(X)$ is separable, the roots of $f(X)$ are distinct. However, the roots of $g(X)$ need not be distinct. We wish to show that for infinitely many values of $c \in K$, the elements $c\alpha + \beta$ are primitive. To do this, we need only show that $\alpha \in K(c\alpha + \beta)$, for then $\beta \in K(c\alpha + \beta)$ and so $K(\alpha, \beta) = K(c\alpha + \beta)$.

The polynomial $h(X) = g(c\alpha + \beta - cx)$ has coefficients in $K(c\alpha + \beta)$ and has α as a root. Thus, $f(X)$ and $g(X)$ have the common factor $x - \alpha$ in some extension of K. Moreover, since α is separable, α is a simple root of $f(X)$ and so no higher power of $x - \alpha$ is a factor of $f(X)$. Therefore, if we can choose $c \in K$ so that $f(X)$ and $h(X)$ have no other common roots in any extension of K, then it would follow that $\gcd(f(X), h(X)) = x - \alpha$, which must therefore be a polynomial over $K(c\alpha + \beta)$. In particular, $\alpha \in K(c\alpha + \beta)$, as desired.

The roots of h are the values of x for which $c\alpha + \beta - cx \neq \beta_i$ and we need only choose c so that none of the roots $\alpha_2, \ldots, \alpha_s$ satisfy this equation, that is, we need only choose c so that

$$c \neq \frac{\beta_i - \beta}{\alpha - \alpha_j}$$

for $i = 2, \ldots, t$ and $j = 2, \ldots, s$. Since K is infinite, there are infinitely many $c \in K$ satisfying this condition.

Now (b) follows from (a) by considering the separable closure K^{sep} of E in K. Since $K \subseteq K^{\text{sep}}$ is separable, with $[K^{\text{sep}} : K] = [E : K]_s$, we can apply part (a) to the separable extension K^{sep}/K. Also, (c) is a direct consequence of (a), as is (d). □

Example 1.1.6.40. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2})$. Here we have

$$f(X) = \min(i, \mathbb{Q}) = X^2 + 1, \quad g(X) = \min(\sqrt{2}, \mathbb{Q}) = X^2 - 2.$$

and so $\alpha_1 = i, \alpha_2 = -i$, and $\beta_1 = \sqrt{2}, \beta_2 = -\sqrt{2}$. According to the previous theorem, $ci + \sqrt{2}$ is primitive provided that

$$c \notin \left\{ \frac{\beta_i - \beta}{\alpha - \alpha_2} : i = 1, 2 \right\} = \{0, \sqrt{2}i\}.$$

In particular, we can choose any nonzero $c \in \mathbb{Q}$.

Theorem 1.1.6.39 is a good illustration of why separability is a technically desirable condition. One may wonder if there is an example of nonsimple extension. To give an example of this, we first provide a nice criterion for simplicity of algebraic extensions.

Proposition 1.1.6.41. *Let E/K be a finite extension with $[E:K]_i = p^d$. Then E/K is simple if and only if d is the smallest nonnegative integer for which $E^{p^d} \subseteq K^{\text{sep}}$.*

Proof. We have seen that if $K \subseteq E$ is simple then d is the smallest such nonnegative integer. For the converse, note first that if K is a finite field then so is E, implying that $E^{\times}$ is cyclic and so E/K is simple. Let us assume that K is an infinite field and looK at the second step in the tower $K \subseteq K^{\text{sep}} \subseteq E$. This step is purely inseparable. Since $K^{\text{sep}} \subseteq E$ is finite, we have

$$E = K^{\text{sep}}(\beta_1, \ldots, \beta_n)$$

If for some $e \leq d$, we have $\beta_i^{p^e} \in K^{\text{sep}}$ for all i, then $E^{p^e} \subseteq K^{\text{sep}}$, contrary to the hypothesis. Hence one of the β_i's, say β, satisfies

$$\beta^{p^d} \in K^{\text{sep}}, \quad \beta^{p^e} \notin K^{\text{sep}} \text{ for } e < d.$$

It follows that

$$[K^{\text{sep}}(\beta) : K^{\text{sep}}]_i = p^d = [E:K]_i \geq [E:K^{\text{sep}}]_i.$$

Since $K^{\text{sep}}(\beta) \subseteq E$, we conclude $[K^{\text{sep}}(\beta) : K^{\text{sep}}]_i = [E : K^{\text{sep}}]_i$, and since the extensions involved are purely inseparable, we get $[K^{\text{sep}}(\beta) : K^{\text{sep}}] = [E : K^{\text{sep}}]$. Hence $E = K^{\text{sep}}(\beta)$.

Our tower now has the form $K \subseteq K^{\text{sep}} \subseteq K^{\text{sep}}(\beta)$ where β is purely inseparable over K^{sep}. In addition, K^{sep}/K is finite and separable and therefore simple. Thus there exist $\alpha \in K^{\text{sep}}$ such that $K^{\text{sep}} = K(\alpha)$ and therefore $E = K(\alpha, \beta)$, where α is separable over K and β is purely inseparable over $K(\alpha)$. By Theorem 1.1.6.39, the extension $K \subseteq K(\alpha, \beta)$ is simple. □

Example 1.1.6.42. By Theorem 1.1.6.39, if we want to construct a nonsimple finite extension, we have to use inseparable elements. Consider the extension E/K, where

$$K = \mathbb{F}_p(u^p, v^p), \quad E = \mathbb{F}_p(u, v).$$

The minimal polynomial of s over K is $X^p - u^p$ and the minimal polynomial of t over $\mathbb{F}_p(u, v^p)$ is $y^p - v^p$, so it follows that E/K is purely inseparable and $[E:K]_i = [E:K] = p^2$. Since $E^p \subseteq \mathbb{F}_p(u,v) = K$, by Proposition 1.1.6.41 the extension E/K is not simple.

Note that E/K has infinitely many intermediate fields: if there are $c, c' \in K$ such that $K(cu+v) = K(c'u+v)$, then we may conclude that $K(u,v) = K(cu+v)$, and in particular

$$[K(cu+v) : K] = p^2.$$

But this is not the case, since $(cu+v)^p = c^p u^p + v^p \in K(u^p, v^p) = K$; hence the minimal polynomial of $cu+v$ over K has degree at most p. Since $K = \mathbb{F}_p(u^p, v^p)$ is infinite, there are infinitely many intermediate fields, and it follows that E is not a simple extension of K.

1.1.6.7 Linearly disjointness Let E and F be two extensions of a field K. By a **composite extension** of E and F we refer to any triple (L, ϕ, ψ), where L is an extension of K, ϕ is a K-homomorphism of E into L and ψ is a K-homomorphism of F into L, and where the field L is generated by $\phi(E) \cup \psi(F)$.

$$\begin{tikzcd} & L & \\ E \arrow[ur, "\phi"] & & F \arrow[ul, "\psi"'] \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

By an **isomorphism** of a composite extension (L, ϕ, ψ) of E and F onto a composite extension (L', ϕ', ψ') of E and F we mean a K-isomorphism σ of L onto L' such that $\phi' = \sigma \circ \phi$ and $\psi' = \sigma \circ \psi$.

Let (L, ϕ, ψ) be a composite extension of E and F. The K-linear mapping of $E \otimes_K F$ into L which sends $x \otimes y$ to $\phi(x)\psi(y)$ is a K-algebra homomorphism; in this part, we shall denote it by $\phi * \psi$. Its image is the subring of L generated by $\phi(E) \cup \psi(F)$.

Proposition 1.1.6.43. *Let E and F be two extensions of K.*

(a) Let (L, ϕ, ψ) be a composite extension of E and F; then the kernel $\mathfrak{p}$ of the homomorphism $\phi * \psi$ of $E \otimes_K F$ into L is a prime ideal.

(b) Let $\mathfrak{p}$ be a prime ideal of $E \otimes_K F$; then there exists a composite extension (L, ϕ, ψ) of E and F such that $\mathfrak{p}$ is the kernel of $\phi * \psi$, and any two such composite extensions are isomorphic.

Proof. Assertion (a) follows from the fact that the kernel of a homomorphism of a ring into a field is a prime ideal. Let $\mathfrak{p}$ be a prime ideal of $E \otimes_K F$, A be the quotient ring $(E \otimes_K F)/\mathfrak{p}$ and L the field of fractions of A. For $x \in E$ (resp. $y \in F$) we denote by $\phi(x)$ (resp. $\psi(y)$) the residue class mod $\mathfrak{p}$ of $x \otimes 1$ (resp. $1 \otimes y$). Then ϕ (resp. ψ) is a K-homomorphism of E (resp. F) into L and $\phi(E) \cup \psi(F)$ generates A as a ring, hence L as a field. Therefore (L, ϕ, ψ) is a composite extension of E and F; we see at once that $\phi * \psi$ is the canonical homomorphism of $E \otimes_K F$ into L, and its kernel is thus equal to $\mathfrak{p}$.

Let (L', ϕ', ψ') be a composite extension of E and F such that the kernel of $\phi' * \psi'$ is equal to $\mathfrak{p}$. Since $\phi * \psi$ and $\phi' * \psi'$ have the same kernel, there exists an isomorphism σ of A onto the image A' of $\phi' * \psi'$, characterized by $\phi' * \psi' = \sigma \circ (\phi * \psi)$. But A' is the subring of L' generated by $\phi'(E) \cup \phi'(F)$, hence L' is the field of fractions of A'. Therefore σ extends to an homomorphism of L onto L' and it is clear that σ is an isomorphism of (L, ϕ, ψ) onto (L', ϕ', ψ'). □

Remark 1.1.6.44. If $\mathfrak{p}$ and $\mathfrak{p}'$ are two distinct prime ideals of $E \otimes_K F$, the corresponding composite extensions of E and F (constructed by the procedure of the above proof) are not isomorphic. However, they may nevertheless be isomorphic as extensions of K.

Corollary 1.1.6.45. *There exist composite extensions of E and F.*

Proof. For since the commutative ring $E \otimes_K F$ is not reduced to 0, it has prime ideals: Krull's theorem proves the existence of maximal ideals and every maximal ideal is prime. □

We can make this corollary more precise as follows. Let (E, ϕ) and (F, ψ) be two extensions of K; choose a maximal ideal $\mathfrak{m}$ of the commutative ring $E \otimes_K F$ and put $L = (E \otimes_K F)/\mathfrak{m}$; then L is an extension of K. For $x \in E$ write $\bar{\phi}(x)$ for the residue class of $x \otimes 1$ mod $\mathfrak{m}$ and similarly put $\bar{\psi}(y)$ for the residue class of $1 \otimes y$ mod $\mathfrak{m}$ for all $y \in F$. We then have a commutative diagram of field homomorphisms

$$\begin{tikzcd}
 & L & \\
E \arrow[ur, "\bar{\phi}"] & & F \arrow[ul, "\bar{\psi}"'] \\
 & K \arrow[ul, "\psi"] \arrow[ur, "\phi"'] &
\end{tikzcd}$$

By replacing $(L, \bar{\phi})$ by an isomorphic extension of E we may suppose that L contains E as subfield and that $\bar{\phi}$ is the canonical injection of E in L. By changing notation we thus obtain the following corollary:

Corollary 1.1.6.46. *Let K and E be two fields and ϕ a homomorphism of K into E. If K is a field containing K as subfield, there exists a field E' containing E as subfield and a homomorphism ϕ' of K' into E' extending ϕ.*

Let A and B be two sub-K-algebras of Ω. There exists an algebra homomorphism $\varphi : A \otimes_K B \to \Omega$ which maps $x \otimes y$ to xy. The image of φ is a subring C of Ω generated by $A \cup B$. Moreover, if (b_μ) is a basis of B over K and (a_λ) a basis of A over K, then C coincides with the set of linear combinations $\sum c_{\lambda\mu} a_\lambda b_\mu$ where $c_{\lambda\mu} \in K$.

We shall say that A and B are **linearly disjoint over $\boldsymbol{K}$**, if φ is an isomorphism of $A \otimes_K B$ onto C. We then have $A \cap B = K$; every free subset of B (resp. A) with respect to K is then free with respect to A (resp. B) ; conversely, for A and B to be linearly disjoint over K, it is sufficient that there should exist one basis of B over K (for example) which is free with respect to A.

Consider particularly the case where A and B are subextensions of Ω, we have the following proposition.

Proposition 1.1.6.47. *Let E and F be two extensions of K contained in a field Ω.*

(a) If F has finite degree over K, then the subring of a generated by $E \cup F$ is a field, coinciding with EF and the degree of EF over E is finite; we have $[EF : E] \leq [F : K]$, with equality ifand only if E and F are linearly disjoint over K. In that case EF is E-isomorphic to $E \otimes_K F$.

(b) If E and F are both of finite degree over K, then EF is of finite degree over K. We have $[EF : K] \leq [E : K][F : K]$ with equality if and only if E and F are linearly disjoint over K.

1.1.7 Exercise

Exercise 1.1.1. Let R be an integral domain containing a subfield K (as a subring). If R is finite-dimensional when regarded as an K-vector space, then it is a field.

Proof. Let α be a nonzero element of R. The map $x \mapsto \alpha x$ is an injective linear map of finite-dimensional K-vector spaces, and is therefore surjective. In particular, there is an element $\beta \in R$ such that $\alpha\beta = 1$. Since α is arbitrary, we conclude that R is a field. □

Exercise 1.1.2. Let $K \subsetneq K(\alpha)$ be a simple extension, with α transcendental over K. Let E be a subfield of $K(\alpha)$ properly containing K. Prove that $K(\alpha)$ is a finite extension of E.

Proof. Let a be an element in E, then

$$a = \frac{f(\alpha)}{g(\alpha)}, \quad f, g \in K[X]$$

Now in the polynomial ring $E[X]$,

$$h(X) := \frac{f(\alpha)}{g(\alpha)} g(X) - f(X) = ag(X) - f(X) \in E[X]$$

satisfies $h(\alpha) =$, hence $E \subseteq K(\alpha)$ is finite. □

Exercise 1.1.3. Let $f(X) \in K[X]$ be a polynomial over a field K of degree n, and let $r_1, \dots, r_n$ be the roots of $f(X)$. For a subset $I \subseteq \{1, \dots, n\}$, denote by r_I the sum $\sum_{i \in I} r_i$. Assume that $r_I \in K$ only for $I = \varnothing$ and $I = \{1, \dots, n\}$. Prove that $f(X)$ is irreducible over K.

Proof. Let

$$p(X) = (X - r_{i_1}) \cdots (X - r_{i_d}) \in K[X]$$

be a factor of $f(X)$. Then the coefficient of X^{n-1} will be

$$(-1)^{d-1}(r_{i_1} + \cdots + r_{i_d}) = (-1)^{d-1} a_{i_1 \dots i_d}$$

which belongs to K. This implies $d = n$, so $f(X)$ is irreducible. □

Exercise 1.1.4. Let K be a field. Prove that the ring of square $n \times n$ matrices $\mathcal{M}_n(F)$ contains an isomorphic copy of every extension of K of degree $\leq n$.

Proof. Assume K is an extension of K with degree n. For any element $\alpha \in K$. Multiplication by α defines a K-linear transformation on K, and since α has a minimal polynomial

$$m_\alpha(X) = t^n + r_{n-1} t^{n-1} + \cdots + r_0$$

we choose the basis $1, \alpha, \dots, \alpha^{n-1}$, then the correponding matrix has the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}$$

□

Exercise 1.1.5. Let E/K be a finite field extension, and let $p(X)$ be the characteristic polynomial of the K-linear transformation of K given by multiplication by α. Prove that $p(\alpha) = 0$.

This gives an effective way to find a polynomial satisfied by an element of an extension. Use it to find a polynomial satisfied by $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Exercise 1.1.6. Let E/K be a finite field extension, and let $\alpha \in K$. The norm of α, $N_{E/K}(\alpha)$, is the determinant of the linear transformation of K given by multiplication by α.

Prove that the norm is multiplicative: for $\alpha, \beta \in f$,

$$N_{E/K}(\alpha\beta) = N_{E/K}(\alpha)N_{E/K}(\beta)$$

Compute the norm of a complex number viewed as an element of the extension $\mathbb{R} \subseteq \mathbb{C}$ (and marvel at the excellent choice of terminology). Do the same for elements of an extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, where d is an integer that is not a square,

Proof. For an element α, assume

$$m_\alpha(X) = t^n + r_{n-1}t^{n-1} + \cdots + r_0$$

we choose $1, \alpha, \ldots, \alpha^{n-1}$, then the map $L_\alpha : x \mapsto \alpha x$ has the matrix:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}$$

from which we get $N_{E/K}(\alpha) = (-1)^n r_0$. The multiplicative comes from that of determinant.

Let $z = a + bi \in \mathbb{C}$, then z has minimal polynomial $X^2 - 2aX + a^2 + b^2$ in $\mathbb{R}$. Hence we have $N_{\mathbb{C}/\mathbb{R}}(z) = a^2 + b^2 = |z|^2$.

Finally, consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$, then $m_{\sqrt{d}} = X^2 - d$, and $N(\sqrt{d}) = -d$. □

Exercise 1.1.7. Define the trace $\operatorname{tr}_{E/K}(\alpha)$ of an element α of a finite extension K of a field K by following the lead of Exercise above. Prove that the trace is additive:

$$\operatorname{tr}_{E/K}(\alpha + \beta) = \operatorname{tr}_{E/K}(\alpha) + \operatorname{tr}_{E/K}(\beta)$$

for $\alpha, \beta \in K$. Compute the trace of an element of an extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$ for d an integer that is not a square.

Proof. For two matrix, $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$. For the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$, $\operatorname{tr}(\sqrt{d}) = 0$. For α satisfying $m_\alpha(X) = t^n + r_{n-1}t^{n-1} + \cdots + r_0$, we have

$$N(\alpha) = (-1)^n r_0, \quad \operatorname{tr}(\alpha) = -r_{n-1}$$

□

Exercise 1.1.8. Let E/K be a finite extension, and let $\alpha \in E$. Assume $[E : K(\alpha)] = r$. Prove that

$$\operatorname{tr}_{E/K}(\alpha) = r \operatorname{tr}_{K(\alpha)/K}(\alpha), \quad N_{E/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^r.$$

Proof. If $f_1, \ldots, f_r$ is a basis of E over $K(\alpha)$ and α has degree d over K, then $(f_i\alpha^j)$ is a basis of E over K by Proposition 1.1.2.11. The matrix corresponding to multiplication by α with respect to this basis consists of r identical square blocks. Hence we get the result from simple linear algebra. □

Exercise 1.1.9. Let p be a prime integer, and let $\alpha = \sqrt[p]{2} \in \mathbb{R}$. Let $g(X) \in \mathbb{Q}[X]$ be any nonconstant polynomial of degree $< p$. Prove that α may be expressed as a polynomial in $g(\alpha)$ with rational coefficients.

Prove that an analogous statement for $\sqrt[4]{2}$ is false.

Proof. Consider the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(g(\alpha)) \subseteq \mathbb{Q}(\alpha).$$

Since $H(X) = g(X) - g(\alpha) \in \mathbb{Q}(g(\alpha))[X]$ satisfies $h(\alpha) = 0$, we see $[\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] < p$. Since p is a prime, this implies $[\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] = 1$ by Corollary 1.1.2.12, which means $\mathbb{Q}(\alpha) = \mathbb{Q}(g(\alpha))$. Now the claim follows.

For $\sqrt[4]{2}$, consider $g(X) = X^2$. Since any polynomial of $\sqrt{2}$ can be written into $a + b\sqrt{2}$. We see the claim is false in this case □

Exercise 1.1.10. Let $\xi = \sqrt{2+\sqrt{2}}$.

- Find the minimal polynomial of ξ over $\mathbb{Q}$, and show that $\mathbb{Q}(\xi)$ has degree 4 over $\mathbb{Q}$.
- Prove that $\sqrt{2-\sqrt{2}}$ is another root of the minimal polynomial of ξ.
- Prove that $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$.
- By Corollary 1.1.2.6, sending ξ to $\sqrt{2-\sqrt{2}}$ defines an automorphism of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$. Find the matrix of this automorphism w.r.t. the basis $1, \xi, \xi^2, \xi^3$.
- Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ is cyclic of order 4.

Proof.

- $(\xi^2-2)^2 = 2$, so $\xi^4 - 4\xi^2 + 2 = 0$, $m_\xi = X^4 - 4X^2 + 2 = (X^2-2)^2 - 2$, the roots of it are $\pm\sqrt{2\pm\sqrt{2}}$.
- A simple computation:

  $$\xi^2 = 2+\sqrt{2}, \quad \xi^3 = 2\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}, \quad \xi^4 = 6+4\sqrt{2}$$

  Note that

  $$\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2}$$

  so we have $\sqrt{2-\sqrt{2}} = \sqrt{2}\xi^{-1}$. We can see from above that $\sqrt{2} \in \mathbb{Q}(\xi)$, so $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$.

- Compute: denote $\sqrt{2-\sqrt{2}} =: \xi'$, and the automorphism φ, then we have $\xi' = \sqrt{2}\xi^{-1}$, and from $\xi^4 - 4\xi^2 + 2 = 0$ we obtain $\xi^{-1} = 2\xi - \xi^3/2$.

  $$\begin{aligned} &\varphi(1) = 1 \\ &\varphi(\xi) = \xi' = \sqrt{2}\xi^{-1} = (\xi^2-2)(2\xi - \xi^3/2) = \xi^3 - 3\xi \\ &\varphi(\xi^2) = \xi'^2 = 2-\sqrt{2} = 4-\xi^2 \\ &\varphi(\xi^3) = \xi'^3 = (4-\xi^2)\xi' = (4-\xi^2)(\xi^3-3\xi) = 7\xi^3 - 12\xi - \xi^5 = 3\xi^3 - 10\xi \end{aligned}$$

  so the matrix representation is

  $$A = \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & -3 & 0 & -10 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 3 \end{pmatrix}$$

- we know that $\mathbb{Q}(\xi) = \mathbb{Q}(-\sqrt{2+\sqrt{2}})$ and $\mathbb{Q}(-\sqrt{2-\sqrt{2}}) = \mathbb{Q}(\xi')$. And $\varphi^2 = id$. This means the extension is Galois, hence $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))| = 4$.

  We should clarify that calculating the composition of automorphisms should be done in this way: Let choose φ as an example, φ maps ξ to $\xi' = \xi^3 - 3\xi$, so φ^2 maps ξ to $\varphi(\xi^3 - 3\xi) = \xi'^3 - 3\xi' = (3\xi^3 - 10\xi) - 3(\xi^3 - 3\xi) = -\xi$. Now it is clear that $\varphi^4 = id$. So $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ has an element with order 4, hence is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

  By the way, the matrix corresponding to φ has order 4, that is, $\varphi^4 = I_4$. In fact we have

  $$A^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

□

1.2 Galois theory

1.2.1 Galois connections

The traditional Galois correspondence between intermediate fields of an extension and subgroups of the Galois group is one of the main themes of this chapter. We choose to approach this theme through a more general concept, however.

1.2.1.1 Definition of Galois connection

Definition 1.2.1.1. Let P and Q be partially ordered sets. A **Galois connection** on the pair (P, Q) is a pair (Π, Ω) of maps $\Pi : P \to Q$ and $\Omega : Q \to P$, where we write $\Pi(p) = p^e$ and $\Omega(q) = q^c$, with the following properties:

(1) (**Order-reversing**) For all $p, q \in P$ and $r, s \in Q$,

$$p \le q \Rightarrow q^e \le p^e, \quad r \le s \Rightarrow s^c \le r^c.$$

(2) (**Extensive**) For all $p \in P$, $q \in Q$,

$$p \le p^{ec}, \quad q \le q^{ce}.$$

Lurking within a Galois connection we find two closure operations.

Definition 1.2.1.2. Let P be a partially ordered set. A map $p \mapsto \text{cl}(p)$ on P is an (algebraic) **closure operation** if the following properties hold:

(1) (**Extensive**) For all $p \in P$, $p \le \text{cl}(p)$.

(2) (**Idempotent**) For all $p \in P$, $\text{cl}(\text{cl}(p)) = \text{cl}(p)$.

(3) (**Isotone**) For all $p, q \in P$, $p \le q \Rightarrow \text{cl}(p) \le \text{cl}(q)$.

An element $p \in P$ is said to be **closed** if $\text{cl}(p) = p$. The set of all closed elements in P is denoted by $\text{Cl}(p)$.

Theorem 1.2.1.3. *Let (Π, Ω) be a Galois connection on (P, Q). Then the maps*

$$p \mapsto p^{ec}, \quad q \mapsto q^{ce}$$

are closure operations on P and Q, respectively, and we write $p^{ec} = \text{cl}(p)$ and $q^{ce} = \text{cl}(q)$. Moreover,

(a) $p^{ece} = p^e$, that is,

$$\text{cl}(p^e) = \text{cl}(p)^e = p^e.$$

(b) $q^{cec} = q^c$, that is,

$$\text{cl}(q^c) = \text{cl}(q)^c = q^c$$

Proof. Since $p \le p^{ec}$, the order-reversing property of e gives

$$p^{ece} \le p^e \le (p^e)^{ce}.$$

and so $p^e = p^{ece}$, from which (a) follows. Part (b) is similar. □

Theorem 1.2.1.4. *The maps $\Pi : P \to \text{Cl}(Q)$ and $\Omega : Q \to \text{Cl}(P)$ are surjective and the restricted maps $\Pi : \text{Cl}(P) \to \text{Cl}(Q)$ and $\Omega : \text{Cl}(Q) \to \text{Cl}(P)$ are inverse bijections.*

Proof. Since $\text{cl}(p^e) = p^e$, we see that p^e is closed, that is, Π maps P into $\text{Cl}(P)$. Moreover, Π is surjective since if $q \in \text{Cl}(Q)$, then $q = \text{cl}(q) = (q^c)^e$. To see that Π is injective when restricted to closed elements, if $p, q \in \text{Cl}(P)$ and $p^e = q^e$, then $p^{ec} = q^{ec}$, that is, $p = q$. Similar arguments apply to Ω. Finally, since

$$\Omega \circ \Pi(\text{cl}(p)) = \text{cl}(\text{cl}(p)) = \text{cl}(p)$$

we see that $\Omega \circ \Pi = \text{id}$ on $\text{Cl}(P)$ and similarly, $\Pi \circ \Omega = \text{id}$ on $\text{Cl}(Q)$. □

Now we give some examples of Galois connections.

Example 1.2.1.5. Let X and Y be nonempty sets and $P = \mathscr{P}(X)$ and $Q = \mathscr{P}(Y)$ be the corresponding power sets. Let $R \subseteq X \times Y$ be a relation on $X \times Y$. Then the maps

$$S \in \mathscr{P}(X) \mapsto S^e = \{y \in Y : (x,y) \in R \text{ for all } x \in S\},$$

and

$$T \in \mathscr{P}(Y) \mapsto T^c = \{x \in X : (x,y) \in R \text{ for all } y \in T\}$$

form a Galois connection on $(\mathscr{P}(X), \mathscr{P}(Y))$.

Example 1.2.1.6. Let $n \geq 1$ and let K be a field. Let $P = \mathscr{P}(K[X_1, \ldots, X_n])$ be the set of all subsets of polynomials over K in the variables $X_1, \ldots, X_n$. Let $Q = \mathscr{P}(K^n)$ be the set of all subsets of K^n, the set of all ordered n-tuples over K. Let $\Pi : \mathscr{P}(K[X_1, \ldots, X_n]) \to \mathscr{P}(K^n)$ be defined by

$$\Pi(S) = \{x \in K^n : f(X) = 0 \text{ for all } f \in S\}$$

and let $\Omega : \mathscr{P}(K^n) \to \mathscr{P}(K[X_1, \ldots, X_n])$ be defined by

$$\Omega(T) = \{f \in K[X_1, \ldots, X_n] : f(X) = 0 \text{ for all } x \in T\}$$

Then (Π, Ω) is a Galois connection on $(\mathscr{P}(K[X_1, \ldots, X_n]), \mathscr{P}(K^n))$.

In the examples given above, the partially ordered sets P and Q are both lattices. In this situation, we have the follwoing useful result.

Theorem 1.2.1.7. *Let (Π, Ω) be a Galois connection on a pair (P, Q) of lattices.*

(a) *If P is a complete lattice, then so is $\mathrm{Cl}(P)$, under the same meet as P. A similar statement holds for Q.*

(b) *De Morgan's laws hold in $\mathrm{Cl}(P)$ and $\mathrm{Cl}(Q)$, that is, for $p, q \in \mathrm{Cl}(P)$ and $r, s \in \mathrm{Cl}(Q)$,*

$$(p \wedge q)^e = p^e \vee q^e, \quad (p \vee q)^e = p^e \wedge q^e,$$

and

$$(r \wedge s)^c = r^c \vee s^c, \quad (r \vee s)^c = r^c \wedge s^c,$$

Proof. For (a), first, since $1 \in P$ has the property that $1 \geq \mathrm{cl}(1) \geq 1$, it follows that $1 \in \mathrm{Cl}(P)$. Suppose that $p_i \in \mathrm{Cl}(P)$. Then the meet $\bigwedge p_i$ exists in P and since $\bigwedge p_i \leq p_j$ for all j, we have

$$\mathrm{cl}(\bigwedge p_i) \leq \mathrm{cl}(p_j) = p_j$$

whence $\mathrm{cl}(\bigwedge p_i) \leq \bigwedge p_j$. Since the reverse inequality holds as well, equality holds and $\bigwedge p_i \in \mathrm{Cl}(P)$. Since joins can be defined in terms of meets, ($\bigvee T$ is the meet of all upper bounds of T), it follows that $\mathrm{Cl}(P)$ is a complete lattice under meet in P. A similar argument can be made for Q.

For (b), observe first that $p \wedge q \leq p$ and $p \wedge q \leq q$ imply that $(p \wedge q)^e \geq p^e$ and $(p \wedge q)^e \geq q^e$, whence $(p \wedge q)^e \geq p^e \vee q^e$. Furthermore, if $r \geq p^e$ and $r \geq q^e$ for $r \geq \mathrm{Cl}(Q)$, then $r^c \leq p$ and $r^c \leq q$, whence $r^c \leq p \wedge q$. Thus, $r \geq (p \wedge q)^e$. It follows by definition of join that $(p \wedge q)^e = p^e \vee q^e$. The other parts of De Morgan's laws are proved similarly. □

In many examples of Galois connections, P and Q have both top and bottom elements. The following remark on the closeness of them is useful.

Proposition 1.2.1.8. *Let (Π, Ω) be a Galois connection on (P, Q), where P and Q have top and bottom elements. Then*

(a) *1_P and 1_Q are closed, and we have*

$$1_P = \Omega(0_Q), \quad 1_Q = \Pi(0_P).$$

(b) *0_P is closde if and only if $0_P = \Omega(1_Q)$, and 0_Q is closed if and only if $0_Q = \Pi(1_P)$.*

Proof. A top element is closed, since $1_P \leq \mathrm{cl}(1_P) \leq 1_P$, and similar for 1_Q. Also, note that a top element is the image of the corresponding bottom element (if it exists), for $1_P = \Omega(\Pi(p))$ is the image of $\Pi(p)$ and since $0_Q \leq \Pi(p)$, the image of 0_Q must be at least as large as $\Pi(p)$, and therefore equal to 1_P.

Now, since $\Pi(0_P) = 1_Q$, it is closed if and only if $0_P = \Omega(\Pi(0_P)) = \Pi(1_Q)$. Similar, since $\Omega(0_Q) = 1_P$, it is closed if and only if $0_Q = \Pi(\Omega(0_Q)) = \Pi(1_P)$. □

1.2.1.2 Indexed Galois connections Let $\mathbb{Z}^+$ denote the set of positive integers. In the set $\mathbb{Z}^+ \cup \{\infty\}$, we observe some obvious understandings about ∞, in particular, $\infty \leq \infty$, $n \leq \infty$ for all $n \in \mathbb{Z}^+$, $n \cdot \infty = \infty$ for $n \in \mathbb{Z}^+$ and $\infty \leq n \leq \infty$ implies $n = \infty$.

Definition 1.2.1.9. A Galois connection (Π, Ω) on (P, Q) is **indexed** if

(a) For each $p, q \in P$ with $p \leq q$, there exists a number $(q, p) \in \mathbb{Z}^+ \cup \{\infty\}$, called the degree, or index of q over p.

(b) For each $r, s \in Q$ with $r \leq s$, there exists a number $(s, r) \in \mathbb{Z}^+ \cup \{\infty\}$, called the degree, or index of s over r.

Moreover, the following properties must hold:

(1) (**(Degree is multiplicative**) If $s_1, s_2, s_3 \in P$ or Q, then

$$s_1 \leq s_2 \leq s_3 \Rightarrow (s_3 : s_1) = (s_3 : s_2)(s_2 : s_1).$$

(2) (**Degree is nonincreasing**) If $p, q \in P$ then

$$p \leq q \Rightarrow (p^e : q^e) \leq (q : p).$$

If $r, s \in Q$ then

$$r \leq s \Rightarrow (r^c : s^c) \leq (s : r).$$

(3) (**Equality by degree**) If $s, t \in P$ or Q, then

$$(s : t) = 1 \Leftrightarrow s = t$$

If $(s : t) < \infty$, then t is said to be a finite extension of s. If P has a top and bottom element then the index of P is $\text{index}(P) := (1_P : 0_P)$, and similarly for Q.

From now on, when we write $(q : p)$, it is with the tacit assumption that $p \leq q$.

The importance of indexing is described in the next theorem. It says that if a Galois connection is indexed, then the connection preserves the index of closed elements and that any finite extension of a closed element is also closed.

Theorem 1.2.1.10. *Let (Π, Ω) be an indexed Galois connection on (P, Q).*

*(a) (**Degree-preserving on closed elements**) If $p, q \in \text{Cl}(P)$ and $p \leq q$ then $(q : p) = (p^e : q^e)$.*

*(b) (**Finite extensions of closed elements are closed**) If $p \in \text{Cl}(P)$ and $(q : p) < \infty$ then $q \in \text{Cl}(P)$. In particular, if 0_P is closed and $(1_P : 0_P)$ is finite then all elements of P are closed.*

A similar statement holds for Q.

Proof. For (a), we have

$$(q : p) \geq (p^e : q^e) \geq (q^{ec} : q^{ec}) = (q : p).$$

so equality holds throughout.

For (b), if $p \in \text{Cl}(P)$ and $(q : p) < \infty$, then

$$(q : p) \geq (p^e : q^e) \geq (q^{ec} : p^{ec}) = (q^{ec} : p) = (\text{cl}(q) : q)(q : p).$$

and since $(q : p) < \infty$, we may cancel to get $(\text{cl}(q) : q) = 1$, which shows that q is closed. □

Thus, in an indexed Galois connection, the maps are degree-preserving, order-reversing bijections between the collections of closed sets $\text{Cl}(P)$ and $\text{Cl}(Q)$.

Proposition 1.2.1.11. *Let (Π, Ω) be an indexed Galois connection on (P, Q). If $p, q \in P$, $\text{cl}(p) \leq q$, and one of the following holds*

(a) $(q : p) = (p^e : q^e)$ and $(q : \text{cl}(p)) < \infty$.

(b) $(q : p) = (p^e : q^e) < \infty$.

then p is closed.

Proof. Suppose that $(q : \mathrm{cl}(p)) < \infty$. Then q is closed by Theorem 1.2.1.10 and since $\mathrm{cl}(p)^e = p^e$, we have

$$(q : \mathrm{cl}(p)) = (p^e : q^e).$$

Now if $(p^e : q^e) = (q : p)$, then we have $(q : \mathrm{cl}(p)) = (q : p)$. This implies $(\mathrm{cl}(p) : p) = 1$ if either $(q : \mathrm{cl}(p)) < \infty$ or $(q : p) < \infty$, and so $p = \mathrm{cl}(p)$ is closed. □

The following nonstandard definition will come in handy.

Definition 1.2.1.12. Let (Π, Ω) be a Galois connection on (P, Q), we say that P is **completely closed** if every element of P is closed, and similarly for Q. Also, the pair (P, Q) (or the connection) is **completely closed** if all elements of P and all elements of Q are closed.

We have remarked that the top elements 1_P and 0_Q, if they exist, are always closed, but the bottom elements 0_P and 0_Q need not be closed. However, the most important example of a Galois connection, namely, the Galois correspondence of a field extension E/K, which is the subject of our investigations, has the property that 0_Q is closed. So let us assume that 0_Q is closed and see what we can deduce.

Theorem 1.2.1.13 (0_Q is closed). *Let (Π, Ω) be an indexed Galois connection on (P, Q), where P and Q have top and bottom elements. Assume that 0_Q is closed. Then*

$$\mathrm{index}(Q) \leq \mathrm{index}(P).$$

Also,

(a) If $\mathrm{index}(Q) < \infty$ or $\mathrm{index}(P) < \infty$, then Q is completely closed.

(b) If $\mathrm{index}(P) < \infty$ and 0_P is closed, then (P, Q) is completely closed.

Proof. Since 0_Q is closed, by Proposition 1.2.1.8 we have $1_P^e = 0_Q$, and therefore

$$\mathrm{index}(P) = (1_P : 0_P) \geq (0_P^e : 1_P^e) = (1_Q : 1_P^e) = (1_Q : 0_Q) = \mathrm{index}(Q)$$

it follows that if P has finite index, then so does Q. Hence, if either P or Q has finite index, then Q is completely closed.

Finally, if P has finite index and 0_P is also closed, then the connection is completely closed by Theorem 1.2.1.10. □

1.2.2 The Galois correspondence

Now we describe the main theme of this chapter.

Definition 1.2.2.1. The **Galois group** of a field extension E/K, denoted by $\mathrm{Gal}(E/K)$, is the group $\mathrm{Aut}_K(E)$ of all automorphisms of E over K. The group $\mathrm{Gal}(E/K)$ is also called the Galois group of E over K.

Note that when the extension E/K is algebraic, by Theorem 1.1.4.2

$$\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E) = \mathrm{Hom}_K(E, E),$$

and when E is normal over K, by Theorem 1.1.5.7

$$\mathrm{Gal}(E/K) = \mathrm{Hom}_K(E, \overline{E}).$$

Let E/K be a field extension and let $\mathcal{F}$ be the complete lattice of all intermediate fields of $K \subseteq E$, ordered by set inclusion. Let $\mathcal{G}$ be the complete lattice of all subgroups of the Galois group $\mathrm{Gal}(E/K)$, ordered by set inclusion. We define two maps $\Pi : \mathcal{F} \to \mathcal{G}$ and $\Omega : \mathcal{G} \to \mathcal{F}$ by

$$\Pi(K) = \mathrm{Gal}(E/K), \quad \Omega(H) = E^H$$

where E^H is the **fixed field** of H.

Theorem 1.2.2.2. *Let E/K. The pair of maps*

$$(\Pi : K \mapsto \mathrm{Gal}(E/K), \Omega : H \mapsto E^H)$$

is a Galois connection on $(\mathcal{F}, \mathcal{G})$, called the Galois correspondence of the extension E/K.

Proof. It is clear from the definition that Π and Ω are inclusion-reversing. Also, any element of K is fixed by every element of $\mathrm{Gal}(E/K)$, that is, $K \subseteq E^{\mathrm{Gal}(E/K)}$. Finally, any $\sigma \in H$ fixes every element in E^H, that is, $H \subseteq \mathrm{Gal}(E/E^H)$. Thus the claim follows. □

Since $\mathcal{F}$ and $\mathcal{G}$ are complete lattices, Theorem 1.2.1.7 provides the following corollary.

Corollary 1.2.2.3. *The set $\mathrm{Cl}(\mathcal{F})$ of closed intermediate fields and the set $\mathrm{Cl}(\mathcal{G})$ of closed subgroups of $\mathrm{Gal}(E/K)$ are complete lattices, where meet is intersection. In particular, the intersection of closed intermediate fields is closed and the intersection of closed subgroups is closed.*

We would like to show that the Galois correspondence of an extension E/K is indexed, where $(K : L) = [K : L]$ is the degree of the extension K/L and $(H : J)$ is the index of the subgroup J in the group H. We know that the degrees are multiplicative and that

$$[K : L] = 1 \Leftrightarrow K = L, \quad [H : J] = 1 \Leftrightarrow H = J.$$

The next theorem shows that the map $\Pi : K \mapsto \mathrm{Gal}(E/K)$ is degree-nonincreasing.

Proposition 1.2.2.4. *For the tower $K \subseteq E \subseteq F \subseteq L$, we have*

$$[\mathrm{Gal}(L/E) : \mathrm{Gal}(L/F)] \leq [F : E]_s \leq [F : E]$$

as elements in $\mathbb{Z}^+ \cup \{\infty\}$.

Proof. Consider the function $\Phi : \mathrm{Gal}(L/E) \to \mathrm{Hom}_K(F, L)$ that maps $\sigma \in \mathrm{Gal}(L/E)$ to its restriction $\sigma|_F \in \mathrm{Hom}_K(F, L)$. Then $\Phi(\sigma) = \Phi(\tau)$ if and only if σ and τ agree on F, that is, if and only if $\sigma\mathrm{Gal}(L/F) = \tau\mathrm{Gal}(L/F)$. Hence Φ is constant on the cosets of $\mathrm{Gal}(L/F)$ in $\mathrm{Gal}(L/E)$ and so induces an injection on $\mathrm{Gal}(L/E)/\mathrm{Gal}(L/F)$, whence

$$[\mathrm{Gal}(L/E) : \mathrm{Gal}(L/F)] = |\operatorname{im}(\Phi)| \leq |\mathrm{Hom}_K(F, L)| \leq [F : K]_s.$$

This finishes the proof. □

Proposition 1.2.2.5. *Let E/K be an extension and let $J \subseteq H \subseteq \mathrm{Gal}(E/K)$. Then*

$$[E^J : E^H] \leq [H : J].$$

Proof. First, if $[H : J]$ is infinite, then there is nothing to prove, so let us assume that $[H : J] < \infty$, that is, $H/J = \{h_1 J, \ldots, h_m J\}$ is a finite set. Thus, $S = \{h_1, \ldots, h_m\}$ is a complete set of distinct coset representatives for H/J, and we may assume that $h_1 \in J$.

Let $E^{H/J}$ denote the set of all functions from H/J into E. Then $E^{H/J}$ is a vector space over E, where if $\sigma, \tau \in E^{H/J}$ and $a, b \in E$, then

$$(a\sigma + b\tau)(hJ) = a\sigma(hJ) + b\tau(hJ).$$

Moreover, since the functions $\epsilon_i : H/J \to E$ defined by $\epsilon_i(h_k J) = \delta_{i,k}$ form a basis for $E^{H/J}$ over E, we have

$$\dim_E(E^{H/J}) = |H/J| = [H : J].$$

Thus, we have two vector spaces: E^J is a vector space over E^H of dimension $[E^J : E^H]$ and $E^{H/J}$ is a vector space over E of dimension $[H : J]$. We wish to show that $\dim_{E^H}(E^J) \leq \dim_E(E^{H/J})$.

To do this, we will show that $\alpha_1, \ldots, \alpha_n \in E^J$ are linearly independent over E^H if and only if the evaluation functions $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n \in E^{H/J}$, defined by

$$\widetilde{\alpha}_k(h_i J) = h_i(\alpha_k)$$

are linearly independent over E. Note that if $h_1 J = h_2 J$ then $h_1^{-1} h_2 \in J$ and so

$$(h_1^{-1} h_2)(\alpha_k) = \alpha_k$$

(recall that $\alpha_k \in E^J$) which implies that $h_1(\alpha_k) = h_2(\alpha_k)$, that is, $\widetilde{\alpha}_k(h_1J) = \widetilde{\alpha}_k(h_2J)$. Hence, $\widetilde{\alpha}_k$ is well-defined.

Let $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n \in E^{H/J}$ be linear independent over E. If there are $e_1, \ldots, e_s \in E^H$ such that

$$e_1\alpha_1 + \cdots + e_s\alpha_s = 0$$

then we have

$$\begin{aligned}(e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s)(h_kJ) &= e_1h_k(\alpha_1) + \cdots + e_sh_k(\alpha_s)\\ &= h_k(e_1\alpha_1 + \cdots + e_s\alpha_s) = 0\end{aligned}$$

for all $h_k \in S$. Therefore $e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s = 0$, which implies $e_1 = \cdots = e_s = 0$ by linearly independence of $\widetilde{\alpha}_k$'s over E.

Now assume that $\alpha_1, \ldots, \alpha_n \in E^J$ are linearly independent over E^H and, by reindexing if necessary, let

$$e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s = 0$$

be a nontrivial linear combination over E that is shortest among all nontrivial linear combinations equal to 0. Thus, $e_i \neq 0$ for all i. Dividing by e_s if necessary, we may also assume that $e_s = 1$. Thus

$$e_1\widetilde{\alpha}_1 + \cdots + e_{s-1}\widetilde{\alpha}_{s-1} + \widetilde{\alpha}_s = 0. \tag{1.2.2.1}$$

Then applying this to h_kJ gives

$$e_1h_k(\alpha_1) + \cdots + e_{s-1}h_k(\alpha_{s-1}) + h_k(\alpha_s) = 0.$$

for all $h_k \in S$. Since the α_i's are fixed by any element of J, and any $h \in H$ has the form $h = h_kj$ for some $j \in J$, we deduce that

$$e_1h(\alpha_1) + \cdots + e_{s-1}h(\alpha_{s-1}) + h(\alpha_s) = 0 \tag{1.2.2.2}$$

for all $h \in H$. In particular, if $h = 1$, then

$$e_1\alpha_1 + \cdots + e_{s-1}\alpha_{s-1} + \alpha_s = 0. \tag{1.2.2.3}$$

which implies, owing to the independence of the α_i's over E^H, that not all of the e_i's can lie in E^H. Let us assume that $e_1 \notin E^H$. Hence, there is a $\tau \in H$ for which $\tau(e_1) \neq e_1$.

We can replace h by $\tau^{-1}h$ in (1.2.2.2) to get

$$e_1\tau^{-1}h(\alpha_1) + \cdots + e_{s-1}\tau^{-1}h(\alpha_{s-1}) + \tau^{-1}h(\alpha_)s = 0.$$

Applying τ gives

$$\tau(e_1)h(\alpha_1) + \cdots + \tau(e_{s-1})h(\alpha_{s-1}) + h(\alpha_s) = 0$$

for all $h \in H$ and so

$$(\tau e_1)\widetilde{\alpha}_1 + \cdots + (\tau e_{s-1})\widetilde{\alpha}_{s-1} + \widetilde{\alpha}_s = 0.$$

Finally, subtracting (1.2.2.1) from (1.2.2.3) gives

$$(\tau e_1 - e_1)\widetilde{\alpha}_1 + \cdots + (\tau e_{s-1} - e_{s-1})\widetilde{\alpha}_{s-1} = 0.$$

whose first coefficient is nonzero. But this is shorter than (1.2.2.1), a contradiction that completes the proof. □

Thus, the Galois correspondence of an extension E/K is indexed. We can now summarize our results in a famous theorem.

Theorem 1.2.2.6 (Fundamental Theorem of Galois Theory I). *The Galois correspondence (Π, Ω) of an extension E/K is an indexed Galois connection and the bottom group 0_Q is closed. The restrictions of Π and Ω to closed elements are order-reversing, degreepreserving inverse bijections as well as lattice anti-isomorphisms, that is, if K_i are closed intermediate fields and H_i are closed subgroups, then*

$$\mathrm{Gal}(E/\bigcap K_i) = \bigvee \mathrm{Gal}(E/K_i), \quad \mathrm{Gal}(E/\bigvee K_i) = \bigcap \mathrm{Gal}(E/K_i),$$

and

$$E^{\bigcap H_i} = \bigvee E^{H_i}, \quad E^{\bigvee H_i} = \bigcap E^{H_i}.$$

We should note that the joins in the previous theorem are joins in the corresponding lattices. Thus, for instance, $\bigvee \mathrm{Gal}(E/K_i)$ is the smallest closed subgroup of $\mathrm{Gal}(E/K)$ containing all of the subgroups $\mathrm{Gal}(E/K_i)$, and this need not be the smallest subgroup of $\mathrm{Gal}(E/K)$ containing these groups.

As a result of the closedness of $0_Q = \{1\} = \mathrm{Gal}(E/E)$, Theorem 1.2.1.13 gives the following.

Corollary 1.2.2.7. *Let (Π, Ω) be the Galois correspondence of E/K. Then*

$$|\mathrm{Gal}(E/K)| \leq [E : K].$$

Also,

(a) If $|\mathrm{Gal}(E/K)| < \infty$ or $[E : K] < \infty$, then $\mathcal{G}$ is completely closed.

(b) If $[E : K] < \infty$ and K is closed, then $\mathcal{F}$ and $\mathcal{G}$ are completely closed.

1.2.3 Closed elements in the Galois correspondence

We turn our attention to the question of which intermediate fields of an extension and which subgroups of the Galois group are closed. We know on general principles that top elements are always closed. Thus, E and $\mathrm{Gal}(E/K)$ are closed. Moreover, the bottom group $\{1\} = \mathrm{Gal}(E/E)$ is also closed. We also know that any finite extension of a closed element is closed.

Now we require a definition. A normal separable extension E/K is called a **Galois extension**, or simply **Galois**. The next theorem follows from the relevant properties of normal and separable extensions. We state it separably.

Proposition 1.2.3.1 (Properties of Galois extensions).

*(a) (**Full extension Galois implies upper step Galois**) Let $K \subseteq E \subseteq L$. If L/K is Galois then the upper step L/K is Galois.*

*(b) (**Closed under lifting**) The class of Galois extensions is closed under lifting.*

*(c) (**Closed under arbitrary composites and intersections**) The class of Galois extensions is closed under arbitrary composites and intersections.*

The importance of Galois extension is revealed in the following theorem.

Theorem 1.2.3.2 (Fundamental Theorem of Galois Theory II). *Let E/K be algebraic and consider the Galois correspondence on E/K.*

*(1) (**Closed fields**) The closed intermediate fields are precisely the fixed fields, that is, the fields of the form E^H for some $H \subseteq \mathrm{Gal}(E/K)$.*

(a) An intermediate field K is closed if and only if E/K is Galois.

(b) Any extension of a closed intermediate field is closed.

(c) If E/K is a Galois extension, then $\mathcal{F}$ is completely closed.

*(2) (**Closed groups**) The closed subgroups of $\mathrm{Gal}(E/K)$ are precisely the Galois groups of E, that is, the subgroups of the form $\mathrm{Gal}(E/K)$, for some intermediate field K.*

(a) Any finite extension of a closed subgroup is closed.

(b) $\{1\}$ is closed and so any finite subgroup of $\mathrm{Gal}(E/K)$ is closed.

(c) When E/K is finite, so is $\mathrm{Gal}(E/K)$ and so $\mathcal{G}$ is completely closed.

(3) If E/K is a finite Galois extension, then the correspondence is completely closed.

Proof. First, suppose that K is closed and let $\alpha \in E \setminus K$. Then the finite extension $K(\alpha) \subseteq K$ of K is also closed and so

$$d := [\mathrm{Gal}(E/K) : \mathrm{Gal}(E/K(\alpha))] = [K(\alpha) : K] < \infty.$$

Let $S = \{\sigma_1, \dots, \sigma_d\}$ be a representatives for the coset $\mathrm{Gal}(E/K)/\mathrm{Gal}(E/K(\alpha))$. Each element of S gives a distinct value on α, that is, a distinct root of $\min(\alpha, K)$, for if $\sigma_i(\alpha) = \sigma_j(\alpha)$, then $\sigma_i \circ \sigma_j^{-1} \in \mathrm{Gal}(E/K(\alpha))$, which is not possible for $i \neq j$. Hence, the d roots of $\min(\alpha, K)$ are $\{\sigma_1(\alpha), \dots, \sigma_d(\alpha)\}$, which are distinct and lie in E. Thus, α is separable and $\min(\alpha, K)$ splits in E, implying that E/K is a Galois extension.

For the converse, suppose that E/K is Galois. If $\alpha \in \mathrm{cl}(K) = E^{\mathrm{Gal}(E/K)}$ has minimal polynomial $f(X) = \min(\alpha, K)$, then $f(X)$ can have no roots other than α. For if β is a root of $f(X)$ in some extension, then there is an embedding $\sigma : E \to \bar{K}$ over K for which $\sigma(\alpha) = \beta$. But since E is normal over K, it follows that $\sigma \in \mathrm{Gal}(E/K)$ and so $\beta = \sigma(\alpha) = \alpha$. Thus $f(X)$ has only one distinct root. Since E/K is separable, it must be linear, which implies that $\alpha \in K$. Thus, $\mathrm{cl}(K) = K$ and K is closed.

Now let K be a closed intermediate field, so that E/K is Galois. If L is an arbitrary extension of K (not necessarily finite), then by Proposition 1.2.3.1 the extension E/L is also Galois, and therefore L is closed. □

Now we give some examples of non Galois extensions to show that in the general algebraic case, not all subgroups need be closed.

Example 1.2.3.3. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Since

$$[\mathbb{Q} : \mathbb{Q}(\sqrt[3]{2})] = 3$$

is prime, the only intermediate fields are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})$ (by Corollary 1.1.2.12). Concerning $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$, since $\sqrt[3]{2} \in \mathbb{R}$, we have an extension $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$; since $\sqrt[3]{2}$ is the only cube root of 2 in $\mathbb{R}$, we see that the minimal polynomial $X^3 - 2$ of $\sqrt[3]{2}$ has a single root in $\mathbb{Q}(\sqrt[3]{2})$. By Corollary 1.1.2.6, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ consists of a single element: it is trivial. Thus, in this example the Galois correspondence acts between a set with two elements and a singleton:

$$\{\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})\} \rightleftarrows \{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))\} = \{e\}$$

In particular, the function associating with each intermediate field the corresponding automorphism group is not injective.

Example 1.2.3.4. For this example, we shall use the fact that for any prime power p^d, there exists a unique finite field $\mathbb{F}_{p^d}$ of size p^d and $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ if and only if $d \mid e$. Let $K = \mathbb{F}_p$ and let $E = \overline{\mathbb{F}}_p$. Since K is a finite field, it is perfect and so E/K is separable. Since E is algebraically closed, E/K is normal. Hence E/K is a Galois extension and therefore K is closed. The extension E/K is not finite, however, since $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$ and $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \overline{\mathbb{F}}_p$ for all $d \geq 1$.

Let $H = \langle \sigma \rangle$ be the subgroup of $\mathrm{Gal}(E/K)$ generated by the Frobenius homomorphism $\sigma : x \mapsto x^p$. The fixed field E^H is the set of all $\alpha \in E$ for which $\alpha = \alpha^p$, in other words, the roots in E of the polynomial $f(X) = X^p - X$. But $f(X)$ already has p roots in K, and so $E^H = K$. It then follows that

$$\mathrm{cl}(H) = \mathrm{Gal}(E/E^H) = \mathrm{Gal}(E/K).$$

Hence, all we need do is show that $H \neq \mathrm{Gal}(E/K)$ to conclude that H is not closed. The key is that any $\tau \in H$ has the form $\tau = \sigma^d$ for some $d \geq 1$ and so the fixed set of τ is

$$\{\alpha \in E : \sigma^d(\alpha) = \alpha\} = \{\alpha \in E : \alpha^{p^d} - \alpha = 0\} = \mathbb{F}_{p^d}$$

which is a finite set. Thus, it suffices show that there is an element of $\mathrm{Gal}(E/K)$ that fixes infinitely many elements of E. To this end, let q be another prime and consider the field

$$F = \mathbb{F}_{p^q} \cup \mathbb{F}_{p^{q^2}} \cup \mathbb{F}_{p^{q^3}} \cup \cdots$$

Then F is a proper subfield of E, since it does not contain, for instance, the subfield $\mathbb{F}_{p^{q+1}}$. Hence $[E : F] > 1$ and since E/F is Galois, the group $\mathrm{Gal}(E/F)$ is not trivial. But if $\tau \in \mathrm{Gal}(E/F)$, then τ fixes the infinite field F.

The Galois correspondence begins with a field extension E/K and the corresponding Galois group $\mathrm{Gal}(E/K)$. We may also begin with a field E and a subgroup G of $\mathrm{Aut}(E)$. Then we can form the fixed field

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$$

and consider the Galois correspondence of the extension E/E^G.

Proposition 1.2.3.5. *Let E be a field and let G be a group of automorphisms of E.*

(a) If E/E^G is algebraic, then it is Galois and all intermediate fields are closed.

(b) If E/E^G is finite, then all intemediate fields and all subgroups are closed.

(c) If G is closed (which happens if G is finite), then $G = \mathrm{Gal}(E/E^G)$ is the top group of the correspondence.

$$\begin{tikzcd}
E \arrow[dd, dash] & \mathrm{Gal}(E/E^G) \arrow[d, dash] \\
 & G \arrow[d, dash] \arrow[dl] \\
K = E^G \arrow[uur] & \{1\}
\end{tikzcd}$$

Proof. Suppose E/E^G is algebraic. Then since the base field E^G is closed, E/E^G is a Galois extension. If moreover $[E : E^G] < \infty$, then the correspondence is completely closed by Theorem 1.2.3.2. If G is closed, then $G = \mathrm{Gal}(E/E^G)$, so it is the top group. □

1.2.4 The Krull topology on Galois group

Let E/K be algebraic. The closure $\mathrm{cl}(H)$ of a subgroup H of the Galois group $\mathrm{Gal}(E/K)$ can be characterized in a useful way. The following nonstandard definition will help.

Definition 1.2.4.1. Let E/K be algebraic. Let H be a subgroup of the Galois group $\mathrm{Gal}(E/K)$. A function $\tau : E \to E$ is a **limit point** of H if for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$, that is, τ agrees with some member of H on S. Let $\overline{H}$ denote the set of closure points of H.

The name "limit point" is justified in the following proposition.

Proposition 1.2.4.2. *Let E/K be algebraic and let H be a subgroup of the Galois group $\mathrm{Gal}(E/K)$. Then $\mathrm{cl}(H)$ is the set of limit points of H. More specifically, the following are equivalent:*

(i) *$\tau \in \mathrm{cl}(H)$,*

(ii) *for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$.*

Consequently, a subgroup H of $\mathrm{Gal}(E/K)$ is closed if and only if it contains all of its closure points. In particular, any subgroup of the form $\mathrm{Gal}(E/K)$ contains all of its closure points.

Proof. First, note that a closure point τ of H is a member of the Galois group $\mathrm{Gal}(E/K)$, in fact, τ is in the closure of H, that is

$$\overline{H} \subseteq \mathrm{Gal}(E/E^H) = \mathrm{cl}(H).$$

Indeed, τ is a homomorphism because it agrees with a homomorphism on any finite set in E and it fixes each element of E^H because every member of $\mathrm{Gal}(E/E^H)$ fixes E^H.

We claim that $\overline{H} = \mathrm{cl}(H)$. Since $H \subseteq \overline{H} \subseteq \mathrm{cl}(H)$, the result would follow if H were closed, but of course, it may not be. However, given any finite set $S \subseteq E$, we need only work with the finite extension $E^H \subseteq E^H(S)$, whose Galois group is $\mathrm{Gal}(E^H(S)/E^H)$. In this case, all subgroups are closed. The problem is that we want $H|_{E^H(S)}$ to be in the Galois group and this requires that $E^H \subseteq E^H(S)$ be normal. No problem really: we just pass to a normal closure. Consider the extension

$$E^H \subseteq K = \langle E^H(S)/K \rangle$$

which is finite, normal, contains S and has Galois group $\mathrm{Gal}(K/E^H)$. Since all subgroups are closed, $H|_K$ is a closed subgroup of the Galois group $\mathrm{Gal}(K/E^H)$. Hence, in the Galois correspondence on $E^H \subseteq K$, we have

$$H|_K \subseteq \overline{H|_K} = \mathrm{cl}(H|_K) = \mathrm{Gal}(K/\mathrm{Inv}(H|_K)).$$

It follows that any $\sigma \in$ agrees with a member of $H|_K$ on S. But if $\tau \in \mathrm{cl}(H) = \mathrm{Gal}(E/E^H)$, then

$$\tau|_K \in \mathrm{Gal}(E/\mathrm{Inv}(H))|_K = \mathrm{Gal}(K/\mathrm{Inv}(H|_K))$$

and so $\tau|_K$ agrees with a member of $H|_K$ on S, that is, τ agrees with a member of H on S. Thus, $\overline{H} \in \mathrm{cl}(H)$, as desired. □

We now extend the definition of closure point to apply to any set of functions in E^E, not just subgroups of the Galois group. In particular, a function $\tau \in E^E$ is a closure point of $H \subseteq E^E$ if for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$.

It is not hard to show that the operation $H \mapsto \overline{H}$ is an algebraic closure operation. In addition, we have $\overline{\varnothing} = \varnothing$ and

$$\overline{H \cup K} = \overline{H} \cup \overline{K}$$

To see the latter, note that if $f \in \overline{H \cup K}$, then for any finite subset $S \subseteq E$, the function f agrees with an element of $H \cup K$ on S. But if $f \notin \overline{H}$, then there is a finite set $S \subseteq E$ for which f does not agree with any element of H on S. Similarly, if $f \notin \overline{K}$, then there is a finite set $R \subseteq E$ for which f does not agree with any element of K on R. However, $R \cup S$ is a finite set and so there must be some element $g \in H \cup K$ that agrees with f on $R \cup S$, and therefore on both R and S, that is, $f = g$ on R and $f = g$ on S. But $g \in H$ or $g \in K$, either one of which provides a contradiction.

It follows that the operation $H \mapsto \overline{H}$ is also a topological closure operation. Hence, the set of all complements of closed elements forms a toplology on E^E. This topology is actually quite famous.

Definition 1.2.4.3. Let E^E be the set of all functions from E into E. The **finite topology** on E^E is defined by specifying as subbasis all sets of the form

$$S_{u,v} = \{f : E \to E : f(u) = v\}$$

where $u, v \in E$. Thus, a basis for E^E consists of all sets of the form

$$\{f : E \to E : f(u_1) = v_1, \dots, f(u_n) = v_n\}$$

where $u_i, v_i \in E$.

To show that the topology obtained from closure points is the finite topology, let A be any subset of E^E. If $f \in E^E$ is in the closure of A under the finite topology, then any basis set that containing f also contains an element of A. It follows that for any finite set $S \subseteq E$, there is a $g \in A$ for which $f|_S = g|_S$, that is, $f|_S \in A|_S$. In other words, f is a closure point of A.

On the other hand, if f is a closure point of A, then f agrees with some element of A on any finite set and so any basis element containing f must intersect A, showing that f is in the closure of A. Thus we may content us to write the closure $\overline{A}$ with no ambiguous.

Theorem 1.2.4.4. *Let E/K be algebraic. Then the Galois group* $\mathrm{Gal}(E/K)$ *is closed in the finite topology on E^E. Moreover, a subgroup $H \subseteq$* $\mathrm{Gal}(E/K)$ *is closed in the Galois correspondence if and only if it is closed in the finite subspace topology on* $\mathrm{Gal}(E/K)$.

The subspace topology of the finite topology inherited by $\mathrm{Gal}(E/K)$ is called the Krull topology on $\mathrm{Gal}(E/K)$. We may phrase the previous theorem as follows: A subgroup of $\mathrm{Gal}(E/K)$ is **Galois-closed** if and only if it is **Krull-closed**.

We must remark that the previous theorem just says that the subgroups of $\mathrm{Gal}(E/K)$ are closed with the Krull topology, but not the converse. In fact, there are many other closed subsets of $\mathrm{Gal}(E/K)$, for example the union $H \cup K$ of two subgroups of $\mathrm{Gal}(E/K)$, which is not a subgroup in general.

Since $\mathrm{Gal}(E/K)$ is also a group, we may wonder whether the Krull topology makes $\mathrm{Gal}(E/K)$ a topological group. This is indeed the case, as we will show now.

Proposition 1.2.4.5. *Let E/K be algebraic. Then $G :=$* $\mathrm{Gal}(E/K)$ *is a topological group with the Krull topology, and a neighbourhood base of* 1 *in G is given by*

$$G_S = \{\sigma \in \mathrm{Gal}(E/K) : \sigma(s) = s \textit{ for all } s \in S\} \tag{1.2.4.1}$$

where $S \subseteq E$ is a finite set.

Proof. Let $m : G \times G \to G$ denote the composition on G and $i : G \to G$ denote the inverse operation on G. We will prove that, for any subset $A \times B \subseteq G \times G$,

$$m(\overline{A \times B}) \subseteq \overline{m(A \times B)}, \quad i(\overline{A}) \subseteq \overline{i(A)}. \tag{1.2.4.2}$$

To do this, first let $(\tau, \sigma) \in \overline{A \times B}$. Then for any finite subset $S \subseteq E$, there exists $\gamma \in A$ and $\nu \in B$ such that

$$\sigma|_S = \nu|_S, \quad \tau|_{\nu(S)} = \gamma|_{\nu(S)},$$

which implies

$$(\tau\circ\sigma)|_S = (\gamma\circ\nu)|_S$$

and therefore $m(\tau,\sigma) = \tau\circ\sigma \in \overline{m(A\times B)}$.

Next let $\tau \in \bar{A}$. Then for any finite subset $S \subseteq E$, there exists $\eta \in A$ such that $\tau|_{\tau^{-1}(S)} = \eta|_{\tau^{-1}(S)}$, and therefore

$$\tau^{-1}|_S = \eta^{-1}|_S.$$

This implies $i(\tau) \in \overline{i(A)}$, and finishes the proof of (1.2.4.2).

Finally, we consider the neighbourhoods of 1 in G. Let

$$U = \{\sigma \in \mathrm{Gal}(E/K) : \sigma(u_1) = v_1, \dots, \sigma(u_n) = v_n\}$$

be a basis of G. Then U contains 1 if and only if $u_i = v_i$ for all i, that is, U is the form of (1.2.4.1). □

Remark 1.2.4.6. Since a finite subextension F/K of E is determined by finitely many elements, a neighborhood basis of 1 in G is also given by

$$G_F : \{\sigma \in \mathrm{Gal}(E/K) : \sigma|_F = \mathrm{id}\}$$

where F is a subfield of E and F/K is a finite extension.

We now prove some topological properties for the group $\mathrm{Gal}(E/K)$.

Proposition 1.2.4.7. *The Galois group G of a Galois extension E/K is compact, Hausdorff, and totally disconnected.*

Proof. We first show that G is Hausdorff. If $\sigma \neq \tau$, then $\sigma^{-1}\tau \neq 1$, and so it moves some element of E, i.e., there exists an $\alpha \in E$ such that $\sigma(\alpha) \neq \tau(\alpha)$. For any S containing α, σG_S and τG_S are disjoint because their elements act differently on α. Hence they are disjoint open subsets of G containing σ and τ respectively.

We next show that G is compact. We first noted that, if S is a finite set stable under G, then G_S is a normal subgroup of G ($\sigma G_S \sigma^{-1} = G_{\sigma(S)} = G_S$), and it has finite index because

$$[G : G_S] = |S|$$

by the class formula. Since every finite set is contained in a stable finite set (each element of E is algebraic over K, and its orbit is the set of its conjugates, which is finite), the argument for the Hausdorffness of G shows that the map

$$G \to \prod_{S \text{ finite and stable}} G/G_S$$

is injective. When we endow G/G_S with the product topology, the induced topology on G is that for which the G_S form an open neighbourhood base of 1, i.e., it is the Krull topology. According to the Tychonoff theorem, $\prod G/G_S$ is compact, and so it remains to show that G is closed in the product. For each $S_1 \subseteq S_2$, there are continuous maps

$$\begin{tikzcd}
\prod G/G_S \arrow[r] \arrow[dr] & G/G_{S_2} \arrow[d] \\
 & G/G_{S_1}
\end{tikzcd}$$

where $G/G_{S_2} \to G/G_{S_1}$ is the quotient map. Let $E(S_1, S_2)$ be the closed subset of $\prod G/G_S$ on which the two maps agree. Then $E(S_1, S_2)$ is closed. Since the image of G is exactly the intersection $\bigcap_{S_1\subseteq S_2} E(S_1, S_2)$, it follows that G is closed in $\prod G/G_S$, and hence compact.

Finally, for each finite set S stable under G, G_S is a subgroup that is open and hence closed. Since $\bigcap G_S = \{1\}$, this shows that the connected component of G containing 1 is just $\{1\}$. By homogeneity, a similar statement is true for every element of G. □

Corollary 1.2.4.8. *Let G be the Galois group of a Galois extension E/K. Let $\mathcal{S}$ be the collection of finite subsets in E, then*

$$G \cong \varprojlim_{S\in\mathcal{S}} G/G_S.$$

Proof. This follows from the proof above, in view of the realization of the inverse limit. □

1.2.5 Normal subgroups and normal extensions

We now wish to discuss intermediate fields $K \subseteq E \subseteq L$ and their Galois groups $\mathrm{Gal}(E/K)$. We begin with a result concerning the conjugates of a Galois group.

Definition 1.2.5.1. Let $K \subseteq E, F \subseteq L$. If there is a $\sigma \in \mathrm{Gal}(L/K)$ for which $\sigma(E) = F$, then E and F are said to be **conjugate**.

Proposition 1.2.5.2 (Galois Group of Conjugations). *Let $K \subseteq E, F \subseteq L$ be extensions.*

(a) For any $\sigma \in \mathrm{Hom}_K(L, \overline{L})$, we have

$$\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/\sigma(E)).$$

(b) If E is normal over K, then for any $\sigma \in \mathrm{Hom}_K(L, \overline{L})$, we have

$$\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/E).$$

(c) If L is normal over K, then for any $\sigma \in \mathrm{Hom}_K(L, \overline{L})$, we have

$$\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E)).$$

(d) If L/K is Galois, then E and F are conjugate if and only if the Galois groups $\mathrm{Gal}(L/E)$ and $\mathrm{Gal}(L/F)$ are conjugate.

Proof. We first prove (a). Let $\tau \in \mathrm{Gal}(\sigma(L)/\sigma(E))$. Then $\sigma^{-1}\tau\sigma$ is an automorphism of L. Moreover, since τ fixes $\sigma(E)$, we have for $\alpha \in E$,

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

and so $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$. Hence

$$\mathrm{Gal}(\sigma(L)/\sigma(E)) \subseteq \sigma\mathrm{Gal}(L/E)\sigma^{-1}.$$

For the reverse inclusion, let $\mu = \sigma\tau\sigma^{-1}$, where $\tau \in \mathrm{Gal}(L/E)$. Then μ is an automorphism of $\sigma(L)$ and if $\alpha \in E$, then $\tau(\alpha) = \alpha$ and so

$$\mu(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha),$$

which shows that $\mu \in \mathrm{Gal}(\sigma(L)/\sigma(E))$.

Part (b) follows from (a), since if $K \lhd E$ then any $\sigma \in \mathrm{Hom}_K(E, \overline{E})$ satisfies $\sigma(E) = E$. Part (c) is similar. For (d), if $\sigma(E) = F$, then part (a) implies that

$$\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/F).$$

Conversely, if $\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/F)$ then (a) implies that $\mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/F)$. Since $\sigma(E)$ and F are both closed, taking fixed field gives $\sigma(E) = F$. □

Theorem 1.2.5.3 (Fundamental Theorem of Galois Theory III). *Let $K \subseteq E \subseteq L$ be extensions and $\Phi : \mathrm{Gal}(L/E) \to \mathrm{Hom}_K(E, L)$ be the restriction map $\sigma \mapsto \sigma|_E$.*

(a) If $K \lhd E$ then $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$ and Φ induces an embedding

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)} \hookrightarrow \mathrm{Gal}(E/K),$$

which is an homeomorphism if $K \lhd L$.

(b) If $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$, $K \lhd L$ and E is closed (that is, L/E is Galois), then $K \lhd E$ and Φ induces an homeomorphism

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

(c) If L/K is Galois, then $K \lhd E$ if and only $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$.

Proof. The map Φ is continuous since for any finite subset $S \subseteq E$ we have

$$\Phi^{-1}(\mathrm{Gal}(E/K)_S) = \{\sigma \in \mathrm{Gal}(L/K) : (\sigma|_E)(s) = s \text{ for all } s \in S\} = \mathrm{Gal}(L/K)_S$$

which is open in $\mathrm{Gal}(L/K)$. Note that Φ is then closed, beging a continuous map from a compact space to a Hausdorff space.

If $K \lhd E$, then the restriction map Φ has image in $\mathrm{Hom}_K(E,E) = \mathrm{Gal}(E/K)$. Now, by Proposition 1.2.5.2, since E/K is normal, for any $\sigma \in \mathrm{Gal}(L/K)$ we have

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/\sigma(E)) = \mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/E), \tag{1.2.5.1}$$

and therefore $\mathrm{Gal}(L/E)$ is normal in $\mathrm{Gal}(L/K)$. Since $\ker \Phi = \mathrm{Gal}(L/E)$, it induced an embedding

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

If L is also normal over K, then Φ is surjective, since any $\sigma \in \mathrm{Gal}(E/K)$ can be extended to an embedding of L into $\overline{L}$ over L, which must be an element of $\mathrm{Gal}(L/K)$. Hence the embedding is an isomorphism.

Conversely, if $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(L/K)$ and L/E is Galois, then taking fixed fields in (1.2.5.1) gives $\mathrm{cl}(\sigma(E)) = \mathrm{cl}(E)$. Thus, if E is closed, then $\sigma(E) \subseteq E$ for all $\sigma \in \mathrm{Gal}(L/K)$. If in addition $K \lhd L$, then $\sigma(E) \subseteq E$ for all $\sigma \in \mathrm{Hom}_K(L, \overline{L})$, that is, E is normal over K. □

Remark 1.2.5.4. There is a parallel between Galois theory and the theory of **covering spaces** in topology. In this analogy, Galois extensions correspond to **regular covers**; the Galois group of an extension corresponds to the group of **deck transformations**; and Theorem 1.2.5.3 corresponds to the fact that the quotient of a regular cover by a normal subgroup of the group of deck transformations is again a regular cover.

More general (connected) covers correspond to more general algebraic extensions. A space is **simply connected** if and only if it admits no nontrivial connected covers, so this notion corresponds in field theory to the condition that a field K admits no nontrivial algebraic extensions, that is, that K is **algebraically closed**. Viewing the fundamental group of a space as the group of deck transformations of its fundamental cover suggests that we should think of the Galois group of the algebraic closure $K \subseteq \overline{K}$ as the fundamental group of a field K.

In algebraic geometry this analogy is carried out to its natural consequences. A covering map of algebraic varieties $X \to Y$ determines a field extension $K(Y) \subseteq K(X)$, where $K(X)$, $K(Y)$ are the fields of rational functions (in the affine case, these are just the fields of fractions of the corresponding coordinate rings). One can then use Galois theory to transfer to the algebra-geometric environment notions such as the fundamental group, without appealing to topological notions (such as continuous maps from S^1), which would be problematic in e.g., positive characteristic.

Example 1.2.5.5 (Galois group of $X^4 - 2$). The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, \mathbf{i})$ is a spliting field of $X^4 - 2$, and has degree 8, as we have seen in Example 1.1.5.5. The roots of this polynomial are $\alpha = \sqrt[4]{2}$, $-\alpha$, $\mathbf{i}\alpha$ and $-\mathbf{i}\alpha$, and so any member of the Galois group G is a permutation of these roots. One way to help find the Galois group is to look for an intermediate field N that is normal, because the elements of $\mathrm{Gal}(N/\mathbb{Q})$ are precisely the restrictions of the members of G. Now since any extension of degree 2 is normal, we have $\mathbb{Q} \lhd \mathbb{Q}(\mathbf{i})$; the elements of $\mathrm{Gal}(\mathbb{Q}(\mathbf{i})/\mathbb{Q})$ are the identity 1 and the map $\tau : \mathbf{i} \to -\mathbf{i}$. Since $[\mathbb{Q}(\alpha, \mathbf{i}) : \mathbb{Q}(\mathbf{i})] = 4$, we have $\min(\alpha, \mathbb{Q}(\mathbf{i})) = X^4 - 2$ and so each of the automorphisms 1 and τ can be extended to an element of G by sending α to any of the roots of $X^4 - 2$. This gives all elements of G:

The extensions of 1	The extensions of τ
$1 : \mathbf{i} \mapsto \mathbf{i}, \alpha \mapsto \alpha$	$\tau : \mathbf{i} \mapsto -\mathbf{i}, \alpha \mapsto \alpha$
$\sigma : \mathbf{i} \mapsto \mathbf{i}, \alpha \mapsto \mathbf{i}\alpha$	$\tau\sigma : \mathbf{i} \mapsto -\mathbf{i}, \alpha \mapsto -\mathbf{i}\alpha$
$\sigma^2 : \mathbf{i} \mapsto \mathbf{i}, \alpha \mapsto -\alpha$	$\tau\sigma^2 : \mathbf{i} \mapsto -\mathbf{i}, \alpha \mapsto -\alpha$
$\sigma^3 : \mathbf{i} \mapsto \mathbf{i}, \alpha \mapsto -\mathbf{i}\alpha$	$\tau\sigma^3 : \mathbf{i} \mapsto -\mathbf{i}, \alpha \mapsto \mathbf{i}\alpha$

Note that G can not be abelian, because otherwise any subgroup of G is normal, and thus any intermediate field of $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \mathbf{i})$ is normal. However, the extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is not normal. Since

$|G| = 8$, this then implies $G = Q_8$ or $G = D_4$. Note that G has a normal subgroup $\langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma^3\}$ of order 4, and we have $\tau\sigma\tau = \sigma^3$. These together imply that $G \cong D_4$.

Now we want to determine all subgroups of G. All nontrivial subgroups of G have order 2 or 4. The subgroups of order 2 correspond to the elements of order 2:

$$\{1, \sigma^2\}, \quad \{1, \tau\}, \quad \{1, \tau\sigma\}, \quad \{1, \tau\sigma^2\}, \quad \{1, \tau\sigma^3\}.$$

The subgroups of order 4 are

$$\{1, \sigma, \sigma^2, \sigma^3\}, \quad \{1, \tau, \tau\sigma^2, \sigma^2\}, \quad \{1, \tau\sigma, \tau\sigma^3, \sigma^2\}.$$

Therefore the lattice of subgroups of G is

$$\begin{tikzcd}
 & & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & {\{1,\tau,\tau\sigma^2,\sigma^2\}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & {\{1,\sigma,\sigma^2,\sigma^3\}} \arrow[d, dash] & {\{1,\tau\sigma,\tau\sigma^3,\sigma^2\}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
{\{1,\tau\}} \arrow[drr, dash] & {\{1,\tau\sigma^2\}} \arrow[dr, dash] & {\{1,\sigma^2\}} \arrow[d, dash] & {\{1,\tau\sigma\}} \arrow[dl, dash] & {\{1,\tau\sigma^3\}} \arrow[dll, dash] \\
 & & \{1\} & &
\end{tikzcd}$$

Of course, the lattice of intermediate (fixed) fields is a reflection of this. To compute fixed fields, we use the fact that $\{1, \mathbf{i}\}$ is a basis for $\mathbb{Q}(\mathbf{i})$ over $\mathbb{Q}$ and $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis for $\mathbb{Q}(\mathbf{i}, \alpha)$ over $\mathbb{Q}(i)$ and so the products form a basis for $\mathbb{Q}(r, i)$ over $\mathbb{Q}$. Hence, each $\xi \in E = \mathbb{Q}(\alpha, \mathbf{i})$ has the form

$$\xi = a + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + d_1\mathbf{i} + d_2\mathbf{i}\alpha + d_3\mathbf{i}\alpha^2 + d_4\mathbf{i}\alpha^3.$$

Using this, the fixed fields are easy to compute:

$E^{\{1,\tau\}} = \mathbb{Q}(\alpha)$	$E^{\{1,\tau,\tau\sigma^2,\sigma^2\}} = \mathbb{Q}(\alpha^2)$
$E^{\{1,\tau\sigma^2\}} = \mathbb{Q}(\mathbf{i}\alpha)$	$E^{\{1,\sigma,\sigma^2,\sigma^3\}} = \mathbb{Q}(\mathbf{i})$
$E^{\{1,\sigma^2\}} = \mathbb{Q}(\alpha^2, \mathbf{i})$	$E^{\{1,\tau\sigma,\tau\sigma^3,\sigma^2\}} = \mathbb{Q}(\mathbf{i}\alpha^2)$
$E^{\{1,\tau\sigma\}} = \mathbb{Q}((1-\mathbf{i})\alpha)$	
$E^{\{1,\tau\sigma^3\}} = \mathbb{Q}((1+\mathbf{i})\alpha)$	

We collect these results into the following diagram

$$\begin{tikzcd}
 & & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \mathbb{Q}(\alpha^2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\mathbf{i}) \arrow[d, dash] & \mathbb{Q}(\mathbf{i}\alpha^2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[drr, dash] & \mathbb{Q}(\mathbf{i}\alpha) \arrow[dr, dash] & \mathbb{Q}(\alpha^2, \mathbf{i}) \arrow[d, dash] & \mathbb{Q}((1+\mathbf{i})\alpha) \arrow[dl, dash] & \mathbb{Q}((1-\mathbf{i})\alpha) \arrow[dll, dash] \\
 & & \mathbb{Q}(\alpha, \mathbf{i}) & &
\end{tikzcd}$$

Note that in the diagram, $\mathbb{Q}(\alpha^2, \mathbf{i}) = \mathbb{Q}(\sqrt{2}, \mathbf{i}) = \mathbb{Q}(\sqrt{2} + \mathbf{i})$ is the spliting field of $X^4 - X^2 - 2$ over $\mathbb{Q}$. This justify the fact that $\mathrm{Gal}(\mathbb{Q}(\alpha, \mathbf{i})/\mathbb{Q}(\alpha^2, i)) = \langle\sigma^2\rangle$ is a normal subgroup.

1.2.6 Galois groups of lifting and composites

We now examine the behavior of Galois groups under lifting and under composites. As usual, we assume that all composites mentioned are defined.

Let $K \subseteq E$ be normal and let $K \subseteq F$. Any $\sigma \in \mathrm{Gal}(EF/F)$, the Galois group of the lifting, is uniquely determined by what it does to E (since it fixes F) and so the restriction map $\sigma \mapsto \sigma|_E$ is an injection.

Since E/K is normal, it follows that $\sigma|_E \in \mathrm{Gal}(E/K)$. But $\sigma|_E$ may fix more than K: It also fixes every element of E that is fixed by σ, that is,

$$\sigma|_E \in \mathrm{Gal}(E/E \cap EF^{\mathrm{Gal}(EF/F)}) = \mathrm{Gal}(E/E \cap \mathrm{cl}(F)).$$

Note that the restriction map is a homomorphism, and hence an embedding of $\mathrm{Gal}(EF/F)$ into $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$. We will show that this embedding is actually an isomorphism and

$$\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap \mathrm{cl}(F)).$$

Proposition 1.2.6.1. *Let $K \subseteq E$ be normal and let $K \subseteq F$. The restriction map*

$$\Phi : \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$$

defined by $\Phi(\sigma) = \sigma|_E$ is a homeomorphism.

Proof. We first prove that the map is continuous. For any finite set S of elements of E, we have

$$\Phi^{-1}(\mathrm{Gal}(E/E \cap \mathrm{cl}(F))_S) = \mathrm{Gal}(EF/F)_S,$$

which is open. Therefore Φ is continuous by homogeneity.

We next show that the map is an isomorphism of groups (neglecting the topology). Since Φ is injective, we only need to show it is also surjective. To avoid confusion, let us use the notation Inv_E for the fixed field with respect to the Galois correspondence on E/K, and Inv_{EF} for the fixed field with respect to the Galois correspondence on EF/F. Let $H := \mathrm{im}\,\Phi$, then we observe that

$$\begin{aligned} \mathrm{Inv}_E(H) &= \{\alpha \in E : \tau(\alpha) = \alpha \text{ for all } \tau \in \mathrm{im}\,\Phi\} \\ &= \{\alpha \in E : (\sigma|_E)(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(EF/F)\} \\ &= \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(EF/F)\} \\ &= E \cap \mathrm{Inv}_{EF}(\mathrm{Gal}(EF/F)) = E \cap \mathrm{cl}(F), \end{aligned}$$

Therefore $\overline{H} = \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$, which implies H is dense in $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$. But H is closed, being a continuous image of a compact space in a Hausdorff space, so $H = \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$.

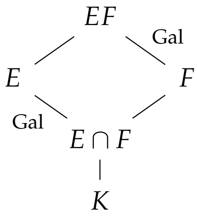
Finally, since Φ is a continuous bijection, it is a homeomorphism, since $\mathrm{Gal}(EF/F)$ is a compact space and $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$ is Hausdorff. □

For a Galois extension E/K, the previous theorem simplifies a bit.

Proposition 1.2.6.2 (The Galois group of a lifting). *Suppose $K \subseteq E$ is a Galois extension and $K \subseteq F$ is an arbitrary extension. Then the lifting $F \subseteq EF$ is a Galois extension. Moreover, the restriction map* $\mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/E \cap F)$ *defined by $\sigma \mapsto \sigma|_E$ is an isomorphism. Also,*

(a) $E \cap F = K$ *implies* $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/K)$.

(b) *If $K \subseteq E$ is finite, then* $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/K)$ *implies $E \cap F = K$.*



Proof. If E/K is Galois, then EF/F is Galois, implying that F is closed. Therefore the statement in Proposition 1.2.6.1 simplifies to (a). As for (b), since all is finite, if $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/E \cap F)$ then taking fixed fields gives the claim. □

Corollary 1.2.6.3. *Suppose that $K \subseteq E_i$ is a finite Galois extension for $i = 1, \dots, n-1$ and $K \subseteq E_n$ is a finite extension. then*

$$[E_1 \cdots E_n : K] = \prod_{i=1}^{n} [E_i : E_i \cap (E_{i+1} \cdots E_n)] = \frac{\prod_{i=1}^{n} [E_i : K]}{\prod_{i=1}^{n} [E_i \cap (E_{i+1} \cdots E_n) : K]},$$

where $E_n \cap (E_{n+1}) := K$.

Proof. The case $n = 2$ comes from Proposition 1.2.6.2, and the general case follows by induction. □

Corollary 1.2.6.4. *Let E and F be field extensions of K and let L be an algebraically closed field containing K. Moreover let E/K be Galois. If $\rho : E \to L$ and $\sigma : F \to L$ are K-homomorphisms such that $\rho|_{E\cap F} = \sigma|_{E\cap F}$, then there exists an K-homomorphism τ such that $\tau|_E = \rho$ and $\tau|_F = \sigma$.*

Proof. By Theorem 1.1.4.4, σ can be extended to a K-homomorphism $\widetilde{\sigma} : EF \to L$. As $\widetilde{\sigma}|_{E\cap F} = \rho|_{E\cap F}$, we have

$$\rho^{-1} \circ (\widetilde{\sigma}|_E) =: \epsilon \in \mathrm{Gal}(E/E \cap F).$$

According to Proposition 1.2.6.2, there exists a unique $\eta \in \mathrm{Gal}(EF/F)$ such that $\epsilon = \eta|_E$. Define $\tau = \widetilde{\sigma} \circ \eta^{-1}$, we see that $\tau : EF \to L$ is a K-homomorphism such that $\tau|_E = \rho$ and $\tau|_F = \sigma$. □

Example 1.2.6.5. We have studied cyclotomic fields $\mathbb{Q}(\zeta_n)$ as extensions of $\mathbb{Q}$; $\mathbb{Q}(\zeta_n)$ is the splitting field of $X^n - 1$, so these extensions are Galois; we have proved (Proposition 1.3.6.6) that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to the group of units in $\mathbb{Z}/n\mathbb{Z}$.

Now let K be any field of characteristic zero. The splitting field of $X^n - 1$ over K is the composite $K(\zeta_n)$ of K and $\mathbb{Q}(\zeta_n)$. By Proposition 1.2.6.2 the extension $K \subseteq K(\zeta_n)$ is Galois, and $\mathrm{Aut}_K(K(\zeta_n))$ is isomorphic to a subgroup of the group of units of $\mathbb{Z}/n\mathbb{Z}$.

Example 1.2.6.6. We return to Example 1.2.3.4, where we consider the extension $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ and found a dense proper subgroup in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$: the subgroup H generated by the Frobenius homomorphism σ. We now use this to determine the structure of G.

Recall that $\widehat{\mathbb{Z}}$ is the limit ring of the homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$. It is isomorphic to the direct product of p-adic intergers, where p is a positive prime. Let $\alpha \in \widehat{\mathbb{Z}}$ be represented by the sequence (a_i). Since $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if $m \mid n$, it is easy to see how to define the automorphism $\sigma^\alpha \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$: Just let σ^α be $(\sigma|_{\mathbb{F}_{p^n}})^{a_n}$ on $\mathbb{F}_{p^n}$. If $m \mid n$, since $\sigma|_{\mathbb{F}_{p^m}}$ has order m and $a_m \equiv a_n \bmod n$, we see that

$$(\sigma|_{\mathbb{F}_{p^n}})^{a_n}|_{\mathbb{F}_{p^m}} = (\sigma|_{\mathbb{F}_{p^m}})^{a_n} = (\sigma|_{\mathbb{F}_{p^m}})^{a_m}$$

so this is well-defined. The map $\sigma \mapsto \sigma^\alpha$ gives an isomorphism from $\widehat{\mathbb{Z}}$ to $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

We now turn to the Galois group of a composite. Let $K \lhd E$ and $K \lhd F$. Then any $\sigma \in \mathrm{Gal}(EF/K)$ is completely determined by its action on E and F, that is, by its restrictions $\sigma|_E$ and $\sigma|_F$, or put another way, by the element

$$(\sigma|_E, \sigma|_F) \in \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

Indeed, the map $\Phi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ is an embedding of groups. Moreover, as we will see, in the finite case, if the fields enjoy a form of independence ($E \cap F = K$), then the embedding is an isomorphism.

Proposition 1.2.6.7 (The Galois group of a composite).

(a) *Let $\mathcal{E} = \{E_i : i \in I\}$ be a family of fields, with $K \lhd E_i$ for all $i \in I$. Let $G = \prod \mathrm{Gal}(E_i/K)$ be the direct product of the Galois groups $\mathrm{Gal}(E_i/K)$ and let π_i be projection onto the i-th coordinate. Then the map*

$$\Phi : \mathrm{Gal}(\bigvee E_i/K) \to \prod \mathrm{Gal}(E_i/K), \quad \sigma \mapsto (\sigma|_{E_i})$$

is an embedding of groups, and Φ is an isomorphism if

$$E_j \cap \Big(\bigvee_{i\neq j} E_i\Big) = K$$

for all $j \in I$.

(b) *If $\mathcal{E} = \{E_1, \dots, E_n\}$ is a finite family of finite Galois extensions, then the map Φ is an isomorphism if and only if*

$$E_i \cap (E_{i+1} \dots E_n) = K$$

for all $i = 1, \dots, n$.

Proof. Since $K \lhd E_i$, by Theorem 1.2.5.3, each individual restriction map $\Phi_j : \sigma \mapsto \sigma|_{E_j}$ is a surjective homomorphism from $\mathrm{Gal}(\bigvee E_i/K)$ onto $\mathrm{Gal}(E_j/K)$, with kernel $\mathrm{Gal}(\bigvee E_i/E_j)$. Hence, Φ is a homomorphism from $\mathrm{Gal}(\bigvee E_i/K) \to \prod \mathrm{Gal}(E_i/K)$. As to the kernel of Φ, if $\Phi(\sigma) = 1$, then

$$\sigma|_{E_j} = \Phi_j(\sigma) = \pi_j(\Phi(\sigma)) = 1$$

and so $\sigma = 1$ on each E_j, which implies that $\sigma = 1$. Hence, $\ker \Phi = \{1\}$ and Φ is an embedding. If moreover $E_j \cap (\bigvee_{i \neq j} E_j) = K$, then by Proposition 1.2.6.2 we have

$$\mathrm{Gal}(E_j/K) \cong \mathrm{Gal}(\bigvee E_i / \bigvee_{i \neq j} E_i),$$

where the isomorphism is given by restriction. This implies the direct summand $\mathrm{Gal}(E_j/K)$ is contained in $\operatorname{im} \Phi$. Since this holds for all j, it follows that Φ is surjective, and hence an isomorphism.

When $\mathcal{E}$ is a finite family of finite Galois extensions, all Galois groups are finite and all subgroups and intermediate fields are closed. Since Φ is injective, we have

$$|\operatorname{im} \Phi| = |\mathrm{Gal}(E_1 \cdots E_n/K)| = [E_1 \cdots E_n : K] = \frac{\prod_{i=1}^n [E_i : K]}{\prod_{i=1}^n [E_i \cap (E_{i+1} \cdots E_n) : K]}$$

and also

$$\left| \prod \mathrm{Gal}(E_i/K) \right| = \prod_{i=1}^n |\mathrm{Gal}(E_i/K)| = \prod_{i=1}^n [E_i : K].$$

Therefore Φ is surjective if and only if $E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \ldots, n$. □

If $K \subseteq E$ is a finite Galois extension whose Galois group is a direct product $G_1 \times \cdots \times G_n$, then we may wish to find intermediate fields E_i whose Galois groups (over K) are isomorphic to the individual factors G_i in the direct product.

Corollary 1.2.6.8. *Suppose that $K \subseteq E$ is a Galois extension with Galois group of the form*

$$\mathrm{Gal}(E/K) = G_1 \times \cdots \times G_n.$$

If

$$H_i = G_1 \times \cdots \times \{1\} \times \cdots \times G_n$$

where $\{1\}$ is in the i-th coordinate and if $E_i = E^{H_i}$, then

(a) $K \subseteq E_i$ is Galois, with Galois group $\mathrm{Gal}(E/E_i) \cong G_i$.

(b) $E = E_1 \vee \cdots \vee E_n$.

(c) $E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \ldots, n$.

Proof. Since $G_i \lhd G$, $K \subseteq E$ is normal, and $E_i = E^{H_i}$ is closed, it follows from Theorem 1.2.5.3(b) that $K \lhd E_i$ and

$$\mathrm{Gal}(E_i/K) \cong \frac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/E_i)} = \frac{G}{H_i} \cong G_i.$$

In addition, $E_1 \cdots E_n/K$ is Galois and since

$$\mathrm{Gal}(E/\bigvee E_i) = \bigcap \mathrm{Gal}(E/E_i) = \bigcap H_i = \{1\} = \mathrm{Gal}(E/E)$$

taking fixed fields gives $E = \bigvee E_i$. Hence,

$$\mathrm{Gal}(\bigvee E_i/K) = \mathrm{Gal}(E/K) = \prod G_i \cong \prod \mathrm{Gal}(E_i/K)$$

and Proposition 1.2.6.7 implies that $E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \ldots, n$. □

1.2.7 Exercise

Exercise 1.2.1. Prove that quadratic extensions are Galois.

Proof. Let $K \subseteq E$ be a quadratic extension, and $\alpha \in K$. Let $f(X)$ be the minimal polynomial of α, then $\deg f > 1$, since $\alpha \notin K$. But $\deg f \leq [E : K] = 2$, this shows that $\deg f = 2$, hence $E = K(\alpha)$. Now if $f(X)$ is not separable, then $f(X) = (X - \alpha)^2 = X^2 - 2a + a^2$. Which means $a \in K$, a contradiction. □

Exercise 1.2.2.

- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois, with cyclic Galois group.
- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3+\sqrt{5}})$ is Galois and its Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is not Galois, and compute its Galois closure $\mathbb{Q} \subseteq K$. Prove that $\mathrm{Aut}_{\mathbb{Q}}(F) \cong D_4$.

Proof.

- The minimal polynomial of $\zeta := \sqrt{3+\sqrt{5}}$ is $X^4 - 6X^2 + 4$. The roots of it are
$$\pm\sqrt{3 \pm \sqrt{5}}$$
Note that
$$\sqrt{3+\sqrt{5}}\sqrt{3-\sqrt{5}} = \sqrt{9-5} = 2$$
so the extension is Galois.
- The minimal polynomial of $\zeta := \sqrt{1+\sqrt{2}}$ is $X^4 - 2X^2 - 1$. The roots of it are
$$\pm\sqrt{1 \pm \sqrt{2}}$$
We also find that
$$\sqrt{1+\sqrt{2}}\sqrt{1-\sqrt{2}} = \sqrt{1-2} = i$$
so the extension is not Galois.

□

Exercise 1.2.3. Let E/K be a Galois extension of degree n, and let E be an intermediate field. Assume that $[E : K]$ is the smallest prime dividing n. Prove $K \subseteq E$ is Galois.

Proof. This comes from the corresponding result in group theory. □

Exercise 1.2.4. Let E/K be a Galois extension of degree 75. Prove that there exists an intermediate field F, with $K \subsetneq F \subsetneq E$, such that the extension $K \subseteq F$ is Galois.

Proof. $75 = 3 \cdot 5^2$. So a group of order 75 has a unique 5-Sylow sugroup, which is therefore normal. □

Exercise 1.2.5. Find two algebraic extensions $K \subseteq E$, $K \subseteq F$ and embeddings $K \subseteq \overline{K}$, $\sigma_1 : F \subseteq \overline{K}$, $\sigma_2 : F \subseteq \overline{K}$ extending $K \subseteq \overline{K}$ such that the composites $E\sigma_1(F)$, $E\sigma_2(F)$ are not isomorphic.

Prove that no such example exists if E and F are Galois over K.

Proof. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$. Embedding $\mathbb{Q}(\sqrt[4]{2})$ as $F_1 = \mathbb{Q}(\sqrt[4]{2})$ and $F_2 = \mathbb{Q}(\sqrt[4]{2}i)$. Then
$$\mathbb{Q}(\sqrt{2})F_1 = \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{2})F_2 = \mathbb{Q}(\sqrt{2}i)$$
they are not isomorphic. □

Exercise 1.2.6. Let E/K be a Galois extension, and let $\alpha \in K$. Prove that
$$N_{E/K}(\alpha) = \prod_{\sigma \in \mathrm{Aut}_K(F)} \sigma(\alpha), \quad \mathrm{tr}_{E/K}(\alpha) = \sum_{\sigma \in \mathrm{Aut}_K(F)} \sigma(\alpha).$$

Exercise 1.2.7. Use Hilbert's theorem 90 to find all rational roots a, b of the equation $a^2 + b^2 d = 1$, where d is a positive integer that is not a square.

Proof. Consider the extension $D = \mathbb{Q}(\sqrt{d}i)$, then by Exercise 1.2.6, we know that

$$N_{D/\mathbb{Q}}(a + b\sqrt{d}) = (a + \sqrt{d}i)(a - \sqrt{d}i) = a^2 + db^2$$

Then

$$a^2 + db^2 = 1 \Leftrightarrow N_{D/\mathbb{Q}}(a + b\sqrt{d}i) = 1 \Leftrightarrow a + b\sqrt{d} = \beta/\varphi(\beta)$$

where $\varphi(a + b\sqrt{d}i) = a - b\sqrt{d}i$. So we conclude that

$$a^2 + db^2 = 1 \Leftrightarrow a + b\sqrt{d} = \frac{x + y\sqrt{d}i}{x - y\sqrt{d}i} = \frac{x^2 - dy^2}{x^2 + dy^2} + \frac{2xy\sqrt{d}i}{x^2 + dy^2}$$

□

1.3 Applications of Galois theory

In this section, we pass from the highly theoretical material of the previous section to the somewhat more concrete, where we apply the results to some special Galois correspondences.

1.3.1 The Galois group of a polynomial

The **Galois group of a polynomial** $f(X) \in K[X]$, denoted by $\mathrm{Gal}_K(f(X))$, is defined to be the Galois group of a splitting field E of $f(X)$ over K. If

$$f(X) = p_1(X)^{e_1} p_2^{e_2}(X) \cdots p_s(X)^{e_s}$$

is a factorization of $f(X)$ into powers of distinct irreducible polynomials over K, then E is also a splitting field for the polynomial $g(X) = p_1(X) \cdots p_s(X)$. Moreover, the extension E/K is separable (and hence Galois) if and only if each $p_i(X)$ is a separable polynomial. To see this, let E_i be the splitting field for $p_i(X)$ satisfying $K \subseteq E_i \subseteq E$. Then if $K \subseteq E$ is separable, so is the lower step $K \subseteq E_i$ and therefore so is $p_i(X)$. Conversely, if each factor $p_i(X)$ is separable over K, then E is separably generated over K and so $K \subseteq E$ is separable.

Let $\{\alpha_1, \dots, \alpha_n\}$ be the set of roots of $f(X)$, then $\mathrm{Gal}_K(f)$ consists exactly of the permutations σ of $\{\alpha_1, \dots, \alpha_n\}$ such that, for $P \in K[X_1, \dots, X_n]$,

$$P(\alpha_1, \dots, \alpha_n) = 0 \Leftrightarrow P(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = 0. \tag{1.3.1.1}$$

To see this, note that the kernel of the map

$$K[X_1, \dots, X_n] \to E_f, \quad X_i \mapsto \alpha_i \tag{1.3.1.2}$$

consists of the polynomials $P(X_1, \dots, X_n)$ such that $P(\alpha_1, \dots, \alpha_n) = 0$. Let σ be a permutation of the α_i's satisfying the condition (1.3.1.1). Then the map

$$K[X_1, \dots, X_n] \to E_f, \quad X_i \mapsto \sigma(\alpha_i)$$

factors through the map (1.3.1.2), and defines an K-isomorphism $E_f \to E_f$, i.e., an element of the Galois group. This shows that every permutation satisfying the condition (1.3.1.1) extends uniquely to an element of $\mathrm{Gal}_K(f)$, and it is obvious that every element of $\mathrm{Gal}_K(f)$ arises in this way.

1.3.1.1 Symmetric polynomials In this part, we discuss the relationship between the roots of a polynomial and its coefficients. It is well known that the constant coefficient of a polynomial $f(X)$ is the product of its roots and the linear term of $f(X)$ is the negative of the sum of the roots. We wish to expand considerably on these statements.

We first introduce the general polynomial and elementary symmetric functions. If K is a field and $t_1, \dots, t_n$ are algebraically independent over K, the polynomial

$$g(X) = \prod_{i=1}^{n}(X - t_i)$$

is referred to as a general polynomial over K of degree n. Since the roots $t_1, \ldots, t_n$ of the general polynomial $g(X)$ are algebraically independent, this polynomial is, in some sense, the most general polynomial of degree n. It can be shown by induction that the general polynomial can be written in the form

$$g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$$

where the coefficients are given by

$$s_1 = \sum_i t_i, \quad s_2 = \sum_{i<j} t_i t_j, \quad \ldots \quad , s_n = \prod_{i=1}^{n} t_i$$

and are called the **elementary symmetric polynomials** in the variables t_i.

As an example of what can be gleaned from the general polynomial, we deduce immediately the following lemma.

Lemma 1.3.1.1. *Let $f(X) \in K[X]$. The coefficients of $f(X)$ are, except for sign, the elementary symmetric polynomials of the roots of $f(X)$. In particular, if*

$$f(X) = X^n - s_1 X^{n-1} + \cdots + (-1) s_n$$

has roots $r_1, \ldots, r_n$ in a splitting field, then

$$s_k = \sum_{i_1 < \cdots < i_k} r_{i_1} \cdots r_{i_k}.$$

Proposition 1.3.1.2. *The elementary symmetric polynomials $s_1, \ldots, s_n$ are algebraically independent over K.*

Proof. Since $K \subseteq K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$, where the upper step is algebraic (each t_i is a root of the general polynomial, which has coefficients in $K(s_1, \ldots, s_n)$), Theorem 1.4.1.9 implies that $S = \{s_1, \ldots, s_n\}$ contains a transcendental basis for $K(t_1, \ldots, t_n)$ over K. But $\{t_1, \ldots, t_n\}$ is a transcendental basis and so $\operatorname{tr.deg}(K(t_1, \ldots, t_n)/K) = n$. Hence, S is a transcendental basis. □

Let us compute the Galois group G of $K(t_1, \ldots, t_n)$ over $K(s_1, \ldots, s_n)$. Since $K(t_1, \ldots, t_n)$ is a splitting field for $g(X)$ over $K(s_1, \ldots, s_n)$, and since has $g(X)$ no multiple roots, the extension

$$K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$$

is finite and Galois and so

$$|G| = [K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)] \leq n!$$

We claim that G is isomorphic to the symmetric group $\mathfrak{S}_n$.

Proposition 1.3.1.3. *Let $t_1, \ldots, t_n$ be algebraically independent over K and let $s_1, \ldots, s_n$ be the elementary symmetric polynomials in $t_1, \ldots, t_n$.*

(a) The extension $K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$ is Galois of degree $n!$, with Galois group G isomorphic to the symmetric group $\mathfrak{S}_n$.

(b) $\operatorname{Inv}(G) = K(s_1, \ldots, s_n)$, that is, any rational function in $t_1, \ldots, t_n$ that is fixed by the maps in G is a rational function in $s_1, \ldots, s_n$.

(c) The general polynomial $g(X)$ is irreducible over $K[s_1, \ldots, s_n]$.

Proof. Let $\sigma \in \mathfrak{S}_n$, we defined a map

$$\sigma^* : K(t_1, \ldots, t_n) \to K(t_1, \ldots, t_n), \quad f(t_1, \ldots, t_n) \mapsto f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).$$

Since the t_i's are algebraically independent over K, this is a well-defined automorphism of $K(t_1, \ldots, t_n)$ over K, which fixes the elementary symmetric polynomials s_i's. Thus, σ^* is an automorphism of $K(t_1, \ldots, t_n)$ over $K(s_1, \ldots, s_n)$, that is, $\sigma^* \in G$. Moreover, each σ^* is distinct, since if $\sigma^* = \tau^*$, then $t_{\sigma(i)} = t_{\tau(i)}$ for all i and so $\sigma = \tau$. It follows that G is isomorphic to $\mathfrak{S}_n$ and

$$[K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)] = n!.$$

Since the extension is Galois, the field $K(s_1, \ldots, s_n)$ is closed, so $\operatorname{Inv}(G) = K(s_1, \ldots, s_n)$. To prove (c), observe that if $g(X)$ were equal to $p(X)q(X)$ where $\deg p = d > 0$ and $\deg q = e > 0$, then the Galois group of $g(X)$ would have size at most $d!e! < (d+e)! = n!$. Hence $g(X)$ is irreducible. □

Now we are ready to define symmetric polynomials (and rational functions).

Definition 1.3.1.4. A rational function $f(t_1, \dots, t_n) \in K(t_1, \dots, t_n)$ is **symmetric** in $t_1, \dots, t_n$ if

$$f(t_{\sigma(1)}, \dots, t_{\sigma(n)}) = f(t_1, \dots, t_n)$$

for all permutations $\sigma \in \mathfrak{S}_n$, that is, if $f \in \operatorname{Inv}(G) = K(s_1, \dots, s_n)$, where G is the Galois group of the extension $K(s_1, \dots, s_n) \subseteq K(t_1, \dots, t_n)$.

A famous theorem of Isaac Newton describes the symmetric polynomials.

Theorem 1.3.1.5 (Newton's Theorem). *Let $t_1, \dots, t_n$ be algebraically independent over K and let $s_1, \dots, s_n$ be the elementary symmetric polynomials in $t_1, \dots, t_n$.*

(a) A polynomial $f(X) \in K[t_1, \dots, t_n]$ is symmetric in $t_1, \dots, t_n$ if and only if it is a polynomial in $s_1, \dots, s_n$, that is, if and only if

$$f(t_1, \dots, t_n) = p(s_1, \dots, s_n)$$

for some polynomial $p(t_1, \dots, t_n)$ over K. Moreover, if $f(t_1, \dots, t_n)$ has integer coefficients, then so does $p(s_1, \dots, s_n)$.

(b) Let $f(X) \in K[X]$. Then the set of symmetric polynomials over K in the roots of $f(X)$ is equal to the set of polynomials over K in the coefficients of $f(X)$. In particular, any symmetric polynomial over K in the roots of $f(X)$ is an element of K.

(c) Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. Then the set of symmetric polynomials over $\mathbb{Z}$ in the roots of $f(X)$ is equal to the set of polynomials over $\mathbb{Z}$ in the coefficients of $f(X)$. In particular, any symmetric polynomial over $\mathbb{Z}$ in the roots of $f(X)$ is an integer.

Proof. Statements (b) and (c) follow from statement (a) and Lemma 1.3.1.1. If $f(t_1, \dots, t_n)$ has the form $p(s_1, \dots, s_n)$, then it is clearly symmetric. For the converse, the proof consists of a procedure that can be used to construct the polynomial $p(t_1, \dots, t_n)$. Unfortunately, while the procedure is quite straightforward, it is recursive in nature and not at all practical.

We use induction on n. The theorem is true for $n = 1$, since $s_1 = t_1$. Assume that the theorem is true for any number of variables less than n and let $f(t_1, \dots, t_n)$ be symmetric. By collecting powers of t_n, we can write

$$f(t_1, \dots, t_n) = a_0 + a_1 t_n + \cdots + a_d t_n^d.$$

where each a_i is a polynomial in $t_1, \dots, t_{n-1}$. Since f is symmetric in $t_1, \dots, t_{n-1}$ and $t_1, \dots, t_n$ are independent, each of the coefficients a_i is symmetric in $t_1, \dots, t_{n-1}$. By the inductive hypothesis, we may express each a_i as a polynomial in the elementary symmetric polynomials on $t_1, \dots, t_{n-1}$. If these elementary symmetric polynomials are denoted by $u_1, \dots, u_{n-1}$, then

$$f(t_1, \dots, t_n) = p_0 + p_1 t_n + \cdots + p_d t_n^d$$

where each p_i is a polynomial in $u_1, \dots, u_{n-1}$, with integer coefficients if f has integer coefficients.

Note that the symmetric functions s_i can be expressed in terms of the symmetric functions u_i as follows

$$\begin{aligned} s_1 &= u_1 + t_n \\ s_2 &= u_2 + u_1 t_n \\ &\vdots \\ s_{n-1} &= u_{n-1} + u_{n-2} t_n \\ s_n &= u_{n-1} t_n \end{aligned} \tag{1.3.1.3}$$

These expressions can be solved for the u_i's in terms of the s_i's, giving

$$\begin{aligned} u_1 &= s_1 - t_n \\ u_2 &= s_2 - u_1 t_n = s_2 - s_1 t_n + t_n^2 \\ u_3 &= s_3 - u_2 t_n = s_3 - s_2 t_n + s_1 t_n^2 - t_n^3 \\ &\vdots \\ u_{n-1} &= s_{n-1} - u_{n-2} t_n = s_{n-1} - s_{n-2} t_n + \cdots + (-1)^{n-1} t_n^{n-1}. \end{aligned} \tag{1.3.1.4}$$

and from the last equation in (1.3.1.3),

$$0 = s_n - u_{n-1}t_n = s_n - s_{n-1}t_n + \cdots + (-1)^n t_n^n. \tag{1.3.1.5}$$

Substituting these expressions for the u_i's, and gather together powers of t_n, we get

$$f(t_1, \ldots, t_n) = r_0 + r_1 t_n + \cdots + r_m t_n^m$$

where each r_i is a polynomial in $s_1, \ldots, s_{n-1}$, with integer coefficients if f has integer coefficients. If $m \geq n$, we may reduce the degree in t_n by using (1.3.1.5), which also introduces the term s_n. Hence,

$$f(t_1, \ldots, t_n) = g_0 + g_1 t_n + \cdots + g_{n-1} t_n^{n-1} \tag{1.3.1.6}$$

where each g_i is a polynomial in $s_1, \ldots, s_n$, with integer coefficients if $f(X)$ has integer coefficients. Since the left side of (1.3.1.6) is symmetric in the s_i's, we may interchange t_n and t_i, for each $i = 1, \ldots, n-1$, to get

$$f(t_1, \ldots, t_n) = g_0 + g_1 t_i + \cdots + g_{n-1} t_i^{n-1}$$

valid for all $i = 1, \ldots, n$. Hence, the polynomial

$$P(X) = g_0 + g_1 X + \cdots + g_{n-1} X^{n-1} - f(t_1, \ldots, t_n)$$

has degree (in X) at most $n-1$ but has n distinct roots $t_1, \ldots, t_n$, whence it must be the zero polynomial. Thus, $g_i = 0$ for $i > 0$ and $f(t_1, \ldots, t_n) = g_0 = g_0(s_1, \ldots, s_n)$ as desired. □

Example 1.3.1.6. Let $g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$ be the general polynomial with algebraically independent roots $r_1, \ldots, r_n$. Let

$$p_i(r_1, \ldots, r_n) = r_1^i + \cdots + r_n^i$$

Since the p_i's are symmetric polynomials in the roots of $g(X)$, Theorem 1.3.1.5 implies that they can be expressed as symmetric polynomials in the elementary symmetric polynomials $s_1, \ldots, s_n$. Newton's identities are

$$p_k s_0 - p_{k-1} s_1 + p_{k-2} s_2 + \cdots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0 \tag{1.3.1.7}$$

valid for $k \geq 1$, where $s_0 = 1$ and $s_i = 0$ for $i > n$. For $k > n$, this equality is easy to prove by considering the sum

$$\begin{aligned} 0 = \sum_{i=1}^n r_i^{k-n} g(r_i) &= \sum_{i=1}^n (r_i^k - s_1 r_i^{k-1} + \cdots + (-1)^n r_i^{k-n} s_n) \\ &= \sum_{i=1}^n r_i^k - s_1 \sum_{i=1}^n r_i^{k-1} + \cdots + (-1)^n s_n \sum_{i=1}^n r_i^{k-n} \\ &= p_k - p_{k-1} s_1 + \cdots + (-1)^k p_{k-n} s_k \end{aligned}$$

and an similar argument prove the case $k = n$. For $1 \leq k < n$, we proceed by induction on n. Let $N_k^{(n)}(r_1, \ldots, r_n)$ denote the left-sider of (1.3.1.7). Then we can see

$$N_k^{(n)}(r_1, \ldots, r_{n-1}, 0) = N_k^{(n-1)}(r_1, \ldots, r_{n-1}).$$

This implies $r_n \mid N_k^{(n)}(r_1, \ldots, r_{n-1}, 0)$, and hence $s_n = r_1 \cdots r_n \mid N_k^{(n)}(r_1, \ldots, r_n)$ by symmetricity on $r_1, \ldots, r_n$. But this is impossible for $k < n$, since $p_{k-i} s_i$ does not contain the term $r_1 \ldots r_n$ for $i < n$. This implies $N_k^{(k)}(r_1, \ldots, r_n) = 0$.

Example 1.3.1.7.

1.3.1.2 The discriminant of a polynomial

We have seen that the Galois group $\mathrm{Gal}_K(f(X))$ of a polynomial of degree n is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_n$ and that the Galois group of a general polynomial is isomorphic to $\mathfrak{S}_n$ itself. A special symmetric function of the roots of $f(X)$, known as the discriminant, provides a tool for determining whether the Galois group is isomorphic to a subgroup of the alternating group $\mathfrak{A}_n$.

Let $f(X)$ be a polynomial over K, with roots $r_1, \ldots, r_n$ in a splitting field E. Let

$$\Delta = \prod_{i<j}(r_i - r_j)$$

The **discriminant** of $f(X)$ is $D = \Delta^2$, which is clearly symmetric in the roots.

Proposition 1.3.1.8. *Let $f(X) \in K[X]$ have degree n and splitting field E. Let $\sqrt{D}$ be any square root of the discriminat D of $f(X)$.*

(1) $D = 0$ if and only if $f(X)$ has multiple roots.

(2) Assume that $D \neq 0$ and $\mathrm{char}(K) \neq 2$.

(a) $\sqrt{D} \in K$ if and only if $\mathrm{Gal}_K(f(X))$ is isomorphic to a subgroup of $\mathfrak{A}_n$.

(b) $\sqrt{D} \notin K$ if and only if $\mathrm{Gal}_K(f(X))$ is isomorphic to a subgroup of $\mathfrak{S}_n$ that contains half odd and half even permutations. In this case,

$$E^{\mathrm{Gal}_K(f(X))\cap\mathfrak{A}_n} = K(\sqrt{D}).$$

(3) If $D \neq 0$ and $\mathrm{char}(K) = 2$, then $\sqrt{D} \in K$ but $\mathrm{Gal}_K(f(X))$ need not be isomorphic to a subgroup of $\mathfrak{A}_n$.

Proof. Let $\Delta = \sqrt{D}$. Each transposition of the roots sends Δ to $-\Delta$, so for any $\sigma \in \mathrm{Gal}_K(f(X))$,

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

If $\mathrm{char}(K) = 2$, then $\sigma(\Delta) = \Delta$ for all $\sigma \in \mathrm{Gal}_K(f(X))$ and so Δ is always in the base field K. If $\mathrm{char}(K) \neq 2$, then $\sigma \in \mathrm{Gal}_K(f(X))$ fixes Δ if and only if σ is an even permutation. Put another way, $\Delta \in E^{\mathrm{Gal}_K(f(X))}$ if and only if $\mathrm{Gal}_K(f(X))$ contains only even permutations, that is, $\mathrm{Gal}_K(f(X)) \subseteq \mathfrak{A}_n$.

If $\Delta \notin K$ then $\mathrm{Gal}_K(f(X))$ must contain an odd permutation, and thus exactly half of its elements are even. Hence, if $\Delta \notin K$ then $G = \mathrm{Gal}_K(f(X))$ has even order and $|G \cap \mathfrak{A}_n| = |G|/2$, that is,

$$[G : G \cap \mathfrak{A}_n] = 2.$$

Since all groups are closed, it follows that

$$[E^{G\cap\mathfrak{A}_n} : E^G] = [G : G \cap \mathfrak{A}_n] = 2.$$

Since $[K(\Delta) : K] = 2$ and $K(\Delta) \subseteq E^{G\cap\mathfrak{A}_n}$, we get

$$K(\Delta) = E^{G\cap\mathfrak{A}_n}.$$

Thus, $K(\Delta)$ is the fixed field of the subgroup of even permutations in $\mathrm{Gal}_K(f(X))$. □

The usefulness of Proposition 1.3.1.8 comes from the fact that D can actually be computed without knowing the roots of $f(X)$ explicitly. This follows from the fact that Δ is the Vandermonde determinant

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & \vdots & \cdots & \vdots \\ r_1^{n-1} & r_2^{n-2} & \cdots & r_n^{n-1} \end{vmatrix}$$

Multiplying this by its transpose gives

$$D = \begin{vmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \cdots & \vdots \\ p_{n-1} & pn & \cdots & p_{2n-2} \end{vmatrix}$$

where $p_i = r_1^i + \cdots + r_n^i$. Newton's identities can then be used to determine the u_i's in terms of the coefficients of the polynomial $f(X)$.

1.3.2 The Galois groups of some polynomials

1.3.2.1 The quadratic Quadratic extensions (extensions of degree 2) hold no surprises. Let

$$f(X) = X^2 + bX + c = (X - \alpha)(X - \beta)$$

be a quadratic over K, with splitting field E. To compute the discriminant, observe that

$$p_1 = \alpha + \beta = -b, \quad p_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = b^2 - 2c.$$

Hence

$$D = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2c \end{vmatrix} = 2(b^2 - 2c) - b^2 = b^2 - 4c$$

a familiar quantity.

If $D = 0$, then $f(X)$ has a double root α and

$$f(X) = (X - \alpha)^2 = X^2 - 2\alpha X + \alpha^2.$$

The root α will lie in K for most well-behaved base fields K. In particular, if $\mathrm{char}(K) \neq 2$, then $2\alpha \in K$ implies $\alpha \in K$. If char2 $= 2$ and K is perfect (a finite field, for example) then $(X - \alpha)^2$ must be reducible over K and so $\alpha \in K$.

However, the following familiar example shows that $f(X)$ may have a multiple root not lying in K. Let $K = \mathbb{F}_2(t^2)$ where t is transcendental over $\mathbb{F}_2$ and let

$$f(X) = X^2 - t^2 = (X - t)^2.$$

Since $t \notin \mathbb{F}_2(t^2)$, this polynomial is irreducible over $\mathbb{F}_2(t^2)$, but has a multiple root t.

If $D \neq 0$, then $f(X)$ has distinct roots and there are two possibilities:

(1) The roots lie in K, $f(X)$ is reducible and $\mathrm{Gal}_K(f(X))$ is trivial.

(2) The roots do not lie in K, $f(X)$ is irreducible and $\mathrm{Gal}_K(f(X)) \cong \mathfrak{S}_2$ is generated by the transposition (12) of the roots.

We can summarize these arguments into the following proposition.

Proposition 1.3.2.1. *Let $f(X) \in K[X]$ have degree 2.*

(1) If $D = 0$ then $f(X)$ has a double root α. If $\mathrm{char}(K) \neq 2$ or K is perfect, then $\alpha \in K$. In any case, $\mathrm{Gal}_K(f(X))$ is trivial.

(2) If $D \neq 0$ then $f(X)$ has distinct roots and there are two possibilities:

(a) The roots lie in K, $f(X)$ is reducible and $\mathrm{Gal}_K(f(X))$ is trivial.

(b) The roots do not lie in K, $f(X)$ is irreducible and $\mathrm{Gal}_K(f(X))$ is generated by the transposition of the roots.

When $\mathrm{char}(K) \neq 2$, we can distinguish the two cases as follows: Case (a) holds if $\sqrt{D} \in K$ and case (b) holds if $\sqrt{D} \notin K$.

1.3.2.2 The cubic Let $f(X) \in K[X]$ be a polynomial of degree 3. Then it has the following form:

$$f(X) = X^3 + bX^2 + cX + d = (X - r)(X - s)(X - t) \in K[X]$$

If $f(X)$ is reducible, then it can be factored over K:

$$f(X) = (X - r)(X^2 + pX + q)$$

where $g(X) = X^2 + pX + q$ is irreducible over K. Hence the Galois group is isomorphic to $\mathfrak{S}_2$ if $g(X)$ is irreducible, and is $\{1\}$ is $g(X)$ is also reducible.

Now let us assume that $f(X)$ is irreducible, and let E be its splitting field. A lengthy computation gives

$$\Delta = -4b^3d + b^2c^2 + 18bcd - 4c^3 - 27d^2,$$

but one may remember the trick of shifting x by $a/3$ (in characteristic $\neq 3$), with the effect of killing the coefficient of X^2:

$$f(X - \frac{a}{3}) = X^3 + pX + q$$

for suitable p and q. This does not change D (shifting all roots α_i by the same amount has no effect on the differences $\alpha_i - \alpha_j$), yet

$$D = -4p^3 - 27q^2$$

is a little more memorable.

If $D = 0$, then $f(X)$ has multiple roots and since each root must have the same multiplicity, we are left with $\mathrm{char}(K) = 3$ and

$$f(X) = (X - r)^3 = X^3 - r^3$$

Hence, the extension $K \subseteq K(r) = E$ is purely inseparable of degree 3 and the Galois group is trivial.

If $D \neq 0$, then $f(X)$ has no multiple roots and is therefore separable. Hence, $K \subseteq E$ is Galois and

$$3 \leq |\mathrm{Gal}_K(f(X))| = [E : K] = 3!$$

which leaves the possibilities $[E : K] = 3$ or $[E : K] = 6$.

We can now give a complete analysis for the cubic. Note that when $\mathrm{char}(K) \neq 2$, knowledge of irreducibility and the value of $\sqrt{D}$ determine the Galois group and the splitting field.

Proposition 1.3.2.2 (The cubic). *Let $f(X) \in K[X]$ be a separable polynomial of degree 3, with splitting field E and Galois group $G = \mathrm{Gal}_K(f(X))$. Then there are four mututally exclusive possibilities, each of which can be characterized in three equivalent ways:*

(1) (a) $[E : K] = 1$,
 (b) $E = K$,
 (c) $G = \{1\} = \mathfrak{A}_2$,
 (d) *(For* $\mathrm{char}(K) \neq 2$*) $f(X)$ is reducible and $\sqrt{D} \in K$.*

(2) (a) $[E : K] = 2$,
 (b) *$f(X)$ is reducible and $E = K(r)$ is a splitting field for $f(X)$, where r is a root not in K.*
 (c) $G = \mathfrak{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$,
 (d) *(For* $\mathrm{char}(K) \neq 2$*) $f(X)$ is reducible and $\sqrt{D} \notin K$.*

(3) (a) $[E : K] = 3$,
 (b) *$f(X)$ is irreducible and $E = K(r)$ is the splitting field for K, for any root r.*
 (c) $G = \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$.
 (d) *(For* $\mathrm{char}(K) \neq 2$*) $f(X)$ is irreducible and $\sqrt{D} \in K$.*

(4) (a) $[E : K] = 6$,
 (b) *$f(X)$ is irreducible and $E = K(\sqrt{D}, r)$ is the splitting field for $f(X)$, for any root r.*
 (c) $G = \mathfrak{S}_3$.
 (d) *(For* $\mathrm{char}(K) \neq 2$*) $f(X)$ is irreducible and $\sqrt{D} \notin K$.*

Proof. Since f is separable, E/K is a Galois extension, so we have $[E : K] = |G|$. This is aldeary enough to classifies the Galois group G. We turn to other equivalences.

Let f be reducible:

$$f(X) = (X - r)(X^2 + px + q).$$

If $\mathrm{char}(K) \neq 2$, then $G = \{1\}$ if and only if $g(X) := X^2 + pX + q$ is reducible, and $G = \mathfrak{S}_2$ if and only if $g(X)$ is irreducible. Since

$$D_f = (r - t)^2(r - s)^2(t - s)^2 = (r^2 - (t + s)r + ts)^2(t - s)^2 = (r^2 - (t + s)r + ts)^2 D_g,$$

we see $\sqrt{D}_f \in K$ if and only if $\sqrt{D}_g \in K$, Hence the claim of (1) and (2) follows.

Now assume that f is irreducible, so that no roots of $f(X)$ lies in K. Then since any root of $f(X)$ has degree 3 over K, we conclude that $[E : K] = |G| \geq 3$. By Proposition 1.3.1.8 $\sqrt{D} \in K$ if and only if $G \subseteq \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, which then implies $G = \mathfrak{A}_3$. Therefore (3) holds. The other case is $\sqrt{D} \notin K$, which implies $G = \mathfrak{S}_3$ by order consideration. This completes the proof. □

We know that $D \in K$. For $K = \mathbb{Q}$, we can learn more about the roots of a cubic by looking at the sign of D. A cubic $f(X)$ over $\mathbb{Q}$ has either one real root r and two nonreal roots $\{a + bi, a - bi\}$ or three real roots r, s and t. In the former case,

$$\Delta = (r - a - bi)(r - a + bi)2bi = |(r - a) + bi|^2 2bi$$

and so $D < 0$. In the latter case $D = (r - s)^2(r - t)^2(s - t)^2 > 0$.

Proposition 1.3.2.3 (The cubic over $\mathbb{Q}$). *Let $f(X) \in \mathbb{Q}[X]$ have degree 3. Then*

(a) $D < 0$ if and only if $f(X)$ has exactly one real root,

(b) $D > 0$ if and only if $f(X)$ has three real roots.

Example 1.3.2.4. Let $f(X) = X^3 - 2X^2 - X + 1$ over $\mathbb{Q}$. Any rational root of $f(X)$ must be $\mathfrak{m}1$ and so $f(X)$ is irreducible. The discriminant is $D = 49 > 0$, so $f(X)$ has three real roots. Since $\sqrt{D} = 7 \in \mathbb{Q}$, we have $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $f(X)$ has splitting field $\mathbb{Q}(r)$, for any root r.

Example 1.3.2.5. For any prime p, the polynomial $f(X) = X^3 - p$ is irreducible over $\mathbb{Q}$ and has discriminant $D = -27p^2 < 0$, whose square root is not in $\mathbb{Q}$. Hence, $f(X)$ has one real root and two nonreal roots, the Galois group of $\mathrm{Gal}_{\mathbb{Q}}(f(X))$ is isomorphic to $\mathfrak{S}_3$ and $f(X)$ has splitting field $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})$.

Example 1.3.2.6. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p, where p is prime. Assume that $f(X)$ has $p - 2$ real roots and 2 nonreal, complex roots. Then the Galois group of $f(X)$ is $\mathfrak{S}_p$.

Indeed, complex conjugation induces an automorphism of the splitting field and acts by interchanging the two nonreal roots, so the Galois group G, as a subgroup of $\mathfrak{S}_p$, contains a transposition. On the other hand, the degree of the splitting field (and hence $|G|$) is divisible by p, because it contains a simple extension of order p, obtained by adjoining any one root to $\mathbb{Q}$. Since p is prime, G contains an element of order p by Cauchy's theorem; the only elements of order p in $\mathfrak{S}_p$ are p-cycles, so G contains a p-cycle. It follows that $G = \mathfrak{S}_p$.

For example, the Galois group of $f(X) = X^5 - 5X - 1$ over $\mathbb{Q}$ is $\mathfrak{S}_5$, giving a concrete example of a quintic that cannot be solved by radicals

1.3.3 Geometric impossibilities

1.3.3.1 Constructions by straightedge and compass We begin with two points O, P in the ordinary, real plane. You are allowed to mark more points and other geometric figures in the plane, but only according to the following rules:

- If you have constructed two points A, B, then you can draw the line joining them (using your straightedge).
- If you have constructed two points A, B, then you can draw the circle with center at A and containing B (using your compass).
- You can mark any number of points of intersection of any two distinct lines, line and circle, or circles that you have drawn already.

The general question is to decide whether a figure can or cannot be constructed this way. Three problems of this kind became famous in antiquity:

- trisecting angles.
- squaring circles.
- doubling cubes.

Preppendicular lines and parallel lines are constructible.

Definition 1.3.3.1. A real number r is **constructible** if the point $(r, 0)$ is constructible with straightedge and compass (assuming $O = (0, 0)$ and $P = (1, 0)$, as above). We will denote by $\mathscr{C}_{\mathbb{R}} \subseteq \mathbb{R}$ the set of constructible real numbers.

Also, we can identify the real plane with $\mathbb{C}$, placing O at 0 and P at 1, and we say that $z = x + iy$ is **constructible** if the point (x, y) is constructible by straightedge and compass. We will denote by $\mathscr{C}_{\mathbb{C}} \subseteq \mathbb{C}$ the set of constructible complex numbers. Summarizing the foregoing discussion, we have proved:

Proposition 1.3.3.2. *A point (x, y) is constructible by straightedge and compass if and only if $x + iy \in \mathscr{C}_{\mathbb{C}}$, if and only if $x, y \in \mathscr{C}_{\mathbb{R}}$.*

Proposition 1.3.3.3. *The subset $\mathscr{C}_{\mathbb{R}}$ of constructible numbers is a subfield of $\mathbb{R}$. Likewise, $\mathscr{C}_{\mathbb{C}}$ is a subfield of $\mathbb{C}$, and in fact $\mathscr{C}_{\mathbb{C}} = \mathscr{C}_{\mathbb{R}}(i)$.*

We may view $\mathscr{C}_{\mathbb{R}}$ and $\mathscr{C}_{\mathbb{C}}$ as extensions of $\mathbb{Q}$, drawing a bridge between constructibility by straightedge and compass and field theory: we will be able to understand constructibility of geometric figures if we can understand the field extensions

$$\mathbb{Q} \subseteq \mathscr{C}_{\mathbb{R}} \subseteq \mathscr{C}_{\mathbb{C}}.$$

1.3.3.2 Constructible numbers and quadratic extensions Our goal is to prove the following amazingly explicit description of $\mathscr{C}_{\mathbb{R}}$ (immediately implying one for $\mathscr{C}_{\mathbb{C}}$).

Theorem 1.3.3.4. *Let $\gamma \in \mathbb{R}$. Then $\gamma \in \mathscr{C}_{\mathbb{R}}$ if and only if there exist real numbers $\delta_1, \ldots, \delta_k$ such that $\forall j = 1, \ldots, k$*

$$[\mathbb{Q}(\delta_1, \ldots, \delta_j) : \mathbb{Q}(\delta_1, \ldots, \delta_{j-1})] = 2$$

and $\gamma \in \mathbb{Q}(\delta_1, \ldots, \delta_k)$.

Proof. Let's first argue in the geometry to algebra direction. A configuration of points, lines, and circles obtained by a straightedge-and-compass construction may be described by the coordinates of the points and the equations of the lines and circles. Suppose that at one stage in a given construction all coordinates of all points and all coefficients in the equations of lines and circles belong to a field F; we will say that the configuration is **defined over** K.

Then we claim that for every object constructed at the next stage, there exists a number $\delta \in \mathbb{R}$, of degree at most 2 over K, such that the new configuration is defined over $F(\delta)$. The only if part of the theorem follows by induction on the number of steps in the construction, since at the beginning the configuration (that is, the pair of points $O = (0, 0)$, $P = (1, 0)$) is defined over $\mathbb{Q}$.

Verifying our claim amounts to verifying it for the basic operations defining straightedge-and-compass constructions. Clearly the point of intersection of two lines defined over K has coordinates in K and that lines and circles determined by points with coordinates in K are defined over K. So $\delta = 1$ works in all these cases.

For the intersection of a line ℓ and a circle C, assume that ℓ is not parallel to the y-axis (the argument is entirely analogous otherwise) and that it does meet C; let

$$y = mx + r$$

be the equation of ℓ and let

$$x^2 + y^2 + ax + by + c = 0$$

be the equation of C. We are assuming that $a, b, c, m, r \in K$. Then the x coordinates of the points of intersection of ℓ and C are the solutions of the equation

$$x^2 + (mx + r)^2 + ax + b(mx + r) + c = 0$$

The quadratic formula shows that these coordinates belong to the field $F(\sqrt{D})$ where D is the discriminant of this polynomial: explicitly,

$$D = (2mr + bm + a)^2 - 4(m^2 + 1)(r^2 + br + c)$$

but this is unimportant. What is important is that $D \in K$; hence $\delta = \sqrt{D}$ satisfies our requirement.

For the intersection of two (distinct) circles defined over K, nothing new is needed: if

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases}$$

are two circles, subtracting the two equations shows that their points of intersection coincide with the points of intersection of a circle and a line:

$$\begin{cases} x^2+y^2+a_1x+b_1y+c_1=0 \\ (a_1-a_2)x+(b_1-b_2y)+(c_1-c_2)=0 \end{cases}$$

with the same conclusion as in the previous case.

This completes the verification of the only if part of the theorem. To prove that every element of an extension as stated is constructible, again argue by induction: it suffices to show that if (i) $\delta \in \mathbb{R}$, (ii) all elements of K are constructible, and (iii) $r = \delta^2 \in K$, then δ is constructible (note that in order to construct an element of degree 2 over K, it suffices to construct the square root of the discriminant of its minimal polynomial). Therefore, all we have to show is that we can **take square roots** by a straightedge-and-compass construction. Here is the picture (if $r > 1$) If $A = (r, 0)$ is constructible, so is $B = (-r, 0)$; C

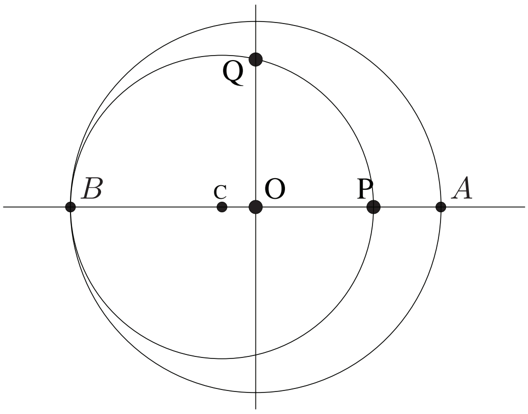


Figure 1.1: squre root

is the midpoint of the segment BP (midpoints are constructible); the circle with center C and containing P intersects the positive y-axis at a point $Q = (0, \delta)$, and elementary geometry shows that $\delta^2 = r$. Therefore δ is constructible, concluding the proof of the theorem. □

Corollary 1.3.3.5. *Let $\gamma \in \mathscr{C}_{\mathbb{C}}$ be a constructible number. Then $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is a power of* 2.

Proof. By Proposition 1.3.3.3 and Theorem 1.3.3.4, there exist $\delta_1, \dots, \delta_k \in \mathbb{R}$ such that

$$\gamma \in \mathbb{Q}(\delta_1, \dots, \delta_k, i)$$

and each δ_j has degree ≤ 2 over $\mathbb{Q}(\delta_1, \dots, \delta_{j-1})$. Repeated application of Proposition 1.1.2.11 shows that

$$[\mathbb{Q}(\delta_1, \dots, \delta_k, i) : \mathbb{Q}]$$

is a power of 2, and since

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\delta_1, \dots, \delta_k, i)$$

the claim follows from Corollary 1.1.2.12. □

As an example, constructing a regular 7-gon would amount to constructing a 7-th (complex) root of $1, \zeta$. By definition, ζ satisfies

$$t^7 - 1 = (t-1)(t^6 + t^5 + \cdots + t + 1)$$

as $\zeta \neq 1$, ζ must satisfy the cyclotomic polynomial $t^6 + \cdots + 1$. This is irreducible, hence again we find that ζ has degree 6 over $\mathbb{Q}$, and Corollary 1.3.3.5 implies that the regular 7-gon cannot be constructed with straightedge and compass.

Of course 7 is not too special: if p is a positive prime integer, the **cyclotomic polynomial** of degree $p-1$ is irreducible; hence

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

where ζ_p is the complex p-th root of 1 with argument $2\pi/p$. Therefore, Corollary 1.3.3.5 reveals that if p is prime, then the regular p-gon can be constructed only if $p-1$ is a power of 2. This is even more restrictive than it looks at first, due to the following simple lemma.

Lemma 1.3.3.6. *If $2^k + 1$ is prime, then K is a power of 2.*

Proof. First note the fractorization:

$$t^{2m+1} + 1 = (t+1)(t^{2m} - t^{2m-1} + \cdots + 1).$$

Thus K is not odd. Assume that $k = 2m$, then $2^k + 1 = 2^{2m} + 1 = 4^m + 1$. Repeat this argument we see m is also odd, and finally we conclude that K is a power of 2. □

Primes of the form $2^{2^\ell} + 1$ are called **Fermat primes**. Therefore for a prime p, the regular p-gon if constructible only if p is a Fermat prime.

We now use Galois theory to deal with the constructibility of regular n-gons. The key ingredient is the following result.

Proposition 1.3.3.7. *Let E/K be a Galois extension, and assume $[F : K] = p^r$ for some prime p and $r \geq 0$. Then there exist intermediate fields*

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_r = F$$

such that $[E_i : E_{i-1}] = p$ for $i = 1, \ldots, r$.

Proof. As the Galois correspondence is bijective for Galois extensions, this statement follows immediately from the fact that a group of order p^r, with p prime, has a complete series of p-subgroups. □

Theorem 1.3.3.8. *The regular n-gon is constructible by straightedge and compass if and only if $\phi(n)$ is a power of 2, if and only if $n = 2^m p_1 \cdots p_r$, where $m \geq 0$ and the factors p_i are distinct Fermat primes.*

Proof. We first prove the first equivalence. One direction is proved in Theorem 1.3.3.4. For the converse, assume $\phi(n) = 2^r$ for some r. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ is Galois (it is the splitting field of $\Phi_n(X)$), of order $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = 2^r$. Proposition 1.3.3.7 shows that the condition given in Theorem 1.3.3.4 is satisfied and therefore that ζ_n is constructible, as needed.

Now let $\phi(n)$ be a power of 2. From the equation

$$\phi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \cdots p_i^{k_i-1}(p_i - 1)$$

we see that if $k_i - 1 > 0$, then $p_i = 2$. If $k_i - 1 = 0$, then $p_i = 2^m + 1$ should be a prime, so p_i is a Fermat prime. Hence $n = 2^m p_1 \cdots p_r$. The converse can also be deduced from the equality above. □

1.3.4 The fundamental theorem of algebra

Theorem 1.3.4.1. *$\mathbb{C}$ is algebraically closed.*

Proof. Let $f(X) \in \mathbb{C}[X]$ be a nonconstant polynomial; we have to prove that $f(X)$ has roots in $\mathbb{C}$. Note that if $f(X)$ has no roots in $\mathbb{C}$, then neither does $f(X)\overline{f(X)} \in \mathbb{R}[X]$; that is, we may assume that $f(X)$ has real coefficients.

Now consider a tower $\mathbb{R} \subseteq \mathbb{C} \subseteq E$, where E is a splitting field for $p(X) = (X^2 + 1)f(X)$ over $\mathbb{R}$. Since $[\mathbb{C} : \mathbb{R}] = 2$ divides $[E : \mathbb{R}]$, we conclude that $[E : \mathbb{R}] = 2^k m$, for some $k > 1$ with m odd. Our goal is to show that $E = \mathbb{C}$, showing that $f(X)$ splits over $\mathbb{C}$.

Let P be a 2-Sylow subgroup of $\mathrm{Gal}_{\mathbb{R}}(f(X))$. Then $|P| = 2^k$ and so

$$[E^P : \mathbb{R}] = [\mathrm{Gal}_{\mathbb{R}}(f(X)) : P] = m.$$

By intermediate value theorem, every real polynomial with odd degree must have a root in $\mathbb{R}$, it follows that any nontrivial finite extension of $\mathbb{R}$ must have even degree (its primitive element must has even degree). From this we deduce that $m = 1$ and $G = \mathrm{Gal}_{\mathbb{R}}(f(X))$ is a 2-group of order 2^k. Thus we have the tower

$$\{1\} \subseteq \mathrm{Gal}_{\mathbb{C}}(f(X)) \subseteq G$$

in which $|\mathrm{Gal}_{\mathbb{C}}(f(X))| = 2^{k-1}$. Therefore, according to Cauchy's theorem, $\mathrm{Gal}_{\mathbb{C}}(f(X))$ has a subgroup of any order dividing 2^{k-1}. But $\mathrm{Gal}_{\mathbb{C}}(f(X))$ cannot have a subgroup of order 2^{k-2} that is, index 2: if H is such a group, then

$$\{1\} \subseteq H \subseteq \mathrm{Gal}_{\mathbb{C}}(f(X)) \subseteq G$$

and then

$$2 = [E^H : E^{\mathrm{Gal}_{\mathbb{C}}(f(X))}] = [E^H : \mathbb{C}],$$

which is impossible, since $\mathbb{C}$ does not have any irreducible polynomial of degree 2. It follows that $|\mathrm{Gal}_{\mathbb{C}}(f(X))| = 1$ and so $|G| = 2$, which implies that $[E : \mathbb{R}] = 2$, whence $E = \mathbb{C}$. □

1.3.5 Finite fields

Let F be a finite field, and let p be its characteristic. We know that F may be viewed as an extension

$$\mathbb{F}_p \subseteq F$$

of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; let $n = [F : F_p]$. Since F has dimension n as a vector space over $\mathbb{F}_p$, it is isomorphic to $\mathbb{F}_p^n$ as a vector space, and in particular $|F| = p^n$ is a power of p.

1.3.5.1 Finite fields as splitting fields Let F be a finite field of size q. Then $F^\times$ has order $q-1$ and so every element $\alpha \in F$ has exponent $q-1$, that is, $\alpha^{q-1} = 1$. It follows that every element of F is a root of the polynomial

$$f_q(X) = X^q - X$$

Since $f_q'(X) = -1$, this polynomial has no multiple roots and so F is precisely the set of roots of $f_q(X)$ in some splitting field. In fact, since F is a field, it is a splitting field for $f_q(X)$ over the prime subfield $\mathbb{F}_p$. We have the following theorem:

Theorem 1.3.5.1. *Let $q = p^n$ be a power of a prime integer p.*

(a) The splitting field of the polynomial $f_q(X) = X^q - X$ over $\mathbb{F}_p$ is a field with precisely q elements.

(b) Let F be a field with exactly q elements; then F is a splitting field for $X^q - X$ over $\mathbb{F}_p$. The polynomial $X^q - X$ is separable over $\mathbb{F}_p$.

In particular, for every prime power q there exists one and only one finite field of order q, up to isomorphism.

Proof. Let F be the splitting field of $X^q - X$ over $\mathbb{F}_p$. Let E be the set of roots of $f(X) = X^q - X$ in F. Since $f'(X) = qX^{q-1} - 1 = -1$ (as $q = 0$ in characteristic p), we have $(f(X), f'(X)) = 1$; hence by Proposition 1.1.6.3 $f(X)$ is separable, and E consists of precisely q elements. We claim that E is a field, and it follows that $E = F$.

To see that E is a field, let $a, b \in E$. Then $a^q = a$ and $b^q = b$; it follows that

$$(a-b)^q = a^p + (-1)^q b^q = a^q - b^q = a - b.$$

(note that $(-1)^q = -1$ if p is odd and $(-1)^q = +1 = -1$ if $p = 2$). If $b \neq 0$,

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}.$$

Thus E is closed under subtraction and division by a nonzero element, proving that E is a field and concluding the proof of the first statement.

To prove the second statement, let F be a field with exactly q elements. The nonzero elements of F form a group under multiplication consisting of $q-1$ elements. Therefore for any elments in $a \in F^\times$ we have $a^{q-1} = 1$. Of course $0^q - 0 = 0$, so the polynomial $X^q - X$ has q roots in F; it follows that F is a splitting field for $X^q - X$, as stated. The final statement comes from the uniqueness of splitting fields. This completes the proof. □

Let us refer to the polynomial $f_q(X) = X^q - X$ as the **defining polynomial** of the finite field $\mathbb{F}_{p^n}$. In view of this theorem, we will often refer to the finite field $\mathbb{F}_{p^n}$.

An immediate consequence of the splitting field characterization of finite fields is that any extension of finite fields is normal.

Corollary 1.3.5.2. *The extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is a finite Galois extension. Hence, in the Galois correspondence for $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, all intermediate fields and all subgroups are closed.*

Example 1.3.5.3. Let p be a prime integer. Then we claim that the polynomial $X^4 + 1$ is **reducible** over $\mathbb{F}_p$ (and therefore over every finite field).

Since $X^4 + 1 = (X+1)^4$ in $\mathbb{F}_2[X]$, the statement holds for $p = 2$. Thus, we may assume that p is an odd prime. Then we claim that $X^4 + 1$ divides $X^{p^2} - X$. Indeed, the square of every odd number is congruent to 1 mod 8; hence $X^8 - 1$ divides $X^{p^2-1} - 1$, which implies

$$(X^4 + 1) \mid (X^8 - 1) \mid (X^{p^2-1} - 1) \mid (X^{p^2} - X)$$

It follows that X^4+1 factors completely in the splitting field of $X^{p^2}-X$, that is, in $\mathbb{F}_{p^2}$. If α is a root of X^4+1 in $\mathbb{F}_{p^2}$, we have the extensions

$$\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$$

therefore $[\mathbb{F}_p(\alpha):\mathbb{F}_p]$ divides $[\mathbb{F}_{p^2}:\mathbb{F}_p]=2$. That is, α has degree 1 or 2 over $\mathbb{F}_p$. But then its minimal polynomial is a factor of degree 1 or 2 of (X^4+1), showing that the latter is reducible.

Now we wish to examine the subfields of a finite field $\mathbb{F}_{p^n}$. Note that if d and n are positive integers and $n=kd+r$ for $0\le r<d$, then it is easy to see $X^d-1 \mid X^n-1$ if and only if $d\mid n$. This yields the following result on subfields of $\mathbb{F}_{p^n}$.

Proposition 1.3.5.4 (Classfication of Subfields of $\mathbb{F}_{p^n}$). *The following are equivalent:*

(i) *The interger d divides n.*

(ii) *The defining polynomial $f_{p^d}(X)$ divides the defining polynomial $f_{p^n}(X)$.*

(iii) *The field $\mathbb{F}_{p^d}$ is contained in $\mathbb{F}_{p^n}$.*

Put another way, the following lattices are isomorphic:

(a) *$\{d : d$ divides $n\}$, under division.*

(b) *$\{f_{p^d}(X) : f_{p^d}(X)$ divides $f_{p^n}(X)\}$, under division.*

(c) *Subfields of $\mathbb{F}_{p^n}$, under set inclusion.*

Moreover, $\mathbb{F}_{p^n}$ has exactly one subfield of size p^d, for each d divides n, and each extension $\mathbb{F}_{p^d}\subseteq\mathbb{F}_{p^n}$ is simple.

Proof. To start with, we first prove the following facts:

$$p^d-1 \mid p^n-1 \Leftrightarrow d\mid n \Leftrightarrow X^d-1\mid X^n-1 \tag{1.3.5.1}$$

In fact, write $n=kd+r$ with $0\le r<d$, then

$$X^n-1 = X^{kd+r}-X^r+X^r-1 = X^r(X^{kd}-1)+X^r-1.$$

Since $X^d-1 \mid X^{kd}-1$, this implies

$$X^n-1 \equiv X^r-1 \mod X^d-1$$

which proves (1.3.5.1) immediately. Now apply these results with Theorem 1.3.5.1, we obtain that

$$d\mid n \Leftrightarrow p^d-1\mid p^n-1 \Leftrightarrow X^{p^d-1}-1 \mid X^{p^n-1}-1 \Leftrightarrow f_{p^d}(X)\mid f_{p^n}(X).$$

which says (i) and (ii) are equivalent. Moreover, by Theorem 1.3.5.1,

$$\mathbb{F}_{p^d}\subseteq\mathbb{F}_{p^n} \Leftrightarrow \mathrm{Root}(f_{p^d}(X))\subseteq \mathrm{Root}(f_{p^n}(X)) \Leftrightarrow f_{p^d}(X)\mid f_{p^n}(X).$$

so (ii) and (iii) are also equivalent. Moreover, if $\mathbb{F}_{p^n}$ has two distinct subfields of size p^d, then the polynomial $f_{p^d}(X)$ would have more than p^d roots in $\mathbb{F}_{p^n}$, which is impossible.

For the last statement, recall that the multiplicative group of nonzero elements of a finite field is cyclic. If $\alpha\in\mathbb{F}_{p^n}$ is a generator of this gorup, then α will generate $\mathbb{F}_{p^n}$ over any subfield. If $d\mid n$, then $\mathbb{F}_{p^n}=\mathbb{F}_{p^d}(\alpha)$, so this extension is simple. □

These results can be translated into rather precise information on the structure of the polynomial ring over a finite field. For example,

Corollary 1.3.5.5. *Let F be a finite field. Then for all integers $n\ge 1$ there exist irreducible polynomials of degree n in $F[X]$.*

Proof. We know $F=\mathbb{F}_q$ for some prime power q. By Proposition 1.3.5.4 there is an extension $\mathbb{F}_q\subseteq\mathbb{F}_{q^n}$, generated by an element α. Then $[F_{q^n}:\mathbb{F}_q]=n$, and it follows that the minimal polynomial of α over $F=\mathbb{F}_q$ is an irreducible polynomial of degree n in $F[X]$. □

In fact, our analysis of extensions of finite fields tells us about explicit factorizations, leading to an inductive algorithm for the computation of irreducible polynomials in $\mathbb{F}_q[X]$:

Corollary 1.3.5.6. *Let $F = \mathbb{F}_q$ be a finite field, and let n be a positive integer. Then the factorization of $X^{q^n} - X$ in $F[X]$ consists of all irreducible monic polynomials of degree d, as d ranges over the positive divisors of n. In particular, all these polynomials factor completely in $\mathbb{F}_{q^n}$, and each irreducible polynomial appears only once in the factorization.*

Proof. By Theorem 1.3.5.1, $\mathbb{F}_{q^n}$ is the splitting field of $X^{q^n} - X$ over $\mathbb{F}_p$, and hence over $\mathbb{F}_q = F$.

If $f(X)$ is a monic irreducible polynomial of degree d, then $F[X]/(f(X)) = F(\alpha)$ is an extension of degree d of F, that is, an isomorphic copy of $\mathbb{F}_{q^d}$. By Proposition 1.3.5.4, if $d \mid n$, then there is an embedding of $\mathbb{F}_{q^d}$ in $\mathbb{F}_{q^n}$. But then α must be a root of $X^{q^n} - X$, and hence $X^{q^n} - X$ is a multiple of $f(X)$, as this is the minimal polynomial of α. This proves that every irreducible polynomial of degree $d \mid n$ is a factor of $X^{q^n} - X$.

Conversely, if $f(X)$ is an irreducible factor of $X^{q^n} - X$, then $\mathbb{F}_{q^n}$ contains a root α of $f(X)$; we have the extensions $F = \mathbb{F}_q \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, and $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^d}$ for $d = \deg \alpha$. It follows that $d \mid n$, again by Proposition 1.3.5.4.

For the last statement, note that $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$, so $X^{p^n} - X$ is separable by Proposition 1.1.6.3. This implies each irreducible polynomial appears only once in $X^{p^n} - X$. □

The picture we are trying to convey is the following: the q^n roots of $X^{q^n} - X$ clump into disjoint subsets, with each subset collecting the roots of each and every irreducible polynomial of degree $d \mid n$ in $F[X]$.

Example 1.3.5.7. Let's contemplate the case $q = 2$: $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

- $n = 1$: the polynomial $X^2 - X$ factors as the product of X and $(X - 1)$ (which we could write as $(X + 1)$ just as well, since we are working over $\mathbb{F}_2$). These are all the irreducible polynomials of degree 1 over $\mathbb{F}_2$.
- $n = 2$: the polynomial $X^4 - X$ must factor as the product of all irreducible polynomials of degree 1 and 2; in fact
$$X^4 - X = X(X - 1)(X^2 + X + 1)$$
and the conclusion is that there is exactly one irreducible polynomial of degree 2 over $\mathbb{F}_2$, namely $X^2 + X + 1$.
- $n = 3$: the quotient of $X^8 - X$ by $X(X - 1)$ is a polynomial of degree 6, which must therefore be the product of the two irreducible polynomials of degree 3 over $\mathbb{F}_2$. It takes a moment to find them:
$$X^3 + X^2 + 1, \quad X^3 + X + 1$$
It also follows that $\mathbb{F}_8$ may be realized in two ways as a quotient of $\mathbb{F}_2[X]$ modulo an irreducible polynomial:
$$\frac{\mathbb{F}_2[X]}{(X^3 + X^2 + 1)} \cong \frac{\mathbb{F}_2[X]}{(X^3 + X + 1)}$$

Since extensions of finite fields are simple extensions, our previous work allows us to be much more precise. Restricting our attention to the extensions $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, for a prime p, we know these can be realized as simple extensions by an element with minimal polynomial of degree n. This polynomial is necessarily separable ($\mathbb{F}_p$ is perfect), so Corollary 1.1.2.6 immediately gives us the size of the automorphism group: $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$.

Proposition 1.3.5.8. *The Galois group G of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is cyclic of order n, generated by the Frobenius automorphism.*

Proof. We have seen that the Frobenius isomorphism σ is an automorphism of $\mathbb{F}_{p^n}$. If $\alpha \in \mathbb{F}_p$, then $\sigma(\alpha) = \alpha^p = \alpha$ and so σ fixes $\mathbb{F}_p$ and is therefore in the Galois group G. Moreover, the n automorphisms
$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$$
are distinct elements of G, for if $\sigma^k = 1$ then $\alpha^{p^k} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$ and so $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^d}$, which implies that $k \geq n$. Finally, since $|G| = n$, we see that $G = \langle \sigma \rangle$. □

Corollary 1.3.5.9. *Let $d \mid n$ be positive integers, then the Galois group G of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^d}$ is cyclic of order n/d, generated by the automorphism $\sigma^d : \alpha \mapsto \alpha^{p^d}$.*

Proof. Let σ^d be the automorphism prescribed above. Then σ^d fixes $\mathbb{F}_{p^d}$.and hence is in G, and it has order d/n. By Theorem 1.2.5.3 we have

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \frac{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})},$$

and in particular $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})| = n/d$. Since σ^d also has order n/d, the claim follows. □

Corollary 1.3.5.10. *The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is isomomorphic to $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $F = \mathbb{F}_q$ be a finite field. We show that the absolute Galois group is isomomorphic to $\widehat{\mathbb{Z}}$. For this, let $\mathcal{N}$ be the category associated to the poset $\mathbb{N}$ of division partial order, and we still denote by n the objects of $\mathcal{N}$. By Proposition 1.3.5.4 we have an inverse system of groups

$$\big(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathcal{N}}$$

where for $m \mid n$ the map $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the restriction map; that is, the image of an automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is obtained by simply restricting the domain of σ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$. Since $\mathbb{F}_{q^m}$ are all the finite subextensions of $\overline{\mathbb{F}}_q$, by Corollary 1.2.4.8, we see the inverse limit of this inverse system is exactly $\mathrm{Gal}(\overline{F}_q/\mathbb{F}_q)$. But Corollary 1.3.5.9 suggests that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ and the restriction map corresponds to the quotient map $\mathbb{Z}/n\mathbb{Z} \to Z/m\mathbb{Z}$. Thus the inverse system $\big(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathcal{N}}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathcal{N}}$ and the claim follows from this. □

1.3.5.2 The algebraic closure of a finite field To conclude, we determine the algebraic closure of a finite field $\mathbb{F}_p$. Since $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is algebraic for all positive integers n, an algebraic closure of $\mathbb{F}_p$ must contain all of the fields $\mathbb{F}_{p^n}$. Since $n! \mid (n+1)!$, it follows that $\mathbb{F}_{p^{n!}} \subseteq \mathbb{F}_{p^{(n+1)!}}$ and so the union

$$\Gamma(p) = \bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$$

is an extension field of $\mathbb{F}_p$ that contains $\mathbb{F}_{p^n}$ for all $n \geq 1$. Moreover, if E is a field for which $\mathbb{F}_{p^n} \subseteq E$ for all n, then $\Gamma(p) \subseteq E$, that is, $\Gamma(p)$ is the smallest field containing each $\mathbb{F}_{p^n}$.

Theorem 1.3.5.11. *The field $\Gamma(p)$ is the algebraic closure of $\mathbb{F}_p$.*

Proof. Every element of $\Gamma(p)$ lies in some $\mathbb{F}_{p^{n!}}$, whence it is algebraic over $\mathbb{F}_p$. Thus $\Gamma(p)$ is algebraic over $\mathbb{F}_p$. Now let $f(X)$ be an irreducible polynomial over $\Gamma(p)$ of degree d. Then the coefficients of $f(X)$ lie in some $\mathbb{F}_{p^{n!}}$ and so $f(X)$ is irreducible as a polynomial over $\mathbb{F}_{p^{n!}}$. Hence, the splitting field for $f(X)$ is $\mathbb{F}_{p^{n!d}} \subseteq \Gamma(p)$ and so $\Gamma(p)$ splits over $\Gamma(p)$. □

1.3.6 Cyclotomic polynomials and fields

Let K be a field. By a **root of unity** (in K) we shall mean an element $\zeta \in K$ such that $\zeta^n = 1$ for some integer $n > 1$. If the characteristic of K is p, then the equation

$$X^{p^d} = 1$$

has only one root, namely 1, and hence there is no p^d-th root of unity except 1.

Let n be an integer > 1 and not divisible by the characteristic p. The polynomial

$$X^n - 1$$

is separable because its derivative is $nX^{n-1} \neq 0$, and the only root of the derivative is 0, so there is no common root. Hence in $\overline{K}$ the polynomial $X^n - 1$ has n distinct roots, which are roots of unity. They obviously form a group, and we know that every finite multiplicative group in a field is cyclic. Thus the group of n-th roots of unity is cyclic. A generator for this group is called a **primitive n-th root** of unity.

If μ_n denotes the group of all n-th roots of unity in $\bar{n}$ and m, n are relatively prime integers, then

$$\mu_{mn} \cong \mu_m \times \mu_n$$

This follows because μ_m, μ_n cann ot have any element in common except 1, and because $\mu_m \mu_n$ consequently has mn elements, each of which is an mn-th root of unity. Hence $\mu_m \mu_n = \mu_{mn}$ and the decomposition is that of a direct product.

As a matter of notation, to avoid double indices, especially in the prime power case, we write $\mu[n]$ for μ_n. So if p is a prime, $\mu[p^r]$ is the group of p^r-th roots of unity. Then $\mu[p^\infty]$ denotes the union of all $\mu[p^r]$ for all positive integers r.

Let K be any field. Let n be not divisible by the characteristic p. Let ζ_n be a primitive n-th root of unity in $\overline{K}$. Let σ be an embedding of $K(\zeta)$ in $\overline{K}$ over K. Then

$$(\sigma(\zeta))^n = \sigma(\zeta^n) = 1$$

so that $\sigma(\zeta)$ is an n-th root of unity also. Hence $\sigma(\zeta) = \zeta^i$ for some integer $i = i(\sigma)$, uniquely determined mod n. It follows that σ maps $K(\zeta)$ into itself, and hence that $K(\zeta)$ is normal over K. If τ is another automorphism of $K(\zeta)$ over K then

$$\sigma(\tau(\zeta)) = \zeta^{i(\sigma)i(\tau)}$$

Since σ and τ are automorphisms, it follows that $i(\sigma)$ and $i(\tau)$ are coprime to n. In this way we get a homomorphism of the Galois group G of $K(\zeta)$ over K into the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of integers prime to n, mod n. Our homomorphism is clearly injective since $i(\sigma)$ is uniquely determined by σ mod n, and the effect of σ on $K(\zeta)$ is determined by its effect on ζ. We conclude that $K(\zeta)$ is abelian over K. We know that the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$. Hence the degree $[K(\zeta) : K]$ divides $\phi(n)$.

For a specific field K, the question arises whether the image of $\mathrm{Gal}(K(\zeta)/K)$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ is all of $(\mathbb{Z}/n\mathbb{Z})^\times$. Looking at $K = \mathbb{R}$ or $\mathbb{C}$, one sees that this is not always the case. We now give an important example when it is the case.

Define the n-th **cyclotomic polynomial** $\Phi_n(X)$ to be

$$\Phi_n(X) = \prod_{\zeta \text{ primitive } n\text{-th root of } 1} (X - \zeta) = \prod_{\substack{1 \le m \le n \\ (m,n)=1}} (X - \zeta_n^m)$$

which has degree $\phi(n)$.

Example 1.3.6.1. If $n = p$ is prime, then every nonidentity element of $\mu_p \cong C_p$ is a generator: every p-th root of 1 is primitive except 1 itself. Therefore

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1$$

Lemma 1.3.6.2. *For all positive integers n,*

$$X^n - 1 = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X)$$

Proof. If $n = de$, then every d-th root ζ of 1 is an n-th root of 1, because $\zeta^n = \zeta^{de} = (\zeta^d)^e = 1$. In particular, every primitive d-th root ζ of 1 is an n-th root of 1.

On the other hand, every $\zeta \in \mu_n$ generates a subgroup H of μ_n, and $H = \mu_d$ for d equal to the order of ζ, a divisor of n. Thus, every $\zeta \in \mu_n$ is a primitive d-th root of 1 for some $d \mid n$.

Thus the set of n-th roots of 1 equals the union of the sets of primitive d-th roots of 1, as d ranges over all positive divisors of n. The statement follows immediately:

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{\substack{1 \le d \le n \\ d \mid n}} \left(\prod_{\zeta \text{ primitive } d\text{-th root of } 1} (X - \zeta) \right) = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X)$$

as claimed. □

Lemma 1.3.6.2 yields an inductive computation of cyclotomic polynomials; the fact that $\Phi_n(X) \in \mathbb{Z}[X]$ follows from this fact. Explicitly,

Corollary 1.3.6.3. *The cyclotomic polynomials $\Phi_n(X)$ have integer coefficients.*

Proof. Use induction on n. Note that $\Phi_1(X) = x - 1$, and assume we have shown that all $\Phi_m(X)$ have integer coefficients for $m < n$. In particular, $f(X) := \prod_{1 \leq d | n, d < n} \Phi_d(X)$ is a monic polynomial with integer coefficients. Since $f(X)$ is monic, we can divide it into $X^n - 1$ with remainder, within $\mathbb{Z}[X]$: there exist $q(X), r(X) \in \mathbb{Z}[X]$ such that

$$X^n - 1 = q(X)f(X) + r(X)$$

with $r(X) = 0$ or $\deg r(X) < \deg f(X)$. On the other hand, by Lemma 1.3.6.2,

$$X^n - 1 = f(X)\Phi_n(X)$$

in $\mathbb{C}[X]$. Therefore

$$f(X)(\Phi_n(X) - q(X)) = r(X)$$

in $\mathbb{C}[X]$. But this forces $r(X) = 0$ (otherwise we would have $\deg r(X) > \deg f(X)$). Therefore $\Phi_n(X) = q(X) \in \mathbb{Z}[X]$. □

Proposition 1.3.6.4. *For all positive n, $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$.*

Proof. Arguing by contradiction, assume $\Phi_n(X)$ is reducible. Then its roots ζ_n^m, with $(m, n) = 1$, are divided among the factors; we can choose a root ζ_n^m of one irreducible monic factor $f(X)$, such that another root ζ_n^{mp} (for some prime p not dividing n) is not a root of $f(X)$. Write

$$\Phi_n(X) = f(X)g(X)$$

since $\Phi_n(X) \in \mathbb{Z}[X]$ and $\Phi_n(X), f(X)$ are monic, $f(X)$ and $g(X)$ have integer coefficients. By our choice, $f(X)$ is the minimal polynomial of ζ_n^m over $\mathbb{Q}$, and $g(\zeta_n^{mp}) = 0$.

It follows that ζ_n^m is a root of $g(X^p)$, and hence $f(X) \mid g(X^p)$. Therefore we can write

$$g(X^p) = f(X)h(X)$$

with $h(X) \in \mathbb{Z}[X]$. Reading the last equation modulo p, we get (again using $(a+b)^p = a^p + b^p$, and denoting cosets by bar)

$$\bar{g}(X)^p = \bar{f}(X)\bar{h}(X) \text{in } \mathbb{F}_p[X].$$

In particular, $\bar{f}(X)$ and $\bar{g}(X)$ must have a nontrivial common factor $\bar{\ell}(X)$ in $\mathbb{F}_p[X]$. But then

$$\ell^2(X) \mid \bar{f}(X)\bar{g}(X)$$

the reduction of $\Phi_n(X)$ modulo p must have a multiple factor.

This implies that $X^n - 1 \in \mathbb{F}_p[X]$ has a multiple factor; that is, it is inseparable. However, its derivative $nX^{n-1} \in \mathbb{F}_p[X]$ is nonzero (because p does not divide n by assumption), and Proposition 1.1.6.3 implies that $X^n - 1$ is separable in $\mathbb{F}_p[X]$.

This contradiction shows that our assumption that $\Phi_n(X)$ is reducible must be nonsense, proving the statement. □

Definition 1.3.6.5. The splitting field $\mathbb{Q}(\zeta_n)$ for the polynomial $X^n - 1$ over $\mathbb{Q}$ is the n-th **cyclotomic field**.

Proposition 1.3.6.6. *The Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has cardinality $\phi(n)$ (Corollary 1.1.2.6; the roots are distinct since $\Phi_n(X)$ is separable), so the homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism. □

Corollary 1.3.6.7. *If n, m are relative prime integers, then*

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

Proof. We note that ζ_n and ζ_m are both contained in $\mathbb{Q}(\zeta_{mn})$ since ζ_{mn}^n is a primitive m-th root of unity. Furthermore, $\zeta_m\zeta_n$ is a primitive mn-th root of unity. Hence

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$$

Our assertion then follows from the multiplicativity $\phi(mn) = \phi(m)\phi(n)$ and Proposition 1.2.6.2. □

Example 1.3.6.8. The reader should consider Example 1.1.5.3 again: by what we have just proved, the automorphism group of the splitting field of $X^8 - 1$ is isomorphic to the group of units in $\mathbb{Z}/8\mathbb{Z}$; this group is immediately seen to be isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, confirming the claim made in Example 1.1.5.3.

1.3.7 Cyclic extensions

1.3.7.1 Hilbert's theorem 90 Let G be a group. A ***G*-module** is an abelian group M together with an action of G, i.e., a map $G \times M \to M$ such that

- $\sigma(m+n) = \sigma m + \sigma n$ for $m, n \in M$.
- $(\sigma\tau)m = \sigma(\tau m)$ for $\sigma, \tau \in G$ and $m \in M$.
- $1m = m$ for $m \in M$.

Thus, to give an action of G on M is the same as giving a homomorphism $G \to \mathrm{Aut}(M)$ (automorphisms of M as an abelian group).

Example 1.3.7.1. Let E be a Galois extension of K with Galois group G. Then $(E, +)$ and $(E^\times, \times)$ are G-modules.

Let M be a G-module. A **crossed homomorphism** is a map $f : G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

for all $\sigma, \tau \in G$. Note that the condition implies that $f(1) = f(1) + f(1)$, and so $f(1) = 0$.

Example 1.3.7.2.

(a) Let $f : G \to M$ be a crossed homomorphism. For any $g \in G$,

$$\begin{aligned} f(\sigma^2) &= f(\sigma) + \sigma f(\sigma), \\ f(\sigma^3) &= f(\sigma) + \sigma f(\sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \\ &\vdots \\ f(\sigma^n) &= f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma) \end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f : G \to M$ is determined by its value, x say, on σ, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0 \tag{1.3.7.1}$$

Moreover, if $x \in M$ satisfies (1.3.7.1), then the formulas $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$ define a crossed homomorphism $f : G \to M$. Thus, for a finite cyclic group $G = \langle \sigma \rangle$, there is a one-to-one correspondence

$$\{\text{crossed homomorphisms } f : G \to M\} \leftrightarrows \{x \in M \text{ satisfying } (1.3.7.1)\}.$$

(b) For every $x \in M$, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x$$

for all $\sigma \in G$. A crossed homomorphism of this form is called a **principal crossed homomorphism**.

(*c*) If G acts trivially on M, i.e., $\sigma m = m$ for all $\sigma \in G$ and $m \in M$, then a crossed homomorphism is simply a homomorphism, and there are no nonzero principal crossed homomorphisms.

The sum and difference of two crossed homomorphisms is again a crossed homomorphism, and the sum and difference of two principal crossed homomorphisms is again principal. Thus we can define

$$H^1(G,M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}$$

(quotient abelian group). An exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

gives rise to an exact sequence

$$0 \longrightarrow M^G \longrightarrow N^G \longrightarrow L^G \xrightarrow{\delta} H^1(G,M) \longrightarrow H^1(G,N) \longrightarrow H^1(G,L)$$

Let $\ell \in L^G$, and let $n \in N$ map to ℓ. For all $\sigma \in G$, $\sigma n - n$ lies in the submodule M of N, and the crossed homomorphism $\sigma \mapsto \sigma n - n : G \to M$ represents $\delta(\ell)$.

Example 1.3.7.3. Let $\pi : \widetilde{X} \to X$ be the universal covering space of a topological space X, and let Γ be the group of covering transformations. Under some fairly general hypotheses, a Γ-module M will define a sheaf $\mathcal{M}$ on X, and $H^1(X,\mathcal{M}) \cong H^1(\Gamma, M)$. For example, when $M = \mathbb{Z}$ with the trivial action of Γ, this becomes the isomorphism $H^1(X,\mathbb{Z}) \cong H^1(\Gamma,\mathbb{Z}) = \mathrm{Hom}(\Gamma,\mathbb{Z})$.

Theorem 1.3.7.4. *Let E be a finite Galois extension of K with group G; then $H^1(G,E^\times) = 0$ and $H^1(G,E) = 0$.*

Proof. Let f be a crossed homomorphism $G \to E^\times$. In multiplicative notation, this means that

$$f(\sigma\tau) = f(\sigma)\cdot(\sigma f(\tau))$$

for $\sigma,\tau \in G$, and we have to find a $\gamma \in E^\times$ such that $f(\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G$. Because the $f(\tau)$ are nonzero, Corollary 1.1.4.8 implies that

$$\sum_{\tau \in G} f(\tau)\tau : E \to E$$

is not the zero map, i.e., there exists an $\alpha \in E$ such that

$$\beta := \sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0.$$

But then, for $\sigma \in G$,

$$\begin{aligned}\sigma(\beta) = \sigma\Big(\sum_{\tau\in G} f(\tau)\tau(\alpha)\Big) &= \sum_{\tau\in G}\sigma(f(\tau))\sigma(\tau(\alpha))\\ &= f(\sigma)^{-1}\sum_{\tau\in G} f(\sigma\tau)(\sigma\tau)(\alpha) = f(\sigma)^{-1}\beta.\end{aligned}$$

Therefore $f(\sigma) = \beta/\sigma(\beta)$ and we can take $\gamma = \beta^{-1}$.

For the additive version, let $f : G \to E$ be a crossed homomorphism. Then we have

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

for $\sigma,\tau \in G$. Let $\gamma \in E$ an element in E such that $\mathrm{tr}(\gamma) \neq 0$ (this element exists by linearly independence), and consider

$$\beta := \sum_{\tau\in G} f(\tau)\tau(\gamma).$$

Then we have

$$\begin{aligned}\sigma(\beta) = \sigma\Big(\sum_{\tau\in G} f(\tau)\tau(\gamma)\Big) &= \sum_{\tau\in G}\sigma(f(\tau))\sigma(\tau(\gamma))\\ &= \sum_{\tau\in G} f(\sigma\tau)(\sigma\tau)(\gamma) - f(\sigma)\sum_{\tau\in G}(\sigma\tau)(\gamma) = \beta - f(\sigma)\mathrm{tr}(\gamma).\end{aligned}$$

Since $\mathrm{tr}(\gamma) \neq 0$, we obtain $f(\sigma) = \beta/\mathrm{tr}(\gamma) - \sigma(\beta/\mathrm{tr}(\gamma))$, so f is principal. □

Corollary 1.3.7.5 (Hilbert's theorem 90, multiplicative version). *Let E be a finite cyclic extension of K and let σ generate* $\mathrm{Gal}(E/K)$. *Let $\alpha \in E$, if $N(\alpha) = 1$, then $\alpha = \beta/\sigma(\beta)$ for some $\beta \in E$.*

Proof. Let $n = [E : K]$. The condition on α is that $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$, and so by (1.3.7.1) there is a crossed homomorphism $f : G \to E^\times$ with $f(\sigma) = \alpha$. Theorem 1.3.7.4 now shows that f is principal, which means that there is a $\beta \in E$ such that $\alpha = \beta/\sigma(\beta)$. □

Corollary 1.3.7.6 (Hilbert's theorem 90, additive version). *Let E be a finite cyclic extension of K and let σ generate* $\mathrm{Gal}(E/K)$. *Let $\alpha \in E$, if* $\mathrm{tr}(\alpha) = 0$, *then $\alpha = \beta - \sigma(\beta)$ for some $\beta \in E$.*

Proof. Let $n = [E : K]$. The condition on α is that $\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha) = 1$, and so by (1.3.7.1) there is a crossed homomorphism $f : G \to E$ with $f(\sigma) = \alpha$. Theorem 1.3.7.4 now shows that f is principal, which means that there is a $\beta \in E$ such that $\alpha = \beta/\sigma(\beta)$. □

1.3.7.2 Abelian and Cyclic Extensions Extensions are often named after their Galois groups. Here is a very important example.

Definition 1.3.7.7. A Galois extension E/K is **abelian** if its Galois group $\mathrm{Gal}(E/K)$ is abelian and **cyclic** if the Galois group is cyclic.

The basic properties of abelian and cyclic extensions are given in the next proposition. Note that abelian and cyclic extensions are not (quite) distinguished.

Proposition 1.3.7.8 (Property of abelian and cyclic extensions).

- *(**Composite of abelian is abelian**) If $K \subseteq E_i$ are abelian, then $K \subseteq \bigvee E_i$ is abelian.*
- *(**Lifting of abelian (cyclic) is abelian (cyclic)**) If $K \subseteq E$ is abelian (cyclic) and $K \subseteq F$, then $F \subseteq EF$ is abelian (cyclic).*
- *(**Steps in an abelian (cyclic) tower are abelian (cyclic)**) If $K \subseteq E \subseteq F$ with $K \subseteq E \subseteq F$ abelian (cyclic), then $K \subseteq E$ and $E \subseteq F$ are abelian (cyclic).*

Proof. Let $K \subseteq E_i$ be abelian extensions, then since E_i/K are Galois, the extension $K \subseteq \bigvee E_i$ is also Galois. Moreover, by Proposition 1.2.6.7, the Galois group $\mathrm{Gal}(\bigvee E_i/K)$ is a subgroup of $\prod \mathrm{Gal}(E_i/K)$, which is abelian, and hence is also abelian.

Now consider a lifting of abelian (cyclic) extension. By Proposition 1.2.6.2 the extension $F \subseteq EF$ is Galois, and $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap F)$. Note that $\mathrm{Gal}(E/E \cap F)$ is a subgroup of $\mathrm{Gal}(E/K)$, and hence is abelian (cyclic) if $\mathrm{Gal}(E/K)$ is abelian (cyclic).

Finally, consider a tower $K \subseteq E \subseteq F$, where F/K is abelian (cyclic). Since all subgroups of $\mathrm{Gal}(F/K)$ is then normal, we see E/K and F/E are both Galois extensions, and $\mathrm{Gal}(E/K)$, $\mathrm{Gal}(F/E)$ are isomorphic to subgroups of $\mathrm{Gal}(F/K)$, which are abelian (cyclic). □

Abelian and cyclic extensions fail to be distinguished because, and only because if the steps in a tower are abelian (cyclic), this does not imply that the full extension is abelian (cyclic). What does it imply?

Suppose that

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = E$$

is a tower in which each step K_{i+1}/K_i is abelian (cyclic). Taking Galois groups gives the series

$$\{1\} = \mathrm{Gal}(E/E) \subseteq \mathrm{Gal}(E/K_{n-1}) \subseteq \cdots \subseteq \mathrm{Gal}(E/K_1) \subseteq \mathrm{Gal}(E/K_0) = \mathrm{Gal}(E/K).$$

Consider the subtower $K_i \subseteq K_{i+1} \subseteq E$. Since the lower step is normal, it follows from Theorem 1.2.5.3(a) that $\mathrm{Gal}(E/K_{i+1})$ is a normal subgroup of its parent $\mathrm{Gal}(E/K_i)$ and that

$$\frac{\mathrm{Gal}(E/K_i)}{\mathrm{Gal}(E/K_{i+1})} \hookrightarrow \mathrm{Gal}(K_{i+1}/K_i).$$

Since the latter is abelian (cyclic), so is the former. Thus,

$$\{1\} = \mathrm{Gal}(E/E) \lhd \mathrm{Gal}(E/K_{n-1}) \lhd \cdots \lhd \mathrm{Gal}(E/K_1) \lhd \mathrm{Gal}(E/K).$$

where each quotient group is abelian (cyclic). In the language of group theory, this series of subgroups is an **abelian series**. (When the groups are finite, the cyclic case and the abelian case are equivalent.) A group that has an abelian series is said to be **solvable**.

Proposition 1.3.7.9. *If $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$ is a tower of fields in which each step $K_i \subseteq K_{i+1}$ is abelian, then the Galois group* $\mathrm{Gal}(E/K)$ *is solvable.*

In the follows, we classify cyclic extensions under certain conditions, which will be used when we study the solvability of polynomials. The follwoing two theorems are good applications of Hilbert's theorem 90.

Theorem 1.3.7.10. *Let K be a field, n an positive integer coprime to the characteristic of K, and assume that there is a primitive n-th root of unity in K.*

(i) *Let E be a cyclic extension of degree n of K. Then there exists $\alpha \in E$ such that $E = K(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in K$.*

(ii) *Conversely, let $a \in K$. Let α be a root of $X^n - a$. Then $K(\alpha)$ is cyclic over K, of degree d for some $d \mid n$, and α^d is an element of K.*

Proof. Let ζ be a primitive n-th root of unity in K, and let E/K be cyclic with group G. Let σ be a generator of G. We have $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. By Hilbert's theorem 90, there exists $\alpha \in E$ such that $\zeta^{-1} = \alpha/\sigma(\alpha)$. Since ζ is in K, we have $\sigma^i(\alpha) = \zeta^i\alpha$ for $i = 1, \ldots, n$. Hence the elements $\zeta^i(\alpha)$ are n distinct conjugates of α over K, whence $[K(\alpha) : K]$ is at least equal to n. Since $[E : K] = n$, it follows that $E = K(\alpha)$. Furthermore,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n.$$

Hence α^n is fixed under σ, and so under G. Therefore α^n is an element of K, and we let $a = \alpha^n$. This proves the first part of the theorem.

Conversely, let $a \in K$. Let α be a root of $X^n - a$. Then $\alpha\zeta^i$ is also a root for each $i = 1, \ldots, n$, and hence all roots lie in $K(\alpha)$ which is therefore normal over K. All the roots are distinct so $K(\alpha)$ is Galois over K. Let G be the Galois group. If σ is an automorphism of $\mathrm{Gal}(K(\alpha)/K)$ then $\sigma(\alpha)$ is also a root of $X^n - a$. Hence $\sigma(\alpha) = \omega_\sigma\alpha$ where ω_σ is an n-th root of unity, not necessarily primitive. The map $\sigma \mapsto \omega_\sigma$ is obviously a homomorphism of G into the group of n-th roots of unity, and is injective. Since a subgroup of a cyclic group is cyclic, we conclude that G is cyclic, of order d, and $d \mid n$. The image of G is a cyclic group of order d. If σ is a generator of G, then ω_σ is a primitive d-th root of unity. Now we get

$$\sigma(\alpha^d) = \sigma(\alpha)^d = \omega_\sigma^d\alpha^d = \alpha^d.$$

Hence α^d is fixed under G, whence is in K, and our theorem is proved. □

We now pass to cyclic extensions of degree p in characteristic p.

Theorem 1.3.7.11 (Artin-Schreier). *Let K be a field of characteristic p.*

(i) *Let E be a cyclic extension of K of degree p. Then there exists $\alpha \in E$ such that $E = K(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ with some $a \in K$.*

(ii) *Conversely, given $a \in K$, the polynomial $f(X) = X^p - X - a$ either has one root in K, in which case all its roots are in K, or it is irreducible. In this latter case, if α is a root then $K(\alpha)$ is cyclic of degree p over K.*

Proof. Let E be a cyclic extension of K of degree p, and σ be a generator of $\mathrm{Gal}(E/K)$. Since $-1 \in K$, every automorphism in $\mathrm{Gal}(E/K)$ fixes -1, it follows that $\mathrm{tr}(-1) = 0$. By the additive version of Hilbert's theorem 90, there is a element $\alpha \in E$ such that $-1 = \alpha - \sigma(\alpha)$. Then

$$\sigma(\alpha) = \alpha + 1, \quad \sigma^i(\alpha) = \sigma^{i-1}(\alpha) + 1 = \cdots = \alpha + i$$

It follows that the minimal polynomial of α has degree $\geq p$, so $[K(\alpha) : K] \geq p$. But $[E : K] = p$. So $E = K(\alpha)$. Note that

$$\sigma(\alpha^p - \alpha) = \sigma^p(\alpha) - \sigma(\alpha) = (\alpha + 1)^p - \alpha - 1 = \alpha^p - \alpha.$$

Hence $\alpha^p - \alpha$ is fixed under σ, and therefore under $\mathrm{Gal}(E/K)$. It lies in the fixed field K. If we let $a := \alpha^p - \alpha$, we see α satisfies the equation $X^p - X - a = 0$. This proves the first part of the theorem.

Conversely, let $a \in K$. If α is a root of $f(X) = X^p - X - a$, then

$$f(\alpha + 1) = (\alpha + 1)^p - \alpha - 1 - a = \alpha^p - \alpha - a = 0$$

so $\alpha+1$ is also a root. Therefore the roots of $f(X)$ are

$$\alpha_1 := \alpha, \quad \alpha_2 := \alpha+1, \quad \cdots, \quad \alpha_p := \alpha+p-1$$

If $\alpha \in K$, then all α_i is in K. If $\alpha \notin K$, then all α_i is not in K. In this case, any sum $\sum_I$ with $I \neq \{1,\dots,p\}$ and $I \neq \varnothing$ is not an element of K. Therefore $f(X)$ is irreducible by Exercise 1.1.3. Since all roots of $f(X)$ is in $K(\alpha)$, it follows that $K(\alpha)$ is normal over K. Since $f(X)$ has no multiple roots, it follows that $K(\alpha)$ is Galois over K. Since $\alpha+1$ is a root of $f(X)$, there exists an automorphism σ of $K(\alpha)$ over K such that $\sigma(\alpha) = \alpha+1$. Then the powers σ^i give $\sigma^i(\alpha) = \alpha+i$ for $i = 1,\dots,p$ and are distinct. Since $[K(\alpha) : K] = p$, it follows that $\mathrm{Gal}(K(\alpha)/K) = \langle\sigma\rangle$ and is cyclic of order p, there by proving the theorem. □

1.3.8 Solvable and radical extensions

1.3.8.1 Solvable extensions A finite separable extension E/K is said to be **solvable** if the Galois group of the normal closure of E/K is a solvable group. This is equivalent to saying that there exists a solvable Galois extension F of K such that $K \subseteq E \subseteq F$: Indeed, we have $K \subseteq E \subseteq \langle E/K\rangle \subseteq F$ and the Galois group of $\langle E/K\rangle/K$ is a homomorphic image of $\mathrm{Gal}(F/K)$, which is thus solvable.

Proposition 1.3.8.1. *Solvable extensions form a distinguished class of extensions.*

Proof. We first deal with liftings. Let E/K be solvable and F be a field containing K and assume E, F are subfields of some algebraically closed field. Let L be Galois solvable over K and $E \subseteq L$. Then LF is Galois over F and $\mathrm{Gal}(LF/F)$ is a subgroup of $\mathrm{Gal}(L/K)$ by Proposition 1.2.6.2. Hence LF/F is solvable, and it follows that EF/F is slovable.

Now let $K \subseteq E \subseteq F$ be a tower of extensions. If F/K is slovable, then there exists a field L containing F such that L/K is Galois and solvable. The by definition E/K is solvable. For F/E, it is clear that L/E is Galois, and since $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/K)$, it is also solvable. It follows that F/E is solvable.

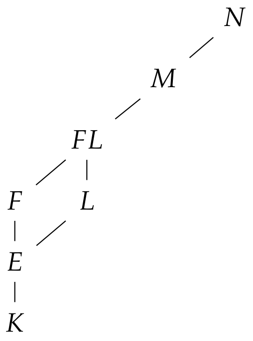


Figure 1.1: A tower of solvable extensions is solvable.

For the converse, assume that F/E and E/K are solvable. Let L be a finite solvable Galois extension of K containing E. Then as a lifting, we see FL/L is solvable. Let M be a finite solvable Galois extension of K containing FL. If σ is any embedding of M over K in a given algebraic closure, then since L/K is Galois, we have $\sigma(L) = L$ and hence $\sigma(M)$ is also solvable extension of L. We let N be the compositum of all extensions $\sigma(M)$ for all embeddings σ of M over K. Then N is Galois over K and is therefore Galois over L. The Galois group $\mathrm{Gal}(N/L)$ is a subgroup of the product $\prod \mathrm{Gal}(\sigma(M)/L)$ by Proposition 1.2.6.7, hence is solvable. Since L is Galois over K, we have a isomorphism

$$\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(N/K)}{\mathrm{Gal}(N/L)}$$

by Theorem 1.2.5.3, which shows $\mathrm{Gal}(N/K)$ is slovable. Since $F \subseteq N$, this proves N is solvable, which completes the proof. □

1.3.8.2 Radical extensions Loosely speaking, when $\mathrm{char}(K) \neq 0$, an extension $K \subseteq E$ is solvable by radicals if it is possible to reach E from K by adjoining a finite sequence of n-th roots of existing elements. More specifically, we have the following definitions, which also deal with the case $\mathrm{char}(K) \neq 0$.

Let $K \subseteq R$ be a finite extension. A **radical series** for $K \subseteq R$ is a tower of fields

$$K = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n = R$$

such that each step R_{i+1}/R_i is one of the following types:

(1) It is obtained by adjoining a root of unity.

(2) It is obtained by adjoining a root of a polynomial $X^n - a$ with $a \in E_i$ and n coprime to the characteristic.

(3) It is obtained by adjoining a root of an equation $X^p - X - a$ with $a \in E_i$, if p is the characteristic of K.

A finite separable extension $K \subseteq R$ that has a radical series is called a **radical extension**. For convenience, we write $K \subseteq R/\{R_i\}$ or $K \subseteq R/\{R_1, \ldots, R_n\}$ to denote the fact that $\{R_i\} = (R_0 \subseteq \cdots \subseteq R_n)$ is a radical series for the extension.

Proposition 1.3.8.2 (Properties of radical extensions).

*(a) (**Lifting**) If $K \subseteq R$ is a radical extension and $K \subseteq S$, then the lifting $S \subseteq RS$ is a radical extension.*

*(b) (**Each step implies full extension**) If $K \subseteq R \subseteq S$, where $K \subseteq R$ and $R \subseteq S$ are radical extensions, then so is the full extension $K \subseteq S$.*

*(c) (**Composite**) If $K \subseteq R$ and $K \subseteq S$ are radical extensions, then so is the composite extension $K \subseteq RS$.*

*(d) (**Normal closure**) If $K \subseteq R$ is a radical extension, then so is $K \subseteq \langle R/K \rangle$.*

Proof. Note that lifting a radical series gives another radical series with the same class of steps, for if $R_{i+1} = R_i(\alpha)$, where α is a root of $f(X) \in R_i[X]$, then

$$SR_{i+1} = (SR_i)(\alpha)$$

where α is a root of $f(X) \in (SR_i)[X]$.

For (a), let $K \subseteq R/\{R_i\}$. Lifting the series $\{R_i\}$ by $K \subseteq S$ gives the radical series

$$S = R_0 S \subseteq R_1 S \subseteq \cdots R_n S = RS$$

and so $S \subseteq RS$ is a radical extension.

For (b), if $K \subseteq R/\{R_i\}$ and $R \subseteq S/\{S_j\}$, then lift the series $\{S_j\}$ by R:

$$R \subseteq RS/(R = RS_0 \subseteq \cdots \subseteq RS_n)$$

and append it to the end of $K \subseteq R/\{R_i\}$ to get

$$K \subseteq RS/(R_0 \subseteq \cdots \subseteq R_n = R = RS_0 \subseteq \cdots \subseteq RS_n)$$

and so $K \subseteq RS = S$ is a radical extension.

For (c), if $K \subseteq R$ and $K \subseteq S$ are radical extensions, then so is the lifting $R \subseteq RS$ and so is the full extension $K \subseteq RS$.

For (d), the normal closure is

$$\langle R/K \rangle = \bigvee_{\sigma \in \mathrm{Hom}_K(R, \bar{R})} \sigma(R).$$

Since $K \subseteq R$ is a finite separable extension, $\mathrm{Hom}_K(R, \bar{R})$ is a finite set. Hence, the composite above is a finite one. If $K \subseteq R/\{R_i\}$ is a radical series, then so is $K \subseteq \sigma(R)/\{\sigma(R_i)\}$. Hence, $K \subseteq \sigma(R)$ is a radical extension, and therefore so is the finite composite $K \subseteq \langle R/K \rangle$. □

1.3.8.3 Solvability by radicals We are interested in extensions $K \subseteq E$ where E is contained in a radical extension $K \subseteq R$.

Definition 1.3.8.3. A finite separable extension $K \subseteq E$ is **solvable by radicals** if $K \subseteq E \subseteq R$, where $K \subseteq R$ is a radical extension.

Proposition 1.3.8.4.

(a) *The class of extensions that are solvable by radicals is distinguished.*

(b) *If $K \subseteq E$ is solvable by radicals then so is $K \subseteq \langle E/K \rangle$. In fact, if $K \subseteq E \subseteq R$ where $K \subseteq R$ is a radical extension, then*

$$K \subseteq E \subseteq \langle E/K \rangle \subseteq \langle R/K \rangle$$

where $K \subseteq \langle R/K \rangle$ is a normal radical extension.

Proof. Let $K \subseteq E \subseteq F$ be a tower. If $K \subseteq F$ is solvable by radicals then there is a field R containing F such that R/K is a radical extension. It follows that E/K solvable by radicals. For the upper step, R/K radical implies R/E is radical by Proposition 1.3.8.2 and so F/E is solvable by radicals. Now suppose the steps in the tower are radical. Then we have the following extensions:

$$\begin{tikzcd}
 & R_{E/K}R_{F/E} \arrow[dd, dash] \\
R_{F/E} \arrow[ur, dash] & \\
F \arrow[u, dash] & R_{E/K} \\
E \arrow[u, dash] \arrow[ur, dash] & \\
K \arrow[u, dash] &
\end{tikzcd}$$

where $K \subseteq R_{E/K}$ and $E \subseteq R_{F/E}$ are radical extensions. Lifting the extension $E \subseteq R_{F/E}$ by $K \subseteq R_{E/K}$ gives the radical extension $R_{E/K} \subseteq R_{E/K}R_{F/E}$, so the tower

$$K \subseteq R_{E/K} \subseteq R_{E/K}R_{F/E}$$

is radical. It follows that the full extension is radical and so $K \subseteq E$ is solvable by radicals.

As to lifting, if $K \subseteq E \subseteq R$ with R/K radical, the lifting by $K \subseteq F$ gives

$$F \subseteq EF \subseteq RF$$

and since $F \subseteq RF$ is radical, EF/F is solvable by radicals.

The second part of the theorem follows from the fact that if $K \subseteq E \subseteq R$ with R/K is radical, then

$$K \subseteq \langle E/K \rangle \subseteq \langle R/K \rangle$$

with $K \subseteq \langle R/K \rangle$ radical by Proposition 1.3.8.2. □

Now we come to the key result that links the concepts of solvable extension and solvability by radicals.

Theorem 1.3.8.5. *Let E be a finite separable extension of K. Then E is solvable by radicals if and only if E/K is solvable.*

Proof. Assume that E/K is solvable, and let F be a finite solvable Galois extension of K containing E. Let m be the product of all prime divisors the degree $[F : K]$ that are unequal to the characteristic, and let $L = K(\zeta)$ where ζ is a primitive m-th root of unity. Then L/K is abelian. We lift F over L, so that FL is solvable over L. Since every solvable group admits a cyclic composition series whose factor groups are of prime order, we can use the Galois correspondence to find a tower of subfields between L and FL such that each step is cyclic of prime order. By Theorem 1.3.7.10 and 1.3.7.11, we conclude that FL is solvable by radicals over L, and hence is solvable by radicals over K. This proves that E/L is solvable by radicals.

$$\begin{tikzcd}
& FL \arrow[dl, dash] \arrow[dd, dash] \\
F \arrow[d, dash] & \\
E \arrow[d, dash] & L \arrow[dl, dash] \\
K &
\end{tikzcd}$$

Conversely, assume that E/K is solvable by radicals. For any embedding σ of E in $\bar{E}$ over K, the extension $\sigma(E)/K$ is also solvable by radicals. Hence the normal closure F of E/K is solvable by radicals. Let m be the product of all prime divisors the degree $[F : K]$ that are unequal to the characteristic and again let $L = K(\zeta)$ where ζ is a primitive m-th root of unity. It will suffice to prove that FL is solvable over L, because it follows then that FL is solvable over K and hence F/K is slovable by Proposition 1.3.8.1. But FL/L can be decomposed into a tower of extensions, such that each step is prime degree and of the type described in Theorem 1.3.7.10 or Theorem 1.3.7.11, and the corresponding root of unity is in the field L. Hence FL/L is solvable, and our theorem is proved. □

1.3.9 Solvability of polynomial equations by radicals

We begin this part with a brief history of the study of roots of polynomials. Mathematicians of the Middle Ages, and probably those in Babylonia, knew the **quadratic formula** giving the roots of a quadratic polynomial $f(X) = X^2 + bX + c$. Setting $X = x - b/2$ transforms $f(X)$ into a polynomial $g(X)$ with no x term:

$$g(X) = X^2 + c - b^2/4.$$

Note that a number α is a root of $g(X)$ if and only if $\alpha - b/2$ is a root of $f(X)$. The roots of $g(X)$ are $\pm(\sqrt{b^2 - 4c})/2$, and so the roots of $f(X)$ are $(-b \pm \sqrt{b^2 - 4c})/2$.

Here is a derivation of the cubic formula. A cubic $f(X) = X^3 + aX^2 + bX + e$ can be transformed, by setting $X = X - a/3$, into a polynomial $g(X)$ with no X^2 term:

$$g(X) = X^3 + qX + r.$$

and a number α is a root of $g(X)$ if and only if $\alpha - a/3$ is a root of $f(X)$. If α is a root of $g(X)$, write $\alpha = \beta + \gamma$, where β and γ are to be found. Now

$$\begin{aligned}\alpha^3 &= (\beta + \gamma)^3 = \beta^3 + \gamma^3 + 3(\beta^2\gamma + \beta\gamma^2) \\ &= \beta^3 + \gamma^3 + 3\alpha\beta\gamma,\end{aligned}$$

and so evaluating $g(\alpha)$ gives

$$\beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r = 0. \tag{1.3.9.1}$$

Impose the condition that $\beta\gamma = -q/3$ (forcing the middle term of (1.3.9.1) to vanish), we get

$$\beta^3 + \gamma^3 = -r.$$

This, together with our assumption on $\beta\gamma$, allow us to solve β and γ explicitly. In fact, a substitution gives

$$\beta^3 - \frac{q^3}{27\beta^3} = -r,$$

and so the quadratic formula yields

$$\beta^3 = \frac{-r \pm \sqrt{r^2 + 4q^3/27}}{2}, \quad \gamma^3 = \frac{-r \mp \sqrt{r^2 + 4q^3/27}}{2}.$$

If $\omega = e^{2\pi i/3}$ is a primitive cube root of unity, there are now six cube roots available: β, $\omega\beta$, $\omega^2\beta$, γ, $\omega\gamma$, $\omega^2\gamma$; these may be paired to give product $-q/3$:

$$-q/3 = \beta\gamma = (\omega\beta)(\omega^2\gamma) = (\omega^2\beta)(\omega\gamma).$$

It follows that the roots of $g(X)$ are $\beta+\gamma$, $\omega\beta+\omega^2\gamma$, and $\omega^2\beta+\omega\gamma$; this is the cubic formula.

Next we derive the quartic formula. A quartic $f(X) = X^4 + aX^3 + bX^2 + eX + d$ can be transformed, by setting $X = x - a/4$, into a polynomial $g(X)$ with no X^3 term:

$$g(X) = X^4 + qX^2 + rX + s,$$

moreover, a number α is a root of $g(X)$ if and only if $\alpha - a/4$ is a root of $f(X)$. Factor $g(X)$ into quadratics:

$$X^4 + qX^2 + rX + s = (X^2 + kX + l)(X^2 - kX + m)$$

(the coefficient of X in the second factor must be $-k$ because there is no cubic term in $g(X)$). If K, l, and m can be found, then the roots of $g(X)$ can be found by the quadratic formula. Expanding the right side and equating coefficients of like terms gives

$$\begin{aligned} l + m - k^2 &= q, \\ km - kl &= r, \\ lm &= s. \end{aligned}$$

Rewrite the first two equations as

$$\begin{aligned} m + l &= q + k^2, \\ m - l &= r/k. \end{aligned}$$

Adding and subtracting these equations gives

$$m = \frac{q + k^2 + r/k}{2}, \quad l = \frac{q + k^2 - r/k}{2}.$$

These two equations show that we are done if K can be found. But $lm = s$ gives

$$(k^2 + q + r/k)(k^2 + q - r/k) = 4s$$

a cubic in k^2. The cubic formula allows one to solve for k^2, and it is now easy to determine l, m, and the roots of $g(X)$.

The most ambitious goal, in line with what occurs for degrees 2, 3, and 4, would be to produce a formula for the solutions to the general polynomial equation

$$X^n + a_{n-1}X^{n-2} + \cdots + a_0 = 0$$

in terms of the coefficients ai and basic operations such as taking roots. This would be a solution *by radicals* of the equation. Well, such a formula simply does not exist:

Theorem 1.3.9.1. *The general polynomial equation of degree* 5 *or higher admits no solution by radicals.*

Proof. Recall that the extension $K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$ has Galois group $\mathfrak{S}_n$, which is not solvable for $n \geq 5$. Therefore by Theorem 1.3.8.5 this extension is not solvable by radicals. This means there is no formula for the solution of the general polynomial $g(X)$. □

Corollary 1.3.9.2. *Let K be a field of characteristic* 0*, and let $f(X) \in K[X]$ be an irreducible polynomial. Then $f(X)$ is solvable by radicals if and only if its Galois group is solvable.*

Corollary 1.3.9.2 is called **Galois' criterion**. Ruffini (1799) and Abel (1824) had previously established that general formulas in radicals for the solutions of equations of degree ≥ 5 do not exist (that is, Theorem 1.3.9.1); but it was Galois who identified the precise condition given in Corollary 1.3.9.2.

In fact, we could now do more: we know that $\mathfrak{S}_3$ and $\mathfrak{S}_4$ are solvable; from a composition series with cyclic quotients we could in principle decompose explicitly the splitting field of general polynomials of degree 3 and 4 as radical extensions and as a consequence recover the Tartaglia/Cardano/Ferrari formulas for their solutions.

1.3.10 Exercise

Exercise 1.3.1. A subgroup G of $\mathfrak{S}_n$ is **transitive** if the induced action of G on $\{1, \ldots, n\}$ is transitive.

- Prove that if $G \subseteq \mathfrak{S}_n$ is transitive, then $|G|$ is a multiple of n.
- List the transitive subgroups of $\mathfrak{S}_3$.
- Prove that the following subgroups of $\mathfrak{S}_4$ are all transitive:
  (1) $\langle (1234) \rangle \cong \mathbb{Z}/4\mathbb{Z}$ and its conjugates.
  (2) $\langle (12)(34), (13)(24) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  (3) $\langle (12)(34), (1234) \rangle \cong D_4$ and its conjugates.
  (4) $\mathfrak{A}_4$ and $\mathfrak{S}_4$.
- With a bit of stamina, prove that these are the only transitive subgroups of $\mathfrak{S}_4$.

Proof. Since G acts transitively on $\{1, \ldots, n\}$, we have (by the class formula, where G_1 is the isotopy of 1)

$$|G| = n|G_1|.$$

This shows $|G|$ is a multiple of n.

We have

$$\mathfrak{S}_3 = \{e, (12), (13), (23), (123), (132)\}$$

Assume G is a transitive subgroup of $\mathfrak{S}_3$, it must have order 3 or 6. Assume $|G| = 3$, then G must have a element of order 3, hence it contains a 3-cycle. Then

$$\mathfrak{A}_3 = \{e, (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}.$$

If $|G| = 6$, then $G = \mathfrak{S}_3$. So the transitive subgroups of $\mathfrak{S}_3$ are $\mathfrak{A}_3, \mathfrak{S}_3$.

It is easy to verify that the subgroups of $\mathfrak{S}_4$ listed above are transitive. If G is a transitive subgroup of $\mathfrak{S}_n$, then $\sigma G \sigma^{-1}$ acts transitively on $\{\sigma(1), \ldots, \sigma(n)\} = \{1, \ldots, n\}$ for some $\sigma \in \mathfrak{S}_n$. It follows that $\sigma G \sigma^{-1}$ is also a transitive subgroup of $\mathfrak{S}_n$. So the subgroups listed are all transitive subgroup of $\mathfrak{S}_4$, so are their conjugates.

Now Assume G is a transitive subgroup of $\mathfrak{S}_4$. Since G is transitive, by the first point we know 4 divides $|G|$. Therefore, the only possible candidates for $|G|$ are $4, 8, 12, 24$. It's clear that $|G| = 24$ iff $G = \mathfrak{S}_4$, and $|G| = 12$ iff $G = \mathfrak{A}_4$.

If $|G| = 4$, then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $|G| = 8$, then G is a 2-sylow subgroup in $\mathfrak{S}_4$, and so is conjugate to any other 8 subgroups. Since D_4 is transitive, all 8 subgroups are transitive. □

Exercise 1.3.2. Compute the Galois group of the polynomial $X^4 - 2$.

Proof. The splitting field of $X^4 - 2$ is $\mathbb{Q}(i, \sqrt[2]{2})$. So it Galois group G has order 8. Since G is a subgroup of $\mathfrak{S}_4$, we see it is a 2-Sylow subgroup. All such groups are isomorphic to D_4. □

Exercise 1.3.3. Prove that the polynomial $X^5 - 5X - 1$ has exactly 3 real roots (this is a calculus exercise) and is irreducible over $\mathbb{Q}$. Prove that its Galois group is $\mathfrak{S}_5$.

Proof. $f(X) = X^5 - 5X - 1$, then $f(-2) = -23, f(-1) = 3, f(0) = -1, f(2) = 21$. So $f(X)$ has 3 real roots. And by Example 1.3.2.6, $f(X)$ has Galois group $\mathfrak{S}_5$. □

Exercise 1.3.4. Let $f(X) \in K[X]$ be a separable irreducible polynomial of prime degree p over a field K, and let $\alpha_1, \ldots, \alpha_p$ be the roots of $f(X)$ in its splitting field $\bar{K}$. Prove that the Galois group of $f(X)$ contains an element σ of order p, cycling through the roots.

Proof. The splitting field of $f(X)$ contains a simple extension $K \subseteq K(\alpha_1)$ which has degree p. So the order of its Galois group divides p. Since p is a prime, Cauchy's theorem gives an element of order p. □

Exercise 1.3.5. Let $f(X) \in K[X]$ be a separable irreducible polynomial of prime degree p over a field K. Let α be a root of $f(X)$ in $\bar{K}$, and suppose you can express another root of $f(X)$ as a polynomial in α, with coefficients in K. Prove that you can express all roots as polynomials in α and that the Galois group of $f(X)$ is $\mathbb{Z}/p\mathbb{Z}$.

Proof. Assume σ is an element of order p. Without loss of generality, we may assume that $\sigma(\alpha)$ is a plolynomial of α:

$$\alpha = f(\alpha)$$

then

$$\sigma(\sigma(\alpha)) = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

which means $\sigma^2(\alpha)$ is a polynomial of $\sigma(\alpha)$, hence is contained in $K(\alpha)$. Keep this process, we can show that all roots of $f(X)$ is in $K(\alpha)$. This means $K(\alpha)$ is the splitting field of $f(X)$, and $|\mathrm{Gal}_K(f(X))| = p$. In particular, σ is a generator, so $\mathrm{Gal}_K(f(X)) \cong \mathbb{Z}/p\mathbb{Z}$. □

Exercise 1.3.6. Let $f(X) \in K[X]$ be a separable irreducible polynomial of degree n over a field K, and let F be its splitting field. Assume $\mathrm{Aut}_K(F) \cong \mathfrak{S}_n$, and let α be a root of $f(X)$ in K.

- Prove that $\mathrm{Aut}_{K(\alpha)}(F) \cong \mathfrak{S}_{n-1}$.
- Prove that there are no proper subfields of $K(\alpha)$ properly containing K.

Proof. We see $\sigma \in \mathrm{Aut}_{K(\alpha)}(F)$ if and only if $\sigma(\alpha) = \alpha$. Since α is a root of $f(X)$, this means σ only change the other $n-1$ roots. This corresponds the group $\mathfrak{S}_{n-1}$, so $\mathrm{Aut}_{K(\alpha)}(F) \cong \mathfrak{S}_{n-1}$. Since there is no subgroup between $\mathfrak{S}_{n-1}$ and $\mathfrak{S}_n$, the second claim follows. □

Exercise 1.3.7. Prove that every element of a finite field F is a sum of two squares in F.

Proof. If F has characteristic 2, then $x \mapsto x^2$ is an isomorphism of F, so we may consider the case $\mathrm{char} F \neq 2$.

We consider the map $\phi : F^\times \to F^\times$ defined by $\phi(X) = x^2$. The image of ϕ is the subset of F that can be written as a^2 for some $a \in F$. If $\phi(a) = \phi(b)$ then $a = b$ or $a = -b$. Since $\mathrm{char} F \neq 2$, we know that $b \neq -b$, so ϕ is a two-to-one map. This implies that

$$|\operatorname{im} \phi| = \frac{|F^\times|}{2} = \frac{|F|-1}{2}.$$

Since 0 is also a squre element, there are totally

$$\frac{|F|-1}{2} + 1 = \frac{|F|+1}{2}$$

squre elements in F. Let S be the set of all squre elements in F. We just observe that $|S| = (|F|+1)/2$.

For any element $x \in F$, consider the set

$$T = \{x - b^2 \mid b \in F\}$$

We onserve that $|S| = |T|$, and

$$|S| + |T| = |F| + 1 > |F|.$$

Thus $|S| \cap |T| \neq \varnothing$. This immediately implies that x is a sum of squres. □

Exercise 1.3.8. Find the cyclotomic polynomials $\Phi_{2^m}(X)$ for all $m \geq 0$.

Proof. We have by Lemma 1.3.6.2

$$X^{2^m} - 1 = \prod_{i=1}^{m} \Phi_{2^i}(X)$$

so

$$\Phi_{2^m}(X) = \frac{X^{2^m} - 1}{X^{2^{m-1}} - 1} = X^{2^{m-1}} + 1$$

which gives the result. □

Exercise 1.3.9. For a prime p, find the factorization of $\Phi_p(X)$ over $\mathbb{F}_p$.

Proof. We have

$$(a-b)^p = a^p + (-1)^p b^p = a^p - b^p$$

on $\mathbb{F}_p$. So

$$\Phi_p(X) = \frac{X^p - 1}{x - 1} = \frac{(X-1)^p}{X-1} = (X-1)^{p-1}$$

which gives the result. □

Exercise 1.3.10. For a, b, c positive integers with $c > 1$, prove that $c^a - 1$ divides $c^b - 1$ if and only if $a \mid b$. Prove that $X^a - 1$ divides $X^b - 1$ in $\mathbb{Z}[X]$ if and only if $a \mid b$.

Proof. For the interesting implications, assume $c^a - 1 \mid c^b - 1$, write $b = ad + r$, then we have

$$c^b - 1 = c^{ad} \cdot c^r - 1 = c^{ad} \cdot c^r - c^r + c^r - 1 = c^r(c^{ad} - 1) + c^r - 1$$

since $c^a - 1 \mid c^{ad} - 1$, we know that $c^a - 1 \mid c^r - 1$. This implies $a \leq r$, which is a contradiction. So $a \mid d$. □

Exercise 1.3.11. Let a, n be positive integers, with $a > 1$. Prove that if $\Phi_n(a)$ divides $a - 1$, then $n = 1$.

Proof. If $n > 1$, then every primitive n-th root satisfies

$$|a - \zeta| > a - 1$$

Now we have $\Phi_n(a) \mid a - 1$, this is a contradiction, since $|\Phi_n(a)| = \prod |a - \zeta| > a - 1$. □

Exercise 1.3.12. Let a, d, n be positive integers, with $d < n$ and $a > 1$. Assume that $a^d - 1$ divides $a^n - 1$. Prove that $\Phi_n(a)$ divides the quotient $(a^n - 1)/(a^d - 1)$.

Proof. We know that $d \mid n$, so

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{1 \leq d \mid n, d < n} \Phi_d(X)} = \frac{X^n - 1}{\prod_{\substack{1 \leq i \mid n \\ i < n, i \neq d}} \Phi_i(X) \cdot \Phi_d(X)} = \frac{(X^n - 1) \prod_{1 \leq j \mid d, j < d} \Phi_j(X)}{\prod_{\substack{1 \leq i \mid n \\ i < n, i \neq d}} \Phi_i(X)(X^d - 1)}$$

but if $j \mid d$, then $j \mid n$, so for the quotient we have

$$\frac{(X^n - 1) \prod_{1 \leq j \mid d, j < d} \Phi_j(X)}{\prod_{\substack{1 \leq i \mid n \\ i < n, i \neq d}} \Phi_i(X)(X^d - 1)} = \frac{X^n - 1}{X^d - 1} \frac{1}{\prod_{1 \leq i \mid n, i \nmid d} \Phi_i(X)}$$

this show $\Phi_n(X) \mid (X^n - 1)/(X^d - 1)$. □

Exercise 1.3.13. Let R be a finite division ring.

- Prove that the center of R is isomorphic to $\mathbb{F}_q$, for q a prime power. Prove that $|R| = q^n$ for some n.

- For every $x \in R$, prove that the centralizer of x in the multiplicative group $(R^\times, \cdot)$ has order $q^d - 1$ for some $d \leq n$.

- Prove that there are integers $d_1, \ldots, d_r < n$ such that

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}$$

- Deduce that $\Phi_n(q)$ divides $q - 1$ and hence $n = 1$.

- Conclude that R equals its center, showing that R is commutative.

Thus, every finite division ring is a field: this is Wedderburn's little theorem. The argument given here is due to Ernst Witt.

Proof. Note that for any $r \in R^{\times}, x \in R$,

$$rx = xr \Leftrightarrow r^{-1}x = xr^{-1}$$

So the center of R is closed under inversion, hence is a subfield. Set $F := Z_R$, we know that $F \cong \mathbb{F}_q$ for some q a prime power. Then R becomes a K-vector space with finite dimension, denoted it by n. Then $|R| = q^n$.

For every $x \in R$, the centralizer of x is the stablizer of x under congruence action in $R^{\times}$. So it is a subgroup of $R^{\times}$, with order $q^d - 1$. Since $q^d - 1 \mid |R^{\times}| = q^n - 1$, we have $d \mid n$. Recall the class formula:

$$|R^{\times}| = |G| + \sum |R^{\times} : G_x|$$

where G is the set of fixed points, that is, $F \setminus \{0\}$. Since each G_x has order $q^d - 1$ for some $d \mid n$, we get the equation

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}$$

Since $d_i \mid n$, $d_i < n$, we have

$$\frac{X^n - 1}{X^{d_i} - 1} = \prod_{d \mid n, d \nmid d_i} \Phi_d(X)$$

note that $n \mid n$, so $\Phi_n(X)$ is in the product above. Concluding we get

$$\Phi_n(X) \mid \frac{X^n - 1}{X^{d_i} - 1}$$

At the same time, $\Phi_n(X) \mid X^n - 1$. Plug into $x = q$ yields $\Phi_n(q) \mid q - 1$. But this is only possible when $n = 1$. So $F = R$. □

Exercise 1.3.14. Let a, p, n be integers, with p, n positive and p prime, $p \nmid n$.

- Show that $X^n - 1$ has no multiple roots modulo p.
- Show that if p divides $\Phi_n(a)$, then $a^n \equiv 1$ modulo p. (In particular, $p \nmid a$, so $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^{\times}$.)
- Show that if p divides $\Phi_n(a)$, then $a^d \not\equiv 1$ modulo p for every $d < n$.
- Deduce that $p \mid \Phi_n(a)$ if and only if the order of $[a]_p$ in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is n.
- Compute $\Phi_{15}(9)$, and show it is divisible by 31.

Proof. The polynomial $f(X) := X^n - 1$ is separable over $\mathbb{F}_p$, since $f(X)' = nX^{n-1}$. Since $p \nmid n$, we conclude that $(f(X), f(X)') = 1$, so $f(X)$ is separable.

Since

$$a^n - 1 = \prod_{1 \leq d \mid n} \Phi_d(a)$$

modding p we get the claim in the second point.

If there is some $d < n$ such that $a^d \equiv 1$ modulo p, then d must be a divisor of n (order consideration). And from the formula

$$a^d - 1 = \prod_{1 \leq i \mid d} \Phi_i(a)$$

we know that there is some $i < d, i \mid d$ such that $\Phi_i(a) \equiv 0$ modulo p. Agian from

$$a^n - 1 = \prod_{1 \leq d \mid n} \Phi_d(a)$$

and $i \mid d \mid n$, we know that $a^n - 1$ at least has two roots in $\mathbb{F}_p$, which cotradicts our previous result.

One direction is immediate. Assume a has order p, then $a^n = 1$, $a^d \not\equiv 1$ for $d < n$. Then we claim that $\Phi_d(a) \not\equiv 0$ for $d < n$: In fact, for any $d < n$, we have

$$a^d - 1 = \prod_{1 \leq i \mid d} \Phi_i(a)$$

since $a^d \not\equiv 1$, we get the claim. □

Exercise 1.3.15. Let a, p, n be integers, with p, n positive and p prime, $p \nmid n$. Assume that p divides $\Phi_n(a)$. Prove that $p \equiv 1 \bmod n$.

Proof. From Exercise 1.3.14, we know that $[a]_p$ has order n in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. In particular, $n \mid p - 1$. □

1.4 Transcendental extensions

1.4.1 Transcendental basis

Definition 1.4.1.1. Let E/K be a field extension. A subset S of E is **algebraically dependent over $\boldsymbol{K}$** if there exists a finite subset $\{s_1, \dots, s_n\} \subseteq S$ and a nonzero polynomial $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ with $f(s_1, \dots, s_n) = 0$. A subset S of E is **algebraically independent** if it is not algebraically dependent. An extension field E/K is **purely transcendental** if either $E = K$ or E contains an algebraically independent subset S and $E = K(S)$.

In fancier language, consider the map defined by

$$K[S] \to K, \quad f(X_1, \dots, X_n) \mapsto f(s_1, \dots, s_n).$$

Then S is algebraically independent if and only if this map is injective. Since algebraically dependent subsets are necessarily nonempty, it follows that the empty subset $\varnothing$ is algebraically independent. A singleton $\{\alpha\} \subseteq E$ is algebraically dependent if α is algebraic over K. If $\{\alpha\}$ is algebraically independent, then α is transcendental over K, in which case $K(\alpha) \cong K(X)$. The following lemma extends the second case in Proposition 1.1.2.3.

Lemma 1.4.1.2. *Let E/K be a purely transcendental extension with $S = \{s_1, \dots, s_n\}$ is a finite algebraically independent subset. If $K(X_1, \dots, X_n)$ is the function field with indeterminates $X_1, \dots, X_n$, then there is an isomorphism $K(X_1, \dots, X_n) \cong E$ with $X_i \mapsto s_i$ for all i.*

Proof. The bijection $X = \{X_1, \dots, X_n\} \to S$ given by $X_i \mapsto s_i$ extends to an isomorphism $K[X_1, \dots, X_n] \cong K[s_1, \dots, s_n]$, which in turn extends to an isomorphism of fraction fields. □

We can now improve Lemma 1.4.1.2 by removing the finiteness hypothesis.

Theorem 1.4.1.3. *Let E/K be a purely transcendental extension; that is, $E = K(S)$, where S is an algebraically independent subset. Then $E \cong K(X)$, the function field with indeterminates X, where $|X| = |S|$, via an isomorphism $\varphi : K(X) \to E$ with $\varphi(X) \in S$ for all $x \in X$.*

Proof. By the well ordering principle, we may assume that S is well-ordered. Now let X be a set equipped with a bijection $h : X \to S$; we may assume that X is well-ordered by defining $x \leq y$ to mean $h(x) \leq h(y)$. If $y \in X$, define

$$X_y = \{x \in X : x \leq y\} \quad S_y = \{h(x) \in S : x \leq y\}.$$

We prove by transfinite induction that there are isomorphisms $\varphi_y : K(X_y) \to K(S_y)$ with $\varphi_y(x) = h(x)$ for all $x \leq y$ and with φ_{y_2} extending φ_{y_1} whenever $y_1 \leq y_2$. This will suffice, for $K(X) = \bigcup_{y \in X} K(X_y)$ and $E = K(S) = \bigcup_{y \in X} K(S_y)$.

The base step was proved in Lemma 1.4.1.2 with $E = K(S_y) = K(y)$, where y is the smallest element in S. The inductive step wants an isomorphism $\varphi_z : K(X_z) \to K(S_z)$ with $y \mapsto h(y)$ for all $y \leq z$. If z is a successor, say z is the next index after y, then $K(X_y)(z) = K(X_z)$, and Lemma 1.4.1.2 gives an isomorphism $K(X_y)(z) \to K(S_y)(h(z))$. If z is a limit, observe that the family of subfields $K(X_y)$ for all $y < z$ is an increasing chain, and so $K_* = \bigcup_{y<z} K(X_y)$ is a field; similarly, $E_* = \bigcup_{y<z} K(S_y)$ is a field. If $y_1 \leq y_2 < z$, then the isomorphism φ_{y_2} extends φ_{y_1}, so that $\bigcup_{y<z} \varphi_y$ is a (well-defined) isomorphism from K_* to E_*. As the isomorphisms φ_y agree whenever possible, they can be assembled to an isomorphism $\varphi_z : K(X_z) \to K(S_z)$. This finishes the induction process and hence the proof. □

Recall that if V is a vector space and $S = \{v_1, \dots, v_n\}$ is a subset in V, then S is linearly dependent if and only if some v_i is in the subspace spanned by the others. Here is an analog of this for algebraic dependence.

Proposition 1.4.1.4. *Let E/K be an extension field. Then $S \subseteq E$ is algebraically dependent over K if and only if there is $s \in S$ with s is algebraic over $K(S \setminus \{s\})$.*

Proof. If S is algebraically dependent over K, then there is a finite algebraically dependent subset $\{s_1, \dots, s_n\} \subseteq S$; thus, we may assume that S is finite. We prove, by induction on n, that some s_i is algebraic over $K(S \setminus \{s_i\})$.

If $n = 1$, then there is some nonzero $f(X) \in K[X]$ with $f(s_1) = 0$; that is, s_1 is algebraic over K. But $S \setminus \{s_1\} = \varnothing$, and so s_1 is algebraic over $K(S \setminus \{s_1\}) = K(\varnothing) = K$.

For the inductive step, let $S = \{s_1, \dots, s_{n+1}\}$ be algebraically dependent. We may assume that $\{s_1, \dots, s_n\}$ is algebraically independent (otherwise, the inductive hypothesis gives some s_j, for $1 \leq j \leq n$, which is algebraic over $K(s_1, \dots, \widehat{s_j}, \dots, s_n)$ and, hence, algebraic over $K(S \setminus \{s_j\})$). Since S is algebraically dependent, there is a nonzero $f(X_1, \dots, X_n, Y)$ in $K[X_1, \dots, X_n, Y]$ with $f(s_1, \dots, s_n, s_{n+1}) = 0$. We may write

$$f(X_1, \dots, X_n, Y) = \sum_i g_i(X_1, \dots, X_n)Y^i$$

where $g_i \in K[X_1, \dots, X_n]$. Since $f(X_1, \dots, X_n, Y) \neq 0$, some $g_i(X_1, \dots, X_n) \neq 0$, and it follows from the algebraic independence of $\{s_1, \dots, s_n\}$ that $g_i(s_1, \dots, s_n) \neq 0$. Therefore, $h(Y) = \sum_i g_i(s_1, \dots, s_n)Y^i \in K(S)[Y]$ is not the zero polynomial. But $h(s_{n+1}) = f(s_1, \dots, s_n, s_{n+1}) = 0$, so that un+1 is algebraic over $K(s_1, \dots, s_n)$.

For the converse, assume that s is algebraic over $K(S \setminus \{s\})$. We may assume that $S \setminus \{s\}$ is finite. We prove, by induction on $n = |S|$, that S is algebraically dependent.

If $n = 1$, then $S = \{s\}$, and s is algebraic over K. Therefore S is algebraically dependent. For the inductive step, let $S = \{s_1, \dots, s_{n+1}\}$, and we may assume that s_{n+1} is algebraic over $K(\{s_1, \dots, s_n\})$. We may assume that $\{s_1, \dots, s_n\}$ is algebraically independent, since otherwise S, as a superset of it, is also algebraically dependent. By hypotheses, there is a nonzero polynomial $f(Y) = \sum_i c_i Y^i \in K(s_1, \dots, s_n)[Y]$ with $f(s_{n+1}) = 0$. As $f(Y) \neq 0$, we may assume that at least one of its coefficients is nonzero. For all i, the coefficient $c_i \in K(s_1, \dots, s_n)$, so there are rational functions $c_i(X_1, \dots, X_n)$ with $c_i(s_1, \dots, s_n) = c_i$ (because $K(s_1, \dots, s_n) \cong K(X_1, \dots, X_n)$, the function field in n variables). Since $f(s_{n+1}) = 0$, we may clear denominators and assume that each $c_i(X_1, \dots, X_n)$ is a polynomial in $K[x_1, \dots, x_n]$. Moreover, that some $c_i(s_1, \dots, s_n) \neq 0$ implies $c_i(s_1, \dots, s_n) \neq 0$. Hence

$$c(X_1, \dots, X_n, Y) = \sum_i c_i(X_1, \dots, X_n)Y^i \in K[X_1, \dots, X_n, Y]$$

is nonzero and vanishes on $(s_1, \dots, s_{n+1})$; therefore, $S = \{s_1, \dots, s_{n+1}\}$ is algebraically dependent. □

There is a strong parallel between linear dependence in a vector space and algebraic dependence in a field. The analog of a basis in a vector space is a transcendental basis in a field; the analog of dimension is transcendence degree. In fact, both discussions are special cases of theorems about **dependence relations**.

Let E/K be an extension field. If $\alpha \in E$ and $S \subseteq E$, then α is **dependent on S**, denoted by

$$\alpha \preceq S,$$

if α is algebraic over $K(S)$, the subfield of E generated by K and S.

Proposition 1.4.1.5. *Let E/K be an extension field, let $\alpha \in E$, and let $S \subseteq E$.*

(i) *(**Reflexivity**) If $\alpha \in S$, then $\alpha \preceq S$.*

(ii) *(**Compactness**) If $\alpha \in S$, then there exists a finite subset $S_0 \subseteq S$ with $\alpha \preceq S_0$.*

(iii) *(**Transitivity**) Let $T \subseteq E$; if $\alpha \in S$ and each element of S is dependent on T, then α is dependent on T.*

(iv) *(**Exchange Property**) If α is dependent on $S \cup \{\beta\}$ but not on S, then β is dependent on $S \cup \{\alpha\}$ but not on S.*

Proof. It is easy to check (i) and (ii). We now verify (iii). If $\alpha \preceq S$, then α is algebraic over $K(S)$. Suppose there is some $T \subseteq E$ with $s \preceq T$ for every $s \in S$; then it follows from Theorem 1.1.2.20 that $K(T) \subseteq K(S)(T)$ is an algebraic extension. Since α is algebraic over $K(S)$ and hence $K(S)(T)$, it is then algebraic over $K(T)$. That is, α is dependent on T.

Let us verify (iv). The exchange property assumes that $\alpha \preceq S \cup \{\beta\}$ (that is, α is algebraic over $K(S \cup \{\beta\})$) and α is transcendental over $K(S\setminus)$. We first note that $\beta \not\preceq S$: otherwise β is algebraic over $K(S)$, and hence $K(S) \subseteq K(S \cup \{\beta\})$ is algebraic. But this implies α is algebraic over $K(S)$, which contradicts the hypothesis. Now since $K(S \cup \{\beta\}) = K(S)(\beta)$, we conclude from Proposition 1.4.1.4 that $\{\alpha, \beta\}$ is algebraic dependent over $K(S)$. Thus there is a nonzero polynomial $f(X, Y) \in K(S)[X, Y]$ with $f(\alpha, \beta) = 0$. In more detail, $f(X, Y) = g_0(X) + g_1(X)Y + \cdots + g_n(X)Y^n$, where $g_i(X) \in K(S)[X]$. Define $h(Y) = f(\alpha, Y) = \sum_i g^i(\alpha)Y^i \in K(S, \alpha)[Y]$. Since α is not dependent on S, $h(Y)$ is not the zero polynomial. But $h(\beta) = f(\alpha, \beta) = 0$, so β is dependent on $S \cup \{\alpha\}$. □

Returning to extension fields E/K, by Proposition 1.4.1.4 a nonempty subset $S \subseteq E$ is algebraically independent if and only if $s \not\preceq S \setminus \{s\}$ for all $s \in S$. It follows that every subset of an algebraically independent set is itself algebraically independent.

Definition 1.4.1.6. If E/K is an extension field, then a subset $S \subseteq E$ **generates** E if $x \preceq S$ for all $x \in E$. Or equivalently, if E is algebraic over $K(S)$. A **transcendental basis** is a maximal algebraically independent subset of E over K.

Lemma 1.4.1.7. *Let E/K be an extension field. If $S \subseteq E$ is algebraically independent over K and $\alpha \in E$ is transcendental over $K(S)$, then $S \cup \{\alpha\}$ is algebraically independent.*

Proof. Since $\alpha \not\preceq S$, Proposition 1.4.1.5(i) gives $\alpha \notin S$, and so $S \subsetneq S \cup \{\alpha\}$. If $S \cup \{\alpha\}$ is algebraically dependent, then there exists $s \in S \cup \{\alpha\}$ with $s \preceq (S \cup \{\alpha\}) \setminus \{s\}$. If $s = \alpha$, then $(S \cup \{\alpha\}) \setminus \{s\} = S$, contradicting $\alpha \not\preceq S$. Therefore, $s \in S$. Since S is algebraically independent, $s \not\preceq S \setminus \{s\}$. Combining with the observation $(S \cup \{\alpha\}) \setminus \{s\} = (S \setminus \{s\}) \cup \{\alpha\}$, we obtain

$$s \preceq (S \setminus \{s\}) \cup \{\alpha\}, \quad s \not\preceq S \setminus \{s\}.$$

Therefore it follows from the exchange property that $\alpha \preceq (S \setminus \{s\}) \cup \{s\} = S$, contradicting the hypothesis. Therefore $S \cup \{\alpha\}$ is algebraically independent. □

Note that Lemma 1.4.1.7 implies that a if S is a transcendental basis of E, then S automatically generates E: there is no element in E that is transcendental over $K(S)$. We now prove that every algebraically independent set in E can be extended to a maximal algebraically independent set, and hence a transcendantal basis for E.

Theorem 1.4.1.8. *If E/K is an extension field, then E has a transcendental basis. In fact, every algebraically independent subset is part of a transcendental basis.*

Proof. Let S be an algebraically independent subset of E. We use Zorn's Lemma to prove the existence of maximal algebraically independent subsets of E containing S. Let $\mathcal{X}$ be the family of all algebraically independent subsets of E containing S, partially ordered by inclusion. Note that X is nonempty, for $S \in \mathcal{X}$. Suppose that $\mathcal{S} = (S_\alpha)_{\alpha \in A}$ is a chain in $\mathcal{X}$. It is clear that $S^* = \bigcup_{\alpha \in A} S_\alpha$ is an upper bound of $\mathcal{S}$ if it lies in $\mathcal{X}$, that is, if S^* is algebraically independent. If, on the contrary, S^* is algebraically dependent, then there is $s \in S^*$ with $s \preceq S^* \setminus \{s\}$. By the compactness property, there is a finite subset $\{s_1, \ldots, s_n\} \subseteq S^* \setminus \{s\}$ with $s \preceq \{s_1, \ldots, s_n\}$. Now there is $S_0 \in \mathcal{S}$ with $s \in S_0$, and, for each i with $1 \le i \le n$, there is S_{α_i} with $s_i \in S_{\alpha_i}$. Since $\mathcal{S}$ is a chain, one of these, call it S', contains all the others, and the algebraically dependent set $\{s, s_1, \ldots, s_n\}$ is contained in S'. But since S' is algebraically independent, so are its subsets, and this is a contradiction. Zorn's Lemma now provides a maximal element M of $\mathcal{X}$; that is, M is a maximal algebraically independent subset of E containing S. If M is not a basis, then there exists $\alpha \in E$ with $\alpha \not\preceq M$. By Lemma 1.4.1.7, $M \cup \{\alpha\}$ is an algebraically independent set strictly larger than M, contradicting the maximality of M. □

Theorem 1.4.1.9. *If E/K be a field extension. Then a subset $S \subseteq E$ is a transcendental basis for E/K if and only if S is algebraically independent and $E/K(S)$ is algebraic.*

Proof. One direction is clear from our observation, so assume that $S \subseteq E$ is auch that $K(S)/K$ is purely transcendental and $E/K(S)$ is algebraic. By definition, this means S is an algebraically independent set, and that S is maximal. Therefore S is a transcendental basis for E. □

We now prove an important theorem about the cardinality of a transcendental basis for E. It allows us to define the "dimension" of a transcendental extension.

Theorem 1.4.1.10. *Let E/K be a field extension. Then any transcendental basis of E over K has the same cardinality.*

Proof. Let S and T be two transcendantal basis for E over K. If $S = \varnothing$, we claim that $T = \varnothing$. Otherwise, there exists $t \in T$. We have $t \preceq S$ since S generates E and $\varnothing \subseteq T \setminus \{t\}$, so that transitivity gives $t \preceq T \setminus \{t\}$, a contradiction since T is algebraically independent. Therefore, we may assume that both S and T are nonempty.

Now assume that S is finite; say, $S = \{s_1, \ldots, s_n\}$. We claim that some $t_1 \in T$ is transcendental over $K(s_2, \ldots, s_n)$. Assume the contrary, then every element in T is algebraic over $K(s_2, \ldots, s_n)$, whence $K(s_2, \ldots, s_n)(T)$ is algebraic over $K(s_2, \ldots, s_n)$ by Theorem 1.1.2.20. Since E is algebraic over

$K(T)$, it is necessarily algebraic over $K(T)(s_2,\dots,s_n) = K(s_2,\dots,s_n)(T)$. Therefore E is algebraic over $K(s_2,\dots,s_n)$ by Corollary 1.1.2.19. In partial, s_1 is algebraic over $K(s_2,\dots,s_n)$. But S is algebraically independent over K, this is a contradiction. Thus some $t_1 \in T$ must be transcendental over $K(s_2,\dots,s_n)$, and consequently $\{t_1,s_2,\dots,s_n\}$ is algebraic independent by Lemma 1.4.1.7.

Now if s_1 were transcendental over $K(t_1,s_2,\dots,s_n)$, then $\{t_1,s_1,s_2,\dots,s_n\}$ is algebraic independent over K, which is impossible since S is a maximal algebraically independent set. consequently, $K(S)(t_1) = K(t_1,s_2,\dots,s_n)(s_1)$ is algebraic over $K(t_1,s_2,\dots,s_n)$, whence E is algebraic over $K(t_1,s_2,\dots,s_n)$ (Theorem 1.4.1.9). Therefore $\{t_1,s_2,\dots,s_n\}$ is a transcendental basis for E by Theorem 1.4.1.9.

A similar argument shows that some $t_2 \in T$ is transcendental over $K(t_1,s_3,\dots,s_n)$, and hence $\{t_1,t_2,s_3,\dots,s_n\}$ is a transcendental basis for E. Repeating this process we eventually obtain $t_1,\dots,t_n \in T$ such that $\{t_1,\dots,t_n\}$ is a transcendantal basis for E over K. This implies $T = \{t_1,\dots,t_n\}$ and therefore $|T| = |S|$.

Finally, we assume that S is infinite. Then by the argument above, T must also be infinite. If $s \in S$, then s is algebraic over $K(T)$. The coefficients of the minimal polynomial f of s over $K(T)$ all lie in $K(T_s)$ for some finite subset $T_s \subseteq T$. Consequently, $f \in K(T_s)[X]$ and s is algebraic over $K(T_s)$. Choose such a finite set T_s for each s. We claim that $T = \bigcup_{s\in S} T_s$. In fact, if $t \in T \setminus \{T_s\}$, then for any $s \in S$ we have $T_s \subseteq T \setminus \{t\}$ and thus

$$s \preceq T_s \preceq T \setminus \{t\}.$$

This then implies $t \preceq S \preceq T \setminus \{t\}$, which contradicts the algebraically independence of T. With this, we conclude

$$|T| = \left|\bigcup_{s\in S} T_s\right| \le \aleph_0 \cdot |S| = |S|.$$

Reversing the roles of S and T shows that $|S| = |T|$. □

Definition 1.4.1.11. Let E/K be a field extension, the **transcendental degree of E/K** is defined by

$$\operatorname{tr.deg}(E/K) = |S|$$

where $|S|$ is any transcendental degree for E over K.

Proposition 1.4.1.12 (Additivity of transcendental degree). *Let $K \subseteq E \subseteq F$ be field extensions. Then*

$$\operatorname{tr.deg}(F/K) = \operatorname{tr.deg}(F/E) + \operatorname{tr.deg}(E/K).$$

Proof. Let S be a transcendental besis of E over K, and T be that of F over E. Since $S \subseteq E$, $S \cap T = \varnothing$. It suffices if we show $S \cup T$ is a transcendental basis of F over K.

First of all, E is algebraic over $K(S)$ by Theorem 1.4.1.9, and hence over $K(S \cup T)$. Thus $K(S \cup T)(E)$ is algebraic over $K(S \cup T)$ by Theorem 1.1.2.20. Since

$$K(S \cup T) = K(S)(T) \subseteq E(T) \subseteq K(S \cup T)(E),$$

it follows from Corollary 1.1.2.19that $E(T)$ is algebraic over $K(S \cup T)$. Since F is algebraic over $E(T)$ by Theorem 1.4.1.9, we conclude that F is algebraic over $K(S \cup T)$. Now we only need to prove $S \cup T$ is algebraically independent.

Suppose there is a polynomial $f(X_1,\dots,X_n,Y_1,\dots,Y_m)$ such that

$$f(s_1,\dots,s_n,t_1,\dots,t_m) = 0$$

for some $s_1,\dots,s_n \in S$, $t_1,\dots,t_m \in T$. Since S and T are both algebraically independent, the coefficients of s_i, t_j are not trivial. Then we can write

$$h(Y_1,\dots,Y_m) := f(s_1,\dots,s_n,Y_1,\dots,Y_m) \in K(S)[Y_1,\dots,Y_m]$$

satisfies $h(t_1,\dots,t_m) = 0$. Since $s_1,\dots,s_n \in E$, this means T is not algebraically independent over E, which is an contradiction. □

Now we use Proposition 1.4.1.12 to prove the following useful result.

Proposition 1.4.1.13. *Let $K \subseteq E \subseteq L$ be field extensions and suppose that E/K is algebraic. If $S \subseteq L$ is algebraically independent over K, then S is also algebraically independent over E. In other words, L remains algebraically independent over any algebraic extension of the base field.*

Proof. Since $K \subseteq E$ is algebraic, so is the extension $K(S) \subseteq E(S)$. Now, by Proposition 1.4.1.12,

$$\operatorname{tr.deg}(E(S)/E) + \operatorname{tr.deg}(E/K) = \operatorname{tr.deg}(E(S)/K) = \operatorname{tr.deg}(E(S)/K(S)) + \operatorname{tr.deg}(K(S)/K)$$

and so

$$\operatorname{tr.deg}(E(S)/E) = \operatorname{tr.deg}(K(S)/K) = |S|$$

which shows that S must be a transcendence basis for L over E. □

1.4.2 Simple transcendantal extension and Lüroth's theorem

The class of purely transcendental extensions is much less well behaved than the class of algebraic extensions. For example, let α be transcendental over K. Then in the tower $K \subseteq K(\alpha^2) \subseteq K(\alpha)$, the extension $K \subseteq K(\alpha)$ is purely transcendental (and simple) but the second step $K(\alpha^2) \subseteq K(\alpha)$ is not transcendental at all. In addition, if $K \subseteq L$ is purely transcendental and $K \subseteq E \subseteq L$, it does not necessarily follow that the extension L/E is purely transcendental.

However, there is a famous theorem about the simple extension $K \subseteq K(X)$ which identify every intermediate field of this extension. We now prove this theorem to illustrate some of the apparent complexities in dealing with transcendental extensions.

We first consider the automorphism group $\operatorname{Aut}_K(K(X))$. A rational function $\varphi \in K(X)$ is called a **linear fractional transformation** if

$$\varphi = \frac{aX+b}{cX+d}$$

where $a, b, c, d \in K$ and $ad - bc \neq 0$. The function φ can be viewed as a automorphism on $K(X)$ just by sending x to φ. The linear fractional transformations turns out to be the whole groups $\operatorname{Aut}_K(K(X))$. To prove this, we need the following definition.

Definition 1.4.2.1. If $\varphi \in K(X)$ is in lowest terms, then $\varphi = g(X)/h(X)$, where $g(X), h(X) \in K[X]$ and $\gcd(g, h) = 1$. Define the **degree** of φ by

$$\deg(\varphi) = \max\{\deg(g), \deg(h)\}.$$

Now $\varphi \in K(X)$ has height 0 if and only if φ is a constant (that is, $\varphi \in K$), while φ has height 1 if and only if φ is a linear fractional transformation.

Proposition 1.4.2.2. *Let K be a field, let $\varphi = g(X)/h(X) \in K(X)$ be nonconstant, where $g(X) = \sum_i a_i X^i$, $h(X) = \sum_i b_i X^i$, and $\gcd(g, h) = 1$. Then*

(i) φ is transcendental over K.

(ii) $K(X)$ is a finite extension of $K(\varphi)$;

(iii) the minimal polynomial of X over $K(\varphi)$ is $\theta(Y)$, where

$$\theta(Y) = g(Y) - \varphi h(Y) \in K(\varphi)[Y]$$

and therefore $[K(X) : K(\varphi)] = \deg(\varphi)$.

Proof. Let us describe $\theta(Y)$ in more detail (we allow some coefficients of g and h to be zero, so that even though we use the same index i of summation, we are not assuming that g and h have the same degree). We have

$$\theta(Y) = g(Y) - \varphi h(Y) = \sum_i (a_i - \varphi b_i) Y^i.$$

If $\theta(Y)$ is the zero polynomial, then all its coefficients are 0. But h is not the zero polynomial (being the denominator of φ), so h has some nonzero coefficient, say b_i. If the i-th coefficient $a_i - \varphi b_i$ of θ is 0, then $\varphi = a_i/b_i$, contradicting φ not being a constant; thus, $\theta \neq 0$. We compute $\deg(\theta)$:

$$\deg(\theta) = \deg(g(Y) - \varphi h(Y)) = \max\{\deg(g), \deg(h)\} = \deg(\varphi).$$

Now X is a root of θ, because $\varphi = g/h$; therefore x is algebraic over $K(\varphi)$ and $K(X)/K(\varphi)$ is a finite extension field.

Were φ algebraic over K, then $K(\varphi)/K$ would be finite, and so

$$[K(X):K] = [K(X):K(\varphi)][K(\varphi):K]$$

is also finite, a contradiction. Therefore, φ is transcendental over K. Thus we have verifed statements (i) and (ii).

We claim that $\theta(Y)$ is an irreducible polynomial in $K(\varphi)[Y]$. If not, then $\theta(Y)$ factors in $K[\varphi][Y] = K[Y][\varphi]$, by Gauss's Lemma. But $\theta(Y) = g(Y) - \varphi h(Y)$ is of degree one in φ, and $\gcd(g,h) = 1$, so it is irreducible in $K[Y][\varphi]$, contradiction. Finally, since $\deg(\theta) = \deg(\varphi)$, we have $[K(X):K(\varphi)] = \deg(\varphi)$. □

Corollary 1.4.2.3. *Let $\varphi \in K(X)$, where $K(X)$ is the field of rational functions over a field K. Then $K(\varphi) = K(X)$ if and only if φ is a linear fractional transformation.*

Define a map $\rho : \mathrm{GL}(n,K) \to \mathrm{Aut}_K(K(X))$ by

$$\rho : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{aX+b}{cX+d}$$

It is easily checked that ρ is a homomorphism of groups: If $\varphi : x \mapsto (aX+b)/(cX+d)$ and $\psi : X \mapsto (rX+s)/(tX+u)$, then

$$\sigma\begin{pmatrix} r & s \\ t & u \end{pmatrix}\sigma\begin{pmatrix} a & b \\ c & d \end{pmatrix}(X) = (\psi\circ\varphi)(X) = \frac{r\varphi+s}{t\varphi+u} = \frac{\frac{r(aX+b)}{cX+d}+s}{\frac{t(aX+b)}{cX+d}+u} = \frac{r(aX+b)+s(cX+d)}{t(aX+b)+u(cX+d)}$$
$$= \frac{(ra+sc)X+(rb+sd)}{(ta+uc)X+(tb+bd)} = \sigma\Big(\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Big)(X).$$

It is clear that the $\ker\rho = Z(2,K)$, the center of $\mathrm{GL}(n,K)$ consisting of all nonzero 2×2 scalar matrices. Hence, if

$$\mathrm{PGL}(2,K) = \mathrm{GL}(2,K)/Z(2,K)$$

then $\mathrm{Aut}_K(K(X)) \cong \mathrm{PGL}(2,K)$.

Corollary 1.4.2.4. *If $K(X)$ is the field of rational functions over a field K, then* $\mathrm{Aut}_K(K(X)) = \mathrm{PGL}(2,K)$.

We now prove Lüroth's Theorem which classifies all the intermediate fields $K \subsetneq E \subseteq K(X)$, where X is transcendental over K; the proof is essentially a converse of that of Proposition 1.4.2.2.

Lemma 1.4.2.5. *Let K be a field, and let*

$$I(X,Y) = Y^n + \frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + \frac{g_0(X)}{h_0(X)} \in K(X)[Y]$$

where each g_i/h_i is in lowest terms. If $I^*(X,Y) \in K[X][Y]$ is the associated primitive polynomial of I, then

$$\max\{\deg(g_i/h_i)\} \leq \deg_X(I^*),$$

where $\deg_X(I^*)$ *is the highest power of X occurring in I^*.*

Proof. The associated primitive polynomial is then,

$$I^* = cI(X,Y) = cY^n + c\frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + c\frac{g_0(X)}{h_0(X)} \in K[X,Y],$$

where $c = \mathrm{lcm}(h_0, h_1, \ldots, h_{n-1})$. Since c is the lcm, there are $u_i \in K[X]$ with $c = u_i h_i$ for all i. Hence, each coefficient $c(g_i/u_i) = u_i g_i \in K[X]$. Thus

$$\deg_X(I^*) = \max\{\deg(c), \deg(c(g_i/h_i))\} = \max\{\deg(c), \deg(u_i g_i)\}.$$

Now $h_i \mid c$ for all i, so that $\deg(h_i) \leq \deg(c)$. Also, $\deg(g_i) \leq \deg(u_i g_i)$. We conclude that

$$\max_i\{\deg(g_i), \deg(h_i)\} \leq \deg_X(I^*).$$

and this completes the proof. □

Theorem 1.4.2.6 (Lüroth's Theorem). *If $K(X)$ is a simple transcendental extension, then every intermediate field E with $E \neq K$ is also a simple transcendental extension of K: there is $\varphi \in K$ with $E = K(\varphi)$.*

Proof. If $\beta \in E$ is not constant, then Proposition 1.4.2.2 says that β is transcendental over K, the extension $K(X)/K(\beta)$ is algebraic, and $[K(X) : K(\beta)]$ is finite. As $K(\beta) \subseteq E \subseteq K(X)$, we have

$$[K(X) : K(\beta)] = [K(X) : E][E : K(\beta)],$$

so that $K(X)/E$ is a finite extension field. Let $I(X, Y) \in E[Y]$ be the minimal polynomial of X over E:

$$I(X, Y) = Y^n + b_{n-1}Y^{n-1} + \cdots + b_0 \in K[Y]$$

(where $n = [K(X) : E]$). Each coefficient b_i of $I(X, Y)$ is a rational function lying in E, say, $b_i = g_i(X)/h_i(X)$, where $g_i, h_i \in K[X]$ and $\gcd(g_i, h_i) = 1$. Thus,

$$I(X, Y) = Y^n + \frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + \frac{g_0(X)}{h_0(X)} \in E[Y]. \tag{1.4.2.1}$$

We may assume that $X \notin E$ (otherwise $E = K(X)$ and the theorem is obviously true). It follows that not all the coefficients $b_i = g_i/h_i$ of $I(X, Y)$ lie in K, otherwise X is algebraic over K. Choose an index j such that $b_j = g_j/h_j \notin K$, we simplify notation by omitting the subscript j and defining $\varphi = b_j$, $g(X) = g_j(X)$, and $h(X) = h_j(X)$; thus, $\varphi = g/h \in E$ with $\varphi \notin K$. Define

$$\theta(X, Y) = g(Y) - \varphi h(Y) \in K[Y]. \tag{1.4.2.2}$$

Since $\varphi \neq 0$, we have $\theta(X, Y) \neq 0$. But $\theta(X, X) = 0$, so $I(X, Y) \mid \theta(X, Y)$ over K. In other words, there exists $q(X, Y) \in K[Y]$ such that

$$\theta(X, Y) = q(X, Y)I(X, Y). \tag{1.4.2.3}$$

We are in the setting of Gauss's treatment of UFDs, and we now factor each polynomial as the product of its content and its associated primitive polynomial. We have $c(\theta) = 1/h(X)$ and $\theta = c(\theta)\theta^*$, where

$$\theta^*(X, Y) = h(X)g(Y) - g(X)h(Y) \in E[X][Y].$$

Reversing the roles of X and Y, there is an anti-symmetry: $\theta^*(Y, X) = -\theta^*(X, Y)$, thus

$$\deg_X(\theta^*) = \deg_Y(\theta^*).$$

Taking associated primitive polynomials and using (1.4.2.3), we get

$$\theta^*(X, Y) = q^*(X, Y)I^*(X, Y).$$

and therefore

$$\deg_X(\theta^*) = \deg_X(q^*) + \deg_X(I^*).$$

By Lemma 1.4.2.5, we have $\deg_X(I^*) \geq \deg(\varphi) = \deg_X(\theta^*)$, so that $\deg_X(q^*) = 0$; that is, q^* is a function of Y alone. The anti-symmetry of θ^* says that θ^* is primitive as a polynomial in X. But $\theta^* = q^*I^*$, so we must have $\deg_Y(q^*) = 0$; that is, q^* is a constant. Now take y-degree we get

$$\deg_Y(\theta) = \deg_Y(\theta^*) = \deg_Y(I^*) = \deg_Y(I).$$

This then conclude that $[K(X) : K(\varphi)] = [K(X) : E]$, so the claim follows. □

Bibliography

[AGV06] M. Artin, A. Grothendieck, and J. L. Verdier. *Théorie des Topos et Cohomologie Étale des Schémas. Séminaire de Géométrie Algébrique du Bois-Marie 1963-1964 (SGA 4): Tome 3*. Lecture Notes in Mathematics. Springer, 2006.

[BBD82] A. Beilinson, J. Bernstein, and P. Deligne. "Faisceaux pervers". In: *Astérisque* 100.1 (1982).

[Del77] P. Deligne. *Cohomologie Etale: Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2*. Vol. 569. Lecture Notes in Mathematics. Springer, 1977. ISBN: 978-3-540-08066-4 978-3-540-37507-4.

[Del80] P. Deligne. "La conjecture de Weil: II". In: *Publications Mathématiques de l'IHÉS* 52 (1980), pp. 137–252.

[FK13] E. Freitag and R. Kiehl. *Etale cohomology and the Weil conjecture*. Vol. 13. Springer Science & Business Media, 2013.

[GM77] M. Goresky and R. MacPherson. "La dualité de Poincaré pour les espaces singuliers". In: *CR Acad. Sci.* 284 (1977), pp. 1549–1551.

[GM80] M. Goresky and R. MacPherson. "Intersection homology theory". In: *Topology* 19.2 (1980), pp. 135–162.

[Gro57] A. Grothendieck. "Sur quelques points d'algèbre homologique, I". In: *Tohoku Mathematical Journal* 9 (1957), pp. 119–221.

[Gro77] A. Grothendieck. "Cohomologie ℓ-adique et fonctions L". In: *Séminaire de Géométrie Algébrique du Bois-Marie 1965-66* (1977).

[KS05] M. Kashiwara and P. Schapira. *Categories and Sheaves*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2005.