FIELDS

Contents

1. Introduction

In this chapter, we shall discuss the theory of fields. Recall that a *field* is a ring in which all nonzero elements are invertible. Equivalently, the only two ideals of a field are (0) and (1) since any nonzero element is a unit. Consequently fields will be the simplest cases of much of the theory developed later.

The theory of field extensions has a different feel from standard commutative algebra since, for instance, any morphism of fields is injective. Nonetheless, it turns out that questions involving rings can often be reduced to questions about fields. For instance, any domain can be embedded in a field (its quotient field), and any *local ring* (that is, a ring with a unique maximal ideal; we have not defined this term yet) has associated to it its residue field (that is, its quotient by the maximal ideal). A knowledge of field extensions will thus be useful.

2. Basic definitions

Because we have placed this chapter before the chapter discussing commutative algebra we need to introduce some of the basic definitions here before we discuss these in greater detail in the algebra chapters.

Definition 2.1. A *field* is a nonzero ring where every nonzero element is invertible. Given a field a *subfield* is a subring that is itself a field.

For a field k, we write k^* for the subset $k \setminus \{0\}$. This generalizes the usual notation R^* that refers to the group of invertible elements in a ring R.

Definition 2.2. A *domain* or an *integral domain* is a nonzero ring where 0 is the only zerodivisor.

3. Examples of fields

To get started, let us begin by providing several examples of fields. The reader should recall that if R is a ring and $I \subset R$ an ideal, then R/I is a field precisely when I is a maximal ideal.

Example 3.1 (Rational numbers)**.** The rational numbers form a field. It is called the *field of rational numbers* and denoted $\mathbf{Q}$.

Example 3.2 (Prime fields)**.** If p is a prime number, then $\mathbf{Z}/(p)$ is a field, denoted $\mathbf{F}_p$. Indeed, (p) is a maximal ideal in $\mathbf{Z}$. Thus, fields may be finite: $\mathbf{F}_p$ contains p elements.

Example 3.3. In a principal ideal domain, an ideal generated by an irreducible element is maximal. Now, if k is a field, then the polynomial ring $k[x]$ is a principal ideal domain. It follows that if $P \in k[x]$ is an irreducible polynomial (that is, a nonconstant polynomial that does not admit a factorization into terms of smaller degrees), then $k[x]/(P)$ is a field. It contains a copy of k in a natural way. This is a very general way of constructing fields. For instance, the complex numbers $\mathbf{C}$ can be constructed as $\mathbf{R}[x]/(x^2+1)$.

Example 3.4 (Quotient fields)**.** Recall that, given a domain A, there is an imbedding $A \to F$ into a field F constructed from A in exactly the same manner that $\mathbf{Q}$ is constructed from $\mathbf{Z}$. Formally the elements of F are (equivalence classes of) fractions a/b, $a, b \in A$, $b \neq 0$. As usual $a/b = a'/b'$ if and only if $ab' = ba'$. The field F is called the *quotient field*, or *field of fractions*, or *fraction field* of A. The quotient field has the following universal property: given an injective ring map $\varphi : A \to K$ to a field K, there is a unique map $\psi : F \to K$ making

$$\begin{tikzcd}
F \arrow[r, "\psi"'] & K \\
A \arrow[u] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

commute. Indeed, it is clear how to define such a map: we set $\psi(a/b) = \varphi(a)\varphi(b)^{-1}$ where injectivity of φ assures that $\varphi(b) \neq 0$ if $b \neq 0$.

Example 3.5 (Field of rational functions)**.** If k is a field, then we can consider the field $k(x)$ of rational functions over k. This is the quotient field of the polynomial ring $k[x]$. In other words, it is the set of quotients F/G for $F, G \in k[x]$, $G \neq 0$ with the obvious equivalence relation.

Example 3.6. Let X be a Riemann surface. Let $\mathbf{C}(X)$ denote the set of meromorphic functions on X. Then $\mathbf{C}(X)$ is a ring under multiplication and addition of functions. It turns out that in fact $\mathbf{C}(X)$ is a field. Namely, if a nonzero function $f(z)$ is meromorphic, so is $1/f(z)$. For example, let S^2 be the Riemann sphere; then we know from complex analysis that the ring of meromorphic functions $\mathbf{C}(S^2)$ is the field of rational functions $\mathbf{C}(z)$.

4. Vector spaces

One reason fields are so nice is that the theory of modules over fields (i.e. vector spaces), is very simple.

Lemma 4.1. *If k is a field, then every k-module is free.*

Proof. Indeed, by linear algebra we know that a k-module (i.e. vector space) V has a *basis* $\mathcal{B} \subset V$, which defines an isomorphism from the free vector space on $\mathcal{B}$ to V. □

Lemma 4.2. *Every exact sequence of modules over a field splits.*

Proof. This follows from Lemma 4.1 as every vector space is a projective module. □

This is another reason why much of the theory in future chapters will not say very much about fields, since modules behave in such a simple manner. Note that Lemma 4.2 is a statement about the *category* of k-modules (for k a field), because the notion of exactness is inherently arrow-theoretic, i.e., makes use of purely categorical notions, and can in fact be phrased within a so-called *abelian category.*

Henceforth, since the study of modules over a field is linear algebra, and since the ideal theory of fields is not very interesting, we shall study what this chapter is really about: *extensions* of fields.

5. The characteristic of a field

In the category of rings, there is an *initial object* $\mathbf{Z}$: any ring R has a map from $\mathbf{Z}$ into it in precisely one way. For fields, there is no such initial object. Nonetheless, there is a family of objects such that every field can be mapped into in exactly one way by exactly one of them, and in no way by the others.

Let F be a field. Think of F as a ring to get a ring map $f : \mathbf{Z} \to F$. The image of this ring map is a domain (as a subring of a field) hence the kernel of f is a prime ideal in $\mathbf{Z}$. Hence the kernel of f is either (0) or (p) for some prime number p.

In the first case we see that f is injective, and in this case we think of $\mathbf{Z}$ as a subring of F. Moreover, since every nonzero element of F is invertible we see that it makes sense to talk about $p/q \in F$ for $p, q \in \mathbf{Z}$ with $q \neq 0$. Hence in this case we may and we do think of $\mathbf{Q}$ as a subring of F. One can easily see that this is the smallest subfield of F in this case.

In the second case, i.e., when $\operatorname{Ker}(f) = (p)$ we see that $\mathbf{Z}/(p) = \mathbf{F}_p$ is a subring of F. Clearly it is the smallest subfield of F.

Arguing in this way we see that every field contains a smallest subfield which is either $\mathbf{Q}$ or finite equal to $\mathbf{F}_p$ for some prime number p.

Definition 5.1. The *characteristic* of a field F is 0 if $\mathbf{Z} \subset F$, or is a prime p if $p = 0$ in F. The *prime subfield of* F is the smallest subfield of F which is either $\mathbf{Q} \subset F$ if the characteristic is zero, or $\mathbf{F}_p \subset F$ if the characteristic is $p > 0$.

It is easy to see that if $E \subset F$ is a subfield, then the characteristic of E is the same as the characteristic of F.

Example 5.2. The characteristic of $\mathbf{F}_p$ is p, and that of $\mathbf{Q}$ is 0.

6. Field extensions

In general, though, we are interested not so much in fields by themselves but in field *extensions*. This is perhaps analogous to studying not rings but *algebras* over a fixed ring. The nice thing for fields is that the notion of a "field over another field" just recovers the notion of a field extension, by the next result.

Lemma 6.1. *If F is a field and R is a nonzero ring, then any ring homomorphism $\varphi : F \to R$ is injective.*

Proof. Indeed, let $a \in \operatorname{Ker}(\varphi)$ be a nonzero element. Then we have $\varphi(1) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a) = 0$. Thus $1 = \varphi(1) = 0$ and R is the zero ring. □

Definition 6.2. If F is a field contained in a field E, then E is said to be a *field extension* of F. We shall write E/F to indicate that E is an extension of F.

So if F, F' are fields, and $F \to F'$ is any ring-homomorphism, we see by Lemma 6.1 that it is injective, and F' can be regarded as an extension of F, by a slight abuse of language. Alternatively, a field extension of F is just an F-algebra that happens to be a field. This is completely different than the situation for general rings, since a ring homomorphism is not necessarily injective.

Let k be a field. There is a *category* of field extensions of k. An object of this category is an extension E/k, that is a (necessarily injective) morphism of fields

$$k \to E,$$

while a morphism between extensions E/k and E'/k is a k-algebra morphism $E \to E'$; alternatively, it is a commutative diagram

$$\begin{tikzcd}
E \arrow[rr] & & E' \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

The set of morphisms from $E \to E'$ in the category of extensions of k will be denoted by $\operatorname{Mor}_k(E, E')$.

Definition 6.3. A *tower* of fields $E_n/E_{n-1}/\ldots/E_0$ consists of a sequence of extensions of fields E_n/E_{n-1}, E_{n-1}/E_{n-2}, …, E_1/E_0.

Let us give a few examples of field extensions.

Example 6.4. Let k be a field, and $P \in k[x]$ an irreducible polynomial. We have seen that $k[x]/(P)$ is a field (Example 3.3). Since it is also a k-algebra in the obvious way, it is an extension of k.

Example 6.5. If X is a Riemann surface, then the field of meromorphic functions $\mathbf{C}(X)$ (Example 3.6) is an extension field of $\mathbf{C}$, because any element of $\mathbf{C}$ induces a meromorphic — indeed, holomorphic — constant function on X.

Let F/k be a field extension. Let $S \subset F$ be any subset. Then there is a *smallest* subextension of F (that is, a subfield of F containing k) that contains S. To see this, consider the family of subfields of F containing S and k, and take their intersection; one checks that this is a field. By a standard argument one shows, in fact, that this is the set of elements of F that can be obtained via a finite number of elementary algebraic operations (addition, multiplication, subtraction, and division) involving elements of k and S.

Definition 6.6. Let k be a field. If F/k is an extension of fields and $S \subset F$, we write $k(S)$ for the smallest subfield of F containing k and S. We will say that S *generates the field extension* $k(S)/k$. If $S = \{\alpha\}$ is a singleton, then we write $k(\alpha)$ instead of $k(\{\alpha\})$. We say F/k is a *finitely generated field extension* if there exists a finite subset $S \subset F$ with $F = k(S)$.

For instance, $\mathbf{C}$ is generated by i over $\mathbf{R}$.

Exercise 6.7. Show that $\mathbf{C}$ does not have a countable set of generators over $\mathbf{Q}$.

Let us now classify extensions generated by one element.

Lemma 6.8 (Classification of simple extensions)**.** *If a field extension F/k is generated by one element, then it is k-isomorphic either to the rational function field $k(t)/k$ or to one of the extensions $k[t]/(P)$ for $P \in k[t]$ irreducible.*

We will see that many of the most important cases of field extensions are generated by one element, so this is actually useful.

Proof. Let $\alpha \in F$ be such that $F = k(\alpha)$; by assumption, such an α exists. There is a morphism of rings

$$k[t] \to F$$

sending the indeterminate t to α. The image is a domain, so the kernel is a prime ideal. Thus, it is either (0) or (P) for $P \in k[t]$ irreducible.

If the kernel is (P) for $P \in k[t]$ irreducible, then the map factors through $k[t]/(P)$, and induces a morphism of fields $k[t]/(P) \to F$. Since the image contains α, we see easily that the map is surjective, hence an isomorphism. In this case, $k[t]/(P) \simeq F$.

If the kernel is trivial, then we have an injection $k[t] \to F$. One may thus define a morphism of the quotient field $k(t)$ into F; given a quotient $R(t)/Q(t)$ with $R(t), Q(t) \in k[t]$, we map this to $R(\alpha)/Q(\alpha)$. The hypothesis that $k[t] \to F$ is injective implies that $Q(\alpha) \neq 0$ unless Q is the zero polynomial. The quotient field of $k[t]$ is the rational function field $k(t)$, so we get a morphism $k(t) \to F$ whose image contains α. It is thus surjective, hence an isomorphism. □

7. Finite extensions

If F/E is a field extension, then evidently F is also a vector space over E (the scalar action is just multiplication in F).

Definition 7.1. Let F/E be an extension of fields. The dimension of F considered as an E-vector space is called the *degree* of the extension and is denoted $[F : E]$. If $[F : E] < \infty$ then F is said to be a *finite* extension of E.

Example 7.2. The field $\mathbf{C}$ is a two dimensional vector space over $\mathbf{R}$ with basis $1, i$. Thus $\mathbf{C}$ is a finite extension of $\mathbf{R}$ of degree 2.

Lemma 7.3. *Let $K/E/F$ be a tower of algebraic field extensions. If K is finite over F, then K is finite over E.*

Proof. Direct from the definition. □

Let us now consider the degree in the most important special example, that given by Lemma 6.8, in the next two examples.

Example 7.4 (Degree of a rational function field)**.** If k is any field, then the rational function field $k(t)$ is *not* a finite extension. For example the elements $\{t^n, n \in \mathbf{Z}\}$ are linearly independent over k.

In fact, if k is uncountable, then $k(t)$ is *uncountably* dimensional as a k-vector space. To show this, we claim that the family of elements $\{1/(t-\alpha), \alpha \in k\} \subset k(t)$ is linearly independent over k. A nontrivial relation between them would lead to a contradiction: for instance, if one works over $\mathbf{C}$, then this follows because $\frac{1}{t-\alpha}$, when considered as a meromorphic function on $\mathbf{C}$, has a pole at α and nowhere else. Consequently any sum $\sum c_i \frac{1}{t-\alpha_i}$ for the $c_i \in k^*$, and $\alpha_i \in k$ distinct, would have poles at each of the α_i. In particular, it could not be zero.

Amusingly, this leads to a quick proof of the Hilbert Nullstellensatz over the complex numbers. For a slightly more general result, see Algebra, Theorem 35.11.

Lemma 7.5. *A finite extension of fields is a finitely generated field extension. The converse is not true.*

Proof. Let F/E be a finite extension of fields. Let $\alpha_1, \ldots, \alpha_n$ be a basis of F as a vector space over E. Then $F = E(\alpha_1, \ldots, \alpha_n)$ hence F/E is a finitely generated field extension. The converse is not true as follows from Example 7.4. □

Example 7.6 (Degree of a simple algebraic extension)**.** Consider a monogenic field extension E/k of the form discussed in Example 6.4. In other words, $E = k[t]/(P)$ for $P \in k[t]$ an irreducible polynomial. Then the degree $[E : k]$ is just the degree $d = \deg(P)$ of the polynomial P. Indeed, say

$$P = a_d t^d + a_{d-1} t^{d-1} + \ldots + a_0. \tag{7.6.1}$$

with $a_d \neq 0$. Then the images of $1, t, \ldots, t^{d-1}$ in $k[t]/(P)$ are linearly independent over k, because any relation involving them would have degree strictly smaller than that of P, and P is the element of smallest degree in the ideal (P).

Conversely, the set $S = \{1, t, \ldots, t^{d-1}\}$ (or more properly their images) spans $k[t]/(P)$ as a vector space. Indeed, we have by (7.6.1) that $a_d t^d$ lies in the span of S. Since a_d is invertible, we see that t^d is in the span of S. Similarly, the relation $tP(t) = 0$ shows that the image of t^{d+1} lies in the span of $\{1, t, \ldots, t^d\}$ — by what was just shown, thus in the span of S. Working upward inductively, we find that the image of t^n for $n \geq d$ lies in the span of S.

This confirms the observation that $[\mathbf{C} : \mathbf{R}] = 2$, for instance. More generally, if k is a field, and $\alpha \in k$ is not a square, then the irreducible polynomial $x^2 - \alpha \in k[x]$ allows one to construct an extension $k[x]/(x^2 - \alpha)$ of degree two. We shall write this as $k(\sqrt{\alpha})$. Such extensions will be called *quadratic,* for obvious reasons.

The basic fact about the degree is that it is *multiplicative in towers.*

Lemma 7.7 (Multiplicativity)**.** *Suppose given a tower of fields $F/E/k$. Then*

$$[F : k] = [F : E][E : k]$$

Proof. Let $\alpha_1, \dots, \alpha_n \in F$ be an E-basis for F. Let $\beta_1, \dots, \beta_m \in E$ be a k-basis for E. Then the claim is that the set of products $\{\alpha_i \beta_j, 1 \leq i \leq n, 1 \leq j \leq m\}$ is a k-basis for F. Indeed, let us check first that they span F over k.

By assumption, the $\{\alpha_i\}$ span F over E. So if $f \in F$, there are $a_i \in E$ with

$$f = \sum\nolimits_i a_i \alpha_i,$$

and, for each i, we can write $a_i = \sum b_{ij} \beta_j$ for some $b_{ij} \in k$. Putting these together, we find

$$f = \sum\nolimits_{i,j} b_{ij} \alpha_i \beta_j,$$

proving that the $\{\alpha_i \beta_j\}$ span F over k.

Suppose now that there existed a nontrivial relation

$$\sum\nolimits_{i,j} c_{ij} \alpha_i \beta_j = 0$$

for the $c_{ij} \in k$. In that case, we would have

$$\sum\nolimits_i \alpha_i \left(\sum\nolimits_j c_{ij} \beta_j \right) = 0,$$

and the inner terms lie in E as the β_j do. Now E-linear independence of the $\{\alpha_i\}$ shows that the inner sums are all zero. Then k-linear independence of the $\{\beta_j\}$ shows that the c_{ij} all vanish. □

We sidetrack to a slightly tangential definition.

Definition 7.8. A field K is said to be a *number field* if it has characteristic 0 and the extension $K/\mathbf{Q}$ is finite.

Number fields are the basic objects in algebraic number theory. We shall see later that, for the analog of the integers $\mathbf{Z}$ in a number field, something kind of like unique factorization still holds (though strict unique factorization generally does not!).

8. Algebraic extensions

An important class of extensions are those where every element generates a finite extension.

Definition 8.1. Consider a field extension F/E. An element $\alpha \in F$ is said to be *algebraic* over E if α is the root of some nonzero polynomial with coefficients in E. If all elements of F are algebraic then F is said to be an *algebraic extension* of E.

By Lemma 6.8, the subextension $E(\alpha)$ is isomorphic either to the rational function field $E(t)$ or to a quotient ring $E[t]/(P)$ for $P \in E[t]$ an irreducible polynomial. In the latter case, α is algebraic over E (in fact, the proof of Lemma 6.8 shows that we can pick P such that α is a root of P); in the former case, it is not.

Example 8.2. The field $\mathbf{C}$ is algebraic over $\mathbf{R}$. Namely, if $\alpha = a + ib$ in $\mathbf{C}$, then $\alpha^2 - 2a\alpha + a^2 + b^2 = 0$ is a polynomial equation for α over $\mathbf{R}$.

Example 8.3. Let X be a compact Riemann surface, and let $f \in \mathbf{C}(X) - \mathbf{C}$ any nonconstant meromorphic function on X (see Example 3.6). Then it is known that $\mathbf{C}(X)$ is algebraic over the subextension $\mathbf{C}(f)$ generated by f. We shall not prove this.

Lemma 8.4. *Let $K/E/F$ be a tower of field extensions.*

1. *If $\alpha \in K$ is algebraic over F, then α is algebraic over E.*
2. *If K is algebraic over F, then K is algebraic over E.*

Proof. This is immediate from the definitions. □

We now show that there is a deep connection between finiteness and being algebraic.

Lemma 8.5. *A finite extension is algebraic. In fact, an extension E/k is algebraic if and only if every subextension $k(\alpha)/k$ generated by some $\alpha \in E$ is finite.*

In general, it is very false that an algebraic extension is finite.

Proof. Let E/k be finite, say of degree n. Choose $\alpha \in E$. Then the elements $\{1, \alpha, \dots, \alpha^n\}$ are linearly dependent over E, or we would necessarily have $[E : k] > n$. A relation of linear dependence now gives the desired polynomial that α must satisfy.

For the last assertion, note that a monogenic extension $k(\alpha)/k$ is finite if and only if α is algebraic over k, by Examples 7.4 and 7.6. So if E/k is algebraic, then each $k(\alpha)/k$, $\alpha \in E$, is a finite extension, and conversely. □

We can extract a lemma of the last proof (really of Examples 7.4 and 7.6): a monogenic extension is finite if and only if it is algebraic. We shall use this observation in the next result.

Lemma 8.6. *Let k be a field, and let $\alpha_1, \alpha_2, \dots, \alpha_n$ be elements of some extension field such that each α_i is algebraic over k. Then the extension $k(\alpha_1, \dots, \alpha_n)/k$ is finite. That is, a finitely generated algebraic extension is finite.*

Proof. Indeed, each extension $k(\alpha_1, \dots, \alpha_{i+1})/k(\alpha_1, \dots, \alpha_i)$ is generated by one element and algebraic, hence finite. By multiplicativity of degree (Lemma 7.7) we obtain the result. □

The set of complex numbers that are algebraic over $\mathbf{Q}$ are simply called the *algebraic numbers.* For instance, $\sqrt{2}$ is algebraic, i is algebraic, but π is not. It is a basic fact that the algebraic numbers form a field, although it is not obvious how to prove this from the definition that a number is algebraic precisely when it satisfies a nonzero polynomial equation with rational coefficients (e.g. by polynomial equations).

Lemma 8.7. *Let E/k be a field extension. Then the elements of E algebraic over k form a subextension of E/k.*

Proof. Let $\alpha, \beta \in E$ be algebraic over k. Then $k(\alpha, \beta)/k$ is a finite extension by Lemma 8.6. It follows that $k(\alpha + \beta) \subset k(\alpha, \beta)$ is a finite extension, which implies that $\alpha + \beta$ is algebraic by Lemma 8.5. Similarly for the difference, product and quotient of α and β. □

Many nice properties of field extensions, like those of rings, will have the property that they will be preserved by towers and composita.

Lemma 8.8. *Let E/k and F/E be algebraic extensions of fields. Then F/k is an algebraic extension of fields.*

Proof. Choose $\alpha \in F$. Then α is algebraic over E. The key observation is that α is algebraic over a finitely generated subextension of k. That is, there is a finite set $S \subset E$ such that α is algebraic over $k(S)$: this is clear because being algebraic means that a certain polynomial in $E[x]$ that α satisfies exists, and as S we can take the coefficients of this polynomial. It follows that α is algebraic over $k(S)$. In particular, the extension $k(S, \alpha)/k(S)$ is finite. Since S is a finite set, and $k(S)/k$ is algebraic, Lemma 8.6 shows that $k(S)/k$ is finite. Using multiplicativity (Lemma 7.7) we find that $k(S, \alpha)/k$ is finite, so α is algebraic over k. □

The method of proof in the previous argument — that being algebraic over E was a property that *descended* to a finitely generated subextension of E — is an idea that recurs throughout algebra. It often allows one to reduce general commutative algebra questions to the Noetherian case for example.

Lemma 8.9. *Let E/F be an algebraic extension of fields. Then the cardinality $|E|$ of E is at most* $\max(\aleph_0, |F|)$.

Proof. Let S be the set of nonconstant polynomials with coefficients in F. For every $P \in S$ the set of roots $r(P, E) = \{\alpha \in E \mid P(\alpha) = 0\}$ is finite (details omitted). Moreover, the fact that E is algebraic over F implies that $E = \bigcup_{P \in S} r(P, E)$. It is clear that S has cardinality bounded by $\max(\aleph_0, |F|)$ because the cardinality of a countable product of copies of F has cardinality at most $\max(\aleph_0, |F|)$. Thus so does E. □

Lemma 8.10. *Let E/F be a finite or more generally an algebraic extension of fields. Any subring $F \subset R \subset E$ is a field.*

Proof. Let $\alpha \in R$ be nonzero. Then $1, \alpha, \alpha^2, \ldots$ are contained in R. By Lemma 8.5 we find a nontrivial relation $a_0 + a_1\alpha + \ldots + a_d\alpha^d = 0$. We may assume $a_0 \neq 0$ because if not we can divide the relation by α to decrease d. Then we see that

$$a_0 = \alpha(-a_1 - \ldots - a_d\alpha^{d-1})$$

which proves that the inverse of α is the element $a_0^{-1}(-a_1 - \ldots - a_d\alpha^{d-1})$ of R. □

Lemma 8.11. *Let E/F an algebraic extension of fields. Any F-algebra map $f : E \to E$ is an automorphism.*

Proof. If E/F is finite, then $f : E \to E$ is an F-linear injective map (Lemma 6.1) of finite dimensional vector spaces, and hence bijective. In general we still see that f is injective. Let $\alpha \in E$ and let $P \in F[x]$ be a polynomial such that $P(\alpha) = 0$. Let $E' \subset E$ be the subfield of E generated by the roots $\alpha = \alpha_1, \ldots, \alpha_n$ of P in E. Then E' is finite over F by Lemma 8.6. Since f preserves the set of roots, we find that $f|_{E'} : E' \to E'$. Hence $f|_{E'}$ is an isomorphism by the first part of the proof and we conclude that α is in the image of f. □

9. Minimal polynomials

Let E/k be a field extension, and let $\alpha \in E$ be algebraic over k. Then α satisfies a (nontrivial) polynomial equation in $k[x]$. Consider the set of polynomials $P \in k[x]$ such that $P(\alpha) = 0$; by hypothesis, this set does not just contain the zero polynomial. It is easy to see that this set is an *ideal.* Indeed, it is the kernel of the map

$$k[x] \to E, \quad x \mapsto \alpha$$

Since $k[x]$ is a PID, there is a *generator* $P \in k[x]$ of this ideal. If we assume P monic, without loss of generality, then P is uniquely determined.

Definition 9.1. The polynomial P above is called the *minimal polynomial* of α over k.

The minimal polynomial has the following characterization: it is the monic polynomial, of smallest degree, that annihilates α. Any nonconstant multiple of P will have larger degree, and only multiples of P can annihilate α. This explains the name *minimal.*

Clearly the minimal polynomial is *irreducible.* This is equivalent to the assertion that the ideal in $k[x]$ consisting of polynomials annihilating α is prime. This follows from the fact that the map $k[x] \to E, x \mapsto \alpha$ is a map into a domain (even a field), so the kernel is a prime ideal.

Lemma 9.2. *The degree of the minimal polynomial is* $[k(\alpha) : k]$.

Proof. This is just a restatement of the argument in Lemma 6.8: the observation is that if P is the minimal polynomial of α, then the map

$$k[x]/(P) \to k(\alpha), \quad x \mapsto \alpha$$

is an isomorphism as in the aforementioned proof, and we have counted the degree of such an extension (see Example 7.6). □

So the observation of the above proof is that if $\alpha \in E$ is algebraic, then $k(\alpha) \subset E$ is isomorphic to $k[x]/(P)$.

10. Algebraic closure

The "fundamental theorem of algebra" states that **C** is algebraically closed. A beautiful proof of this result uses Liouville's theorem in complex analysis, we shall give another proof (see Lemma 23.1).

Definition 10.1. A field F is said to be *algebraically closed* if every algebraic extension E/F is trivial, i.e., $E = F$.

This may not be the definition in every text. Here is the lemma comparing it with the other one.

Lemma 10.2. *Let F be a field. The following are equivalent*

(1) *F is algebraically closed,*
(2) *every irreducible polynomial over F is linear,*
(3) *every nonconstant polynomial over F has a root,*
(4) *every nonconstant polynomial over F is a product of linear factors.*

Proof. If F is algebraically closed, then every irreducible polynomial is linear. Namely, if there exists an irreducible polynomial of degree > 1, then this generates a nontrivial finite (hence algebraic) field extension, see Example 7.6. Thus (1) implies (2). If every irreducible polynomial is linear, then every irreducible polynomial has a root, whence every nonconstant polynomial has a root. Thus (2) implies (3).

Assume every nonconstant polynomial has a root. Let $P \in F[x]$ be nonconstant. If $P(\alpha) = 0$ with $\alpha \in F$, then we see that $P = (x - \alpha)Q$ for some $Q \in F[x]$ (by division with remainder). Thus we can argue by induction on the degree that any nonconstant polynomial can be written as a product $c \prod (x - \alpha_i)$.

Finally, suppose that every nonconstant polynomial over F is a product of linear factors. Let E/F be an algebraic extension. Then all the simple subextensions $F(\alpha)/F$ of E are necessarily trivial (because the only irreducible polynomials are linear by assumption). Thus $E = F$. We see that (4) implies (1) and we are done. □

Now we want to define a "universal" algebraic extension of a field. Actually, we should be careful: the algebraic closure is *not* a universal object. That is, the algebraic closure is not unique up to *unique* isomorphism: it is only unique up to isomorphism. But still, it will be very handy, if not functorial.

Definition 10.3. Let F be a field. An *algebraic closure* of F is a field $\overline{F}$ containing F such that:

(1) $\overline{F}$ is algebraic over F.
(2) $\overline{F}$ is algebraically closed.

If F is algebraically closed, then F is its own algebraic closure. We now prove the basic existence result.

Theorem 10.4. *Every field has an algebraic closure.*

The proof will mostly be a red herring to the rest of the chapter. However, we will want to know that it is *possible* to embed a field inside an algebraically closed field, and we will often assume it done.

Proof. Let F be a field. By Lemma 8.9 the cardinality of an algebraic extension of F is bounded by $\max(\aleph_0, |F|)$. Choose a set S containing F with $|S| > \max(\aleph_0, |F|)$. Let's consider triples (E, σ_E, μ_E) where

(1) E is a set with $F \subset E \subset S$, and
(2) $\sigma_E : E \times E \to E$ and $\mu_E : E \times E \to E$ are maps of sets such that (E, σ_E, μ_E) defines the structure of a field extension of F (in particular $\sigma_E(a, b) = a +_F b$ for $a, b \in F$ and similarly for μ_E), and
(3) E/F is an algebraic field extension.

The collection of all triples (E, σ_E, μ_E) forms a set I. For $i \in I$ we will denote $E_i = (E_i, \sigma_i, \mu_i)$ the corresponding field extension to F. We define a partial ordering on I by declaring $i \leq i'$ if and only if $E_i \subset E_{i'}$ (this makes sense as E_i and $E_{i'}$ are subsets of the same set S) and we have $\sigma_i = \sigma_{i'}|_{E_i \times E_i}$ and $\mu_i = \mu_{i'}|_{E_i \times E_i}$, in other words, $E_{i'}$ is a field extension of E_i.

Let $T \subset I$ be a totally ordered subset. Then it is clear that $E_T = \bigcup_{i \in T} E_i$ with induced maps $\sigma_T = \bigcup \sigma_i$ and $\mu_T = \bigcup \mu_i$ is another element of I. In other words every totally order subset of I has a upper bound in I. By Zorn's lemma there exists a maximal element (E, σ_E, μ_E) in I. We claim that E is an algebraic closure. Since by definition of I the extension E/F is algebraic, it suffices to show that E is algebraically closed.

To see this we argue by contradiction. Namely, suppose that E is not algebraically closed. Then there exists an irreducible polynomial P over E of degree > 1, see Lemma 10.2. By Lemma 8.5 we obtain a nontrivial finite extension $E' = E[x]/(P)$. Observe that E'/F is algebraic by Lemma 8.8. Thus the cardinality of E' is $\leq \max(\aleph_0, |F|)$. By elementary set theory we can extend the given injection $E \subset S$ to an injection $E' \to S$. In other words, we may think of E' as an element of our set I contradicting the maximality of E. This contradiction completes the proof. □

Lemma 10.5. *Let F be a field. Let $\overline{F}$ be an algebraic closure of F. Let M/F be an algebraic extension. Then there is a morphism of F-extensions $M \to \overline{F}$.*

Proof. Consider the set I of pairs (E, φ) where $F \subset E \subset M$ is a subextension and $\varphi : E \to \overline{F}$ is a morphism of F-extensions. We partially order the set I by declaring $(E, \varphi) \leq (E', \varphi')$ if and only if $E \subset E'$ and $\varphi'|_E = \varphi$. If $T = \{(E_t, \varphi_t)\} \subset I$ is a totally ordered subset, then $\bigcup \varphi_t : \bigcup E_t \to \overline{F}$ is an element of I. Thus every totally ordered subset of I has an upper bound. By Zorn's lemma there exists a maximal element (E, φ) in I. We claim that $E = M$, which will finish the proof. If not, then pick $\alpha \in M$, $\alpha \notin E$. The α is algebraic over E, see Lemma 8.4. Let P be the minimal polynomial of α over E. Let P^φ be the image of P by φ in $\overline{F}[x]$. Since $\overline{F}$ is algebraically closed there is a root β of P^φ in $\overline{F}$. Then we can extend φ to $\varphi' : E(\alpha) = E[x]/(P) \to \overline{F}$ by mapping x to β. This contradicts the maximality of (E, φ) as desired. □

Lemma 10.6. *Any two algebraic closures of a field are isomorphic.*

Proof. Let F be a field. If M and $\overline{F}$ are algebraic closures of F, then there exists a morphism of F-extensions $\varphi : M \to \overline{F}$ by Lemma 10.5. Now the image $\varphi(M)$ is algebraically closed. On the other hand, the extension $\varphi(M) \subset \overline{F}$ is algebraic by Lemma 8.4. Thus $\varphi(M) = \overline{F}$. □

11. Relatively prime polynomials

Let K be an algebraically closed field. Then the ring $K[x]$ has a very simple ideal structure as we saw in Lemma 10.2. In particular, every polynomial $P \in K[x]$ can be written as

$$P = c(x - \alpha_1) \dots (x - \alpha_n),$$

where c is the constant term and the $\alpha_1, \dots, \alpha_n \in k$ are the roots of P (counted with multiplicity). Clearly, the only irreducible polynomials in $K[x]$ are the linear polynomials $c(x - \alpha)$, $c, \alpha \in K$ (and $c \neq 0$).

Definition 11.1. If k is any field, we say that two polynomials in $k[x]$ are *relatively prime* if they generate the unit ideal in $k[x]$.

Continuing the discussion above, if K is an algebraically closed field, two polynomials in $K[x]$ are relatively prime if and only if they have no common roots. This follows because the maximal ideals of $K[x]$ are of the form $(x - \alpha)$, $\alpha \in K$. So if $F, G \in K[x]$ have no common root, then (F, G) cannot be contained in any $(x - \alpha)$ (as then they would have a common root at α).

If k is *not* algebraically closed, then this still gives information about when two polynomials in $k[x]$ generate the unit ideal.

Lemma 11.2. *Two polynomials in $k[x]$ are relatively prime precisely when they have no common roots in an algebraic closure $\overline{k}$ of k.*

Proof. The claim is that any two polynomials P, Q generate (1) in $k[x]$ if and only if they generate (1) in $\overline{k}[x]$. This is a piece of linear algebra: a system of linear equations with coefficients in k has a solution if and only if it has a solution in any extension of k. Consequently, we can reduce to the case of an algebraically closed field, in which case the result is clear from what we have already proved. □

12. Separable extensions

In characteristic p something funny happens with irreducible polynomials over fields. We explain this in the following lemma.

Lemma 12.1. *Let F be a field. Let $P \in F[x]$ be an irreducible polynomial over F. Let $P' = dP/dx$ be the derivative of P with respect to x. Then one of the following two cases happens*

1. *P and P' are relatively prime, or*
2. *P' is the zero polynomial.*

The second case can only happen if F has characteristic $p > 0$. In this case $P(x) = Q(x^q)$ where $q = p^f$ is a power of p and $Q \in F[x]$ is an irreducible polynomial such that Q and Q' are relatively prime.

Proof. Note that P' has degree $< \deg(P)$. Hence if P and P' are not relatively prime, then $(P, P') = (R)$ where R is a polynomial of degree $< \deg(P)$ contradicting the irreducibility of P. This proves we have the dichotomy between (1) and (2).

Assume we are in case (2) and $P = a_d x^d + \ldots + a_0$. Then $P' = da_d x^{d-1} + \ldots + a_1$. In characteristic 0 we see that this forces $a_d, \ldots, a_1 = 0$ which would mean P is constant a contradiction. Thus we conclude that the characteristic p is positive. In this case the condition $P' = 0$ forces $a_i = 0$ whenever p does not divide i. In other words, $P(x) = P_1(x^p)$ for some nonconstant polynomial P_1. Clearly, P_1 is irreducible as well. By induction on the degree we see that $P_1(x) = Q(x^q)$ as in the statement of the lemma, hence $P(x) = Q(x^{pq})$ and the lemma is proved. □

Definition 12.2. Let F be a field. Let K/F be an extension of fields.

1. We say an irreducible polynomial P over F is *separable* if it is relatively prime to its derivative.
2. Given $\alpha \in K$ algebraic over F we say α is *separable* over F if its minimal polynomial is separable over F.
3. If K is an algebraic extension of F, we say K is *separable*[1] over F if every element of K is separable over F.

By Lemma 12.1 in characteristic 0 every irreducible polynomial is separable, every algebraic element in an extension is separable, and every algebraic extension is separable.

Lemma 12.3. *Let $K/E/F$ be a tower of algebraic field extensions.*

[1] For nonalgebraic extensions this definition does not make sense and is not the correct one. We refer the reader to Algebra, Sections 42 and 44.

(1) *If $\alpha \in K$ is separable over F, then α is separable over E.*
(2) *if K is separable over F, then K is separable over E.*

Proof. We will use Lemma 12.1 without further mention. Let P be the minimal polynomial of α over F. Let Q be the minimal polynomial of α over E. Then Q divides P in the polynomial ring $E[x]$, say $P = QR$. Then $P' = Q'R + QR'$. Thus if $Q' = 0$, then Q divides P and P' hence $P' = 0$ by the lemma. This proves (1). Part (2) follows immediately from (1) and the definitions. □

Lemma 12.4. *Let F be a field. An irreducible polynomial P over F is separable if and only if P has pairwise distinct roots in an algebraic closure of F.*

Proof. Suppose that $\alpha \in \overline{F}$ is a root of both P and P'. Then $P = (x - \alpha)Q$ for some polynomial Q. Taking derivatives we obtain $P' = Q + (x - \alpha)Q'$. Thus α is a root of Q. Hence we see that if P and P' have a common root, then P does not have pairwise distinct roots. Conversely, if P has a repeated root, i.e., $(x-\alpha)^2$ divides P, then α is a root of both P and P'. Combined with Lemma 11.2 this proves the lemma. □

Lemma 12.5. *Let F be a field and let $\overline{F}$ be an algebraic closure of F. Let $p > 0$ be the characteristic of F. Let P be a polynomial over F. Then the set of roots of P and $P(x^p)$ in $\overline{F}$ have the same cardinality (not counting multiplicity).*

Proof. Clearly, α is a root of $P(x^p)$ if and only if α^p is a root of P. In other words, the roots of $P(x^p)$ are the roots of $x^p - \beta$, where β is a root of P. Thus it suffices to show that the map $\overline{F} \to \overline{F}$, $\alpha \mapsto \alpha^p$ is bijective. It is surjective, as $\overline{F}$ is algebraically closed which means that every element has a pth root. It is injective because $\alpha^p = \beta^p$ implies $(\alpha - \beta)^p = 0$ because the characteristic is p. And of course in a field $x^p = 0$ implies $x = 0$. □

Let F be a field and let P be an irreducible polynomial over F. Then we know that $P = Q(x^q)$ for some separable irreducible polynomial Q (Lemma 12.1) where q is a power of the characteristic p (and if the characteristic is zero, then $q = 1$[2] and $Q = P$). By Lemma 12.5 the number of roots of P and Q in any algebraic closure of F is the same. By Lemma 12.4 this number is equal to the degree of Q.

Definition 12.6. Let F be a field. Let P be an irreducible polynomial over F. The *separable degree* of P is the cardinality of the set of roots of P in any algebraic closure of F (see discussion above). Notation $\deg_s(P)$.

The separable degree of P always divides the degree and the quotient is a power of the characteristic. If the characteristic is zero, then $\deg_s(P) = \deg(P)$.

Situation 12.7. Here F be a field and K/F is a finite extension generated by elements $\alpha_1, \ldots, \alpha_n \in K$. We set $K_0 = F$ and

$$K_i = F(\alpha_1, \ldots, \alpha_i)$$

to obtain a tower of finite extensions $K = K_n/K_{n-1}/\ldots/K_0 = F$. Denote P_i the minimal polynomial of α_i over K_{i-1}. Finally, we fix an algebraic closure $\overline{F}$ of F.

Let F, K, α_i, and $\overline{F}$ be as in Situation 12.7. Suppose that $\varphi : K \to \overline{F}$ is a morphism of extensions of F. Then we obtain maps $\varphi_i : K_i \to \overline{F}$. In particular, we can take the image of $P_i \in K_{i-1}[x]$ by φ_{i-1} to get a polynomial $P_i^\varphi \in \overline{F}[x]$.

[2] A good convention for this chapter is to set $0^0 = 1$.

Lemma 12.8. *In Situation 12.7 the correspondence*

$$\mathrm{Mor}_F(K, \overline{F}) \longrightarrow \{(\beta_1, \ldots, \beta_n) \textit{ as below}\}, \quad \varphi \longmapsto (\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$$

is a bijection. Here the right hand side is the set of n-tuples $(\beta_1, \ldots, \beta_n)$ of elements of $\overline{F}$ such that β_i is a root of P_i^φ.

Proof. Let $(\beta_1, \ldots, \beta_n)$ be an element of the right hand side. We construct a map of fields corresponding to it by induction. Namely, we set $\varphi_0 : K_0 \to \overline{F}$ equal to the given map $K_0 = F \subset \overline{F}$. Having constructed $\varphi_{i-1} : K_{i-1} \to \overline{F}$ we observe that $K_i = K_{i-1}[x]/(P_i)$. Hence we can set φ_i equal to the unique map $K_i \to \overline{F}$ inducing φ_{i-1} on K_{i-1} and mapping x to β_i. This works precisely as β_i is a root of P_i^φ. Uniqueness implies that the two constructions are mutually inverse. □

Lemma 12.9. *In Situation 12.7 we have $|\mathrm{Mor}_F(K, \overline{F})| = \prod_{i=1}^n \deg_s(P_i)$.*

Proof. This follows immediately from Lemma 12.8. Observe that a key ingredient we are tacitly using here is the well-definedness of the separable degree of an irreducible polynomial which was observed just prior to Definition 12.6. □

We now use the result above to characterize separable field extensions.

Lemma 12.10. *Assumptions and notation as in Situation 12.7. If each P_i is separable, i.e., each α_i is separable over K_{i-1}, then*

$$|\mathrm{Mor}_F(K, \overline{F})| = [K : F]$$

and the field extension K/F is separable. If one of the α_i is not separable over K_{i-1}, then $|\mathrm{Mor}_F(K, \overline{F})| < [K : F]$.

Proof. If α_i is separable over K_{i-1} then $\deg_s(P_i) = \deg(P_i) = [K_i : K_{i-1}]$ (last equality by Lemma 9.2). By multiplicativity (Lemma 7.7) we have

$$[K : F] = \prod [K_i : K_{i-1}] = \prod \deg(P_i) = \prod \deg_s(P_i) = |\mathrm{Mor}_F(K, \overline{F})|$$

where the last equality is Lemma 12.9. By the exact same argument we get the strict inequality $|\mathrm{Mor}_F(K, \overline{F})| < [K : F]$ if one of the α_i is not separable over K_{i-1}.

Finally, assume again that each α_i is separable over K_{i-1}. We will show K/F is separable. Let $\gamma = \gamma_1 \in K$ be arbitrary. Then we can find additional elements $\gamma_2, \ldots, \gamma_m$ such that $K = F(\gamma_1, \ldots, \gamma_m)$ (for example we could take $\gamma_2 = \alpha_1, \ldots, \gamma_{n+1} = \alpha_n$). Then we see by the last part of the lemma (already proven above) that if γ is not separable over F we would have the strict inequality $|\mathrm{Mor}_F(K, \overline{F})| < [K : F]$ contradicting the very first part of the lemma (already prove above as well). □

Lemma 12.11. *Let K/F be a finite extension of fields. Let $\overline{F}$ be an algebraic closure of F. Then we have*

$$|\mathrm{Mor}_F(K, \overline{F})| \leq [K : F]$$

with equality if and only if K is separable over F.

Proof. This is a corollary of Lemma 12.10. Namely, since K/F is finite we can find finitely many elements $\alpha_1, \ldots, \alpha_n \in K$ generating K over F (for example we can choose the α_i to be a basis of K over F). If K/F is separable, then each α_i is separable over $F(\alpha_1, \ldots, \alpha_{i-1})$ by Lemma 12.3 and we get equality by Lemma 12.10. On the other hand, if we have equality, then no matter how we choose

$\alpha_1, \ldots, \alpha_n$ we get that α_1 is separable over F by Lemma 12.10. Since we can start the sequence with an arbitrary element of K it follows that K is separable over F. □

Lemma 12.12. *Let E/k and F/E be separable algebraic extensions of fields. Then F/k is a separable extension of fields.*

Proof. Choose $\alpha \in F$. Then α is separable algebraic over E. Let $P = x^d + \sum_{i<d} a_i x^i$ be the minimal polynomial of α over E. Each a_i is separable algebraic over k. Consider the tower of fields

$$k \subset k(a_0) \subset k(a_0, a_1) \subset \ldots \subset k(a_0, \ldots, a_{d-1}) \subset k(a_0, \ldots, a_{d-1}, \alpha)$$

Because a_i is separable algebraic over k it is separable algebraic over $k(a_0, \ldots, a_{i-1})$ by Lemma 12.3. Finally, α is separable algebraic over $k(a_0, \ldots, a_{d-1})$ because it is a root of P which is irreducible (as it is irreducible over the possibly bigger field E) and separable (as it is separable over E). Thus $k(a_0, \ldots, a_{d-1}, \alpha)$ is separable over k by Lemma 12.10 and we conclude that α is separable over k as desired. □

Lemma 12.13. *Let E/k be a field extension. Then the elements of E separable over k form a subextension of E/k.*

Proof. Let $\alpha, \beta \in E$ be separable over k. Then β is separable over $k(\alpha)$ by Lemma 12.3. Thus we can apply Lemma 12.12 to $k(\alpha, \beta)$ to see that $k(\alpha, \beta)$ is separable over k. □

13. Linear independence of characters

Here is the statement.

Lemma 13.1. *Let L be a field. Let G be a monoid, for example a group. Let $\chi_1, \ldots, \chi_n : G \to L$ be pairwise distinct homomorphisms of monoids where L is regarded as a monoid by multiplication. Then $\chi_1, \ldots, \chi_n$ are L-linearly independent: if $\lambda_1, \ldots, \lambda_n \in L$ not all zero, then $\sum \lambda_i \chi_i(g) \neq 0$ for some $g \in G$.*

Proof. If $n = 1$ this is true because $\chi_1(e) = 1$ if $e \in G$ is the neutral (identity) element. We prove the result by induction for $n > 1$. Suppose that $\lambda_1, \ldots, \lambda_n \in L$ not all zero. If $\lambda_i = 0$ for some, then we win by induction on n. Since we want to show that $\sum \lambda_i \chi_i(g) \neq 0$ for some $g \in G$ we may after dividing by $-\lambda_n$ assume that $\lambda_n = -1$. Then the only way we get in trouble is if

$$\chi_n(g) = \sum\nolimits_{i=1,\ldots,n-1} \lambda_i \chi_i(g)$$

for all $g \in G$. Fix $h \in G$. Then we would also get

$$\begin{aligned} \chi_n(h)\chi_n(g) &= \chi_n(hg) \\ &= \sum\nolimits_{i=1,\ldots,n-1} \lambda_i \chi_i(hg) \\ &= \sum\nolimits_{i=1,\ldots,n-1} \lambda_i \chi_i(h) \chi_i(g) \end{aligned}$$

Multiplying the previous relation by $\chi_n(h)$ and substracting we obtain

$$0 = \sum\nolimits_{i=1,\ldots,n-1} \lambda_i (\chi_n(h) - \chi_i(h)) \chi_i(g)$$

for all $g \in G$. Since $\lambda_i \neq 0$ we conclude that $\chi_n(h) = \chi_i(h)$ for all i by induction. The choice of h above was arbitrary, so we conclude that $\chi_i = \chi_n$ for $i \leq n-1$ which contradicts the assumption that our characters χ_i are pairwise distinct. □

Lemma 13.2. *Let L be a field. Let $n \geq 1$ and $\alpha_1, \ldots, \alpha_n \in L$ pairwise distinct elements of L. Then there exists an $e \geq 0$ such that $\sum_{i=1,\ldots,n} \alpha_i^e \neq 0$.*

Proof. Apply linear independence of characters (Lemma 13.1) to the monoid homomorphisms $\mathbf{Z}_{\geq 0} \to L$, $e \mapsto \alpha_i^e$. □

Lemma 13.3. *Let K/F and L/F be field extensions. Let $\sigma_1, \ldots, \sigma_n : K \to L$ be pairwise distinct morphisms of F-extensions. Then $\sigma_1, \ldots, \sigma_n$ are L-linearly independent: if $\lambda_1, \ldots, \lambda_n \in L$ not all zero, then $\sum \lambda_i \sigma_i(\alpha) \neq 0$ for some $\alpha \in K$.*

Proof. Apply Lemma 13.1 to the restrictions of σ_i to the groups of units. □

Lemma 13.4. *Let K/F and L/F be field extensions with K/F finite separable and L algebraically closed. Then the map*

$$K \otimes_F L \longrightarrow \prod\nolimits_{\sigma \in \mathrm{Hom}_F(K,L)} L, \quad \alpha \otimes \beta \mapsto (\sigma(\alpha)\beta)_\sigma$$

is an isomorphism of L-algebras.

Proof. Choose a basis $\alpha_1, \ldots, \alpha_n$ of K as a vector space over F. By Lemma 12.11 (and a tiny omitted argument) the set $\mathrm{Hom}_F(K,L)$ has n elements, say $\sigma_1, \ldots, \sigma_n$. In particular, the two sides have the same dimension n as vector spaces over L. Thus if the map is not an isomorphism, then it has a kernel. In other words, there would exist $\mu_j \in L$, $j = 1, \ldots, n$ not all zero, with $\sum \alpha_j \otimes \mu_j$ in the kernel. In other words, $\sum \sigma_i(\alpha_j)\mu_j = 0$ for all i. This would mean the $n \times n$ matrix with entries $\sigma_i(\alpha_j)$ is not invertible. Thus we can find $\lambda_1, \ldots, \lambda_n \in L$ not all zero, such that $\sum \lambda_i \sigma_i(\alpha_j) = 0$ for all j. Now any element $\alpha \in K$ can be written as $\alpha = \sum \beta_j \alpha_j$ with $\beta_j \in F$ and we would get

$$\sum \lambda_i \sigma_i(\alpha) = \sum \lambda_i \sigma_i(\sum \beta_j \alpha_j) = \sum \beta_j \sum \lambda_i \sigma_i(\alpha_j) = 0$$

which contradicts Lemma 13.3. □

14. Purely inseparable extensions

Purely inseparable extensions are the opposite of the separable extensions defined in the previous section. These extensions only show up in positive characteristic.

Definition 14.1. Let F be a field of characteristic $p > 0$. Let K/F be an extension.

(1) An element $\alpha \in K$ is *purely inseparable* over F if there exists a power q of p such that $\alpha^q \in F$.
(2) The extension K/F is said to be *purely inseparable* if and only if every element of K is purely inseparable over F.

Observe that a purely inseparable extension is necessarily algebraic. Let F be a field of characteristic $p > 0$. An example of a purely inseparable extension is gotten by adjoining the pth root of an element $t \in F$ which does not yet have one. Namely, the lemma below shows that $P = x^p - t$ is irreducible, and hence

$$K = F[x]/(P) = F[t^{1/p}]$$

is a field. And K is purely inseparable over F because every element

$$a_0 + a_1 t^{1/p} + \ldots + a_{p-1} t^{(p-1)/p}, \quad a_i \in F$$

of K has pth power equal to

$$(a_0 + a_1 t^{1/p} + \ldots + a_{p-1} t^{(p-1)/p})^p = a_0^p + a_1^p t + \ldots + a_{p-1}^p t^{p-1} \in F$$

This situation occurs for the field $\mathbf{F}_p(t)$ of rational functions over $\mathbf{F}_p$.

Lemma 14.2. *Let p be a prime number. Let F be a field of characteristic p. Let $t \in F$ be an element which does not have a pth root in F. Then the polynomial $x^p - t$ is irreducible over F.*

Proof. To see this, suppose that we have a factorization $x^p - t = fg$. Taking derivatives we get $f'g + fg' = 0$. Note that neither $f' = 0$ nor $g' = 0$ as the degrees of f and g are smaller than p. Moreover, $\deg(f') < \deg(f)$ and $\deg(g') < \deg(g)$. We conclude that f and g have a factor in common. Thus if $x^p - t$ is reducible, then it is of the form $x^p - t = cf^n$ for some irreducible f, $c \in F^*$, and $n > 1$. Since p is a prime number this implies $n = p$ and f linear, which would imply $x^p - t$ has a root in F. Contradiction. □

We will see that taking pth roots is a very important operation in characteristic p.

Lemma 14.3. *Let E/k and F/E be purely inseparable extensions of fields. Then F/k is a purely inseparable extension of fields.*

Proof. Say the characteristic of k is p. Choose $\alpha \in F$. Then $\alpha^q \in E$ for some p-power q. Whereupon $(\alpha^q)^{q'} \in k$ for some p-power q'. Hence $\alpha^{qq'} \in k$. □

Lemma 14.4. *Let E/k be a field extension. Then the elements of E purely-inseparable over k form a subextension of E/k.*

Proof. Let p be the characteristic of k. Let $\alpha, \beta \in E$ be purely inseparable over k. Say $\alpha^q \in k$ and $\beta^{q'} \in k$ for some p-powers q, q'. If q'' is a p-power, then $(\alpha + \beta)^{q''} = \alpha^{q''} + \beta^{q''}$. Hence if $q'' \geq q, q'$, then we conclude that $\alpha + \beta$ is purely inseparable over k. Similarly for the difference, product and quotient of α and β. □

Lemma 14.5. *Let E/F be a finite purely inseparable field extension of characteristic $p > 0$. Then there exists a sequence of elements $\alpha_1, \ldots, \alpha_n \in E$ such that we obtain a tower of fields*

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \ldots \supset F(\alpha_1) \supset F$$

such that each intermediate extension is of degree p and comes from adjoining a pth root. Namely, $\alpha_i^p \in F(\alpha_1, \ldots, \alpha_{i-1})$ is an element which does not have a pth root in $F(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, n$.

Proof. By induction on the degree of E/F. If the degree of the extension is 1 then the result is clear (with $n = 0$). If not, then choose $\alpha \in E$, $\alpha \notin F$. Say $\alpha^{p^r} \in F$ for some $r > 0$. Pick r minimal and replace α by $\alpha^{p^{r-1}}$. Then $\alpha \notin F$, but $\alpha^p \in F$. Then $t = \alpha^p$ is not a pth power in F (because that would imply $\alpha \in F$, see Lemma 12.5 or its proof). Thus $F \subset F(\alpha)$ is a subextension of degree p (Lemma 14.2). By induction we find $\alpha_1, \ldots, \alpha_n \in E$ generating $E/F(\alpha)$ satisfying the conclusions of the lemma. The sequence $\alpha, \alpha_1, \ldots, \alpha_n$ does the job for the extension E/F. □

Lemma 14.6. *Let E/F be an algebraic field extension. There exists a unique subextension $E/E_{sep}/F$ such that E_{sep}/F is separable and E/E_{sep} is purely inseparable.*

Proof. If the characteristic is zero we set $E_{sep} = E$. Assume the characteristic is $p > 0$. Let E_{sep} be the set of elements of E which are separable over F. This is a subextension by Lemma 12.13 and of course E_{sep} is separable over F. Given an α in E there exists a p-power q such that α^q is separable over F. Namely, q is that power of p such that the minimal polynomial of α is of the form $P(x^q)$ with P separable algebraic, see Lemma 12.1. Hence E/E_{sep} is purely inseparable. Uniqueness is clear. □

Definition 14.7. Let E/F be an algebraic field extension. Let E_{sep} be the subextension found in Lemma 14.6.

(1) The integer $[E_{sep} : F]$ is called the *separable degree* of the extension. Notation $[E : F]_s$.
(2) The integer $[E : E_{sep}]$ is called the *inseparable degree*, or the *degree of inseparability* of the extension. Notation $[E : F]_i$.

Of course in characteristic 0 we have $[E : F] = [E : F]_s$ and $[E : F]_i = 1$. By multiplicativity (Lemma 7.7) we have

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

even in case some of these degrees are infinite. In fact, the separable degree and the inseparable degree are multiplicative too (see Lemma 14.9).

Lemma 14.8. *Let K/F be a finite extension. Let $\overline{F}$ be an algebraic closure of F. Then $[K : F]_s = |\operatorname{Mor}_F(K, \overline{F})|$.*

Proof. We first prove this when K/F is purely inseparable. Namely, we claim that in this case there is a unique map $K \to \overline{F}$. This can be seen by choosing a sequence of elements $\alpha_1, \ldots, \alpha_n \in K$ as in Lemma 14.5. The irreducible polynomial of α_i over $F(\alpha_1, \ldots, \alpha_{i-1})$ is $x^p - \alpha_i^p$. Applying Lemma 12.9 we see that $|\operatorname{Mor}_F(K, \overline{F})| = 1$. On the other hand, $[K : F]_s = 1$ in this case hence the equality holds.

Let's return to a general finite extension K/F. In this case choose $F \subset K_s \subset K$ as in Lemma 14.6. By Lemma 12.11 we have $|\operatorname{Mor}_F(K_s, \overline{F})| = [K_s : F] = [K : F]_s$. On the other hand, every field map $\sigma' : K_s \to \overline{F}$ extends to a unique field map $\sigma : K \to \overline{F}$ by the result of the previous paragraph. In other words $|\operatorname{Mor}_F(K, \overline{F})| = |\operatorname{Mor}_F(K_s, \overline{F})|$ and the proof is done. □

Lemma 14.9 (Multiplicativity)**.** *Suppose given a tower of algebraic field extensions $K/E/F$. Then*

$$[K : F]_s = [K : E]_s[E : F]_s \quad \textit{and} \quad [K : F]_i = [K : E]_i[E : F]_i$$

Proof. We first prove this in case K is finite over F. Since we have multiplicativity for the usual degree (by Lemma 7.7) it suffices to prove one of the two formulas. By Lemma 14.8 we have $[K : F]_s = |\operatorname{Mor}_F(K, \overline{F})|$. By the same lemma, given any $\sigma \in \operatorname{Mor}_F(E, \overline{F})$ the number of extensions of σ to a map $\tau : K \to \overline{F}$ is $[K : E]_s$. Namely, via $E \cong \sigma(E) \subset \overline{F}$ we can view $\overline{F}$ as an algebraic closure of E. Combined with the fact that there are $[E : F]_s = |\operatorname{Mor}_F(E, \overline{F})|$ choices for σ we obtain the result.

We omit the proof if the extensions are infinite. □

15. Normal extensions

Let $P \in F[x]$ be a nonconstant polynomial over a field F. We say P *splits completely into linear factors over* F or *splits completely over* F if there exist $c \in F^*$, $n \geq 1$, $\alpha_1, \ldots, \alpha_n \in F$ such that

$$P = c(x - \alpha_1) \ldots (x - \alpha_n)$$

in $F[x]$. Normal extensions are defined as follows.

Definition 15.1. Let E/F be an algebraic field extension. We say E is *normal* over F if for all $\alpha \in E$ the minimal polynomial P of α over F splits completely into linear factors over E.

As in the case of separable extensions, it takes a bit of work to establish the basic properties of this notion.

Lemma 15.2. *Let $K/E/F$ be a tower of algebraic field extensions. If K is normal over F, then K is normal over E.*

Proof. Let $\alpha \in K$. Let P be the minimal polynomial of α over F. Let Q be the minimal polynomial of α over E. Then Q divides P in the polynomial ring $E[x]$, say $P = QR$. Hence, if P splits completely over K, then so does Q. □

Lemma 15.3. *Let F be a field. Let M/F be an algebraic extension. Let $M/E_i/F$, $i \in I$ be subextensions with E_i/F normal. Then $\bigcap E_i$ is normal over F.*

Proof. Direct from the definitions. □

Lemma 15.4. *Let E/F be a normal algebraic field extension. Then the subextension $E/E_{sep}/F$ of Lemma 14.6 is normal.*

Proof. If the characteristic is zero, then $E_{sep} = E$, and the result is clear. If the characteristic is $p > 0$, then E_{sep} is the set of elements of E which are separable over F. Then if $\alpha \in E_{sep}$ has minimal polynomial P write $P = c(x - \alpha)(x - \alpha_2) \ldots (x - \alpha_d)$ with $\alpha_2, \ldots, \alpha_d \in E$. Since P is a separable polynomial and since α_i is a root of P, we conclude $\alpha_i \in E_{sep}$ as desired. □

Lemma 15.5. *Let E/F be an algebraic extension of fields. Let $\overline{F}$ be an algebraic closure of F. The following are equivalent*

1. *E is normal over F, and*
2. *for every pair $\sigma, \sigma' \in \mathrm{Mor}_F(E, \overline{F})$ we have $\sigma(E) = \sigma'(E)$.*

Proof. Let $\mathcal{P}$ be the set of all minimal polynomials over F of all elements of E. Set

$$T = \{\beta \in \overline{F} \mid P(\beta) = 0 \text{ for some } P \in \mathcal{P}\}$$

It is clear that if E is normal over F, then $\sigma(E) = T$ for all $\sigma \in \mathrm{Mor}_F(E, \overline{F})$. Thus we see that (1) implies (2).

Conversely, assume (2). Pick $\beta \in T$. We can find a corresponding $\alpha \in E$ whose minimal polynomial $P \in \mathcal{P}$ annihilates β. Because $F(\alpha) = F[x]/(P)$ we can find an element $\sigma_0 \in \mathrm{Mor}_F(F(\alpha), \overline{F})$ mapping α to β. By Lemma 10.5 we can extend σ_0 to a $\sigma \in \mathrm{Mor}_F(E, \overline{F})$. Whence we see that β is in the common image of all embeddings $\sigma : E \to \overline{F}$. It follows that $\sigma(E) = T$ for any σ. Fix a σ. Now let $P \in \mathcal{P}$. Then we can write

$$P = (x - \beta_1) \ldots (x - \beta_n)$$

for some n and $\beta_i \in \overline{F}$ by Lemma 10.2. Observe that $\beta_i \in T$. Thus $\beta_i = \sigma(\alpha_i)$ for some $\alpha_i \in E$. Thus $P = (x - \alpha_1) \ldots (x - \alpha_n)$ splits completely over E. This finishes the proof. $\square$

Lemma 15.6. *Let E/F be an algebraic extension of fields. If E is generated by $\alpha_i \in E$, $i \in I$ over F and if for each i the minimal polynomial of α_i over F splits completely in E, then E/F is normal.*

Proof. Let P_i be the minimal polynomial of α_i over F. Let $\alpha_i = \alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,d_i}$ be the roots of P_i over E. Given two embeddings $\sigma, \sigma' : E \to \overline{F}$ over F we see that

$$\{\sigma(\alpha_{i,1}), \ldots, \sigma(\alpha_{i,d_i})\} = \{\sigma'(\alpha_{i,1}), \ldots, \sigma'(\alpha_{i,d_i})\}$$

because both sides are equal to the set of roots of P_i in $\overline{F}$. The elements $\alpha_{i,j}$ generate E over F and we find that $\sigma(E) = \sigma'(E)$. Hence E/F is normal by Lemma 15.5. $\square$

Lemma 15.7. *Let $L/M/K$ be a tower of algebraic extensions.*

1. *If M/K is normal, then any automorphism τ of L/K induces an automorphism $\tau|_M : M \to M$.*
2. *If L/K is normal, then any K-algebra map $\sigma : M \to L$ extends to an automorphism of L.*

Proof. Choose an algebraic closure $\overline{L}$ of L (Theorem 10.4).

Let τ be as in (1). Then $\tau(M) = M$ as subfields of $\overline{L}$ by Lemma 15.5 and hence $\tau|_M : M \to M$ is an automorphism.

Let $\sigma : M \to L$ be as in (2). By Lemma 10.5 we can extend σ to a map $\tau : L \to \overline{L}$, i.e., such that

$$\begin{tikzcd}
L \arrow[r, "\tau"'] & \overline{L} \\
M \arrow[u] \arrow[ur, "\sigma"'] & K \arrow[l] \arrow[u]
\end{tikzcd}$$

is commutative. By Lemma 15.5 we see that $\tau(L) = L$. Hence $\tau : L \to L$ is an automorphism which extends σ. $\square$

Definition 15.8. Let E/F be an extension of fields. Then $\text{Aut}(E/F)$ or $\text{Aut}_F(E)$ denotes the automorphism group of E as an object of the category of F-extensions. Elements of $\text{Aut}(E/F)$ are called *automorphisms of E over F* or *automorphisms of E/F*.

Here is a characterization of normal extensions in terms of automorphisms.

Lemma 15.9. *Let E/F be a finite extension. We have*

$$|Aut(E/F)| \leq [E : F]_s$$

with equality if and only if E is normal over F.

Proof. Choose an algebraic closure $\overline{F}$ of F. Recall that $[E : F]_s = |\operatorname{Mor}_F(E, \overline{F})|$. Pick an element $\sigma_0 \in \operatorname{Mor}_F(E, \overline{F})$. Then the map

$$\text{Aut}(E/F) \longrightarrow \operatorname{Mor}_F(E, \overline{F}), \quad \tau \longmapsto \sigma_0 \circ \tau$$

is injective. Thus the inequality. If equality holds, then every $\sigma \in \mathrm{Mor}_F(E, \overline{F})$ is gotten by precomposing σ_0 by an automorphism. Hence $\sigma(E) = \sigma_0(E)$. Thus E is normal over F by Lemma 15.5.

Conversely, assume that E/F is normal. Then by Lemma 15.5 we have $\sigma(E) = \sigma_0(E)$ for all $\sigma \in \mathrm{Mor}_F(E, \overline{F})$. Thus we get an automorphism of E over F by setting $\tau = \sigma_0^{-1} \circ \sigma$. Whence the map displayed above is surjective. □

Lemma 15.10. *Let L/K be an algebraic normal extension of fields. Let E/K be an extension of fields. Then either there is no K-embedding from L to E or there is one $\tau : L \to E$ and every other one is of the form $\tau \circ \sigma$ where $\sigma \in Aut(L/K)$.*

Proof. Given τ replace L by $\tau(L) \subset E$ and apply Lemma 15.7. □

16. Splitting fields

The following lemma is a useful tool for constructing normal field extensions.

Lemma 16.1. *Let F be a field. Let $P \in F[x]$ be a nonconstant polynomial. There exists a smallest field extension E/F such that P splits completely over E. Moreover, the field extension E/F is normal and unique up to (nonunique) isomorphism.*

Proof. Choose an algebraic closure $\overline{F}$. Then we can write $P = c(x - \beta_1) \ldots (x - \beta_n)$ in $\overline{F}[x]$, see Lemma 10.2. Note that $c \in F^*$. Set $E = F(\beta_1, \ldots, \beta_n)$. Then it is clear that E is minimal with the requirement that P splits completely over E.

Next, let E' be another minimal field extension of F such that P splits completely over E'. Write $P = c(x - \alpha_1) \ldots (x - \alpha_n)$ with $c \in F$ and $\alpha_i \in E'$. Again it follows from minimality that $E' = F(\alpha_1, \ldots, \alpha_n)$. Moreover, if we pick any $\sigma : E' \to \overline{F}$ (Lemma 10.5) then we immediately see that $\sigma(\alpha_i) = \beta_{\tau(i)}$ for some permutation $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Thus $\sigma(E') = E$. This implies that E' is a normal extension of F by Lemma 15.5 and that $E \cong E'$ as extensions of F thereby finishing the proof. □

Definition 16.2. Let F be a field. Let $P \in F[x]$ be a nonconstant polynomial. The field extension E/F constructed in Lemma 16.1 is called the *splitting field of P over F*.

Lemma 16.3. *Let E/F be a finite extension of fields. There exists a unique smallest finite extension K/E such that K is normal over F.*

Proof. Choose generators $\alpha_1, \ldots, \alpha_n$ of E over F. Let $P_1, \ldots, P_n$ be the minimal polynomials of $\alpha_1, \ldots, \alpha_n$ over F. Set $P = P_1 \ldots P_n$. Observe that $(x - \alpha_1) \ldots (x - \alpha_n)$ divides P, since each $(x - \alpha_i)$ divides P_i. Say $P = (x - \alpha_1) \ldots (x - \alpha_n)Q$. Let K/E be the splitting field of P over E. We claim that K is the splitting field of P over F as well (which implies that K is normal over F). This is clear because K/E is generated by the roots of Q over E and E is generated by the roots of $(x - \alpha_1) \ldots (x - \alpha_n)$ over F, hence K is generated by the roots of P over F.

Uniqueness. Suppose that K'/E is a second smallest extension such that K'/F is normal. Choose an algebraic closure $\overline{F}$ and an embedding $\sigma_0 : E \to \overline{F}$. By Lemma 10.5 we can extend σ_0 to $\sigma : K \to \overline{F}$ and $\sigma' : K' \to \overline{F}$. By Lemma 15.3 we see that $\sigma(K) \cap \sigma'(K')$ is normal over F. By minimality we conclude that $\sigma(K) = \sigma(K')$. Thus $\sigma \circ (\sigma')^{-1} : K' \to K$ gives an isomorphism of extensions of E. □

Definition 16.4. Let E/F be a finite extension of fields. The field extension K/E constructed in Lemma 16.3 is called the *normal closure E over F*.

One can construct the normal closure inside any given normal extension.

Lemma 16.5. *Let L/K be an algebraic normal extension.*

1. *If $L/M/K$ is a subextension with M/K finite, then there exists a tower $L/M'/M/K$ with M'/K finite and normal.*
2. *If $L/M'/M/K$ is a tower with M/K normal and M'/M finite, then there exists a tower $L/M''/M'/M/K$ with M''/M finite and M''/K normal.*

Proof. Proof of (1). Let M' be the smallest subextension of L/K containing M which is normal over K. By Lemma 16.3 this is the normal closure of M/K and is finite over K.

Proof of (2). Let $\alpha_1, \ldots, \alpha_n \in M'$ generate M' over M. Let $P_1, \ldots, P_n$ be the minimal polynomials of $\alpha_1, \ldots, \alpha_n$ over K. Let $\alpha_{i,j}$ be the roots of P_i in L. Let $M'' = M(\alpha_{i,j})$. It follows from Lemma 15.6 (applied with the set of generators $M \cup \{\alpha_{i,j}\}$) that M'' is normal over K. □

The following lemma can sometimes be used to prove properties of the normal closure.

Lemma 16.6. *Let L/K be a finite extension. Let M/L be the normal closure of L over K. Then there is a surjective map*

$$L \otimes_K L \otimes_K \ldots \otimes_K L \longrightarrow M$$

of K-algebras where the number of tensors can be taken $[L : K]_s \leq [L : K]$.

Proof. Choose an algebraic closure $\overline{K}$ of K. Set $n = [L : K]_s = |\operatorname{Mor}_K(L, \overline{K})|$ with equality by Lemma 14.8. Say $\operatorname{Mor}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Let $M' \subset \overline{K}$ be the K-subalgebra generated by $\sigma_i(L)$, $i = 1, \ldots, n$. It follows from Lemma 15.5 that M' is normal over K and that it is the smallest normal subextension of $\overline{K}$ containing $\sigma_1(L)$. By uniqueness of normal closure we have $M \cong M'$. Finally, there is a surjective map

$$L \otimes_K L \otimes_K \ldots \otimes_K L \longrightarrow M', \quad \lambda_1 \otimes \ldots \otimes \lambda_n \longmapsto \sigma_1(\lambda_1) \ldots \sigma_n(\lambda_n)$$

and note that $n \leq [L : K]$ by definition. □

17. Roots of unity

Let F be a field. For an integer $n \geq 1$ we set

$$\mu_n(F) = \{\zeta \in F \mid \zeta^n = 1\}$$

This is called the *group of nth roots of unity* or *nth roots of* 1. It is an abelian group under multiplication with neutral element given by 1. Observe that in a field the number of roots of a polynomial of degree d is always at most d. Hence we see that $|\mu_n(F)| \leq n$ as it is defined by a polynomial equation of degree n. Of course every element of $\mu_n(F)$ has order dividing n. Moreover, the subgroups

$$\mu_d(F) \subset \mu_n(F), \quad d|n$$

each have at most d elements. This implies that $\mu_n(F)$ is cyclic.

Lemma 17.1. *Let A be an abelian group of exponent dividing n such that $\{x \in A \mid dx = 0\}$ has cardinality at most d for all $d|n$. Then A is cyclic of order dividing n.*

Proof. The conditions imply that $|A| \leq n$, in particular A is finite. The structure of finite abelian groups shows that $A = \mathbf{Z}/e_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/e_r\mathbf{Z}$ for some integers $1 < e_1|e_2|\ldots|e_r$. This would imply that $\{x \in A \mid e_1x = 0\}$ has cardinality e_1^r. Hence $r = 1$. □

Applying this to the field $\mathbf{F}_p$ we obtain the celebrated result that the group $(\mathbf{Z}/p\mathbf{Z})^*$ is a cyclic group. More about this in the section on finite fields.

One more observation is often useful: If F has characteristic $p > 0$, then $\mu_{p^n}(F) = \{1\}$. This is true because raising to the pth power is an injective map on fields of characteristic p as we have seen in the proof of Lemma 12.5. (Of course, it also follows from the statement of that lemma itself.)

18. Finite fields

Let F be a finite field. It is clear that F has positive characteristic as we cannot have an injection $\mathbf{Q} \to F$. Say the characteristic of F is p. The extension $\mathbf{F}_p \subset F$ is finite. Hence we see that F has $q = p^f$ elements for some $f \geq 1$.

Let us think about the group of units F^*. This is a finite abelian group, so it has some exponent e. Then $F^* = \mu_e(F)$ and we see from the discussion in Section 17 that F^* is a cyclic group of order $q - 1$. (A posteriori it follows that $e = q - 1$ as well.) In particular, if $\alpha \in F^*$ is a generator then it clearly is true that

$$F = \mathbf{F}_p(\alpha)$$

In other words, the extension $F/\mathbf{F}_p$ is generated by a single element. Of course, the same thing is true for any extension of finite fields E/F (because E is already generated by a single element over the prime field).

19. Primitive elements

Let E/F be a finite extension of fields. An element $\alpha \in E$ is called a *primitive element of E over F* if $E = F(\alpha)$.

Lemma 19.1 (Primitive element)**.** *Let E/F be a finite extension of fields. The following are equivalent*

1. *there exists a primitive element for E over F, and*
2. *there are finitely many subextensions $E/K/F$.*

Moreover, (1) and (2) hold if E/F is separable.

Proof. Let $\alpha \in E$ be a primitive element. Let P be the minimal polynomial of α over F. Let $E \subset M$ be a splitting field for P over E, so that $P(x) = (x-\alpha)(x-\alpha_2)\ldots(x-\alpha_n)$ over M. For ease of notation we set $\alpha_1 = \alpha$. Next, let $E/K/F$ be a subextension. Let Q be the minimal polynomial of α over K. Observe that $\deg(Q) = [E : K]$. Writing $Q = x^d + \sum_{i<d} a_i x^i$ we claim that K is equal to $L = F(a_0, \ldots, a_{d-1})$. Indeed α has degree d over L and $L \subset K$. Hence $[E : L] = [E : K]$ and it follows that $[K : L] = 1$, i.e., $K = L$. Thus it suffices to show there are at most finitely many possibilities for the polynomial Q. This is clear because we have a factorization $P = QR$ in $K[x]$ in particular in $E[x]$. Since we have unique factorization in $E[x]$ there are at most finitely many monic factors of P in $E[x]$.

If F is a finite field (equivalently E is a finite field), then E/F has a primitive element by the discussion in Section 18. Next, assume F is infinite and there are at most finitely many proper subfields $E/K/F$. List them, say $K_1, \ldots, K_N$. Then each $K_i \subset E$ is a proper sub F-vector space. As F is infinite we can find a vector $\alpha \in E$ with $\alpha \notin K_i$ for all i (a vector space can never be equal to a finite union of proper subvector spaces; details omitted). Then α is a primitive element for E over F.

Having established the equivalence of (1) and (2) we now turn to the final statement of the lemma. Choose an algebraic closure $\overline{F}$ of F. Enumerate the elements $\sigma_1, \ldots, \sigma_n \in \text{Mor}_F(E, \overline{F})$. Since E/F is separable we have $n = [E : F]$ by Lemma 12.11. Note that if $i \neq j$, then

$$V_{ij} = \text{Ker}(\sigma_i - \sigma_j : E \longrightarrow \overline{F})$$

is not equal to E. Hence arguing as in the preceding paragraph we can find $\alpha \in E$ with $\alpha \notin V_{ij}$ for all $i \neq j$. It follows that $|\text{Mor}_F(F(\alpha), \overline{F})| \geq n$. On the other hand $[F(\alpha) : F] \leq [E : F]$. Hence equality by Lemma 12.11 and we conclude that $E = F(\alpha)$. □

20. Trace and norm

Let L/K be a finite extension of fields. By Lemma 4.1 we can choose an isomorphism $L \cong K^{\oplus n}$ of K-modules. Of course $n = [L : K]$ is the degree of the field extension. Using this isomorphism we get for a K-algebra map

$$L \longrightarrow \text{Mat}(n \times n, K), \quad \alpha \longmapsto \text{matrix of multiplication by } \alpha$$

Thus given $\alpha \in L$ we can take the trace and the determinant of the corresponding matrix. Of course these quantities are independent of the choice of the basis chosen above. More canonically, simply thinking of L as a finite dimensional K-vector space we have $\text{Trace}_K(\alpha : L \to L)$ and the determinant $\det_K(\alpha : L \to L)$.

Definition 20.1. Let L/K be a finite extension of fields. For $\alpha \in L$ we define the *trace* $\text{Trace}_{L/K}(\alpha) = \text{Trace}_K(\alpha : L \to L)$ and the *norm* $\text{Norm}_{L/K}(\alpha) = \det_K(\alpha : L \to L)$.

It is clear from the definition that $\text{Trace}_{L/K}$ is K-linear and satisfies $\text{Trace}_{L/K}(\alpha) = [L : K]\alpha$ for $\alpha \in K$. Similarly $\text{Norm}_{L/K}$ is multiplicative and $\text{Norm}_{L/K}(\alpha) = \alpha^{[L:K]}$ for $\alpha \in K$. This is a special case of the more general construction discussed in Exercises, Exercises 22.6 and 22.7.

Lemma 20.2. *Let L/K be a finite extension of fields. Let $\alpha \in L$ and let P be the minimal polynomial of α over K. Then the characteristic polynomial of the K-linear map $\alpha : L \to L$ is equal to P^e with $e\deg(P) = [L : K]$.*

Proof. Choose a basis $\beta_1, \ldots, \beta_e$ of L over $K(\alpha)$. Then e satisfies $e\deg(P) = [L : K]$ by Lemmas 9.2 and 7.7. Then we see that $L = \bigoplus K(\alpha)\beta_i$ is a direct sum decomposition into α-invariant subspaces hence the characteristic polynomial of $\alpha : L \to L$ is equal to the characteristic polynomial of $\alpha : K(\alpha) \to K(\alpha)$ to the power e.

To finish the proof we may assume that $L = K(\alpha)$. In this case by Cayley-Hamilton we see that α is a root of the characteristic polynomial. And since the characteristic polynomial has the same degree as the minimal polynomial, we find that equality holds. □

Lemma 20.3. *Let L/K be a finite extension of fields. Let $\alpha \in L$ and let $P = x^d + a_1x^{d-1} + \ldots + a_d$ be the minimal polynomial of α over K. Then*

$$Norm_{L/K}(\alpha) = (-1)^{[L:K]}a_d^e \quad and \quad Trace_{L/K}(\alpha) = -ea_1$$

where $ed = [L : K]$.

Proof. Follows immediately from Lemma 20.2 and the definitions. □

Lemma 20.4. *Let L/K be a finite extension of fields. Let V be a finite dimensional vector space over L. Let $\varphi : V \to V$ be an L-linear map. Then*

$$Trace_K(\varphi : V \to V) = Trace_{L/K}(Trace_L(\varphi : V \to V))$$

and

$$\det_K(\varphi : V \to V) = Norm_{L/K}(\det_L(\varphi : V \to V))$$

Proof. Choose an isomorphism $V = L^{\oplus n}$ so that φ corresponds to an $n \times n$ matrix. In the case of traces, both sides of the formula are additive in φ. Hence we can assume that φ corresponds to the matrix with exactly one nonzero entry in the (i, j) spot. In this case a direct computation shows both sides are equal.

In the case of norms both sides are zero if φ has a nonzero kernel. Hence we may assume φ corresponds to an element of $\text{GL}_n(L)$. Both sides of the formula are multiplicative in φ. Since every element of $\text{GL}_n(L)$ is a product of elementary matrices we may assume that φ either looks like

$$E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda & \ldots \\ 0 & 1 & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix} \quad \text{or} \quad E_1(a) = \begin{pmatrix} a & 0 & \ldots \\ 0 & 1 & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix}$$

(because we may also permute the basis elements if we like). In both cases the formula is easy to verify by direct computation. □

Lemma 20.5. *Let $M/L/K$ be a tower of finite extensions of fields. Then*

$$Trace_{M/K} = Trace_{L/K} \circ Trace_{M/L} \quad and \quad Norm_{M/K} = Norm_{L/K} \circ Norm_{M/L}$$

Proof. Think of M as a vector space over L and apply Lemma 20.4. □

The trace pairing is defined using the trace.

Definition 20.6. Let L/K be a finite extension of fields. The *trace pairing* for L/K is the symmetric K-bilinear form

$$Q_{L/K} : L \times L \longrightarrow K, \quad (\alpha, \beta) \longmapsto \text{Trace}_{L/K}(\alpha\beta)$$

It turns out that a finite extension of fields is separable if and only if the trace pairing is nondegenerate.

Lemma 20.7. *Let L/K be a finite extension of fields. The following are equivalent:*

1. *L/K is separable,*
2. *$Trace_{L/K}$ is not identically zero, and*
3. *the trace pairing $Q_{L/K}$ is nondegenerate.*

Proof. It is clear that (3) implies (2). If (2) holds, then pick $\gamma \in L$ with $\text{Trace}_{L/K}(\gamma) \neq 0$. Then if $\alpha \in L$ is nonzero, we see that $Q_{L/K}(\alpha, \gamma/\alpha) \neq 0$. Hence $Q_{L/K}$ is nondegenerate. This proves the equivalence of (2) and (3).

Suppose that K has characteristic p and $L = K(\alpha)$ with $\alpha \notin K$ and $\alpha^p \in K$. Then $\text{Trace}_{L/K}(1) = p = 0$. For $i = 1, \ldots, p-1$ we see that $x^p - \alpha^{pi}$ is the minimal polynomial for α^i over K and we find $\text{Trace}_{L/K}(\alpha^i) = 0$ by Lemma 20.3. Hence for this kind of purely inseparable degree p extension we see that $\text{Trace}_{L/K}$ is identically zero.

Assume that L/K is not separable. Then there exists a subfield $L/K'/K$ such that L/K' is a purely inseparable degree p extension as in the previous paragraph, see Lemmas 14.6 and 14.5. Hence by Lemma 20.5 we see that $\text{Trace}_{L/K}$ is identically zero.

Assume on the other hand that L/K is separable. By induction on the degree we will show that $\text{Trace}_{L/K}$ is not identically zero. Thus by Lemma 20.5 we may assume that L/K is generated by a single element α (use that if the trace is nonzero then it is surjective). We have to show that $\text{Trace}_{L/K}(\alpha^e)$ is nonzero for some $e \geq 0$. Let $P = x^d + a_1x^{d-1} + \ldots + a_d$ be the minimal polynomial of α over K. Then P is also the characteristic polynomial of the linear maps $\alpha : L \to L$, see Lemma 20.2. Since L/k is separable we see from Lemma 12.4 that P has d pairwise distinct roots $\alpha_1, \ldots, \alpha_d$ in an algebraic closure $\overline{K}$ of K. Thus these are the eigenvalues of $\alpha : L \to L$. By linear algebra, the trace of α^e is equal to $\alpha_1^e + \ldots + \alpha_d^e$. Thus we conclude by Lemma 13.2. □

Let K be a field and let $Q : V \times V \to K$ be a bilinear form on a finite dimensional vector space over K. Say $\dim_K(V) = n$. Then Q defines a linear map $Q : V \to V^*$, $v \mapsto Q(v, -)$ where $V^* = \text{Hom}_K(V, K)$ is the dual vector space. Hence a linear map

$$\det(Q) : \wedge^n(V) \longrightarrow \wedge^n(V)^*$$

If we pick a basis element $\omega \in \wedge^n(V)$, then we can write $\det(Q)(\omega) = \lambda\omega^*$, where ω^* is the dual basis element in $\wedge^n(V)^*$. If we change our choice of ω into $c\omega$ for some $c \in K^*$, then ω^* changes into $c^{-1}\omega^*$ and therefore λ changes into $c^2\lambda$. Thus the class of λ in $K/(K^*)^2$ is well defined and is called the *discriminant of* Q. Unwinding the definitions we see that

$$\lambda = \det(Q(v_i, v_j)_{1 \leq i,j \leq n})$$

if $\{v_1, \ldots, v_n\}$ is a basis for V over K. Observe that the discriminant is nonzero if and only if Q is nondegenerate.

Definition 20.8. Let L/K be a finite extension of fields. The *discriminant of* L/K is the discriminant of the trace pairing $Q_{L/K}$.

By the discussion above and Lemma 20.7 we see that the discriminant is nonzero if and only if L/K is separable. For $a \in K$ we often say "the discriminant is a" when it would be more correct to say the discriminant is the class of a in $K/(K^*)^2$.

Exercise 20.9. Let L/K be an extension of degree 2. Show that exactly one of the following happens

(1) the discriminant is 0, the characteristic of K is 2, and L/K is purely inseparable obtained by taking a square root of an element of K,

(2) the discriminant is 1, the characteristic of K is 2, and L/K is separable of degree 2,
(3) the discriminant is not a square, the characteristic of K is not 2, and L is obtained from K by taking the square root of the discriminant.

21. Galois theory

Here is the definition.

Definition 21.1. A field extension E/F is called *Galois* if it is algebraic, separable, and normal.

It turns out that a finite extension is Galois if and only if it has the "correct" number of automorphisms.

Lemma 21.2. *Let E/F be a finite extension of fields. Then E is Galois over F if and only if $|Aut(E/F)| = [E : F]$.*

Proof. Assume $|\text{Aut}(E/F)| = [E : F]$. By Lemma 15.9 this implies that E/F is separable and normal, hence Galois. Conversely, if E/F is separable then $[E : F] = [E : F]_s$ and if E/F is in addition normal, then Lemma 15.9 implies that $|\text{Aut}(E/F)| = [E : F]$. □

Motivated by the lemma above we introduce the Galois group as follows.

Definition 21.3. If E/F is a Galois extension, then the group $\text{Aut}(E/F)$ is called the *Galois group* and it is denoted $\text{Gal}(E/F)$.

If L/K is an infinite Galois extension, then one should think of the Galois group as a topological group. We will return to this in Section 22.

Lemma 21.4. *Let $K/E/F$ be a tower of algebraic field extensions. If K is Galois over F, then K is Galois over E.*

Proof. Combine Lemmas 15.2 and 12.3. □

Lemma 21.5. *Let L/K be a finite separable extension of fields. Let M be the normal closure of L over K (Definition 16.4). Then M/K is Galois.*

Proof. The subextension $M/M_{sep}/K$ of Lemma 14.6 is normal by Lemma 15.4. Since L/K is separable we have $L \subset M_{sep}$. By minimality $M = M_{sep}$ and the proof is done. □

Let G be a group acting on a field K (by field automorphisms). We will often use the notation

$$K^G = \{x \in K \mid \sigma(x) = x \ \forall \sigma \in G\}$$

and we will call this the *fixed field* for the action of G on K.

Lemma 21.6. *Let K be a field. Let G be a finite group acting faithfully on K. Then the extension K/K^G is Galois, we have $[K : K^G] = |G|$, and the Galois group of the extension is G.*

Proof. Given $\alpha \in K$ consider the orbit $G \cdot \alpha \subset K$ of α under the group action. Consider the polynomial

$$P = \prod\nolimits_{\beta \in G \cdot \alpha} (x - \beta) \in K[x]$$

The key to the whole lemma is that this polynomial is invariant under the action of G and hence has coefficients in K^G. Namely, for $\tau \in G$ we have

$$P^\tau = \prod\nolimits_{\beta \in G \cdot \alpha} (x - \tau(\beta)) = \prod\nolimits_{\beta \in G \cdot \alpha} (x - \beta) = P$$

because the map $\beta \mapsto \tau(\beta)$ is a permutation of the orbit $G \cdot \alpha$. Thus $P \in K^G[x]$. Since also $P(\alpha) = 0$ as α is an element of its orbit we conclude that the extension K/K^G is algebraic. Moreover, the minimal polynomial Q of α over K^G divides the polynomial P just constructed. Hence Q is separable (by Lemma 12.4 for example) and we conclude that K/K^G is separable. Thus K/K^G is Galois. To finish the proof it suffices to show that $[K : K^G] = |G|$ since then G will be the Galois group by Lemma 21.2.

Pick finitely many elements $\alpha_i \in K$, $i = 1, \ldots, n$ such that $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, n$ implies σ is the neutral element of G. Set

$$L = K^G(\{\sigma(\alpha_i); 1 \leq i \leq n, \sigma \in G\}) \subset K$$

and observe that the action of G on K induces an action of G on L. We will show that L has degree $|G|$ over K^G. This will finish the proof, since if $L \subset K$ is proper, then we can add an element $\alpha \in K$, $\alpha \notin L$ to our list of elements $\alpha_1, \ldots, \alpha_n$ without increasing L which is absurd. This reduces us to the case that K/K^G is finite which is treated in the next paragraph.

Assume K/K^G is finite. By Lemma 19.1 we can find $\alpha \in K$ such that $K = K^G(\alpha)$. By the construction in the first paragraph of this proof we see that α has degree at most $|G|$ over K. However, the degree cannot be less than $|G|$ as G acts faithfully on $K^G(\alpha) = L$ by construction and the inequality of Lemma 15.9. □

Theorem 21.7 (Fundamental theorem of Galois theory)**.** *Let L/K be a finite Galois extension with Galois group G. Then we have $K = L^G$ and the map*

$$\{\textit{subgroups of } G\} \longrightarrow \{\textit{subextensions } L/M/K\}, \quad H \longmapsto L^H$$

is a bijection whose inverse maps M to Gal(L/M). The normal subgroups H of G correspond exactly to those subextensions M with M/K Galois.

Proof. By Lemma 21.4 given a subextension $L/M/K$ the extension L/M is Galois. Of course L/M is also finite (Lemma 7.3). Thus $|\text{Gal}(L/M)| = [L : M]$ by Lemma 21.2. Conversely, if $H \subset G$ is a finite subgroup, then $[L : L^H] = |H|$ by Lemma 21.6. It follows formally from these two observations that we obtain a bijective correspondence as in the theorem.

If $H \subset G$ is normal, then L^H is fixed by the action of G and we obtain a canonical map $G/H \to \text{Aut}(L^H/K)$. This map has to be injective as $\text{Gal}(L/L^H) = H$. Hence $|G/H| = [L^H : K]$ and L^H is Galois by Lemma 21.2.

Conversely, assume that $K \subset M \subset L$ with M/K Galois. By Lemma 15.7 we see that every element $\tau \in \text{Gal}(L/K)$ induces an element $\tau|_M \in \text{Gal}(M/K)$. This induces a homomorphism of Galois groups $\text{Gal}(L/K) \to \text{Gal}(M/K)$ whose kernel is H. Thus H is a normal subgroup. □

Lemma 21.8. *Let $L/M/K$ be a tower of fields. Assume L/K and M/K are finite Galois. Then we obtain a short exact sequence*

$$1 \to \textit{Gal}(L/M) \to \textit{Gal}(L/K) \to \textit{Gal}(M/K) \to 1$$

of finite groups.

Proof. Namely, by Lemma 15.7 we see that every element $\tau \in \text{Gal}(L/K)$ induces an element $\tau|_M \in \text{Gal}(M/K)$ which gives us the homomorphism on the right. The map on the left identifies the left group with the kernel of the right arrow. The sequence is exact because the sizes of the groups work out correctly by multiplicativity of degrees in towers of finite extensions (Lemma 7.7). One can also use Lemma 15.7 directly to see that the map on the right is surjective. □

22. Infinite Galois theory

The Galois group comes with a canonical topology.

Lemma 22.1. *Let E/F be a Galois extension. Endow Gal(E/F) with the coarsest topology such that*

$$Gal(E/F) \times E \longrightarrow E$$

is continuous when E is given the discrete topology. Then

1. *for any topological space X and map $X \to Aut(E/F)$ such that the action $X \times E \to E$ is continuous the induced map $X \to Gal(E/F)$ is continuous,*
2. *this topology turns Gal(E/F) into a profinite topological group.*

Proof. Throughout this proof we think of E as a discrete topological space. Recall that the compact open topology on the set of self maps $\text{Map}(E, E)$ is the universal topology such that the action $\text{Map}(E, E) \times E \to E$ is continuous. See Topology, Example 30.2 for a precise statement. The topology of the lemma on $\text{Gal}(E/F)$ is the induced topology coming from the injective map $\text{Gal}(E/F) \to \text{Map}(E, E)$. Hence the universal property (1) follows from the corresponding universal property of the compact open topology. Since the set of invertible self maps $\text{Aut}(E)$ endowed with the compact open topology forms a topological group, see Topology, Example 30.2, and since $\text{Gal}(E/F) = \text{Aut}(E/F) \to \text{Map}(E, E)$ factors through $\text{Aut}(E)$ we obtain a topological group. In other words, we are using the injection

$$\text{Gal}(E/F) \subset \text{Aut}(E)$$

to endow $\text{Gal}(E/F)$ with the induced structure of a topological group (see Topology, Section 30) and by construction this is the coarsest structure of a topological group such that the action $\text{Gal}(E/F) \times E \to E$ is continuous.

To show that $\text{Gal}(E/F)$ is profinite we argue as follows (our argument is necessarily nonstandard because we have defined the topology before showing that the Galois group is an inverse limit of finite groups). By Topology, Lemma 30.4 it suffices to show that the underlying topological space of $\text{Gal}(E/F)$ is profinite. For any subset $S \subset E$ consider the set

$$G(S) = \{f : S \to E \mid \begin{array}{c} f(\alpha) \text{ is a root of the minimal polynomial} \\ \text{of } \alpha \text{ over } F \text{ for all } \alpha \in S \end{array}\}$$

Since a polynomial has only a finite number of roots we see that $G(S)$ is finite for all $S \subset E$ finite. If $S \subset S'$ then restriction gives a map $G(S') \to G(S)$. Also, observe that if $\alpha \in S \cap F$ and $f \in G(S)$, then $f(\alpha) = \alpha$ because the minimal polynomial is linear in this case. Consider the profinite topological space

$$G = \lim_{S \subset E \text{ finite}} G(S)$$

Consider the canonical map

$$c : \mathrm{Gal}(E/F) \longrightarrow G, \quad \sigma \longmapsto (\sigma|_S : S \to E)_S$$

This is injective and unwinding the definitions the reader sees the topology on $\mathrm{Gal}(E/F)$ as defined above is the induced topology from G. An element $(f_S) \in G$ is in the image of c exactly if (A) $f_S(\alpha) + f_S(\beta) = f_S(\alpha + \beta)$ and (M) $f_S(\alpha)f_S(\beta) = f_S(\alpha\beta)$ whenever this makes sense (i.e., $\alpha, \beta, \alpha + \beta, \alpha\beta \in S$). Namely, this means $\lim f_S : E \to E$ will be an F-algebra map and hence an automorphism by Lemma 8.11. The conditions (A) and (M) for a given triple (S, α, β) define a closed subset of G and hence $\mathrm{Gal}(E/F)$ is homeomorphic to a closed subset of a profinite space and therefore profinite itself. □

Lemma 22.2. *Let $L/M/K$ be a tower of fields. Assume both L/K and M/K are Galois. Then there is a canonical surjective continuous homomorphism c : $Gal(L/K) \to Gal(M/K)$.*

Proof. By Lemma 15.7 given $\tau : L \to L$ in $\mathrm{Gal}(L/K)$ the restriction $\tau|_M : M \to M$ is an element of $\mathrm{Gal}(M/K)$. This defines the homomorphism c. Continuity follows from the universal property of the topology: the action

$$\mathrm{Gal}(L/K) \times M \longrightarrow M, \quad (\tau, x) \longmapsto \tau(x) = c(\tau)(x)$$

is continuous as $M \subset L$ and the action $\mathrm{Gal}(L/K) \times L \to L$ is continuous. Hence continuity of c by part (1) of Lemma 22.1. Lemma 15.7 also shows that the map is surjective. □

Here is a more standard way to think about the Galois group of an infinite Galois extension.

Lemma 22.3. *Let L/K be a Galois extension with Galois group G. Let Λ be the set of finite Galois subextensions, i.e., $\lambda \in \Lambda$ corresponds to $L/L_\lambda/K$ with L_λ/K finite Galois with Galois group G_λ. Define a partial ordering on Λ by the rule $\lambda \geq \lambda'$ if and only if $L_\lambda \supset L_{\lambda'}$. Then*

(1) *Λ is a directed partially ordered set,*
(2) *L_λ is a system of K-extensions over Λ and $L = \operatorname{colim} L_\lambda$,*
(3) *G_λ is an inverse system of finite groups over Λ, the transition maps are surjective, and*

$$G = \lim_{\lambda \in \Lambda} G_\lambda$$

as a profinite group, and
(4) *each of the projections $G \to G_\lambda$ is continuous and surjective.*

Proof. Every subfield of L containing K is separable over K (follows immediately from the definition). Let $S \subset L$ be a finite subset. Then $K(S)/K$ is finite and there exists a tower $L/E/K(S)/K$ such that E/K is finite Galois, see Lemma 16.5. Hence $E = L_\lambda$ for some $\lambda \in \Lambda$. This certainly implies the set Λ is not empty. Also, given $\lambda_1, \lambda_2 \in \Lambda$ we can write $L_{\lambda_i} = K(S_i)$ for finite sets $S_1, S_2 \subset L$ (Lemma 7.5). Then there exists a $\lambda \in \Lambda$ such that $K(S_1 \cup S_2) \subset L_\lambda$. Hence $\lambda \geq \lambda_1, \lambda_2$ and Λ is directed (Categories, Definition 21.4). Finally, since every element in L is contained in L_λ for some $\lambda \in \Lambda$, it follows from the description of filtered colimits in Categories, Section 19 that $\operatorname{colim} L_\lambda = L$.

If $\lambda \geq \lambda'$ in Λ, then we obtain a canonical surjective map $G_\lambda \to G_{\lambda'}$, $\sigma \mapsto \sigma|_{L_{\lambda'}}$ by Lemma 21.8. Thus we get an inverse system of finite groups with surjective transition maps.

Recall that $G = \text{Aut}(L/K)$. By Lemma 22.2 the restriction $\sigma|_{L_\lambda}$ of a $\sigma \in G$ to L_λ is an element of G_λ. Moreover, this procedure gives a continuous surjection $G \to G_\lambda$. Since the transition mappings in the inverse system of G_λ are given by restriction also, it is clear that we obtain a canonical continuous map

$$G \longrightarrow \lim\nolimits_{\lambda \in \Lambda} G_\lambda$$

Continuity by definition of limits in the category of topological groups; recall that these limits commute with the forgetful functor to the categories of sets and topological spaces by Topology, Lemma 30.3. On the other hand, since $L = \text{colim}\, L_\lambda$ it is clear that any element of the inverse limit (viewed as a set) defines an automorphism of L. Thus the map is bijective. Since the topology on both sides is profinite, and since a bijective continuous map of profinite spaces is a homeomorphism (Topology, Lemma 17.8), the proof is complete. □

Theorem 22.4 (Fundamental theorem of infinite Galois theory)**.** *Let L/K be a Galois extension. Let $G = Gal(L/K)$ be the Galois group viewed as a profinite topological group (Lemma 22.1). Then we have $K = L^G$ and the map*

$$\{\textit{closed subgroups of } G\} \longrightarrow \{\textit{subextensions } L/M/K\}, \quad H \longmapsto L^H$$

is a bijection whose inverse maps M to $Gal(L/M)$. The finite subextensions M correspond exactly to the open subgroups $H \subset G$. The normal closed subgroups H of G correspond exactly to subextensions M Galois over K.

Proof. We will use the result of finite Galois theory (Theorem 21.7) without further mention. Let $S \subset L$ be a finite subset. There exists a tower $L/E/K$ such that $K(S) \subset E$ and such that E/K is finite Galois, see Lemma 16.5. In other words, we see that L/K is the union of its finite Galois subextensions. For such an E, by Lemma 22.2 the map $\text{Gal}(L/K) \to \text{Gal}(E/K)$ is surjective and continuous, i.e., the kernel is open because the topology on $\text{Gal}(E/K)$ is discrete. In particular we see that no element of $L \setminus K$ is fixed by $\text{Gal}(L/K)$ as $E^{\text{Gal}(E/K)} = K$. This proves that $L^G = K$.

By Lemma 21.4 given a subextension $L/M/K$ the extension L/M is Galois. It is immediate from the definition of the topology on G that the subgroup $\text{Gal}(L/M)$ is closed. By the above applied to L/M we see that $L^{\text{Gal}(L/M)} = M$.

Conversely, let $H \subset G$ be a closed subgroup. We claim that $H = \text{Gal}(L/L^H)$. The inclusion $H \subset \text{Gal}(L/L^H)$ is clear. Suppose that $g \in \text{Gal}(L/L^H)$. Let $S \subset L$ be a finite subset. We will show that the open neighbourhood $U_S(g) = \{g' \in G \mid g'(s) = g(s)\}$ of g meets H. This implies that $g \in H$ because H is closed. Let $L/E/K$ be a finite Galois subextension containing $K(S)$ as in the first paragraph of the proof and consider the homomorphism $c : \text{Gal}(L/K) \to \text{Gal}(E/K)$. Then $L^H \cap E = E^{c(H)}$. Since g fixes L^H it fixes $E^{c(H)}$ and hence $c(g) \in c(H)$ by finite Galois theory. Pick $h \in H$ with $c(h) = c(g)$. Then $h \in U_S(g)$ as desired.

At this point we have established the correspondence between closed subgroups and subextensions.

Assume $H \subset G$ is open. Arguing as above we find that H containes $\text{Gal}(L/E)$ for some large enough finite Galois subextension E and we find that L^H is contained in E whence finite over K. Conversely, if M is a finite subextension, then M is generated by a finite subset S and the corresponding subgroup is the open subset $U_S(e)$ where $e \in G$ is the neutral element.

Assume that $K \subset M \subset L$ with M/K Galois. By Lemma 22.2 there is a surjective continuous homomorphism of Galois groups $\text{Gal}(L/K) \to \text{Gal}(M/K)$ whose kernel is $\text{Gal}(L/M)$. Thus $\text{Gal}(L/M)$ is a normal closed subgroup.

Finally, assume $N \subset G$ is normal and closed. For any $L/E/K$ as in the first paragraph of the proof, the image $c(N) \subset \text{Gal}(E/K)$ is a normal subgroup. Hence $L^N = \bigcup E^{c(N)}$ is a union of Galois extensions of K (by finite Galois theory) whence Galois over K. □

Lemma 22.5. *Let $L/M/K$ be a tower of fields. Assume L/K and M/K are Galois. Then we obtain a short exact sequence*

$$1 \to Gal(L/M) \to Gal(L/K) \to Gal(M/K) \to 1$$

of profinite topological groups.

Proof. This is a reformulation of Lemma 22.2. □

23. The complex numbers

The fundamental theorem of algebra states that the field of complex numbers is an algebraically closed field. In this section we discuss this briefly.

The first remark we'd like to make is that you need to use a little bit of input from calculus in order to prove this. We will use the intuitively clear fact that every odd degree polynomial over the reals has a real root. Namely, let $P(x) = a_{2k+1}x^{2k+1} + \ldots + a_0 \in \mathbf{R}[x]$ for some $k \geq 0$ and $a_{2k+1} \neq 0$. We may and do assume $a_{2k+1} > 0$. Then for $x \in \mathbf{R}$ very large (positive) we see that $P(x) > 0$ as the term $a_{2k+1}x^{2k+1}$ dominates all the other terms. Similarly, if $x \ll 0$, then $P(x) < 0$ by the same reason (and this is where we use that the degree is odd). Hence by the intermediate value theorem there is an $x \in \mathbf{R}$ with $P(x) = 0$.

A conclusion we can draw from the above is that $\mathbf{R}$ has no nontrivial odd degree field extensions, as elements of such extensions would have odd degree minimal polynomials.

Next, let $K/\mathbf{R}$ be a finite Galois extension with Galois group G. Let $P \subset G$ be a 2-sylow subgroup. Then $K^P/\mathbf{R}$ is an odd degree extension, hence by the above $K^P = \mathbf{R}$, which in turn implies $G = P$. (All of these arguments rely on Galois theory of course.) Thus G is a 2-group. If G is nontrivial, then we see that $\mathbf{C} \subset K$ as $\mathbf{C}$ is (up to isomorphism) the only degree 2 extension of $\mathbf{R}$. If G has more than 2 elements we would obtain a quadratic extension of $\mathbf{C}$. This is absurd as every complex number has a square root.

The conclusion: $\mathbf{C}$ is algebraically closed. Namely, if not then we'd get a nontrivial finite extension $K/\mathbf{C}$ which we could assume normal (hence Galois) over $\mathbf{R}$ by Lemma 16.3. But we've seen above that then $K = \mathbf{C}$.

Lemma 23.1 (Fundamental theorem of algebra)**.** *The field $\mathbf{C}$ is algebraically closed.*

Proof. See discussion above. □

24. Kummer extensions

Let K be a field. Let $n \geq 2$ be an integer such that K contains a primitive nth root of 1. Let $a \in K$. Let L be an extension of K obtained by adjoining a root b of the equation $x^n = a$. Then L/K is Galois. If $G = \text{Gal}(L/K)$ is the Galois group, then the map

$$G \longrightarrow \mu_n(K), \quad \sigma \longmapsto \sigma(b)/b$$

is an injective homomorphism of groups. In particular, G is cyclic of order dividing n as a subgroup of the cyclic group $\mu_n(K)$. Kummer theory gives a converse.

Lemma 24.1 (Kummer extensions)**.** *Let L/K be a Galois extension of fields whose Galois group is $\mathbf{Z}/n\mathbf{Z}$. Assume moreover that the characteristic of K is prime to n and that K contains a primitive nth root of 1. Then $L = K[z]$ with $z^n \in K$.*

Proof. Let $\zeta \in K$ be a primitive nth root of 1. Let σ be a generator of $\text{Gal}(L/K)$. Consider $\sigma : L \to L$ as a K-linear operator. Note that $\sigma^n - 1 = 0$ as a linear operator. Applying linear independence of characters (Lemma 13.1), we see that there cannot be a polynomial over K of degree $< n$ annihilating σ. Hence the minimal polynomial of σ as a linear operator is $x^n - 1$. Since ζ is a root of $x^n - 1$ by linear algebra there is a $0 \neq z \in L$ such that $\sigma(z) = \zeta z$. This z satisfies $z^n \in K$ because $\sigma(z^n) = (\zeta z)^n = z^n$. Moreover, we see that $z, \sigma(z), \ldots, \sigma^{n-1}(z) = z, \zeta z, \ldots \zeta^{n-1} z$ are pairwise distinct which guarantees that z generates L over K. Hence $L = K[z]$ as required. □

Lemma 24.2. *Let K be a field with algebraic closure $\overline{K}$. Let p be a prime different from the characteristic of K. Let $\zeta \in \overline{K}$ be a primitive pth root of 1. Then $K(\zeta)/K$ is a Galois extension of degree dividing $p - 1$.*

Proof. The polynomial $x^p - 1$ splits completely over $K(\zeta)$ as its roots are $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. Hence $K(\zeta)/K$ is a splitting field and hence normal. The extension is separable as $x^p - 1$ is a separable polynomial. Thus the extension is Galois. Any automorphism of $K(\zeta)$ over K sends ζ to ζ^i for some $1 \leq i \leq p - 1$. Thus the Galois group is a subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$. □

Lemma 24.3. *Let K be a field. Let L/K be a finite extension of degree e which is generated by an element α with $a = \alpha^e \in K$. Then any sub extension $L/L'/K$ is generated by α^d for some $d|e$.*

Proof. Observe that for $d|e$ the subfield $K(\alpha^d)$ has $[K(\alpha^d) : K] = e/d$ and $[L : K(\alpha^d)] = d$ and that both extensions $K(\alpha^d)/K$ and $L/K(\alpha^d)$ are extensions as in the lemma.

We will use induction on the pair of integers $([L : L'], [L' : K])$ ordered lexicographically. Let p be a prime number dividing e and set $d = e/p$. If $K(\alpha^d)$ is contained in L', then we win by induction, because then it suffices to prove the lemma for $L/L'/K(\alpha^d)$. If not, then $[L'(\alpha^d) : L'] = p$ and by induction hypothesis we have $L'(\alpha^d) = K(\alpha^i)$ for some $i|d$. If $i \neq 1$ we are done by induction. Thus we may assume that $[L : L'] = p$.

If e is not a power of p, then we can do this trick again with a second prime number and we win. Thus we may assume e is a power of p.

If the characteristic of K is p and e is a pth power, then L/K is purely inseparable. Hence L/L' is purely inseparable of degree p and hence $\alpha^p \in L'$. Thus $L' = K(\alpha^p)$ and this case is done.

The final case is where e is a power of p, the characteristic of K is not p, L/L' is a degree p extension, and $L = L'(\alpha^{e/p})$. Claim: this can only happen if $e = p$ and $L' = K$. The claim finishes the proof.

First, we prove the claim when K contains a primitive pth root of unity ζ. In this case the degree p extension $K(\alpha^{e/p})/K$ is Galois with Galois group generated by the automorphism $\alpha^{e/p} \mapsto \zeta\alpha^{e/p}$. On the other hand, since L is generated by $\alpha^{e/p}$ and L' we see that the map

$$K(\alpha^{e/p}) \otimes_K L' \longrightarrow L$$

is an isomorphism of K-algebras (look at dimensions). Thus L has an automorphism σ of order p over K sending $\alpha^{e/p}$ to $\zeta\alpha^{e/p}$. Then $\sigma(\alpha) = \zeta'\alpha$ for some eth root of unity ζ' (as α^e is in K). Then on the one hand $(\zeta')^{e/p} = \zeta$ and on the other hand ζ' has to be a pth root of 1 as σ has order p. Thus $e/p = 1$ and the claim has been shown.

Finally, suppose that K does not contain a primitive pth root of 1. Choose a primitive pth root ζ in some algebraic closure $\overline{L}$ of L. Consider the diagram

$$\begin{tikzcd}
K(\zeta) \arrow[r] & L(\zeta) \\
K \arrow[r] \arrow[u] & L \arrow[u]
\end{tikzcd}$$

By Lemma 24.2 the vertical extensions have degree prime to p. Hence $[L(\zeta) : K(\zeta)]$ is divisible by e. On the other hand, $L(\zeta)$ is generated by α over $K(\zeta)$ and hence $[L(\zeta) : K(\zeta)] \leq e$. Thus $[L(\zeta) : K(\zeta)] = e$. Similarly we have $[K(\alpha^{e/p}, \zeta) : K(\zeta)] = p$ and $[L(\zeta) : L'(\zeta)] = p$. Thus the fields $K(\zeta), L'(\zeta), L(\zeta)$ and the element α fall into the case discussed in the previous paragraph we conclude $e = p$ as desired. □

25. Artin-Schreier extensions

Let K be a field of characteristic $p > 0$. Let $a \in K$. Let L be an extension of K obtained by adjoining a root b of the equation $x^p - x = a$. Then L/K is Galois. If $G = \mathrm{Gal}(L/K)$ is the Galois group, then the map

$$G \longrightarrow \mathbf{Z}/p\mathbf{Z}, \quad \sigma \longmapsto \sigma(b) - b$$

is an injective homomorphism of groups. In particular, G is cyclic of order dividing p as a subgroup of $\mathbf{Z}/p\mathbf{Z}$. The theory of Artin-Schreier extensions gives a converse.

Lemma 25.1 (Artin-Schreier extensions)**.** *Let L/K be a Galois extension of fields of characteristic $p > 0$ with Galois group $\mathbf{Z}/p\mathbf{Z}$. Then $L = K[z]$ with $z^p - z \in K$.*

Proof. Let σ be a generator of $\mathrm{Gal}(L/K)$. Consider $\sigma : L \to L$ as a K-linear operator. Observe that $\sigma^p - 1 = 0$ as a linear operator. Applying linear independence of characters (Lemma 13.1), there cannot be a polynomial of degree $< p$ annihilating σ. We conclude that the minimal polynomial of σ is $x^p - 1 = (x-1)^p$. This implies that there exists $w \in L$ such that $(\sigma - 1)^{p-1}(w) = y$ is nonzero. Then $\sigma(y) = y$, i.e., $y \in K$. Thus $z = y^{-1}(\sigma - 1)^{p-2}(w)$ satisfies $\sigma(z) = z + 1$. Since $z \notin K$ we have $L = K[z]$. Moreover since $\sigma(z^p - z) = (z+1)^p - (z+1) = z^p - z$ we see that $z^p - z \in K$ and the proof is complete. $\square$

26. Transcendence

We recall the standard definitions.

Definition 26.1. Let K/k be a field extension.

(1) A collection of elements $\{x_i\}_{i\in I}$ of K is called *algebraically independent* over k if the map
$$k[X_i; i \in I] \longrightarrow K$$
which maps X_i to x_i is injective.

(2) The field of fractions of a polynomial ring $k[x_i; i \in I]$ is denoted $k(x_i; i \in I)$.

(3) A *purely transcendental extension* of k is any field extension K/k isomorphic to the field of fractions of a polynomial ring over k.

(4) A *transcendence basis* of K/k is a collection of elements $\{x_i\}_{i\in I}$ which are algebraically independent over k and such that the extension $K/k(x_i; i \in I)$ is algebraic.

Example 26.2. The field $\mathbf{Q}(\pi)$ is purely transcendental because π isn't the root of a nonzero polynomial with rational coefficients. In particular, $\mathbf{Q}(\pi) \cong \mathbf{Q}(x)$.

Lemma 26.3. *Let E/F be a field extension. A transcendence basis of E over F exists. Any two transcendence bases have the same cardinality.*

Proof. Let A be an algebraically independent subset of E. Let G be a subset of E containing A that generates E/F. We claim we can find a transcendence basis B such that $A \subset B \subset G$. To prove this, consider the collection $\mathcal{B}$ of algebraically independent subsets whose members are subsets of G that contain A. Define a partial ordering on $\mathcal{B}$ using inclusion. Then $\mathcal{B}$ contains at least one element A. The union of the elements of a totally ordered subset T of $\mathcal{B}$ is an algebraically independent subset of E over F since any algebraic dependence relation would have occurred in one of the elements of T (since polynomials only involve finitely many variables). The union also contains A and is contained in G. By Zorn's lemma, there is a maximal element $B \in \mathcal{B}$. Now we claim E is algebraic over $F(B)$. This is because if it wasn't then there would be an element $f \in G$ transcendental over $F(B)$ since $F(G) = E$. Then $B \cup \{f\}$ would be algebraically independent contradicting the maximality of B. Thus B is our transcendence basis.

Let B and B' be two transcendence bases. Without loss of generality, we can assume that $|B'| \leq |B|$. Now we divide the proof into two cases: the first case is that B is an infinite set. Then for each $\alpha \in B'$, there is a finite set $B_\alpha \subset B$ such that α is algebraic over $F(B_\alpha)$ since any algebraic dependence relation only uses finitely many indeterminates. Then we define $B^* = \bigcup_{\alpha \in B'} B_\alpha$. By construction, $B^* \subset B$, but we claim that in fact the two sets are equal. To see this, suppose that they are not equal, say there is an element $\beta \in B \setminus B^*$. We know β is algebraic over $F(B')$ which is algebraic over $F(B^*)$. Therefore β is algebraic over $F(B^*)$, a contradiction. So $|B| \leq |\bigcup_{\alpha \in B'} B_\alpha|$. Now if B' is finite, then so is B so we can assume B' is infinite; this means
$$|B| \leq |\bigcup\nolimits_{\alpha \in B'} B_\alpha| = |B'|$$
because each B_α is finite and B' is infinite. Therefore in the infinite case, $|B| = |B'|$.

Now we need to look at the case where B is finite. In this case, B' is also finite, so suppose $B = \{\alpha_1, \dots, \alpha_n\}$ and $B' = \{\beta_1, \dots, \beta_m\}$ with $m \leq n$. We perform induction on m: if $m = 0$ then E/F is algebraic so $B = \emptyset$ so $n = 0$. If $m > 0$, there is an irreducible polynomial $f \in F[x, y_1, \dots, y_n]$ such that $f(\beta_1, \alpha_1, \dots, \alpha_n) = 0$ and such that x occurs in f. Since β_1 is not algebraic over F, f must involve some y_i so without loss of generality, assume f uses y_1. Let $B^* = \{\beta_1, \alpha_2, \dots, \alpha_n\}$. We claim that B^* is a basis for E/F. To prove this claim, we see that we have a tower of algebraic extensions

$$E/F(B^*, \alpha_1)/F(B^*)$$

since α_1 is algebraic over $F(B^*)$. Now we claim that B^* (counting multiplicity of elements) is algebraically independent over F because if it weren't, then there would be an irreducible $g \in F[x, y_2, \dots, y_n]$ such that $g(\beta_1, \alpha_2, \dots, \alpha_n) = 0$ which must involve x making β_1 algebraic over $F(\alpha_2, \dots, \alpha_n)$ which would make α_1 algebraic over $F(\alpha_2, \dots, \alpha_n)$ which is impossible. So this means that $\{\alpha_2, \dots, \alpha_n\}$ and $\{\beta_2, \dots, \beta_m\}$ are bases for E over $F(\beta_1)$ which means by induction, $m = n$. □

Definition 26.4. Let K/k be a field extension. The *transcendence degree* of K over k is the cardinality of a transcendence basis of K over k. It is denoted $\mathrm{trdeg}_k(K)$.

Lemma 26.5. *Let $L/K/k$ be field extensions. Then*

$$trdeg_k(L) = trdeg_K(L) + trdeg_k(K).$$

Proof. Choose a transcendence basis $A \subset K$ of K over k. Choose a transcendence basis $B \subset L$ of L over K. Then it is straightforward to see that $A \cup B$ is a transcendence basis of L over k. □

Example 26.6. Consider the field extension $\mathbf{Q}(e, \pi)$ formed by adjoining the numbers e and π. This field extension has transcendence degree at least 1 since both e and π are transcendental over the rationals. However, this field extension might have transcendence degree 2 if e and π are algebraically independent. Whether or not this is true is unknown and whence the problem of determining $\mathrm{trdeg}(\mathbf{Q}(e, \pi))$ is open.

Example 26.7. Let F be a field and $E = F(t)$. Then $\{t\}$ is a transcendence basis since $E = F(t)$. However, $\{t^2\}$ is also a transcendence basis since $F(t)/F(t^2)$ is algebraic. This illustrates that while we can always decompose an extension E/F into an algebraic extension E/F' and a purely transcendental extension F'/F, this decomposition is not unique and depends on choice of transcendence basis.

Example 26.8. Let X be a compact Riemann surface. Then the function field $\mathbf{C}(X)$ (see Example 3.6) has transcendence degree one over $\mathbf{C}$. In fact, *any* finitely generated extension of $\mathbf{C}$ of transcendence degree one arises from a Riemann surface. There is even an equivalence of categories between the category of compact Riemann surfaces and (non-constant) holomorphic maps and the opposite of the category of finitely generated extensions of $\mathbf{C}$ of transcendence degree 1 and morphisms of $\mathbf{C}$-algebras. See [For91].

There is an algebraic version of the above statement as well. Given an (irreducible) algebraic curve in projective space over an algebraically closed field k (e.g. the complex numbers), one can consider its "field of rational functions": basically, functions that look like quotients of polynomials, where the denominator does not identically vanish on the curve. There is a similar anti-equivalence of categories (Algebraic

Curves, Theorem 2.6) between smooth projective curves and non-constant morphisms of curves and finitely generated extensions of k of transcendence degree one. See [Har77].

Definition 26.9. Let K/k be a field extension.

(1) The *algebraic closure of* k *in* K is the subfield k' of K consisting of elements of K which are algebraic over k.
(2) We say k is *algebraically closed in* K if every element of K which is algebraic over k is contained in k.

Lemma 26.10. *Let k'/k be a finite extension of fields. Let $k'(x_1, \ldots, x_r)/k(x_1, \ldots, x_r)$ be the induced extension of purely transcendental extensions. Then $[k'(x_1, \ldots, x_r) : k(x_1, \ldots, x_r)] = [k' : k] < \infty$.*

Proof. By multiplicativity of degrees of extensions (Lemma 7.7) it suffices to prove this when k' is generated by a single element $\alpha \in k'$ over k. Let $f \in k[T]$ be the minimal polynomial of α over k. Then $k'(x_1, \ldots, x_r)$ is generated by $\alpha, x_1, \ldots, x_r$ over k and hence $k'(x_1, \ldots, x_r)$ is generated by α over $k(x_1, \ldots, x_r)$. Thus it suffices to show that f is still irreducible as an element of $k(x_1, \ldots, x_r)[T]$. We only sketch the proof. It is clear that f is irreducible as an element of $k[x_1, \ldots, x_r, T]$ for example because f is monic as a polynomial in T and any putative factorization in $k[x_1, \ldots, x_r, T]$ would lead to a factorization in $k[T]$ by setting x_i equal to 0. By Gauss' lemma we conclude. □

Lemma 26.11. *Let K/k be a finitely generated field extension. The algebraic closure of k in K is finite over k.*

Proof. Let $x_1, \ldots, x_r \in K$ be a transcendence basis for K over k. Then $n = [K : k(x_1, \ldots, x_r)] < \infty$. Suppose that $k \subset k' \subset K$ with k'/k finite. In this case $[k'(x_1, \ldots, x_r) : k(x_1, \ldots, x_r)] = [k' : k] < \infty$, see Lemma 26.10. Hence

$$[k' : k] = [k'(x_1, \ldots, x_r) : k(x_1, \ldots, x_r)] \leq [K : k(x_1, \ldots, x_r)] = n.$$

In other words, the degrees of finite subextensions are bounded and the lemma follows. □

27. Linearly disjoint extensions

Let k be a field, K and L field extensions of k. Suppose also that K and L are embedded in some larger field Ω.

Definition 27.1. Consider a diagram

(27.1.1)
$$\begin{tikzcd} L \arrow[r] & \Omega \\ k \arrow[u] \arrow[r] & K \arrow[u] \end{tikzcd}$$

of field extensions. The *compositum of K and L in Ω* written KL is the smallest subfield of Ω containing both L and K.

It is clear that KL is generated by the set $K \cup L$ over k, generated by the set K over L, and generated by the set L over K.

Warning: The (isomorphism class of the) composition depends on the choice of the embeddings of K and L into Ω. For example consider the number fields $K =$

$\mathbf{Q}(2^{1/8}) \subset \mathbf{R}$ and $L = \mathbf{Q}(2^{1/12}) \subset \mathbf{R}$. The compositum inside $\mathbf{R}$ is the field $\mathbf{Q}(2^{1/24})$ of degree 24 over $\mathbf{Q}$. However, if we embed $K = \mathbf{Q}[x]/(x^8 - 2)$ into $\mathbf{C}$ by mapping x to $2^{1/8}e^{2\pi i/8}$, then the compositum $\mathbf{Q}(2^{1/12}, 2^{1/8}e^{2\pi i/8})$ contains $i = e^{2\pi i/4}$ and has degree 48 over $\mathbf{Q}$ (we omit showing the degree is 48, but the existence of i certainly proves the two composita are not isomorphic).

Definition 27.2. Consider a diagram of fields as in (27.1.1). We say that K and L are *linearly disjoint over k in Ω* if the map

$$K \otimes_k L \longrightarrow KL, \quad \sum x_i \otimes y_i \longmapsto \sum x_i y_i$$

is injective.

The following lemma does not seem to fit anywhere else.

Lemma 27.3. *Let E/F be a normal algebraic field extension. There exist subextensions $E/E_{sep}/F$ and $E/E_{insep}/F$ such that*

1. *$F \subset E_{sep}$ is Galois and $E_{sep} \subset E$ is purely inseparable,*
2. *$F \subset E_{insep}$ is purely inseparable and $E_{insep} \subset E$ is Galois,*
3. *$E = E_{sep} \otimes_F E_{insep}$.*

Proof. We found the subfield E_{sep} in Lemma 14.6. We set $E_{insep} = E^{\mathrm{Aut}(E/F)}$. Details omitted. □

28. Review

In this section we give a quick review of what has transpired above.

Let K/k be a field extension. Let $\alpha \in K$. Then we have the following possibilities:

1. The element α is transcendental over k.
2. The element α is algebraic over k. Denote $P(T) \in k[T]$ its *minimal polynomial*. This is a monic polynomial $P(T) = T^d + a_1 T^{d-1} + \ldots + a_d$ with coefficients in k. It is irreducible and $P(\alpha) = 0$. These properties uniquely determine P, and the integer d is called the *degree of α over k*. There are two subcases:
   (a) The polynomial $\mathrm{d}P/\mathrm{d}T$ is not identically zero. This is equivalent to the condition that $P(T) = \prod_{i=1,\ldots,d}(T - \alpha_i)$ for pairwise distinct elements $\alpha_1, \ldots, \alpha_d$ in the algebraic closure of k. In this case we say that α is *separable* over k.
   (b) The $\mathrm{d}P/\mathrm{d}T$ is identically zero. In this case the characteristic p of k is > 0, and P is actually a polynomial in T^p. Clearly there exists a largest power $q = p^e$ such that P is a polynomial in T^q. Then the element α^q is separable over k.

Definition 28.1. Algebraic field extensions.

1. A field extension K/k is called *algebraic* if every element of K is algebraic over k.
2. An algebraic extension k'/k is called *separable* if every $\alpha \in k'$ is separable over k.
3. An algebraic extension k'/k is called *purely inseparable* if the characteristic of k is $p > 0$ and for every element $\alpha \in k'$ there exists a power q of p such that $\alpha^q \in k$.

(4) An algebraic extension k'/k is called *normal* if for every $\alpha \in k'$ the minimal polynomial $P(T) \in k[T]$ of α over k splits completely into linear factors over k'.
(5) An algebraic extension k'/k is called *Galois* if it is separable and normal.

The following lemma does not seem to fit anywhere else.

Lemma 28.2. *Let K be a field of characteristic $p > 0$. Let L/K be a separable algebraic extension. Let $\alpha \in L$.*

(1) *If the coefficients of the minimal polynomial of α over K are pth powers in K then α is a pth power in L.*
(2) *More generally, if $P \in K[T]$ is a polynomial such that (a) α is a root of P, (b) P has pairwise distinct roots in an algebraic closure, and (c) all coefficients of P are pth powers, then α is a pth power in L.*

Proof. It follows from the definitions that (2) implies (1). Assume P is as in (2). Write $P(T) = \sum_{i=0}^{d} a_i T^{d-i}$ and $a_i = b_i^p$. The polynomial $Q(T) = \sum_{i=0}^{d} b_i T^{d-i}$ has distinct roots in an algebraic closure as well, because the roots of Q are the pth roots of the roots of P. If α is not a pth power, then $T^p - \alpha$ is an irreducible polynomial over L (Lemma 14.2). Moreover Q and $T^p - \alpha$ have a root in common in an algebraic closure $\overline{L}$. Thus Q and $T^p - \alpha$ are not relatively prime, which implies $T^p - \alpha | Q$ in $L[T]$. This contradicts the fact that the roots of Q are pairwise distinct. □

29. Other chapters

Preliminaries

Schemes

Topics in Scheme Theory

Algebraic Spaces

Topics in Geometry

Deformation Theory

Algebraic Stacks

Topics in Moduli Theory

Miscellany

References

[For91] Otto Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics, vol. 81, Springer-Verlag, New York, 1991, Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, 1977.