Contents

2 Fields and Extensions 3
1 Introduction . . . 3
1.1 Examples . . . 3
1.2 The characteristic of a field . . . 5
2 Field extensions . . . 5
2.1 Preliminaries . . . 5
2.2 Finite extensions . . . 7
2.3 Algebraic extensions . . . 8
2.4 Minimal polynomials . . . 10
2.5 Algebraic closure . . . 10
3 Separability and normality . . . 13
3.1 Separable extensions . . . 13
3.2 Purely inseparable extensions . . . 13
4 Galois theory . . . 13
4.1 Definitions . . . 13
4.2 Theorems . . . 13
4.3 Definitions . . . 16
4.4 Theorems . . . 16
5 Transcendental Extensions . . . 18
5.1 Linearly Disjoint Field Extensions . . . 20

Chapter 2
Fields and Extensions

In this chapter, we shall discuss the theory of fields. Recall that a **field** is an integral domain for which all non-zero 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 integral 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.

§1 Introduction

Recall once again that:

Definition 1.1 A **field** is an integral domain where every non-zero element is invertible. Alternatively, it is a set k, endowed with binary operations of addition and multiplication, which satisfy the usual axioms of commutativity, associativity, distributivity, 1 and 0 (and $1 \neq 0$!), and additive and multiplicative inverses.

A **subfield** is a subset closed under these operations: equivalently, it 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.)

1.1 Examples

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 maximal.

Example 1.2 One of the most familiar examples of a field is the rational numbers $\mathbb{Q}$.

Example 1.3 If p is a prime number, then $\mathbb{Z}/(p)$ is a field, denoted $\mathbb{F}_p$. Indeed, (p) is a maximal ideal in $\mathbb{Z}$. Thus, fields may be finite: $\mathbb{F}_p$ contains p elements.

Example 1.4 (Quotients of the polynomial ring) In a principal ideal domain, every prime ideal is principal. Now, by Proposition 5.12, if k is a field, then the polynomial ring $k[x]$ is a PID. 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 $\mathbb{C}$ can be constructed as $\mathbb{R}[x]/(x^2+1)$.

Exercise 2.1 What is $\mathbb{C}[x]/(x^2+1)$?

Example 1.5 (Quotient fields) Recall from **??** that, given an integral domain A, there is an imbedding $A \hookrightarrow K(A)$ into a field $K(A)$ formally constructed as quotients $a/b, a, b \in A$ (and $b \neq 0$) modulo an evident equivalence relation. This is called the **quotient field.** The quotient field has the following universal property: given an injection $\phi : A \hookrightarrow K$ for a field K, there is a unique map $\psi : K(A) \to K$ making the diagram commutative (i.e. a map of A-algebras). Indeed, it is clear how to define such a map: we set

$$\psi(a/b) = \phi(a)/\phi(b),$$

where injectivity of ϕ assures that $\phi(b) \neq 0$ if $b \neq 0$.

If the map is not injective, then such a factorization may not exist. Consider the imbedding $\mathbb{Z} \to \mathbb{Q}$ into its quotient field, and consider the map $\mathbb{Z} \to \mathbb{F}_p$: this last map goes from $\mathbb{Z}$ into a field, but it does not factor through $\mathbb{Q}$ (as p is invertible in $\mathbb{Q}$ and zero in $\mathbb{F}_p$!).

Example 1.6 (Rational function field) 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 $F, G \in k[x]$ with the obvious equivalence relation.

Here is a fancier example of a field.

Example 1.7 Let X be a Riemann surface.[1] Let $\mathbb{C}(X)$ denote the set of meromorphic functions on X; clearly $\mathbb{C}(X)$ is a ring under multiplication and addition of functions. It turns out that in fact $\mathbb{C}(X)$ is a field; this is because 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 $\mathbb{C}(S^2)$ is the field of rational functions $\mathbb{C}(z)$.

One reason fields are so nice from the point of view of most other chapters in this book is that the theory of k-modules (i.e. vector spaces), for k a field, is very simple. Namely:

Proposition 1.8 *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. ▲

Corollary 1.9 *Every exact sequence of modules over a field splits.*

Proof. This follows from **??** and Proposition 1.8, as every vector space is projective. ▲

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 Corollary 1.9 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.

[1] Readers not familiar with Riemann surfaces may ignore this example.

1.2 The characteristic of a field

In the category of rings, there is an *initial object* $\mathbb{Z}$: any ring R has a map from $\mathbb{Z}$ 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. As $\mathbb{Z}$ is the initial object of the category of rings, there is a ring map $f : \mathbb{Z} \to F$, see **??** 1.4. The image of this ring map is an integral domain (as a subring of a field) hence the kernel of f is a prime ideal in $\mathbb{Z}$, see Proposition 4.12. Hence the kernel of f is either (0) or (p) for some prime number p, see Example 4.2.

In the first case we see that f is injective, and in this case we think of $\mathbb{Z}$ 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 $p, q \in \mathbb{Z}$ with $q \neq 0$. Hence in this case we may and we do think of $\mathbb{Q}$ 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 $\mathrm{Ker}(f) = (p)$ we see that $\mathbb{Z}/(p) = \mathbb{F}_p$ 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 $\mathbb{Q}$ or finite equal to $\mathbb{F}_p$ for some prime number p.

Definition 1.10 The **characteristic** of a field F is 0 if $\mathbb{Z} \subset F$, or is a prime p if $p = 0$ in F. The **prime subfield of** F is the smallest subfield of F which is either $\mathbb{Q} \subset F$ if the characteristic is zero, or $\mathbb{F}_p \subset F$ if the characteristic is $p > 0$.

It is easy to see that if E is a field containing k, then the characteristic of E is the same as the characteristic of k.

Example 1.11 The characteristic of $\mathbb{Z}/p$ is p, and that of $\mathbb{Q}$ is 0. This is obvious from the definitions.

§2 Field extensions

2.1 Preliminaries

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.

Proposition 2.1 *If F is a field and R is any ring, then any ring homomorphism $f : F \to R$ is either injective or the zero map (in which case $R = 0$).*

Proof. Indeed, $\ker(f)$ is an ideal in F. But there are only two ideals in F, namely (0) and (1). If f is identically zero, then $1 = f(1) = 0$ in R, so $R = 0$ too. ▲

Definition 2.2 If F is a field contained in a field G, then G is said to be a **field extension** of F. We shall write G/F to indicate that G is an extension of F.

So if F, F' are fields, and $F \to F'$ is any ring-homomorphism, we see by Proposition 2.1 that it is injective,[2] and F' can be regarded as an extension of F, by a slight abuse of notation. 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.

[2] The zero ring is not a field!

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

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

Definition 2.3 A **tower** of field extensions $E'/E/k$ consists of an extension E/k and an extension E'/E.

It is easy to see that any morphism $E \to E'$ in the category of k-extensions gives a tower.

Let us give a few examples of field extensions.

Example 2.4 Let k be a field, and $P \in k[x]$ an irreducible polynomial. We have seen that $k[x]/(P)$ is a field (Example 1.6). Since it is also a k-algebra in the obvious way, it is an extension of k.

Example 2.5 If X is a Riemann surface, then the field of meromorphic functions $\mathbb{C}(X)$ (see Example 1.7) is an extension field of $\mathbb{C}$, because any element of $\mathbb{C}$ 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 easily checks that this is a field. It is easy to see, 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 2.6 If F/k is an extension and $S \subset F$, we write $k(S)$ for the smallest subextension of F containing S. We will say that S **generates** the extension $k(S)/k$.

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

Exercise 2.2 Show that $\mathbb{C}$ does not have a countable set of generators over $\mathbb{Q}$.

Let us now classify extensions generated by one element.

Proposition 2.7 (Simple extensions of a field) *If an extension F/k is generated by one element, then it is F 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. ▲

2.2 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 2.8 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.

Example 2.9 $\mathbb{C}$ is obviously a finite extension of $\mathbb{R}$ (of degree 2).

Let us now consider the degree in the most important special example, that given by Proposition 2.7, in the next two examples.

Example 2.10 (Degree of a simple transcendental extension) If k is any field, then the rational function field $k(t)$ is *not* a finite extension. The elements $\{t^n, n \in \mathbb{Z}\}$ 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 $\mathbb{C}$, then this follows because $\frac{1}{t-\alpha}$, when considered as a meromorphic function on $\mathbb{C}$, 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 if suboptimal proof of the Hilbert Nullstellensatz; see **??**.)

Example 2.11 (Degree of a simple algebraic extension) Consider a monogenic field extension E/k of the form in Example 1.6, say $E = k[t]/(P)$ for $P \in k[t]$ an irreducible polynomial. Then the degree $[E : k]$ is just the degree $\deg P$. Indeed, without loss of generality, we can assume P monic, say

$$P = t^n + a_1 t^{n-1} + \cdots + a_0. \tag{2.1}$$

It is then easy to see that the images of $1, t, \dots, t^{n-1}$ 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 $S = \left\{1, t, \dots, t^{n-1}\right\}$ (or more properly their images) spans $k[t]/(P)$ as a vector space. Indeed, we have by (2.1) that t^n lies in the span of S. Similarly, the relation $tP(t) = 0$ shows that the image of t^{n+1} lies in the span of $\{1, t, \dots, t^n\}$—by what was just shown, thus in the span of S. Working upward inductively, we find that the image of t^M for $M \geq n$ lies in the span of S.

This confirms the observation that $[\mathbb{C} : \mathbb{R}] = 2$, 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.*

Proposition 2.12 (Multiplicativity) *Suppose given a tower $F/E/k$. 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

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

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

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

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

Suppose now that there existed a nontrivial relation

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

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

$$\sum_i \alpha_i \left(\sum_j c_{ij} \beta_j \right) = 0,$$

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 2.13 A field extensions K of $\mathbb{Q}$ is said to be a **number field** if it is a finite extension of $\mathbb{Q}$.

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

2.3 Algebraic extensions

Consider a field extension F/E.

Definition 2.14 An element $\alpha \in F$ is said to be **algebraic** over E if α is the root of some polynomial with coefficients in E. If all elements of F are **algebraic** then F is said to be an algebraic extension.

By Proposition 2.7, 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, it satisfies the polynomial P!); in the former case, it is not.

Example 2.15 $\mathbb{C}$ is algebraic over $\mathbb{R}$.

Example 2.16 Let X be a compact Riemann surface, and $f \in \mathbb{C}(X) - \mathbb{C}$ any nonconstant meromorphic function on X (see Example 1.7). Then it is known that $\mathbb{C}(X)$ is algebraic over the subextension $\mathbb{C}(f)$ generated by f. We shall not prove this.

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

Proposition 2.17 *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 α is algebraic over k, by Example 2.10 and Example 2.11. So if E/k is algebraic, then each $k(\alpha)/k, \alpha \in E$, is a finite extension, and conversely. ▲

We can extract a corollary of the last proof (really of Example 2.10 and Example 2.11): a monogenic extension is finite if and only if it is algebraic. We shall use this observation in the next result.

Corollary 2.18 *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 finite 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 $k(\alpha_1, \dots, \alpha_{i+1})/k(\alpha_1, \dots, \alpha_i)$ is monogenic and algebraic, hence finite. ▲

The set of complex numbers that are algebraic over $\mathbb{Q}$ 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).

Corollary 2.19 *Let E/k be a field extension. Then the elements of E algebraic over k form a field.*

Proof. Let $\alpha, \beta \in E$ be algebraic over k. Then $k(\alpha, \beta)/k$ is a finite extension by Corollary 2.18. It follows that $k(\alpha + \beta) \subset k(\alpha, \beta)$ is a finite extension, which implies that $\alpha + \beta$ is algebraic by Proposition 2.17. ▲

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

Proposition 2.20 (Towers) *Let E/k and F/E be algebraic. Then F/k is algebraic.*

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, $k(S, \alpha)/k(S)$ is finite. Since S is a finite set, and $k(S)/k$ is algebraic, Corollary 2.18 shows that $k(S)/k$ is finite. Together 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, and will be put to use more generality in **??**.

2.4 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 $P(x) \in k[x]$ 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* $m(x) \in k[x]$ of this ideal. If we assume m monic, without loss of generality, then m is uniquely determined.

Definition 2.21 $m(x)$ as 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 $m(x)$ will have larger degree, and only multiples of $m(x)$ 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. But 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.

Proposition 2.22 *The degree of the minimal polynomial is* $[k(\alpha) : k]$.

Proof. This is just a restatement of the argument in **??**: the observation is that if $m(x)$ is the minimal polynomial of α, then the map

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

is an isomorphism as in the aforementioned proof, and we have counted the degree of such an extension (see Example 2.11). ▲

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

2.5 Algebraic closure

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

AC 1 $\overline{F}$ is algebraic over F.

AC 2 $\overline{F}$ is **algebraically closed** (that is, every non-constant polynomial in $\overline{F}[X]$ has a root in $\overline{F}$).

The "fundamental theorem of algebra" states that $\mathbb{C}$ is algebraically closed. While the easiest proof of this result uses Liouville's theorem in complex analysis, we shall give a mostly algebraic proof below (**??**).

We now prove the basic existence result.

Theorem 2.24 *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 K be a field and Σ be the set of all monic irreducibles in $K[x]$. Let $A = K[\{x_f : f \in \Sigma\}]$ be the polynomial ring generated by indeterminates x_f, one for each $f \in \Sigma$. Then let $\mathfrak{a}$ be the ideal of A generated by polynomials of the form $f(x_f)$ for each $f \in \Sigma$.

Claim 1. $\mathfrak{a}$ is a proper ideal.

Proof of claim 1. Suppose $\mathfrak{a} = (1)$, so there exist finitely many polynomials $f_i \in \Sigma$ and $g_i \in A$ such that $1 = f_1(x_{f_1})g_1 + \cdots + f_k(x_{f_k})g_k$. Each g_i uses some finite collection of indeterminates $V_i\{x_{f_{i_1}}, \dots, x_{f_{i_{k_i}}}\}$. This notation is ridiculous, so we simplify it.

We can take the union of all the V_i, together with the indeterminates $x_{f_1}, \dots, x_{f_k}$ to get a larger but still finite set of indeterminates $V = \{x_{f_1}, \dots, x_{f_n}\}$ for some $n \geq k$ (ordered so that the original $x_{f_1}, \dots, x_{f_k}$ agree the first k elements of V). Now we can regard each g_i as a polynomial in this new set of indeterminates V. Then, we can write $1 = f_1(x_{f_1})g_1 + \cdots + f_n(x_{f_n})g_n$ where for each $i > k$, we let $g_i = 0$ (so that we've adjoined a few zeroes to the right hand side of the equality). Finally, we define $x_i = x_{f_i}$, so that we have $1 = f_1(x_1)g_1(x_1, \dots, x_n) + \cdots + f_n(x_n)g_n(x_1, \dots, x_n)$.

Suppose n is the minimal integer such that there exists an expression of this form, so that

$$\mathfrak{b} = (f_1(x_1), \dots, f_{n-1}(x_{n-1}))$$

is a proper ideal of $B = K[x_1, \dots, x_{n-1}]$, but

$$(f_1(x_1), \dots, f_n(x_n))$$

is the unit ideal in $B[x_n]$. Let $\hat{B} = B/\mathfrak{b}$ (observe that this ring is nonzero). We have a composition of maps

$$B[x_n] \to \hat{B}[x_n] \to \hat{B}[x_n]/(\widehat{f_n(x_n)})$$

where the first map is reduction of coefficients modulo $\mathfrak{b}$, and the second map is the quotient by the principal ideal generated by the image $\widehat{f_n(x_n)}$ of $f_n(x_n)$ in $\hat{B}[x_n]$. We know $\hat{B}$ is a nonzero ring, so since f_n is monic, the top coefficient of $\widehat{f_n(x_n)}$ is still $1 \in \hat{B}$. In particular, the top coefficient cannot be nilpotent. Furthermore, since f_n was irreducible, it is not a constant polynomial, so by the characterization of units in polynomial rings, $\widehat{f_n(x_n)}$ is not a unit, so it does not generate the unit ideal. Thus the quotient $\hat{B}[x_n]/(\widehat{f_n(x_n)})$ should not be the zero ring.

On the other hand, observe that each $f_i(x_i)$ is in the kernel of this composition, so in fact the entire ideal $(f_1(x_1), \dots, f_n(x_n))$ is contained in the kernel. But this ideal is the unit ideal, so all of $B[x_n]$ is in the kernel of this composition. In particular, $1 \in B[x_n]$ is in the kernel, and since ring maps preserve identity, this forces $1 = 0$ in $\hat{B}[x_n]/(\widehat{f_n(x_n)})$, which makes this the the zero ring. This contradicts our previous observation, and proves the claim that $\mathfrak{a}$ is a proper ideal.

Now, given claim 1, there exists a maximal ideal $\mathfrak{m}$ of A containing $\mathfrak{a}$. Let $K_1 = A/\mathfrak{m}$. This is an extension field of K via the inclusion given by

$$K \to A \to A/\mathfrak{m}$$

(this map is automatically injective as it is a map between fields). Furthermore every $f \in \Sigma$ has a root in K_1. Specifically, the coset $x_f + \mathfrak{m}$ in $A/\mathfrak{m} = K_1$ is a root of f since

$$f(x_f + \mathfrak{m}) = f(x_f) + \mathfrak{m} = 0.$$

Inductively, given K_n for some $n \geq 1$, repeat the construction with K_n in place of K to get an extension field K_{n+1} of K_n in which every irreducible $f \in K_n[x]$ has a root. Let $L = \bigcup_{n=1}^{\infty} K_n$.

Claim 2. Every $f \in L[x]$ splits completely into linear factors in L.

Proof of claim 2. We induct on the degree of f. In the base case, when f itself is linear, there is nothing to prove. Inductively, suppose every polynomial in $L[x]$ of degree less than n splits completely into linear factors, and suppose

$$f = a_0 + a_1 x + \cdots + a_n x^n \in L[x]$$

has degree n. Then each $a_i \in K_{n_i}$ for some n_i, so let $n = \max n_i$ and regard f as a polynomial in $K_n[x]$. If f is reducible in $K_n[x]$, then we have a factorization $f = gh$ with the degree of g, h strictly less than n. Therefore, inductively, they both split into linear factors in $L[x]$, so f must also. On the other hand, if f is irreducible, then by our construction, it has a root $a \in K_{n+1}$, so we have $f = (x - a)g$ for some $g \in K_{n+1}[x]$ of degree $n - 1$. Again inductively, we can split g into linear factors in L, so clearly we can do the same with f also. This completes the proof of claim 2.

Let $\bar{K}$ be the set of algebraic elements in L. Clearly $\bar{K}$ is an algebraic extension of K. If $f \in \bar{K}[x]$, then we have a factorization of f in $L[x]$ into linear factors

$$f = b(x - a_1)(x - a_2) \cdots (x - a_n). \qquad \blacktriangle$$

for $b \in \bar{K}$ and, a priori, $a_i \in L$. But each a_i is a root of f, which means it is algebraic over $\bar{K}$, which is an algebraic extension of K; so by transitivity of "being algebraic," each a_i is algebraic over K. So in fact we conclude that $a_i \in \bar{K}$ already, since $\bar{K}$ consisted of all elements algebraic over K. Therefore, since $\bar{K}$ is an algebraic extension of K such that every $f \in \bar{K}[x]$ splits into linear factors in $\bar{K}$, $\bar{K}$ is the algebraic closure of K.

TO BE ADDED: two algebraic closures are isomorphic

Let K be an algebraically closed field. Then the ring $K[x]$ has a very simple ideal structure. Since every polynomial $P \in K[x]$ has a root, it follows that there is always a decomposition (by dividing repeatedly)

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

where c is the constant term and the $\{\alpha_i\} \subset k$ are the roots of P. In particular:

Proposition 2.25 *For K algebraically closed, the only irreducible polynomials in $K[x]$ are the linear polynomials $c(x - \alpha)$, $c, \alpha \in K$ (and $c \neq 0$).*

In particular, two polynomials in $K[x]$ are **relatively prime** (i.e., generate the unit ideal) 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.

Definition 2.26 If k is any field, we say that two polynomials in $k[x]$ are **relatively prime** if they generate the unit ideal in $k[x]$.

Proposition 2.27 *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. ▲

§3 Separability and normality

3.1 Separable extensions

Throughout, $F \subset K$ is a finite field extension. We fix once and for all an algebraic closure $\overline{F}$ for F and an embedding of F in M.

Definition 3.1 For an element $\alpha \in K$ with minimal polynomial $q \in F[x]$, we say q and α are **separable** if q has distinct roots (in some algebraic closure $\overline{F}$!), and we say K is separable if this holds for all $\alpha \in K$.

By Proposition 2.27, separability of a polynomial $P \in F[x]$ is equivalent to $(P, P') = 1$ in $F[x]$. Indeed, this follows from the fact that P has no multiple roots if and only if P, P' have no common roots.

Lemma 3.2 *$q(x) \in F[x]$ is separable if and only if $\gcd(q, q') = 1$, where q' is the formal derivative of q.*

3.2 Purely inseparable extensions

Definition 3.3 For an element $\alpha \in K$ with minimal polynomial q, we say α is **purely inseparable** if q has only one root. We say K is splitting if each q splits in K.

Definition 3.4 If $K = F(\alpha)$ for some α with minimal polynomial $q(x) \in F[x]$, then by Lemma 4.3, $q(x) = r(x^{p^d})$, where $p = \operatorname{char} F$ (or 1 if $\operatorname{char} F = 0$) and r is separable; in this case we also denote $\deg_s(K/F) = \deg(r), \deg_i(K/F) = p^d$.

§4 Galois theory

4.1 Definitions

Throughout, $F \subset K$ is a finite field extension. We fix once and for all an algebraic closure M for both and an embedding of F in M. When necessary, we write $K = F(\alpha_1, \dots, \alpha_n)$, and $K_0 = F, K_i = F(\alpha_1, \dots, \alpha_i)$, q_i the minimal polynomial of α_i over F_{i-1}, Q_i that over F.

Definition 4.1 $\operatorname{Aut}(K/F)$ denotes the group of automorphisms of K which fix F (pointwise!). $\operatorname{Emb}(K/F)$ denotes the set of embeddings of K into M respecting the chosen embedding of F.

Definition 4.2 By $\deg(K/F)$ we mean the dimension of K as an F-vector space. We denote K_s/F the set of elements of K whose minimal polynomials over F have distinct roots; by Corollary 4.13 this is a subfield, and $\deg(K_s/F) = \deg_s(K/F)$ and $\deg(K/K_s) = \deg_i(K/F)$ by definition.

4.2 Theorems

Lemma 4.3 *If $\operatorname{char} F = 0$ then $K_s = K$. If $\operatorname{char} F = p > 0$, then for any irreducible $q(x) \in K[x]$, there is some $d \geq 0$ and polynomial $r(x) \in K[x]$ such that $q(x) = r(x^{p^d})$, and r is separable and irreducible.*

Proof. By formal differentiation, $q'(x)$ has positive degree unless each exponent is a multiple of p; in characteristic zero this never occurs. If this is not the case, since q is irreducible, it can have no factor in common with q' and therefore has distinct roots by Lemma 3.2.

If $p > 0$, let d be the largest integer such that each exponent of q is a multiple of p^d, and define r by the above equation. Then by construction, r has at least one exponent which is not a multiple of p, and therefore has distinct roots. ▲

Corollary 4.4 *In the statement of Lemma 4.3, q and r have the same number of roots.*

Proof. α is a root of q if and only if α^{p^d} is a root of r; i.e. the roots of q are the roots of $x^{p^d} - \beta$, where β is a root of r. But if α is one such root, then $(x-\alpha)^{p^d} = x^{p^d} - \alpha^{p^d} = x^{p^d} - \beta$ since $\operatorname{char} K = p$, and therefore α is the only root of $x^{p^d} - \beta$. ▲

Lemma 4.5 *The correspondence which to each $g \in Emb(K/F)$ assigns the n-tuple $(g(\alpha_1), \dots, g(\alpha_n))$ of elements of M is a bijection from $Emb(K/F)$ to the set of tuples of $\beta_i \in M$, such that β_i is a root of q_i over $K(\beta_1, \dots, \beta_{i-1})$.*

Proof. First take $K = F(\alpha) = F[x]/(q)$, in which case the maps $g\colon K \to M$ over F are identified with the elements $\beta \in M$ such that $q(\beta) = 0$ (where $g(\alpha) = \beta$).

Now, considering the tower $K = K_n/K_{n-1}/\dots/K_0 = F$, each extension of which is primitive, and a given embedding g, we define recursively $g_1 \in \operatorname{Emb}(K_1/F)$ by restriction and subsequent g_i by identifying K_{i-1} with its image and restricting g to K_i. By the above paragraph each g_i corresponds to the image $\beta_i = g_i(\alpha_i)$, each of which is a root of q_i. Conversely, given such a set of roots of the q_i, we define g recursively by this formula. ▲

Corollary 4.6 $|\,Emb(K/F)| = \prod_{i=1}^n \deg_s(q_i)$.

Proof. This follows immediately by induction from Lemma 4.5 by Corollary 4.4. ▲

Lemma 4.7 *For any $f \in Emb(K/F)$, the map $Aut(K/F) \to Emb(K/F)$ given by $\sigma \mapsto f \circ \sigma$ is injective.*

Proof. This is immediate from the injectivity of f. ▲

Corollary 4.8 *$Aut(K/F)$ is finite.*

Proof. By Lemma 4.7, $\operatorname{Aut}(K/F)$ injects into $\operatorname{Emb}(K/F)$, which by Corollary 4.6 is finite. ▲

Proposition 4.9 *The inequality*

$$|\,Aut(K/F)| \leq |\,Emb(K/F)|$$

is an equality if and only if the q_i all split in K.

Proof. The inequality follows from Lemma 4.7 and from Corollary 4.8. Since both sets are finite, equality holds if and only if the injection of Lemma 4.7 is surjective (for fixed $f \in \operatorname{Emb}(K/F)$).

If surjectivity holds, let $\beta_1, \dots, \beta_n$ be arbitrary roots of $q_1, \dots, q_n$ in the sense of Lemma 4.5, and extract an embedding $g\colon K \to M$ with $g(\alpha_i) = \beta_i$. Since the correspondence $f \mapsto f \circ \sigma$ ($\sigma \in \operatorname{Aut}(K/F)$) is a bijection, there is some σ such that $g = f \circ \sigma$, and therefore f and g have the same image. Therefore the image of K in M is canonical, and contains $\beta_1, \dots, \beta_n$ for any choice thereof.

If the q_i all split, let $g \in \operatorname{Emb}(K/F)$ be arbitrary, so the $g(\alpha_i)$ are roots of q_i in M as in Lemma 4.5. But the q_i have all their roots in K, hence in the image $f(K)$, so f and g again have the same image, and $f^{-1} \circ g \in \operatorname{Aut}(K/F)$. Thus $g = f \circ (f^{-1} \circ g)$ shows that the map of Lemma 4.7 is surjective. ▲

Corollary 4.10 *Define*

$$D(K/F) = \prod_{i=1}^n \deg_s(K_i/K_{i-1}).$$

Then the chain of equalities and inequalities

$$|\,Aut(K/F)| \leq |\,Emb(K/F)| = D(K/F) \leq \deg(K/F)$$

holds; the first inequality is an equality if and only if each q_i splits in K, and the second if and only if each q_i is separable.

Proof. The statements concerning the first inequality are just Proposition 4.9; the interior equality is just Corollary 4.6; the latter inequality is obvious from the multiplicativity of the degrees of field extensions; and the deduction for equality follows from the definition of $\deg_s$. ▲

Corollary 4.11 *The q_i respectively split and are separable in K if and only if the Q_i do and are.*

Proof. The ordering of the α_i is irrelevant, so we may take each $i = 1$ in turn. Then $Q_1 = q_1$ and if either of the equalities in Corollary 4.10 holds then so does the corresponding statement here. Conversely, clearly each q_i divides Q_i, so splitting or separability for the latter implies that for the former. ▲

Corollary 4.12 *Let $\alpha \in K$ have minimal polynomial q; if the Q_i are respectively split, separable, and purely inseparable over F then q is as well.*

Proof. We may take α as the first element of an alternative generating set for K/F. The numerical statement of Corollary 4.10 does not depend on the particular generating set, hence the conditions given hold of the set containing α if and only if they hold of the canonical set $\alpha_1, \dots, \alpha_n$.

For purely inseparable, if the Q_i all have only one root then $|\,\mathrm{Emb}(K/F)| = 1$ by Corollary 4.10, and taking α as the first element of a generating set as above shows that q must have only one root as well for this to hold. ▲

Corollary 4.13 *K_s is a field and* $\deg(K_s/F) = D(K/F)$.

Proof. Assume $\operatorname{char} F = p > 0$, for otherwise $K_s = K$. Using Lemma 4.3, write each $Q_i = R_i(x^{p^{d_i}})$, and let $\beta_i = \alpha_i^{p^{d_i}}$. Then the β_i have R_i as minimal polynomials and the α_i satisfy $s_i = x^{p^{d_i}} - \beta_i$ over $K' = F(\beta_1, \dots, \beta_n)$. Therefore the α_i have minimal polynomials over K' dividing the s_i and hence those polynomials have but one distinct root.

By Corollary 4.12, the elements of K' are separable, and those of K' purely inseparable over K'. In particular, since these minimal polynomials divide those over F, none of these elements is separable, so $K' = K_s$.

The numerical statement follows by computation:

$$\deg(K/K') = \prod_{i=1}^{n} p^{d_i} = \prod_{i=1}^{n} \frac{\deg(K_i/K_{i-1})}{\deg_s(K_i/K_{i-1})} = \frac{\deg(K/F)}{D(K/F)}. \qquad ▲$$

Theorem 4.14 *The following inequality holds:*

$$|\,Aut(K/F)| \leq |\,Emb(K/F)| = \deg_s(K/F) \leq \deg(K/F).$$

Equality holds on the left if and only if K/F is splitting; it holds on the right if and only if K/F is separable.

Proof. The numerical statement combines Corollary 4.10 and Corollary 4.13. The deductions combine Corollary 4.11 and Corollary 4.12. ▲

4.3 Definitions

Throughout, we will denote as before K/F a finite field extension, and $G = \mathrm{Aut}(K/F)$, H a subgroup of G. L/F is a subextension of K/F.

Definition 4.15 When K/F is separable and splitting, we say it is Galois and write $G = \mathrm{Gal}(K/F)$, the Galois group of K over F.

Definition 4.16 The fixed field of H is the field K^H of elements fixed by the action of H on K. Conversely, G_L is the fixing subgroup of L, the subgroup of G whose elements fix L.

4.4 Theorems

Lemma 4.17 *A polynomial $q(x) \in K[x]$ which splits in K lies in $K^H[x]$ if and only if its roots are permuted by the action of H. In this case, the sets of roots of the irreducible factors of q over K^H are the orbits of the action of H on the roots of q (counting multiplicity).*

Proof. Since H acts by automorphisms, we have $\sigma q(x) = q(\sigma x)$ as a functional equation on K, so σ permutes the roots of q. Conversely, since the coefficients of σ are the elementary symmetric polynomials in its roots, H permuting the roots implies that it fixes the coefficients.

Clearly q is the product of the polynomials q_i whose roots are the orbits of the action of H on the roots of q, counting multiplicities, so it suffices to show that these polynomials are defined over K^H and are irreducible. Since H acts on the roots of the q_i by construction, the former is satisfied. If some q_i factored over K^H, its factors would admit an action of H on their roots by the previous paragraph. The roots of q_i are distinct by construction, so its factors do not share roots; hence the action on the roots of q_i would not be transitive, a contradiction. ▲

Corollary 4.18 *Let $q(x) \in K[x]$; if it is irreducible, then H acts transitively on its roots; conversely, if q is separable and H acts transitively on its roots, then $q(x) \in K^H[x]$ is irreducible.*

Proof. Immediate from Lemma 4.17. ▲

Lemma 4.19 *If K/F is Galois, so is K/L, and Gal$(K/L) = G_L$..*

Proof. K/F Galois means that the minimal polynomial over F of every element of K is separable and splits in K; the minimal polynomials over $L = K^H$ divide those over F, and therefore this is true of K/L as well; hence K/L is likewise a Galois extension. $\mathrm{Gal}(K/L) = \mathrm{Aut}(K/L)$ consists of those automorphisms σ of K which fix L; since $F \subset L$ we have *a fortiori* that σ fixes F, hence $\mathrm{Gal}(K/L) \subset G$ and consists of the subgroup which fixes L; i.e. G_L. ▲

Corollary 4.20 *If K/F and L/F are Galois, then the action of G on elements of L defines a surjection of G onto Gal(L/F). Thus G_L is normal in G and Gal$(L/F) \cong G/G_L$. Conversely, if $N \subset G$ is normal, then K^N/F is Galois.*

Proof. L/F is splitting, so by Lemma 4.17 the elements of G act as endomorphisms (hence automorphisms) of L/F, and the kernel of this action is G_L. By Lemma 4.19, we have $G_L = \mathrm{Gal}(K/L)$, so $|G_L| = |\mathrm{Gal}(K/L)| = [K : L] = [K : F]/[L : F]$, or rearranging and using that K/F is Galois, we get $|G|/|G_L| = [L : F] = |\mathrm{Gal}(L/F)|$. Thus the map $G \to \mathrm{Gal}(L/F)$ is surjective and thus the induced map $G/G_L \to \mathrm{Gal}(L/F)$ is an isomorphism.

Conversely, let N be normal and take $\alpha \in K^N$. For any conjugate β of α, we have $\beta = g(\alpha)$ for some $g \in G$; let $n \in N$. Then $n(\beta) = (ng)(\alpha) = g(g^{-1}ng)(\alpha) = g(\alpha) = \beta$, since $g^{-1}ng \in N$ by normality of N. Thus $\beta \in K^N$, so K^N is splitting, i.e., Galois. ▲

Proposition 4.21 *If K/F is Galois and $H = G_L$, then $K^H = L$.*

Proof. By Lemma 4.19, K/L and K/K^H are both Galois. By definition, $\mathrm{Gal}(K/L) = G_L = H$; since H fixes K^H we certainly have $H < \mathrm{Gal}(K/K^H)$, but since $L \subset K^H$ we have *a fortiori* that $\mathrm{Gal}(K/K^H) < \mathrm{Gal}(K/L) = H$, so $\mathrm{Gal}(K/K^H) = H$ as well. It follows from Theorem 4.14 that $\deg(K/L) = |H| = \deg(K/K^H)$, so that $K^H = L$. ▲

Lemma 4.22 *If K is a finite field, then K^* is cyclic.*

Proof. K is then a finite extension of $\mathbb{F}_p$ for $p = \operatorname{char} K$, hence has order p^n, $n = \deg(K/\mathbb{F}_p)$. Thus $\alpha^{p^n} = \alpha$ for all $\alpha \in K$, since $|K^*| = p^n - 1$. It follows that every element of K is a root of $q_n(x) = x^{p^n} - x$. For any $d < n$, the elements of order at most $p^d - 1$ satisfy $q_d(x)$, which has p^d roots. It follows that there are at least $p^n(p-1) > 0$ elements of order exactly $p^n - 1$, so K^* is cyclic. ▲

Corollary 4.23 *If K is a finite field, then Gal(K/F) is cyclic, generated by the Frobenius automorphism.*

Proof. First take $F = \mathbb{F}_p$. Then the map $f_i(\alpha) = \alpha^{p^i}$ is an endomorphism, injective since K is a field, and surjective since it is finite, hence an automorphism. Since every α satisfies $\alpha^{p^n} = \alpha$, $f_n = 1$, but by Lemma 4.22, f_{n-1} is nontrivial (applied to the generator). Since $n = \deg(K/F)$, $f = f_1$ generates $\mathrm{Gal}(K/F)$.

If F is now arbitrary, by Proposition 4.21 we have $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/\mathbb{F}_p)_F$, and every subgroup of a cyclic group is cyclic. ▲

Corollary 4.24 *If K is finite, K/F is primitive.*

Proof. No element of G fixes the generator α of K^*, so it cannot lie in any proper subfield. Therefore $F(\alpha) = K$. ▲

Proposition 4.25 *If F is infinite and K/F has only finitely many subextensions, then it is primitive.*

Proof. We proceed by induction on the number of generators of K/F.

If $K = F(\alpha)$ we are done. If not, $K = F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F(\beta, \alpha_n)$ by induction, so we may assume $n = 2$. There are infinitely many subfields $F(\alpha_1 + t\alpha_2)$, with $t \in F$, hence two of them are equal, say for t_1 and t_2. Thus, $\alpha_1 + t_2\alpha_2 \in F(\alpha_1 + t_1\alpha_2)$. Then $(t_2 - t_1)\alpha_2 \in F(\alpha_1 + t_1\alpha_2)$, hence α_2 lies in this field, hence α_1 does. Therefore $K = F(\alpha_1 + t_1\alpha_2)$. ▲

Corollary 4.26 *If K/F is separable, it is primitive, and the generator may be taken to be a linear combination of any finite set of generators of K/F.*

Proof. We may embed K/F in a Galois extension M/F by adjoining all the conjugates of its generators. Subextensions of K/F are as well subextensions of K'/F and by Proposition 4.21 the map $H \mapsto (K')^H$ is a surjection from the subgroups of G to the subextensions of K'/F, which are hence finite in number. By Corollary 4.24 we may assume F is infinite. The result now follows from Proposition 4.25. ▲

Corollary 4.27 *If K/F is Galois and $H \subset G$, then if $L = K^H$, we have $H = G_L$.*

Proof. Let α be a primitive element for K/L. The polynomial $\prod_{h \in H}(x - h(\alpha))$ is fixed by H, and therefore has coefficients in L, so α has $|H|$ conjugate roots over L. But since α is primitive, we have $K = L(\alpha)$, so the minimal polynomial of α has degree $\deg(K/L)$, which is the same as the number of its roots. Thus $|H| = \deg(K/L)$. Since $H \subset G_L$ and $|G_L| = \deg(K/L)$, we have equality. ▲

Theorem 4.28 *The correspondences $H \mapsto K^H$, $L \mapsto G_L$ define inclusion-reversing inverse maps between the set of subgroups of G and the set of subextensions of K/F, such that normal subgroups and Galois subfields correspond.*

Proof. This combines Proposition 4.21, Corollary 4.27, and Corollary 4.20. ▲

§5 Transcendental Extensions

There is a distinguished type of transcendental extension: those that are "purely transcendental."

Definition 5.1 A field extension E'/E is purely transcendental if it is obtained by adjoining a set B of algebraically independent elements. A set of elements is algebraically independent over E if there is no nonzero polynomial$P$ with coefficients in E such that $P(b_1, b_2, \cdots b_n) = 0$ for any finite subset of elements $b_1, \ldots, b_n \in B$.

Example 5.2 The field $\mathbb{Q}(\pi)$ is purely transcendental; in particular, $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ with the isomorphism fixing $\mathbb{Q}$.

Similar to the degree of an algebraic extension, there is a way of keeping track of the number of algebraically independent generators that are required to generate a purely transcendental extension.

Definition 5.3 Let E'/E be a purely transcendental extension generated by some set of algebraically independent elements B. Then the transcendence degree $trdeg(E'/E) = \#(B)$ and B is called a transcendence basis for E'/E (we will see later that $trdeg(E'/E)$ is independent of choice of basis).

In general, let F/E be a field extension, we can always construct an intermediate extension $F/E'/E$ such that F/E' is algebraic and E'/E is purely transcendental. Then if B is a transcendence basis for E', it is also called a transcendence basis for F. Similarly, $trdeg(F/E)$ is defined to be $trdeg(E'/E)$.

Theorem 5.4 *Let F/E be a field extension, a transcendence basis exists.*

Proof. Let A be an algebraically independent subset of F. Now pick a subset $G \subset F$ that generates F/E, we can find a transcendence basis B such that $A \subset B \subset G$. Define a collection of algebraically independent sets $\mathcal{B}$ whose members are subsets of G that contain A. The set can be partially ordered inclusion and contains at least one element, A. The union of elements of $\mathcal{B}$ is algebraically independent since any algebraic dependence relation would have occurred in one of the elements of $\mathcal{B}$ since the polynomial is only allowed to be over finitely many variables. The union also satisfies $A \subset \bigcup \mathcal{B} \subset G$ so by Zorn's lemma, there is a maximal element $B \in \mathcal{B}$. Now we claim F is algebraic over $E(B)$. This is because if it wasn't then there would be a transcendental element $f \in G$ (since $E(G) = F$)such that $B \cup \{f\}$ wold be algebraically independent contradicting the maximality of B. Thus B is our transcendence basis. ▲

Now we prove that the transcendence degree of a field extension is independent of choice of basis.

Theorem 5.5 *Let F/E be a field extension. Any two transcendence bases for F/E have the same cardinality. This shows that the $trdeg(E/F)$ is well defined.*

Proof. 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_α such that α is algebraic over $E(B_\alpha)$ 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 $E(B')$ which is algebraic over $E(B^*)$. Therefor β is algebraic over $E(B^*)$, a contradiction. So $\#(B) \leq \sum_{\alpha \in B'} \#(B_\alpha)$. Now if B' is finite, then so is B so we can assume B' is infinite; this means

$$\#(B) \leq \sum_{\alpha \in B'} \#(B_\alpha) = \#(\coprod B_\alpha) \leq \#(B' \times \mathbb{Z}) = \#(B') \tag{2.2}$$

with the inequality $\#(\coprod B_\alpha) \leq \#(B' \times \mathbb{Z})$ given by the correspondence $b_{\alpha_i} \mapsto (\alpha, i) \in B' \times \mathbb{Z}$ with $B_\alpha = \{b_{\alpha_1}, b_{\alpha_2} \cdots b_{\alpha_{n_\alpha}}\}$ 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 $B = \{\alpha_1, \cdots \alpha_n\}$ and $B' = \{\beta_1, \cdots \beta_m\}$ with $m \leq n$. We perform induction on m: if $m = 0$ then F/E is algebraic so $B =$ so $n = 0$, otherwise there is an irreducible polynomial $f \in E[x, y_1, \cdots y_n]$ such that $f(\beta_1, \alpha_1, \cdots \alpha_n) = 0$. Since β_1 is not algebraic over E, f must involve some y_i so without loss of generality, assume f uses y_1. Let $B^* = \{\beta_1, \alpha_2, \cdots \alpha_n\}$. We claim that B^* is a basis for F/E. To prove this claim, we see that we have a tower of algebraic extensions $F/E(B^*, \alpha_1)/E(B^*)$ since α_1 is algebraic over $E(B^*)$. Now we claim that B^* (counting multiplicity of elements) is algebraically independent over E because if it weren't, then there would be an irreducible $g \in E[x, y_2, \cdots y_n]$ such that $g(\beta_1, \alpha_2, \cdots \alpha_n) = 0$ which must involve x making β_1 algebraic over $E(\alpha_2, \cdots \alpha_n)$ which would make α_1 algebraic over $E(\alpha_2, \cdots \alpha_n)$ which is impossible. So this means that $\{\alpha_2, \cdots \alpha_n\}$ and $\{\beta_2, \cdots \beta_m\}$ are bases for F over $E(\beta_1)$ which means by induction, $m = n$.▲

Example 5.6 Consider the field extension $\mathbb{Q}(e, \pi)$ 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 the problem of determining $trdeg(\mathbb{Q}(e, \pi))$ is an open problem.

Example 5.7 let E be a field and $F = E(t)/E$. Then $\{t\}$ is a transcendence basis since $F = E(t)$. However, $\{t^2\}$ is also a transcendence basis since $E(t)/E(t^2)$ is algebraic. This illustrates that while we can always decompose an extension F/E into an algebraic extension F/E' and a purely transcendental extension E'/E, this decomposition is not unique and depends on choice of transcendence basis.

Exercise 2.3 If we have a tower of fields $G/F/E$, then $trdeg(G/E) = trdeg(F/E) + trdeg(G/F)$.

Example 5.8 Let X be a compact Riemann surface. Then the function field $\mathbb{C}(X)$ (see Example 1.7) has transcendence degree one over $\mathbb{C}$. In fact, *any* finitely generated extension of $\mathbb{C}$ 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 category of finitely generated extensions of $\mathbb{C}$ and morphisms of $\mathbb{C}$-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 between smooth projective curves and non-constant morphisms of curves and finitely generated extensions of k of transcendence degree one. See [Har77].

5.1 Linearly Disjoint Field 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 5.9 The compositum of K and L written KL is $k(K \cup L) = L(K) = K(L)$.

Definition 5.10 K and L are said to be linearly disjoint over k if the following map is injective:

$$\theta : K \otimes_k L \to KL \tag{2.3}$$

defined by $x \otimes y \mapsto xy$.

CRing Project contents

I Fundamentals 1

0 Categories 3

1 Foundations 37

2 Fields and Extensions 71

3 Three important functors 93

II Commutative algebra 131

4 The Spec of a ring 133

5 Noetherian rings and modules 157

6 Graded and filtered rings 183

7 Integrality and valuation rings 201

8 Unique factorization and the class group 233

9 Dedekind domains 249

10 Dimension theory 265

11 Completions 293

12 Regularity, differentials, and smoothness 313

III Topics 337

13 Various topics 339

14 Homological Algebra 353

15 Flatness revisited 369

16 Homological theory of local rings 395

17 Étale, unramified, and smooth morphisms 425

18 Complete local rings 459

19 Homotopical algebra 461

20 GNU Free Documentation License 469

CRing Project bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In *Analysis and topology on singular spaces, I (Luminy, 1981)*, volume 100 of *Astérisque*, pages 5–171. Soc. Math. France, Paris, 1982.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Cam88] Oscar Campoli. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, 95(9):868–871, 1988.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Cla11] Pete L. Clark. Factorization in euclidean domains. 2011. Available at `http://math.uga.edu/~pete/factorization2010.pdf`.

[dJea10] Aise Johan de Jong et al. *Stacks Project*. Open source project, available at `http://www.math.columbia.edu/algebraic_geometry/stacks-git/`, 2010.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

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

[GD] Alexander Grothendieck and Jean Dieudonné. *Élements de géometrie algébrique*. Publications Mathématiques de l'IHÉS.

[Ger] Anton Geraschenko (mathoverflow.net/users/1). Is there an example of a formally smooth morphism which is not smooth? MathOverflow. `http://mathoverflow.net/questions/200` (version: 2009-10-08).

[Gil70] Robert Gilmer. An existence theorem for non-Noetherian rings. *The American Mathematical Monthly*, 77(6):621–623, 1970.

[Gre97] John Greene. Principal ideal domains are almost euclidean. *The American Mathematical Monthly*, 104(2):154–156, 1997.

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology.* Cambridge University Press, Cambridge, 2002. Available at `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`.

[Hov07] Mark Hovey. *Model Categories.* American Mathematical Society, 2007.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR08] T. Y. Lam and Manuel L. Reyes. A prime ideal principle in commutative algebra. *J. Algebra*, 319(7):3006–3027, 2008.

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002. An introduction.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series.* Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[McC76] John McCabe. A note on Zariski's lemma. *The American Mathematical Monthly*, 83(7):560–561, 1976.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1998.

[Per04] Hervé Perdry. An elementary proof of Krull's intersection theorem. *The American Mathematical Monthly*, 111(4):356–357, 2004.

[Qui] Daniel Quillen. Homology of commutative rings. Mimeographed notes.

[Ray70] Michel Raynaud. *Anneaux locaux henséliens.* Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin, 1970.

[RG71] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Invent. Math.*, 13:1–89, 1971.

[Ser65] Jean-Pierre Serre. *Algèbre locale. Multiplicités*, volume 11 of *Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1965.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. 2009. arXiv:0903.0517v2.

[SGA72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos.* Lecture Notes in Mathematics, Vol. 269. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Tam94] Günter Tamme. *Introduction to étale cohomology.* Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Vis08] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories, and descent theory. *Published in* FGA Explained, 2008. arXiv:math/0412512v4.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1994.