Notes on Etale cohomology: Preliminaries on field theory

Chunye Yang

March 20, 2026

This will be a preliminary section on the theory of field extensions. Since we will make great use of field extensions as examples and as tools in the study of etale cohomology. Make sure you are familiar with the stuff in this part of the notes before you go to the main chapters. The first two sections are the easier parts where we do some bookkeeping works. What matters is the later four sections. We will be largely follow Serge Lang's Algebra and there will also be another preliminary of Galois theory following this.

1 Finite and Algebraic Extensions

Definition 1.1. Let F be a field, then if F is a subfield of E, i.e. there is an injective map of rings $F \hookrightarrow E$, we say that E is an **extension** of F. We usually write this extension as E/F.

We view E as an F-vector space, and we say this extension is **finite** or **infinite** if the dimension of E as an F-vector space is finite or infinite.

Let F be a subfield of a field E, an element $\alpha \in E$ is said to be **algebraic** over F is there is a polynomial in $F[x]$ with coefficients $a_0, \cdots, a_n$ with $n \geqslant 1$ and not all of them equal to 0, such that:

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

If α is a nonzero algebraic element, then we can always assume that we can find these a_i such that $a_0 \neq 0$.

Remark 1.2. Notice that if E/F is an extension and $\alpha \in E$ is algebraic, it's equivalent to the fact that the F-algebra homomorphism:

$$F[x] \to E, \qquad x \mapsto \alpha$$

has a kernel that is not the zero ideal. Recall that $F[x]$ is a PID, therefore we can assume that this ideal is generated by a unique monic polynomial $p(x)$. Then we have an isomorphism:

$$F[x]/(p(x)) \simeq F[\alpha]$$

where the ring $F[\alpha]$ is the subring of E with elements of the form that is polynomials of α. Since $F[\alpha]$ is entire, $p(x)$ is irreducible. We can normalize $p(x)$ such that the leading coefficient is 1. Then if $q(x)$ is also such a polynomial generating the ideal, then since $p(x), q(x)$ are irreducible, we know that $p(x), q(x)$ are of the same degree, and $p(x) = f \cdot q(x)$ for some $f \in F$. Then by comparing the leading coefficient we can conclude $p(x) = q(x)$. Therefore this is the uniquely determined by the element $\alpha \in F$, and the field extension $E \hookrightarrow F$. Therefore we will write this polynomial as $\mathrm{Irr}(\alpha, F, x)$ and call it **the minimal polynomial of** $\alpha \in F$ **in the extension** E/F.

Definition 1.3. E/F is called **algebraic** if every $\alpha \in E$ is algebraic over F.

We gather some easy properties here without proof. You can prove them easily if you want:

Proposition 1.4. Let E/F be a finite extension, then it's algebraic.

Remark 1.5. The converse of the above result is not true. One example is to consider the field extension $\mathbb{Q} \hookrightarrow \mathbb{C}$. If we consider the subfield of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$, we will see later that this is algebraic but not finite.

Definition 1.6. If E/F is an extension, then we denote by $[E:F]$ the dimension of E as vector spaces over F. It can be infinite.

Proposition 1.7. Let F/k and E/F be two extensions, then:

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

Corollary 1.8. Let F/k and E/F be two extensions, then the extension of E of k is finite if and only if E is finite over F and F is finite over k.

Definition 1.9. We define a **tower** of fields to be a sequence $F_1 \subset F_2 \subset \cdots \subset F_n$ of field extensions. This tower is **finite** iff each step of the extension is finite.

Let k be a field and E/k and extension, let $\alpha \in E$, we will denote by $k(\alpha)$ the smallest subfield of E containing k and α. Notice that if we consider the subset of E consisting of elements of the form $\frac{f(\alpha)}{g(\alpha)}$ where $f, g \in k[x]$ and $g(\alpha)$ not 0 in E. We find that this is indeed a subfield of E containing k and α. And notice that it's contained in any such a subfield contains this subset, therefore $k(\alpha)$ is indeed the subset of E consisting of $\frac{f(\alpha)}{g(\alpha)}$ where $f, g \in k[x]$ and $g(\alpha)$ not 0 in E.

Proposition 1.10. Let $\alpha \in E$ be algebraic over k in the field extension E/k, then we have:

$$k(\alpha) = k[\alpha]$$

and $k(\alpha)$ is finite over k with degree the degree of $\mathrm{Irr}(\alpha, k, x)$.

Proof. We will prove that $k[\alpha]$ is a field, not just a subring of E. Let $p(x) = \mathrm{Irr}(\alpha, k, x)$. Let $f(x) \in k[x]$ be such that $f(\alpha) \neq 0$, then we know that $f(\alpha)$ is not in the ideal generated by $p(x)$, i.e. $p(x)$ doesn't divide $f(x)$, then since $p(x)$ is irreducible, we know that $\gcd(f(x), p(x)) = 1$. Since $k[x]$ is a PID, there will be $g(x), h(x)$ such that:

$$f(x)h(x) + g(x)p(x) = 1$$

Therefore $f(\alpha)h(\alpha) = 1$ so $f(\alpha)$ is invertible in $k[\alpha]$. Therefore everything in $k[\alpha]$ has its inverse in $k[\alpha]$, thus $k[\alpha]$ is a field, therefore $k(\alpha) \subset k[\alpha] \subset k(\alpha)$, therefore $k(\alpha) = k[\alpha]$.

Then consider the powers $1, \alpha, \cdots, \alpha^{d-1}$ where $d = \deg p(x)$. I claim that there are linearly independent, otherwise we have:

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} = 0$$

for not all 0 elements $a_1, \cdots, a_{d-1}$. Let $g(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$, we know that $g(\alpha) = 0$, therefore we know that $p(x)$ divides $g(x)$. But notice that the degree of $g(x)$ is $d-1$ while the degree of $p(x)$ is d, a contradiction.

Finally, for any element in $k[\alpha]$, we know that it's of the form of $f(\alpha)$, suppose that it's not 0, then we know that $p(x)$ doesn't divide $f(x)$, but we can always perform the division algorithm and conclude that:

$$f(x) = p(x)q(x) + r(x)$$

with $\deg r(x) < \deg p(x) = d$, therefore we know that $f(\alpha) = r(\alpha)$, which is a linear combination of $1, \alpha, \cdots, \alpha^{d-1}$. □

Definition 1.11. Let E, F both be extensions of k, then if E, F is both contained in some common field L. Then we will use EF to denote the smallest subfield of L containing E, F. It's called the **compositum** of E and F in L.

Remark 1.12. One important aspect to notice in the above definition is that if E, F are not contained in some common field, then there is no way to define the compositum.

Definition 1.13. Let E/k be a field extension and $\alpha_1, \cdots, \alpha_n \in E$. We will denote by $k(\alpha_1, \cdots, \alpha_n)$ by the smallest subfield of E containing the field k and $\alpha_1, \cdots, \alpha_n$.

Notice that by a similar argument, we can see that the field $k(\alpha_1, \cdots, \alpha_n)$ is the subset of E consisting of elements of the form $\frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)}$ where f, g are in $k[x_1, \cdots, x_n]$ and $g(\alpha_1, \cdots, \alpha_n) \neq 0$.

Definition 1.14. Let E/k be a field extension and we will say E/k is finitely generated as a field extension if there are finitely many $\alpha_1, \cdots, \alpha_n \in E$ such that $E = k(\alpha_1, \cdots, \alpha_n)$.

Remark 1.15. Notice that this is not the same as the definition of finitely generated algebra where we require $k[\alpha_1, \cdots, \alpha_n] = E$ instead of $k(\alpha_1, \cdots, \alpha_n) = E$. Without further assumptions of $\alpha_1, \cdots, \alpha_n$, we can not conclude $k[\alpha_1, \cdots, \alpha_n] = k(\alpha_1, \cdots, \alpha_n)$.

Definition 1.16. If $\{E_i\}_{i \in I}$ is a family of subfields of L, then we define the compositum of this arbitrary family to be the smallest subfield of L containing all E_i.

Notice that let E/k be any field extension, we observe that E is the union of all of the subfields $k(\alpha_1, \cdots, \alpha_n)$ as $(\alpha_1, \cdots, \alpha_n)$ ranges over all the finite subsets of E. We observe that E is the compositum of all $k(\alpha_1, \cdots, \alpha_n)$.

One quick example of a finitely generated field extension is a finite extension.

Proposition 1.17. If E/k is finitely generated, i.e. there are finitely many elements in E such that $E = k(\alpha_1, \cdots, \alpha_n)$. Let F/k be another extension of k such that E, F are contained in a common field L, then I claim that the compositum EF is finitely generated over F and $EF = F(\alpha_1, \cdots, \alpha_n)$.

Proof. First, notice that $F(\alpha_1, \cdots, \alpha_n)$ in L indeed contains F, E. Then suppose that we have a subfield L' of L containing E, F. Consider let x be an element in $F(\alpha_1, \cdots, \alpha_n)$, then we know that is of the form $f(\alpha_1, \cdots, \alpha_n)$ where $f \in F[x_1, \cdots, x_n]$, notice that this polynomial can be written $\sum_i f_i g_i(x_1, \cdots, x_n)$ where $f_i \in F$ and $g_i(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$. Then we know that $f(\alpha_1, \cdots, \alpha_n)$ can be written as a sum $\sum_i f_i g_i(\alpha_1, \cdots, \alpha_n)$ where $g_i \in E$, therefore we know that $x \in L'$, thus $F(\alpha_1, \cdots, \alpha_n) \subset L'$. □

Again, let E, F be extension of k in a common field L, then we often draw the following diagram to indicate the compositum:

$$\begin{array}{ccc} EF & \longleftarrow & F \\ \uparrow & & \uparrow \\ E & \longleftarrow & k \end{array}$$

This probably will remind you of the fibered product diagram and you will ask when is EF equal to $E \otimes_k F$. Obviously this doesn't happen all the times since we know $E \otimes_k F$ may not even be a field. We will discuss this interesting question later.

We sometimes call EF/F the **translation** of E/k or a **lifting** of E to F.

Suppose that we have a tower of field extensions in a common larger field L:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \cdots, \alpha_n)$$

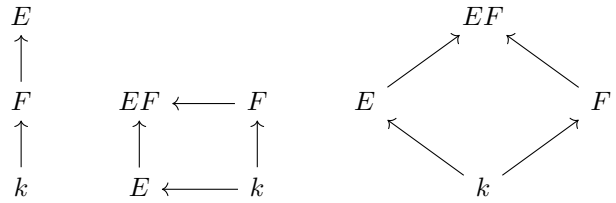
We first notice that $k(\alpha_1, \alpha_2)$ is the same as $k(\alpha_1)(\alpha_2)$. This is easy to argue, since $k(\alpha_1)(\alpha_2)$ is a field containing k, α_1, α_2, thus by definition contains $k(\alpha_1, \alpha_2)$, also $k(\alpha_1, \alpha_2)$ contains $k(\alpha_1)$ and α_2, therefore we get the inverse inclusion. If we assume that each $\alpha_1, \cdots, \alpha_n$ are algebraic over k, then for example, we know that α_2 is also algebraic over $k(\alpha_1)$. Therefore we know that each step is generated by a single element algebraic over it. Therefore we get:

Proposition 1.18. Let $E = k(\alpha_1, \cdots, \alpha_n)$ be a finitely generated extension of a field k, and assume α_i is algebraic over k, then we know E/k is finite.

Definition 1.19. Let $\mathcal{C}$ be a certain class of extension of fields E/F, we say $\mathcal{C}$ is **distinguished** if it satisfies the following conditions:

1. Let $E/F/k$ be a tower of fields, then extension E/k is in $\mathcal{C}$ iff F/k and E/F is in $\mathcal{C}$.
2. If E/k is in $\mathcal{C}$, let F be another extension of k such that E, F are contained in a common larger field L, then EF/F is in $\mathcal{C}$.
3. Let E/k, F/k be two extensions of k contained in a common larger field L, then if E/k and F/k are in $\mathcal{C}$, so is EF/k.

These three conditions are illustrated using diagrams:



I will let you check that the condition 3 in the above definition indeed follows from $1, 2$.

Proposition 1.20. The class of algebraic extensions and the class of finite extensions are distinguished.

Proof. We only write partial proof as this is not so hard.

For example if E/k is finite then $E = k(\alpha_1, \cdots, \alpha_n)$ where α_i algebraic over k, then EF/F is $F(\alpha_1, \cdots, \alpha_n)$ and α_i algebraic over F.

Then suppose that $\alpha \in E$ is algebraic over F, and F/k is algebraic, we hope to show α is algebraic over k. Since α is algebraic over F, we know that there are $a_0, \cdots, a_n \in F$ such that:

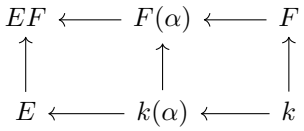
$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

Then consider $k(a_0, \cdots, a_n)$, which is finite over k. Notice that if we consider:

$$k \subset k(a_0, \cdots, a_n) \subset k(a_0, \cdots, a_n)(\alpha)$$

notice that each is finite, therefore the composition is finite.

Consider the following diagram:

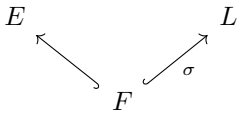


I claim that when α ranges over all elements in E, EF is the union of all $F(\alpha)$. Notice that the union is first indeed still a field and is contained in EF. We also notice that the union contains E, F, therefore the union is EF. Then we know that since α is algebraic over k, it's algebraic over F, therefore the union is also algebraic. □

Remark 1.21. It can be proved that the class of finitely generated field extensions is also distinguished. We can see that condition 2 is easy to prove. But to prove condition 1, some transcendental extensions is needed. Since we won't need it here. We do not include it here.

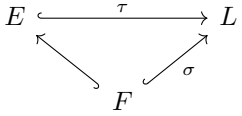
2 Algebraic closure

Consider the following diagram:



where E, L are both extensions of F, and we denote the extension L/F using σ. Notice that F is isomorphic to the image of σ in L, denoted as F^σ.

Definition 2.1. Using the above notation, we will say that an extension $\tau : E \hookrightarrow L$ is said to be **over** σ if the following diagram commutes:



We also say that τ **extends** σ or is an extension of σ, if σ is the identity, then we say that τ is an embedding over F.

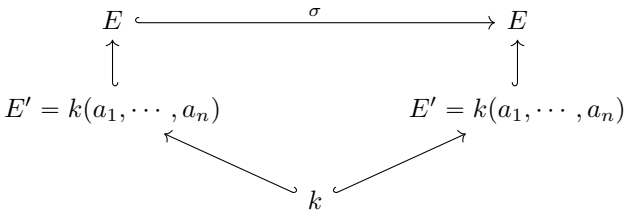
Remark 2.2. We don't want to always keep track of is σ the identity or not. Note that what notice that is we always keep track of the injective map σ, and we will always say that τ is an extension over F.

Following the notation of Serge Lang, we will use **exponential notations** of σ, and we will write F^σ and f^σ for F and f a polynomial in $F[x]$ and σ apply to the coefficients.

Remark 2.3. Let $f(x) \in F[x]$, we also have $f^\sigma(x) \in L[x]$. If we assume that $\alpha \in E$ is a root of $f(x)$, then I claim that $\tau(\alpha)$ is a root of $f^\sigma(x)$.

Lemma 2.4. Let E/k be an **algebraic** extension of fields, then any embedding of E to itself over k is an automorphism.

Proof. We only need to prove it's surjective. Let α be an element of E, then let $p(x)$ be the minimal polynomial of α, we know that $p(x)$ only has finitely many distinct roots in E, say they are $a_1, \cdots, a_n$, then we consider the following diagram:



Notice that elements in $k(a_1, \cdots, a_n)$ are $\frac{f(a_1,\cdots,a_n)}{g(a_1,\cdots,a_n)}$, then we know that after we apply σ, since σ fixes k and always maps roots of f to roots of f, then we know that the image of $f(a_1, \cdots, a_n)$ is just $f'(a_1, \cdots, a_n)$ and the image of $g(a_1, \cdots, a_n)$ is just $g'(a_1, \cdots, a_n) \neq 0$. Then we know that the image of σ of E' lies in E'. Notice that this is still injective and we know that it's between k-vector space of the same dimension, then surjective, therefore we are done. □

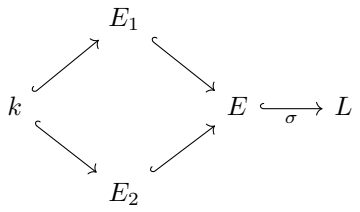
Let E, F be extensions of a field k contained in some larger field L. We can think of the subring $E[F]$ of L. You can think of them as the subset containing of elements of the form $f(\alpha_1, \cdots, \alpha_n)$ where $f \in E[x_1, \cdots, x_n]$ and $\alpha_1, \cdots, \alpha_n \in F$ and n range over all nonnegative integers. Obviously this is also the subset $a_1b_1 + \cdots + a_nb_n$ where $a_i \in E$ and $b_i \in F$. Therefore $E[F] = F[E]$. Notice that $E[F]$ and $F[E]$ are domains, then we can think of it's field of fractions. Clearly it contains both E and F, therefore contains EF. The faction field is by definition the smallest field containing $E[F]$, and we know that EF contains $E[F]$ therefore EF is contained in the fraction field, therefore they are equal. Then we get a description of EF, i.e. they are elements of the form:

$$\frac{a_1b_1 + \cdots + a_nb_n}{a'_1b'_1 + \cdots + a'_mb'_m}$$

where $a_i, a'_i \in E$ and b_i, b'_i are in F.

Lemma 2.5. Let E_1, E_2 be extension of k contained in a larger field E. If $\sigma : E \hookrightarrow L$ is an embedding of E in some L, then:

$$\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$$



Proof. Basically, this is just saying:

$$\sigma(\frac{a_1b_1 + \cdots + a_nb_n}{a'_1b'_1 + \cdots + a'_mb'_m}) = \frac{\sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n)}{\sigma(a'_1)\sigma(b'_1) + \cdots + \sigma(a'_m)\sigma(b'_m)}$$

□

Proposition 2.6. Let k be a field and f a polynomial in $k[x]$ of degree $\geqslant 1$, then there is a field extension E of k such that f has a root.

Proof. Take an irreducible factor $p(x)$ of $f(x)$ and consider $k \hookrightarrow k[x]/(p(x))$. □

Remark 2.7. If you are a really recalcitrant set-theory lover, you may want to take a look at Serge Lang's proof so that your mind is at rest.

Corollary 2.8. Let k be a field, and let $f_1, \cdots, f_n$ are polynomials in $k[x]$, then there is an extension E of k such that each f_i has a root in E.

Definition 2.9. We define a field L to be **algebraically closed** if every polynomial in $L[x]$ has root in L.

Theorem 2.10. If k is a field, then there is a field extension E of k, not necessarily algebraic over k, that is algebraically closed.

Proof. We will first construct a field extension of k, called E_1 such that all polynomials of degree $\geqslant 1$ has a root in E_1.

Consider the set of all polynomials $f(x)$ in $k[x]$ with degree at least 1. For each such $f(x)$, we associate it with a symbol X_f and assume all the symbols is the set S. We consider $k[S]$, the polynomial ring with coefficients in k and variables in S.

Then this is where the clever part comes in to play. Let's consider the ideal in $k[S]$ generated by all polynomials $f(X_f)$ in $k[S]$ is not the unit ideal for each $f \in k[x]$ with degree at least 1. Recall that if it is, then there is a finite combination:

$$g_1f_1(X_{f_1}) + \cdots + g_nf_n(X_{f_n}) = 1$$

For notational simplicity, let's use X_i instead of X_{f_i}. Recall that each g_1 only involves a finite number of variables, then combine them with the variables in $f_i(X_i)$, say only $X_1, \cdots, X_N$ shows up in this equation. Therefore our relation is:

$$\sum_{i=1}^{n} g_i(X_1, \cdots, X_N)f_i(X_i) = 1$$

Recall that $f_i(X_i)$ still has coefficients in k, then we can assume that there is a finite extension F of k such that all f_i has a root. Then think of g_i, f_i as polynomials in $F[X_1, \cdots, X_N]$. Suppose that the root of f_i is α_i in F, then we consider the F-algebra morphism:

$$F[X_1, \cdots, X_N] \to F[\{X_1, \cdots, X_N\} - \{X_1, \cdots, X_n\}]$$

We find that we map 1 to 0, a contradiction. In other words, the following diagram gives us a contradiction:

$$\begin{array}{ccccc} k[S] & \longrightarrow & k[X_1, \cdots, X_N] & & \\ \downarrow & & \downarrow & & \\ F[S] & \longrightarrow & F[X_1, \cdots, X_N] & \longrightarrow & F[\{X_1, \cdots, X_N\} - \{X_1, \cdots, X_n\}] \end{array}$$

Then we consider the maximal ideal m containing the ideal generated by $f(X_f)$. Then consider:

$$k \to k[S] \to k[S]/m$$

We take $E_1 = k[S]/m$, we are done.

Then we can construct E_2 where all polynomials in $E_1[x]$ with degree at least 1 have a root. Therefore we get E_n for all $n \geqslant 1$ and we take $E_0 = k$. Then we can take the union of all E_n for $n \geqslant 0$, this suffices, I will let you see why. □

Corollary 2.11. Let k be a field, there is an extension k^a which is algebraic over k and algebraically closed.

Proof. Let E/k be the field extension constructed above, then we take the subset k^a of E which is algebraic over k. This is a field, since if α is such an element, we consider $k(\alpha)$, this is contained in k^a, and we know that α has it's inverse in $k(\alpha)$ as $k(\alpha)$ is a field, then to check the product, summation we use $k(\alpha_1, \alpha_2)$.

Then k^a/k is algebraic then we only need to prove that it's algebraically closed. Let $f(x)$ be a polynomial in $k^a[x]$, we know that it has a root $\alpha \in E$, then we know that α is algebraic over k^a, and k^a is algebraic over k, we know that α is also algebraic over k, therefore $\alpha \in k^a$, we are done. □

Remark 2.12. One quick observation is that in an algebraically closed field L, any polynomial $f(x)$ with degree at least 1 can be factored to:

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

And we know that since c is the leading coefficient of $f(x)$ if $f(x) \in k[x]$ for some subfield of L, then $c \in k$.

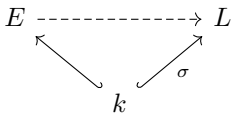
Our next goal is the following: suppose that $k \hookrightarrow L$ is an embedding of k into an algebraically closed field, not necessarily algebraic over k. We have another algebraic extension E/k, we want to know what are the extensions of σ, i.e. $\tau : E \hookrightarrow L$ such that it's restriction to k is σ.

The easiest case is when $E = k(\alpha)$, i.e. it's generated by an algebraic element α, let $p(x)$ be it's minimal polynomial, we know that since L is algebraically closed, then let $\beta_1, \cdots, \beta_n$ be all distinct roots of $p(x)$ in L. We know that τ must map a root of $p(x)$ to a root of $p(x)$, then we know that α can only be mapped to β_i for some i. Then recall that any k-algebra homomorphism $k(\alpha) = k[\alpha] \to L$ is determined by where α is mapped to, it's just we need to check if a certain definition makes sense. Indeed if $f(\alpha) = g(\alpha)$, then we know that $p(x)$ divides $f - g$, therefore we know that 0 divides $f(\alpha) - g(\alpha)$, therefore they are equal. Therefore we get the following result:

Proposition 2.13. Let $\sigma : L/k$ be an extension such that L is algebraically closed, then if $E = k(\alpha)/k$ is an algebraic extension, there are at most d ways to extend σ, d being the degree of the minimal polynomial of α.

We know that there are at most d ways to extend the map, but can we know when there exactly d ways and when we know that there are less than d ways. It will be an important question we will investigate later.

Theorem 2.14. Consider the following diagram of extensions:



where L is algebraically closed and E is algebraic over k, then there exists a dotted arrow extending σ.

If E itself is both algebraically closed and algebraic over k, L is also both algebraically closed and algebraic over k, then any such dotted arrow extending σ is an isomorphism.

Proof. Let's first deal with the existence of such an arrow, which uses Zorn's lemma. We don't want to go into details thus we give the idea. Consider the set of subfields of E and extension of σ, it's not empty and a partially ordered subset, by taking unions you find any such families of extensions has an upper bound, you apply Zorn's lemma get a maximal element and you check it's E using the fact that E is algebraic over k.

Then suppose both E and L are algebraically closed and algebraic over k, then we know that if τ extends σ, then $\tau(E)$ is also algebraically closed and we know that $\tau : E \to L$ is also algebraic then $L/\sigma(E)$ is also algebraic, but $\sigma(E)$ is algebraically closed, therefore we know that $\sigma(E) = L$. □

Corollary 2.15. Let k be a field and let E, E' be algebraic extensions of k. Assume that E, E' are algebraically closed, then there is an k-algebra isomorphism:

$$\tau : E \to E'$$

Proof. The existence of such an isomorphism is just a direct application of the above theorem. □

Definition 2.16. We will cal any extension of k that is both algebraic and algebraically closed **an algebraic closure** of k, denoted by k^a. The above corollary shows that any two such algebraic closures are isomorphic, though not through a canonical or unique isomorphism.

Remark 2.17. We see that even though there is always such an isomorphism, this isomorphism is not in any sense unique, which is quite contrary to what we see for universal objects in a category (i.e. initial or final objects not just objects defined by universal property, which can have nontirvial automorphisms, it's just this automorphism will not be an automorphism preserving the representing pair). Let's explain this a little bit here:

Let $\mathcal{C}$ be a category and A, B are objects. Let $\mathrm{Iso}(A, B)$ be the set of isomorphisms between A, B, and suppose that $\sigma : A \to B$ is an isomorphism. I will let you check that we have a bijection induced by σ:

$$\mathrm{Aut}(A) \to \mathrm{Aut}(B), \qquad \varphi \mapsto \sigma \circ \varphi \circ \sigma^{-1}$$

Suppose that τ is another such isomorphism, we know that $\tau^{-1} \circ \sigma$ and $\tau \circ \sigma^{-1}$ are automorphisms of A and B respectively, therefore any two isomorphisms τ, σ differ by an automorphism of A or B. Therefore if the automorphism of A is trivial, then so is the automorphism of B. Therefore any two isomorphisms between A and B will be equal to each other.

This is what happens with objects determined by universal property where we know that the only automorphism is the identity, i.e. the automorphism group is trivial. Therefore if such an object is isomorphic to any other object, the isomorphism is also unique. Conversely, if the automorphism group is not trivial, we know that isomorphisms between A and B are not unique as well. As what we will see later, there will be a lot of interesting automorphisms of algebraic closures.

Remark 2.18. If k is a field which is not finite, then it can be proved that any of it's algebraic closure has the same cardinality as k.

For example if k is countable, we can enumerate all polynomials in k with arbitrary number of variables, they we know that any finite extension of k is countable since elements in that finite extension is $\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\beta_1,\cdots,\beta_m)}$, then we know that the algebraic extension is a countable union of finite extensions. We can first argue by degree and for a fixed degree extension, it's a finite dim vector space over k, therefore the same cardinality.

Such observations can be useful, for example the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is not $\mathbb{C}$ since $\mathbb{Q}^a$ is countable while $\mathbb{C}$ is not.

3 Splitting fields and normal extensions

Definition 3.1. Let k be a field and let f be a polynomial in $k[x]$ of degree $\geqslant 1$. We say an extension L/k is a **splitting field** is f splits into linear factors in L:

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

with $\alpha_i \in K$ and such that K is $k(\alpha_1, \cdots, \alpha_n)$.

In particular, a splitting field of $f(x) \in k[x]$ is algebraic over k.

Theorem 3.2. Let K be a splitting field of the polynomial $f(x) \in k[x]$. Then if E is another splitting field of f, then there is a k-algebra isomorphism $E \to L$. Moreover, if we have an embedding:

$$k \hookrightarrow L \hookrightarrow k^a$$

i.e. we choose an algebraic closure of k in the beginning, then any k-algebra embedding of E to k^a is a k-algebra isomorphism between E and L.

Proof. We notice that in the extension $k \hookrightarrow L \hookrightarrow k^a$, k^a is also an algebraic closure of L.

Since we know that E/k is algebraic, we proved before that there is always a k-algebra extension $\sigma : E \hookrightarrow k^a$. We only need to show that this induces an isomorphism between E and L.

Let's assume that in E the polynomial f factors as $f(x) = c(X - \beta_1) \cdots (X - \beta_n)$ with $\beta_i \in E$ and $c \in k$. Consider it's image under the embedding σ, which is $c(x - \sigma(\beta_1)) \cdots (x - \sigma(\beta_n))$. We know that $f(x)$ in k^a

factors uniquely as $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, we know that $\sigma(\beta_i)$ is just a permutation of α_i. We also know that f factors in in L, therefore we know that $L = k(\alpha_1, \cdots, \alpha_n)$. Therefore we know that the image of E in k^a is contained in L. It show surjectivity, we know that elements in $k(\alpha_1, \cdots, \alpha_n)$ are fractions of polynomials in α_i, each α_i comes from some β_j by σ, therefore is surjective. □

Remark 3.3. For any field k and any field $f(x) \in k[x]$ with degree at least 1, it always has a splitting field. First we consider the algebraic closure k^a of k, then take the subfield generated by all the roots of $f(x)$.

Definition 3.4. Let I be an index set and let $f_i(x)$ be a family of polynomial in $k[x]$, an extension K/k is a **splitting field for this family of polynomials** if every $f_i(x)$ splits into linear factors in K and K is generated by all the roots of the polynomials, i.e. K is equal to the subfield generated by all the roots.

In most of applications, we will only use a finite set as the index set, but since most of the proofs we give later will not be simpler even if we restrict to the finite condition, we will adopt this more general situation.

Notice that the splitting field of any family of polynomials exists. In k^a, we take the splitting field K_i of $f_i(x)$ and consider the compositum, clearly all $f_i(x)$ factors in the compositum and clearly the splitting field contains all K_i, therefore the compositum, therefore the compositum is the splitting field.

Corollary 3.5. Let K/k be a splitting field for the family $\{f_i\}_{i\in I}$ in k^a and let E be another splitting field. Then any k-algebra embedding of E to k^a induces an isomorphism between E and L.

Proof. We notice that any such embedding embeds E_i to K_i, thus an isomorphism, therefore E is mapped into L. Notice that L is the compositum of K_i, and the image of E contains all K_i, therefore L is contained in the image, therefore this is an isomorphism. □

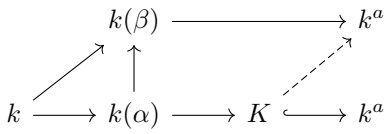
Remark 3.6. If we consider a finite set of polynomials, we know that the splitting field of this set of polynomials is the same as the splitting field of a single polynomial, i.e. the product of these finitely many polynomials.

Theorem 3.7. Let K be an algebraic extension of k, contained in an algebraic closure k^a of k. Then the following conditions are equivalent:

1. Every k-algebra embedding of K to k^a induces an automorphism of K.
2. K is the splitting field of a family of polynomials in $k[x]$.
3. Every irreducible polynomial of $k[x]$ which has a root in K splits into a linear factor in K.

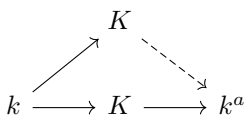
Definition 3.8. A field extension satisfying the above conditions is called **normal**. In particular, a normal extension is algebraic.

Proof. Let's prove $1 \Rightarrow 2$ first: let α be an element of K and let $p_\alpha(x)$ be the irreducible polynomial over k. Let β be a root of $p_\alpha(x)$ in k^a, I claim that β is in K^a. To see why, I claim that there is a k-algebra embedding of $k(\alpha) = k[\alpha]$ to $k(\beta) = k[\beta]$ defined by mapping α to β. This is well defined because β is also a root of the minimal polynomial. Then consider the following diagram:



where the dotted morphism is because $k(\alpha) \hookrightarrow K$ is algebraic and k^a is algebraically closed. Notice this is also a k-algebra extension, therefore we know from the hypothesis that this induces an automorphism of E, therefore $\beta \in E$. Therefore E is the splitting field of $p_\alpha(x)$ for all $\alpha \in E$.

Then let's prove $2 \Rightarrow 1$: Assume that K is the splitting field of $\{f_i\}$. Consider the following diagram:



where we have a k-embedding of K to k^a. Let α be a root of some f_i, we know that for any k-embedding σ, $\sigma\alpha$ is also a root of f_i, then since K is the splitting field, $\sigma\alpha$ is in K. Since K is generated by the roots of these f_i's, we know that K is mapped to itself. Since K is algebraic over k, we know that any such k-embedding is in fact an automorphism.

Notice that $1 \Rightarrow 3$ is already proved, since if $p(x)$ is an irreducible polynomial in $k[x]$ which has a root α in K, then $p(x)$ is the minimal polynomial of α with some possible multiplication of elements in k. Then we proved that for any roots of the polynomial in k^a, it's contained in K, therefore the polynomials factors in K into linear factors.

Conversely, let's prove $3 \Rightarrow 1$: recall that we only need to show that any such embedding maps K into itself. Let $\alpha \in K$, let $p(x)$ be the irreducible polynomial of α, then we know that $p(x)$ factors in K, then all roots of $p(x)$ is in K. Then since a k-embedding maps roots of $p(x)$ to roots of $p(x)$, therefore the image of α is in K, we are done. □

Example 3.9. Let's show that any degree 2 extension is normal.

First, notice that a degree 2 extension is always generated by one element. Say K/k is degree 2, let α be in K but not in k, then we know that we have $k \subset k(\alpha) \subset K$. Then we know that since α is algebraic over k, it has a minimal polynomial, at least of degree 2, therefore we know that $k(\alpha)$ is at least of degree 2 over k.

Then consider the algebraic closure of K, we know that $p(x)$ has roots α, α', we know that $p(x) = (x-\alpha)(x-\alpha')$, then we know that $\alpha + \alpha' \in K$, then since $\alpha \in K$, then $\alpha' \in K$, therefore K is the splitting field of $p(x)$, we are done.

Remark 3.10. It should be mentioned that normal extensions is not distinguished. The reason is that towers of normal extensions is not normal. To see why, consider the following example:

Consider the algebraic extension:

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

This is an extension of degree 4 as $x^4 - 2$ is the minimal polynomial by Eisenstein's criterion. This is not normal as we know that if we consider the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, this polynomials has a root $i\sqrt[4]{2}$, which is not in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. Therefore this is not normal by condition 3 in the previous theorem.

However, we know that we can write the extension as:

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

We know that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ thus the first extension is of degree 2. Notice that $x^2 - \sqrt{2}$ is the minimal polynomial (can you figure out why $\sqrt[4]{2}$ is not in $\mathbb{Q}(\sqrt{2})$? hint: using dimension of the two extensions), thus the second extension is of degree 2. Therefore the two extensions are both normal, but the tower is not normal.

However, we do have condition 2 and 3 in the definition of distinguished class of extensions for normal extensions:

Theorem 3.11.
1. Normal extensions remain normal under lifting.
2. If $k \subset E \subset K$ is a tower of extension and K is normal over k, then K is normal over E.
3. If K_2, K_2 are normal extensions of k contained in a common larger field L, then $K_1K_2, K_1 \cap K_2$ is normal over k.

Proof. Let K/k be a normal extension and F/k is an arbitrary extension contained in some common larger field. Recall that we proved that algebraic extension is preserved under lifting, therefore we know KF/F is algebraic, then let's assume that it's contained in one algebraic closure F^a of F. Then let's consider an embedding of KF over F to F^a. We want to show that it gives an isomorphism with KF. Notice that since this embedding is over F, it's also over k. Recall that F^a is algebraically closed, therefore we know that the algebraic closure of K, i.e. K^a is contained in F^a, then we know that the extension of EF to F^a, when restricted to K, we know that the image is going to be still algebraic over k, therefore it's contained in K^a, therefore since K is normal over k, this induces an automorphism of K. Then we have $(KF)^\sigma = K^\sigma F^\sigma = KF$, therefore we are done.

Then let's prove the second assertion: this is basically the fact that any embedding of K over E is also an embedding of K over k, we are done using condition 1 in the previous theorem.

Finally, notice that K_1K_2 is also algebraic over k, then any embedding σ of K_1K_2 over k to k^a satisfies:

$$\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$$

The assertion of the intersection is because:

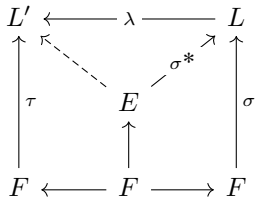
$$\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2)$$

□

4 Separable extensions

Let E be an algebraic extension of F and let $\sigma : F \to L$ be an extension of F in an algebraically closed field L. We will investigate more closely about extension of σ to E. Notice that such extension of σ maps E on a subfield of L which is algebraic over F. Then we can always take the algebraic closure of F insider L and assume that L is itself algebraic over F.

We will use S_σ to denote the set of extensions of σ to L. We are interested in the cardinality of this set and hope that this could indicate something about the algebraic extension E/F. But one thing we need to notice here is that we want this cardinality to be independent of the algebraic closure we choose for F. So suppose that $\tau : F \to L'$ is another algebraic closure of F. Then consider the following diagram:



where λ is an isomorphism such that $\lambda \circ \sigma = \tau$. Then we know that given any extension of σ, say σ^*, we get an extension of τ, i.e. $\lambda \circ \sigma^*$. This gives us a map $S_\sigma \to S_\tau$ and I will let you check that the inverse is given by λ^{-1}, therefore indeed S_σ and S_τ has the same cardinality.

Definition 4.1. Due to the discussion above, we know that the cardinality of S_λ only depends on the extension E/F, therefore we will call the cardinality of the set S_σ for any chosen algebraic closure of F $\sigma : F \to L$ the **separable degree** of E over F and denoted by:

$$[E : F]_s$$

Theorem 4.2. Let $k \subset F \subset E$ be a tower of algebraic extensions then:

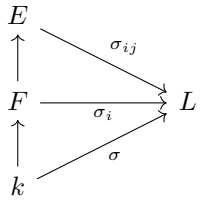
$$[E : k]_s = [E : F]_s[F : k]_s$$

Further more if E/k is a finite extension, then:

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

that is the separable degree of E/k is at most the degree of E/k.

Proof. Let's first prove the multiplicativity result. Consider the following diagram:



We notice that for $k \to L$, we have $\{\sigma_i\}_{i\in I}$ possible extensions of σ, then for each σ_i, we have $\{\sigma_{ij}\}_{j\in J}$ possible extensions. Moreover, given any such an extension of σ to E, we know that by restricting it to F we know that this extension is one of the σ_{ij}. Then some set-theory tells you the product formula holds.

Then suppose that E/k is finite, then recall that we can produce a tower:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \cdots \subset k(\alpha_1, \cdots, \alpha_r)$$

Recall that degree and separable degree are multiplicative, then we only need to show that this inequality holds for each step. Therefore we can assume that extension if $k(\alpha)/k$, then we know that in this case, if the degree of the minimal polynomial of α is d, there are at most d ways to extend σ. □

Corollary 4.3. Let $k \subset F \subset E$ is a tower of finite extensions, then:

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

is this equality holds in each step of the extension.

Remark 4.4. It will be shown later that in the case of a finite extension E/k, then $[E : k]_s$ always divides $[E : k]$. We will denote by $[E : k]_i$ to be the quotient and call it the **inseparable degree** of $[E : k]$. We will discuss this later in the section of inseparable extensions.

Definition 4.5. If E/k is a finite extension, then we will say E is **separable** over k if $[E : k]_s = [E : k]$.

If E/k is an algebraic extension, then an element $\alpha \in E$ is called **separable** if $k(\alpha)/k$ is a separable extension. You can easily prove that this is equivalent to say that the minimal polynomial of α has no multiple roots in an given algebraic closure.

Let $g(x) \in k[x]$ be a polynomial, it's called separable if it has no multiple roots in any algebraic closure. Let α be a root of an algebraic closure, then it's easy to see that $k(\alpha)/k$ is separable.

One quick notice is that if $k \subset F \subset E$ is a tower of algebraic extensions, then if $\alpha \in E$ is separable over k, then it's separable over F, i.e. we know that the minimal polynomial of α in F divides that in k.

Proposition 4.6. Let E/k be a finite extension, then E is separable over k iff every element in E is separable over k.

Proof. Recall that since E/k is finite we have the tower:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \cdots, \alpha_n)$$

Notice that each step is separable, if we assume all elements of E is separable over k, then we know that the finial extension is separable.

Conversely, we already know that if E/k is separable, for each α, we consider $k(\alpha)$:

$$k \subset k(\alpha) \subset E$$

then E/k being separable implies that each step is separable, in particular $k(\alpha)/k$ is, thus α is separable. □

In particular, we notice in the following argument that if $K = k(\alpha_1, \cdots, \alpha_n)$ with all α_i separable over n, we know K/k is separable.

Definition 4.7. Let K/k be an algebraic extension, then we say that this extension is separable over k iff every finitely generated subextensions are separable over k. You can easily check using the above proposition that this is equivalent to the fact that all elements in K is separable over k.

Proposition 4.8. If E/k is an algebraic extension generated by $\{\alpha_i\}$, then if every α_i is separable over k, then E/k is separable.

Proof. Note that the converse is true by definition.

To prove this, it suffice to prove that any element of E lies in some finitely generated subfield $k(\alpha_{i1}, \cdots, \alpha_{in})$, but we know that $k(\alpha_i)$ consists of elements that are fractions of polynomials with finitely many α_i, therefore we are done by the previous proposition. □

Then in the following discussion, by separable extensions, we mean algebraic separable extension, not necessarily finite.

Theorem 4.9. Separable extensions forms a distinguished class.

Proof. Let's first consider towers of extensions $k \subset F \subset E$, we know if E/k is separable, we know that F/k is separable since elements in F is in E. Moreover we proved E/F is also separable before. Conversely, let's assume that F/k and E/F are separable, then if E/k is finite, we are done. If not, let $\alpha \in E$, we want to show that $k(\alpha)/k$ is separable. Let the minimal polynomial of α with coefficients in F be the one with coefficients $a_n, \cdots, a_0$. Let $F_0 = k(a_0, \cdots, a_n)$, we know that $k \subset F_0$ is separable. Then we only need to prove that $F_0 \subset F_0(\alpha)$ is separable. Notice that the this minimal polynomial has no multiple roots. We know that the minimal polynomial of α in F_0 must divide that in F, therefore α is separable over F_0, therefore $F_0(\alpha)$ is separable over F_0, we are done.

For the lifting property, let E/k be separable over k and F/k is an arbitrary extension, both contained in some larger field. Let $\alpha \in E$, since it's separable over k, we know that it must be separable over F. Since EF is $F(\{\alpha_e\}_{e \in E})$, we conclude from the previous result EF is separable over F. □

Remark 4.10. Let E/k be a finite extension of k, recall that we proved that the intersection of normal extensions of k in E is still normal. Obviously, this is the smallest normal extension of k in E. Recall that for a finite extension, the number of distinct embeddings of E to E^a over k is only finitely many, say $\sigma_1, \cdots, \sigma_n$. Then consider the compositum of $\sigma_1(E), \cdots, \sigma_n(E)$ in the algebraic closure E^a. I claim that this compositum is a normal extension of k. To see why, first we notice that it's algebraic over k as a compotitum of several algebraic extensions. Suppose that we have an embedding τ of the compositum to E^a over k, we know it's $\tau\sigma_1(E) \cdots \tau\sigma_n(E)$. Since we know that $\tau\sigma_1, \cdots, \tau\sigma_n$ is just a permutation of $\sigma_1, \cdots, \sigma_n$, therefore we know that $\tau\sigma_1(E) \cdots \tau\sigma_n(E)$ is still in $\sigma_1(E), \cdots, \sigma_n(E)$ since it's over k and is injective, we know that it's an automorphism. Therefore $\sigma_1(E), \cdots, \sigma_n(E)$ is a normal extension of k containing E.

On the other hand, we know that any normal extension of k containing E will contain $\sigma_1 E, \cdots, \sigma_n E$. Therefore it must contain the compositum, therefore we know that $\sigma_1(E), \cdots, \sigma_n(E)$ is the smallest normal extension of k containing E.

Assume further that E/k is a finite separable extensions, then we consider all the embeddings of E to k^a, we know that for each such embedding σ, σE is still separable over k, then we know that by induction that $\sigma_1 E \cdots \sigma_n E$ will be separable over k. Therefore we know that the smallest normal extension of k containing E is also separable over k.

Now let E/k be algebraic, not necessarily finite, we still can talk about the embeddings of E to k^a over k. Say these embeddings are σ_i, then we can consider the compositum of $\sigma_i E$. I claim that this is normal since we know that the compositum if still algebraic over k and we know that any embedding of the compositum over k to k^a maps itself to itself (here we can use the fact that this compositum is the union of all of the finite compositums). Therefore the compositum is again normal. Moreover if E is separable, then so is each $\sigma_i E$, then again use the fact that the compositum is the union of finite compositums, we conclude that the compositum is separable as well.

Definition 4.11. Let k be a field and we consider all the separable extension in it's algebraic closure k^a and then take the compositum of all these subextension, we again get a separable extension, which can be viewed as the largest separable extension of k in k^a. We will call this extension the **separable closure** of k, denoted by k^s.

Definition 4.12. Let E/k be an algebraic extension, then let σ be any embedding of E to k^a over k. We call $\sigma(E)$ the **conjugate** of E in k^a. Then we see that the smallest normal extension of E in k^a is the compositum of all conjugates of E.

Let α be algebraic over k, if $\sigma_1, \cdots, \sigma_r$ are distinct embeddings of $k(\alpha)$ into k^a over k, we will call $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ the **conjugates** of α in k^a. We see that these $\sigma_i(\alpha)$ are just the distinct roots of the minimal polynomial of α, say of $p(x)$. Then we know that the smallest normal extension of k in k^a containing $k(\alpha)$ is $k(\sigma_1\alpha, \cdots, \sigma_n\alpha)$.

Theorem 4.13. Primitive element theorem Let E be a finite extension of k, then there is an element $\alpha \in E$ such that $E = k(\alpha)$ if and only if there is only a finite number of fields F such that $k \subset F \subset E$. If E/k is separable, then there exists such an α.

Proof. First, if k is a finite field, then so is E, consider the multiplicative group of E. Recall that we have a general fact that for a finite abelian group of n elements, it's cyclic iff $x^d = 1$ has at most d solutions for all d that divides n. This is because we have the structure theorem for finite abelian groups where $G = \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ with $n_i | n_{i+1}$, then I will let you check why this is true. Then in a field, we know that $x^d = 1$ at most has d solutions, we are done. Then we know that E is generated by one element, i.e. the primitive element in the multiplicative group. Therefore let's assume k is infinite.

Let's first assume that there are only finitely many F in between k, K. Let $\alpha, \beta \in E$, I claim that $k(\alpha, \beta)$ is generated by a single element. First, since $c \in k$ can take infinitely many values if we consider $k(\alpha + c\beta)$, we know that there has to be some $c_1 \neq c_2$ such that $\alpha + c_1\beta = \alpha + c_2\beta$, therefore we know that $\beta(c_1 - c_2)$ is in the same field, therefore β is in that field, so α is in that field, therefore $k(\alpha, \beta) = k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$.

Then since E is a finite extension, we know that $E = k(\alpha_1, \cdots, \alpha_n)$. Recall that we can write E as $k(\alpha_1, \cdots, \alpha_{n-2})(\alpha_{n-1}, \alpha_n)$, then we know that there is a c_n such that $k(\alpha_1, \cdots, \alpha_{n-2})(\alpha_{n-1}, \alpha_n) = k(\alpha_1, \cdots, \alpha_{n-2})(\alpha_{n-1} + c\alpha_n)$, then we keep proceeding by induction to conclude this field extension is generated by one element.

Conversely, suppose that $E = k(\alpha)$ and let $f(x) \in k[x]$ be the minimal polynomial of α over k. Let F/k be an extension such that we have $k \subset F \subset K$, let $g_F(x)$ be the minimal polynomial of α over F. We know that $g_F(x)$ divides $f(x)$. Consider $g_F(x)$ and $f(x)$ in an algebraic closure of E, then we know that since $g_F(x)$ divides $f(x)$ and is with coefficients 1, we know that we only have finitely many possibilities. Therefore we get a map from the intermediate extensions to the set of polynomials in $E[x]$:

$$F \mapsto g_F(x)$$

The previous discussion tells us that the image is a finite so if we can show this map is injective, we are done. To show this, consider the subfield F_0 of F generated over k by the coefficients of $g_F(x)$, then we know that $g_F(x)$ is now in $F_0[x]$ and since $g_F(x)$ is irreducible over F, it's irreducible over F_0. Then we know that $g_F(x)$ is again the minimal polynomial of α over F_0. Therefore we know that the degree of E/F_0 is the degree of E/F, therefore $F = F_0$. Suppose that F, F' are two intermediate fields such that they are mapped to the same $g_F(x)$, then we know that F_0 is the subfield of both F, F', then we know that $F = F' = F_0$, we are done.

Finally as for the assertion related to finite separable extensions, suppose that K/k is a finite separable extension, we can assume that $K = k(\alpha_1, \cdots, \alpha_n)$, by induction we can assume that $K = k(\alpha, \beta)$ where α, β are separable over k. Consider the distinct embeddings $\sigma_1, \cdots, \sigma_n$ of $k(\alpha, \beta)$ over k to k^a. We know that since this is separable, the degree of $k(\alpha, \beta)/k$ is n. Then consider the polynomial:

$$p(x) = \prod_{i \neq j} (\sigma_i\alpha + X\sigma_i\beta - \sigma_j\alpha - x\sigma_j\beta)$$

By definition, this is not the zero polynomial and therefore there is c such that $p(c) \neq 0$ since k is an infinite field, therefore we know that $\sigma_i(\alpha + c\beta)$ will be distinct, therefore we know that the separable degree of $k(\alpha + c\beta)$ is at least n, which means that the degree is at least n. However since the degree of $k(\alpha, \beta)$ is n and $k(\alpha + c\beta) \subset k(\alpha, \beta)$, we know that they are equal. □

In particular, there are only finitely many intermediate fields in between E/k if E is finite separable over k. If $E = k(\alpha)$, we will call α the **primitive element** of E over k.

5 Finite fields

Finite fields is going to be of great interest in the study of arithmetic geometry. As we have now developed enough theory, let's use them to discuss finite fields in this section. This is very interesting for it's own sake and it will also give examples to the general theory we develop before.

First let F be a finite field of q elements, we know that there is always a ring map $\mathbb{Z} \to F$, consider it's kernel, which is not 0, thus is generated by a prime number p, therefore we have an injective map $\mathbb{Z}/p\mathbb{Z}$ to F. Notice that $\mathbb{Z}/p\mathbb{Z}$ is a field, and I will let you see why (use gcd is probably easier). We will denote this field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. Therefore we know that F is of characteristic p and contains $\mathbb{F}_p$. It's also a finite

dimensional vector space since F itself is finite. Let's assume that the dimension is n, then we know that F has p^n distinct elements.

One quick question is that is there a field for each n, i.e. a field of p^n elements over $\mathbb{F}_p$. If there exists such fields, what are the relation between different such fields. Let's first answer these questions. I first claim that if we consider the multiplicative group of F, i.e. F^*, there are $q-1$ elements, and for any $x \in F^*$, since multiplying with x gives a permutation, we know that if $a_1, \cdots, a_{q-1}$ are all the elements in the multiplicative group:

$$x^{q-1}a_1 \cdots a_{q-1} = a_1 \cdots a_{q-1} \Rightarrow x^{q-1} = 1$$

Therefore every element x in the group satisfies the relation $x^{q-1} = 1$. Notice that x^{q-1} has at most $q-1$ solutions, therefore the elements in F^* are all the solutions of $x^{q-1} = 1$. If we take 0 into consideration, then we know every element in F satisfies $f(x) = x^q - x = 0$. Moreover $x^q - x$ factors into linear products:

$$f(x) = \prod_{\alpha \in F} (x - \alpha)$$

Notice that $f(x)$ is in $\mathbb{F}_p[x]$, therefore we know F is the splitting field of $f(x)$, therefore in particular, if such a field exists then it's the splitting field of $x^q - x$. Then we know from our study of splitting field that there is an isomorphism over $\mathbb{F}_q$ between any two such fields, thus any two such fields are isomorphic.

To prove it's existence, we want to show that the splitting field of $f(x) = x^{p^n} - x$ in the algebraic closure of $\mathbb{F}_p$ is indeed the field we are looking for. First, let's prove that the splitting field only consists of roots of $f(x)$. Let α, β be the roots of $f(x)$, then we know that:

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0$$

Therefore $\alpha + \beta$ is also a root. You can prove similarly $\alpha\beta$ is also a root. Finally, we know that:

$$(-\beta)^{p^n} = \pm\beta$$

it's $-\beta$ if p is odd, it's β is p is even, therefore we know that if $p \neq 2$, $(-\beta)^{p^n} = -\beta$, therefore $-\beta - (-\beta) = 0$. If $p = 2$, since we know that $+1 = -1$ in $\mathbb{Z}/2\mathbb{Z}$, we are done. This proves that since the spliting field is just additions, multiplications and inverses of the roots of $x^p - x$, then all elements in the splitting field are roots of $x^{p^n} - x$. Moreover, we know that the derivative of $x^{p^n} - x = -1$, therefore there is no multiple roots of $f(x)$, i.e. there are p^n distinct roots in $\mathbb{F}_p^q$, therefore we know that the splitting field of $x^{p^n} - x$ has exactly p^n elements, thus proving the existence. We summarize our result in the following theorem:

Theorem 5.1. For a prime number p and each integer $n \geqslant 1$, there is a finite field of order p^n denoted by $\mathbb{F}_{p^n}$, which is the splitting field of the polynomial $X^{p^n} - x$ in the algebraic closure $\mathbb{F}_p^a$ with the elements of the field the distinct roots of this polynomial. Any finite field F is isomorphic to exactly one $\mathbb{F}_{p^n}$.

We usually write $q = p^n$ and $\mathbb{F}_q$ instead of $\mathbb{F}_{p^n}$. Notice that when we use such notations we are implying that we are considering questions in a given algebraic closure of $\mathbb{F}_p$.

Corollary 5.2. Let $\mathbb{F}_q$ be a finite field and let n be an integer $\geqslant 1$, in a given algebraic closure $\mathbb{F}_p^a$, there is one and only one extension of $\mathbb{F}_q$ of degree n and this extension is $\mathbb{F}_{q^n}$.

Proof. Recall that if we let $q = p^m$, then $q^n = p^{mn}$, then we consider the splitting field of $x^{q^n} - x$ in the given algebra closure $\mathbb{F}_p$, we know that first since $\mathbb{F}_q$ is the splitting field of $x^q - x$ and it's elements are roots of this polynomial, then this new splitting field indeed contains $\mathbb{F}_q$.

Suppose that there is any other such field in $\mathbb{F}_p^a$, we know that since it's degree n over $\mathbb{F}_q$, it's degree mn over $\mathbb{F}_p$, therefore we know that it's the splitting field of $x^{q^n} - x$, therefore we know that the embedding of this field to $\mathbb{F}_p^a$ gives an isomorphism to $\mathbb{F}_{q^n}$ (as they are both splitting fields of $x^{q^n} - x$), therefore the two are the same set in $\mathbb{F}_p^a$, we are done. □

Proposition 5.3. Suppose that F is a finite field, then the multiplicative subgroup is cyclic.

Proof. Notice that the multiplicative group of the finite field is finite and abelian, then we use the structure structure to conclude that it's of the form:

$$\mathbb{Z}/n_1 \times \cdot \times \mathbb{Z}/n_r$$

where $n_i | n_{i+1}$. This implies that if G is a finite group with n elements, then it's cyclic iff for any $x^d - 1 = 0$ there are only at most d elements in the group solving this equation for each $d|n$. This is trivial in a field, we are done. □

Our next topic is to determine all automorphisms of a finite field $\mathbb{F}_q$:

First, we notice that if $q = p^n$ and $\mathbb{F}_q$ is ta finite field with q elements, we can consider the Frobenius mapping:

$$\varphi : \mathbb{F}_q \to \mathbb{F}_q, \qquad x \mapsto x^p$$

Since the characteristic of $\mathbb{F}_q$ is p, we know that this is indeed an additive morphism, thus a ring morphism. Clearly it's injective as it's not the 0-map. Since $\mathbb{F}_q$ is finite, then injective implies surjective, we know that the Frobenius morphism is indeed an isomorphism. Recall that for any element $x \in \mathbb{F}_p$, we know that $x^p = x$, therefore the Frobenius map fixes $\mathbb{F}_p$, thus is an $\mathbb{F}_p$-algebra automorphism.

Theorem 5.4. The group of automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$ is of degree n, where $q = p^n$, is cyclic of degree n, generated by the Frobenius morphism φ.

Proof. First we notice that we actually don't have to assume that the automorphism group of $\mathbb{F}_q$ is over $\mathbb{F}_p$. Let $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ be an automorphism of $\mathbb{F}_q$, we know that this necessarily fixed $\mathbb{F}_p$, since we know that 1 must be mapped to 1.

Notice that since in $\mathbb{F}_q$ every element x satisfies $x^{p^n} = x$, therefore we know that φ^n is the identity. Then assume that d is the minimal positive integer such that $\varphi^d = \mathrm{Id}$, therefore $x^{p^d} = x$ for all $x \in \mathbb{F}_q$. Notice that this equation has at most p^d solutions, therefore $d \geqslant n$, therefore $d = n$.

Now let $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ be an automorphism, this is an embedding of $\mathbb{F}_q$ to $\mathbb{F}_q^a$ over $\mathbb{F}_p$, therefore there are at most n such embeddings by the separable degree argument, therefore φ^i for $1 \leqslant i \leqslant d$ are all the automorphisms. □

Theorem 5.5. Let m, n be integers at least 1, then any algebraic closure of F_p, the subfield of $\mathbb{F}_{p^n}$ is contained in $\mathbb{F}_{p^m}$ iff $n|m$.

If $\mathbb{F}_{p^n}$ is contained in $\mathbb{F}_{q^m}$, we set $q = p^n$ and let $m = nd$, then $\mathbb{F}_{p^m}$ is normal and separable over $\mathbb{F}_q$ and the group of automorphisms of $\mathbb{F}_{p^m}$ is cyclic of order d, generated by φ^n where φ is the Frobenius map.

Proof. Let's first prove the first assertion. The key here is to notice that for example in a given algebraic closure $\mathbb{F}_p^a$, for example in $\mathbb{F}_{p^n}$, if we want all elements in $\mathbb{F}_{p^n}$ to satisfy the relation:

$$x^y = x$$

for some integer y, then y is necessarily p^{dn} for some nonnegative integer d. The reason is simple, we know that for all $x \in \mathbb{F}_{p^n}$, it satisfies $x^{p^n} = x$, then we check that if y is at least p^n, if not, then we know that x^y can't be all equal to x for all x. If it's at least p^n, we know we can see if it's at least p^{2n}, if not we know that:

$$y = p^n \cdot (p^n - s) + r$$

Then we know that $x^y = x^{r-s}$ for some $r < p^n$ and $s < p^n$, therefore we know that:

$$-p^n < r - s < p^n$$

Therefore x^{r-s} is not x, a contradiction. We can similarly show that if x is larger than p^{2n} but not large enough to reach p^{3n}, then:

$$y = p^{2n}(p^n - s) + r$$

Then again x^y is not x for some x. Then since y is a finite integer, this process end after finitely many steps.

Using this observation, we notice that if $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, then we know that for all $x \in \mathbb{F}^{p^n}$:

$$x^{p^m} = x$$

Therefore we know that $p^m = p^{dn}$, we are done. Conversely the same equation tells us $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.

Then to show that $\mathbb{F}_{p^m}$ is normal over $\mathbb{F}_{p^n}$, we know that $\mathbb{F}_{p^m}$ is the splitting field of $x^{p^m} - x$, therefore normal. It's separable over $\mathbb{F}_{p^n}$ because for every $x \in \mathbb{F}_{p^m}$, it minimal polynomial over $\mathbb{F}_{q^n}$ should divide $x^{p^m} - x$, which has no multiple roots. Therefore the minimal polynomial has no repeated roots, we are done.

Finally to figure out the automorphisms of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^n}$, we can argue like how we find automorphism of $\mathbb{F}_{p^n}$. First, we notice that $x \mapsto x^{p^n}$, i.e. φ^n is indeed an automorphism over $\mathbb{F}_q$ and $(\varphi^n)^i$ for $1 \leqslant i \leqslant d$ are d distinct automorphisms since d is the minimal positive integer such that $(\varphi^n)^d$ is the identity. Then notice that the degree of $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is d, therefore there are at most d these automorphisms, we are done. □

6 Inseparable extensions

Definition 6.1. Suppose that k is a field and $f(x) \in k[x]$ is a polynomial of the form:

$$f(x) = (x - \alpha)^m g(x)$$

with $(x - \alpha)$ not dividing $g(x)$. Then we will say that α is a multiple root if $m > 1$ and say the multiplicity is m. Otherwise, we say it's a simple root.

Proposition 6.2. Let k be a field and k^a one of k's algebraic closure. Let $\alpha \in k^a$ and $f(x)$ is minimal polynomial. If the characteristic of $k = 0$, then roots of $f(x)$ is a simple root, i.e. f is a separable polynomial. If the characteristic is $p > 0$, then there is an integer $\mu \geqslant 0$ such that every root of $f(x)$ has multiplicity p^μ and:

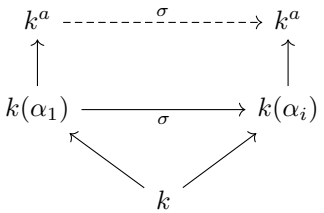
$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s$$

Moreover α^{p^μ} is separable over k.

Proof. Let $\alpha, \cdots, \alpha_r$ be the distinct roots of $f(x)$ in the algebraic closure k^a and let $\alpha = \alpha_1$. Let m be the multiplicity of α in f. We know that for $1 \leqslant i \leqslant r$, there is an k-algebra isomorphism:

$$\sigma : k(\alpha_1) \to k(\alpha_i)$$

clearly this is defined by mapping α_1 to α_i, which is well-defined, then we know that it's injective between two k-vector spaces of the same dimension, therefore an isomorphism. Consider the following diagram:



where the dotted morphism is the extension of σ which is still called γ, note that it's a k-algebra homomorphism. Notice that $f^\sigma = f$. Therefore:

$$f(x) = \sigma(f(x)) = \prod_{j=1}^{r} (x - \sigma\alpha_j)^{m_j}$$

where m_j is the multiplicity of α_j. Since $k^a[x]$ is a UFD, we conclude that the multiplicity of α_1 is the same as the multiplicity of all the other roots α_i.

Now say that we are in the case when char$k = 0$, we know that is $f(x)$ has a multiple root, say α_1, then α_1 will be the root of $f(x)$ and $f'(x)$ and both of them are in $k[x]$, which is a contradiction since we

know that $f'(x)$ is a nonzero polynomial whose degree is one lower than $f(x)$. Therefore we conclude that in characteristic 0 case, minimal polynomials will not has multiple roots.

In positive characteristics, if $f(x)$ has multiple roots, we know that it must be the case that $f'(x) = 0$, therefore we know that this can only happen when $f(x) = g(x^p)$ for some polynomial $g(x) \in k[x]$ that is to say, the power of x each term of $f(x)$ must be divisible by p. Therefore we know that α^p is the root of a polynomial of degree less than f. Notice that $g(x)$ is still irreducible, we know that if it's reducible and $g(x) = h(x)k(x)$, then we know that $f(x) = h(x^p)h(x^p)$, thus $f(x)$ is reducible thus a contradiction. Then we ask does $g(x)$ have multiple roots, and keep going. Eventually the degree of the polynomial will be less than p, and we can no longer perform this procedure any more, but this also implies that the polynomial has no multiple roots anymore. Therefore we can assume that in the end there is a nonnegative integer μ such that α^{p^μ} is the root of a separable polynomial $h(x)$.

Notice that $h(x^{p^\mu}) = f(x)$. We know that the degree of f is p times larger than that of g, therefore we know that:

$$[k(\alpha) : k(\alpha^p)] = p$$

We keep going and inductively we get:

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu$$

Moreover since h is separable, we know that $[k(\alpha^{p^\mu}) : k] = [k(\alpha^{p^\mu}) : k]_s$. Suppose that $\beta_1, \cdots, \beta_s$ are the distinct roots of β, then we know that:

$$h(x) = (x - \beta_1) \cdots (x - \beta_s)$$

since $f(x) = h(x^p)$ we know that $f(x) = (x^{p^\mu} - \beta_1) \cdots (x^{p^\mu} - \beta_s)$. We know that in k^a, there are $\alpha_1, \cdots, \alpha_s$ such that $\alpha_i^{p^\mu} = \beta_i$, therefore we know that:

$$f(x) = \prod_{i=1}^{s} (x - \alpha_i)^{p^\mu}$$

Recall that $f(x) = \prod_{j=1}^{r} (x - \alpha_j)^m$, then we know that by the fact that $k^a[x]$ is a UFD that $r = s$ we know that we can assume that the roots of $h(x)$ are α^{p^μ}.

In particular:

$$[k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s$$

Then we know that:

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^\mu})][k(\alpha^{p^\mu}) : k] = p^\mu \cdot [k(\alpha^{p^\mu}) : k]_s = p^\mu \cdot [k(\alpha) : k]_s$$

□

Corollary 6.3. For any finite field extension E/k, the separable degree $[E : k]_s$ divides the degree $[E : k]$, the quotient is always 1 if char$k = 0$ and it's a power of p if the characteristic is $p > 0$.

Proof. We know that for any finite extension, we can realize it as a tower of extensions, each time adjoining one more element, then we can use the previous result and the fact that the degree and separable degree is multiplicative in towers. □

Definition 6.4. If E/k is a finite extension, then we will call the quotient $\frac{[E:k]}{[E:k]_s}$ the **inseparable degree** of E/k, and denoted by $[E : k]_i$.

Then by definition, we see that a finite extension is separable iff $[E : k]_i = 1$.

Mover, since degree and separable degree is multiplicative in towers of finite extensions, we conclude that if $k \subset F \subset E$ is a tower of finite extensions, then $[E : k]_i = [E : F]_i \cdot [F : k]_i$.

Since the we know that in the case of char$k = 0$, any algebraic extension is separable, thus no interesting stuff happens. Therefore, we assume later in this section that $p > 0$.

Definition 6.5. Let K/k be an algebraic extension, then an element $\alpha \in K$ is said to be **purely inseparable** over k if there is an integer $n \geqslant 0$ such that $\alpha^{p^n} \in k$.

Remark 6.6. If K/k is algebraic, then by definition, you can check that for every $\alpha \in k$, it's both separable and purely inseparable.

Theorem 6.7. Let E/k be an algebraic extension then the following conditions are equivalent:

1. $[E : k]_s = 1$.
2. Every element in E is purely inseparable over k.
3. For every $\alpha \in E$, the minimal polynomial of α over k is of the type $x^{p^n} - a$ with some $n \geqslant 0$ and $a \in k$ and $\alpha^{p^n} = a$.
4. There is a set of generators $\{\alpha_i\}_{i \in I}$ of E over k such that each α_i is purely inseparable over k.

Proof. Let's first prove $1 \Rightarrow 2$. Notice that for any $\alpha \in E$, we have a tower $k \subset k(\alpha) \subset E$. Recall that separable degree is multiplicative for algebraic extensions, then we know that $[k(\alpha) : k] = 1$. Therefore if we think about the minimal polynomial of α, say $f(x)$, it has only one distinct zero. Let $m = [k(\alpha) : k]$, and we know that the factorization of $f(x)$ over $k(\alpha)$ is $(x - \alpha)^m$. We know from the previous result that:

$$m = [k(\alpha) : k] = p^n \cdot [k(\alpha) : k]_s = p^n \cdot 1$$

Therefore we know that $f(x) = x^{p^n} - \alpha^{p^n}$ and we know that $\alpha^{p^n} \in k$.

If $\alpha \in E$ is purely inseparable, that is there is a n such that $\alpha^{p^n} \in k$, let $f(x)$ be it's minimal polynomial. Consider the polynomial $(x - \alpha)^{p^n}$, we know that since α^{p^n} is in k, this is a polynomial in $k[x]$ and we know that α is it's root. Therefore we know that $f(x)$ divides this polynomial, thus it's $(x - \alpha)^m$. We know that $m = p^r s$ for some s prime to p since the degree of $[k(\alpha) : k]$, by the previous theorem is $p^r \cdot [k(\alpha) : k]$. Then we consider:

$$f(x) = (X^{p^r} - \alpha^{p^r})^s = x^{rp^r} + s\alpha^{p^r} x^{(s-1)p^r} + \cdots$$

Then since $s\alpha^{p^r} \in k$, we know that $\alpha^{p^r} \in k$, therefore we know that $X^{p^r} - \alpha^{p^r}$ is in $k[x]$ and it divides $f(x)$, therefore it's the minimal polynomial.

Clearly condition 3 implies 4 since if an element satisfies 3 then it's purely inseparable, and we know that E is generated over k by all of the elements in E.

Finally let's prove $4 \Rightarrow 1$: we want to prove that $[E : k]_s = 1$, that is there is only one k-embedding from E to the algebraic closure. Let σ be such an embedding, then we know that if the minimal polynomial of α_i is $f_i(x)$. Then we know that $f_i(x)$ only has one distinct root. σ maps α_i to another root of f_i, which is α_i itself, therefore σ is the identity on all α_i, thus is the identity on all elements of E. □

Definition 6.8. Let E/k be an algebraic extension satisfying the above equivalent conditions, then it said to be a **purely inseparable** extension.

Proposition 6.9. Purely inseparable extensions form a distinguished class of extension.

Proof. The tower result follows from the separable degree is multiplicative.

If E/k is inseparable and F/k is an arbitrary lifting, we first know that E/k is generated by a family of purely inseparable elements. Then we know that EF is generated over F by the same family of purely inseparable elements, we know that being purely inseparable means that there is a power p^n such that it lies in k. Since F contains k, then the same power lies in F as well, we are done. □

Proposition 6.10. Let E be an algebraic extension of k and let E_0 be the compositum of all subfields F of E such that $k \subset F$ and F is separable over k. Then E_0 is separable over k and E is a purely inseparable extension of E_0.

Proof. First we know that since separable extensions form a distinguished class, we know that E_0 is indeed separable over k. We can easily see that E_0 consists of all separable elements of E over k. Then recall that we say that for every $\alpha \in E$, there will be some μ such that α^μ is separable over k, therefore it's in E_0, therefore E/E_0 is purely inseparable. □

Proposition 6.11. If E/k is both separable and purely inseparable, then $E = k$.

Proof. Recall that if α is purely inseparable, then it's minimal polynomial in the algebraic closure is $(x-\alpha)^{p^n}$, but it's also separable, therefore the polynomial must be $(x-\alpha)$, therefore $\alpha \in k$. □

Proposition 6.12. Let K/k be a normal extension and let K_0/k be the maximal subextension that is separable over k, then K_0/k is again normal.

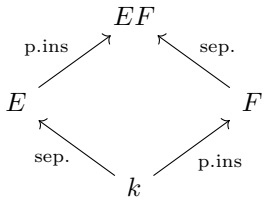
Proof. Suppose that we have a k-embedding of K_0 to the algebraic closure. We want to show that it induces an automorphism. We only need to show that it maps into itself. Notice that K_0 consists of all elements of K that is separable over k, then if $\alpha \in K_0$ is separable, then we know that $\sigma(\alpha)$ is also separable, then we know that $\sigma(\alpha) \in K_0$, we are done. □

Proposition 6.13. Let E, F be two finite field extensions of k and assume that E/k is separable and F/k is purely inseparable. Then if E, F are subfields of some larger field then:

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

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

Proof. If we assume the assertion, then $[EF : k]_s = [EF : F]_s \cdot [F : k]_s = [EF : F]_s$, therefore this in particular implies that EF/F is separable. Similarly $[EF : k]_i = [EF : E]_i \cdot [E : k]_i = [EF : E]_i$, therefore EF/E is purely inseparable. Therefore this conclusion is equivalent to the diagram:

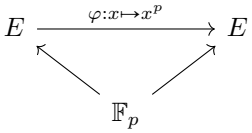


But we know that both purely inseparable and separable extensions are stable under lifting, we are done. □

Recall that if E is a field of characteristic p, then we notice that the subset $E^p = \{x^p : x \in E\}$ is a subfield of E. The key here is that we know that $x^p + y^p = (x+y)^p$. Similarly we can define E^{p^n} for all $n \geqslant 1$.

Proposition 6.14. If E/k is a finite extension, then if $E^p k = E$, E is separable over k, if E is separable over k, then $E^{p^n} k = E$ for all $n \geqslant 1$.

Proof. First, if $E^p k = E$, we conclude that $E^{p^n} k = E$ for all $n \geqslant 1$. To see why, you may consider the following diagram:



and then conclude that φ is an automorphism. However, we don't know this since we only know that E is finite over some k, so E is not necessarily algebraic over $\mathbb{F}_p$. Instead, notice that $E^p = (E^p k)^p = E^{p^2} k^p$, therefore we know that:

$$E = E^p k = E^{p^2} k^p k = E^{p^2} k$$

Then use induction we get our assertion. Therefore in the converse, we only need to prove for $n = 1$.

Let's first assume $E^p k = E$, and since E/k is finite, we can assume that $E = k(\alpha_1, \cdots, \alpha_n)$, then recall that if we let E_0 to be the maximal subfield of separable extension of k in E. Then we know that E is purely inseparable over E_0, then we know that for each α_i, there is a n_i such that $\alpha_i^{p^{n_i}} \in E_0$, therefore we take the largest n_i, say it's n, we know $E^{p^n} \subset E_0$. However, we know that $E = E^{p^n} k$, therefore $E = E^{p^n} k \subset E_0 k = E_0$, therefore $E_0 = E$ is separable over k.

Conversely, if E is separable over k, then consider:

$$k \subset kE^p \subset E$$

Then we know that E is separable over kE^p, however we know that for every $\alpha \in E$, $\alpha^p \in E^p k$, therefore we know that E is both purely inseparable over kE^p and separable over kE^p, therefore we get $E = kE^p$. □

Recall that we proved before that given an algebraic extension, we can decompose it into a maximal separable extension and a purely inseparable extension above it. Usually, we can't reverse this order, i.e. decompose it into first a purely inseparable extension and then a separable one. However, there is an very important case where we can:

Theorem 6.15. Let K/k be normal and let G be the group of automorphisms of K over k. Let K^G be the fixed field of G, then K^G is purely inseparable over k and K is separable over K^G. Moreover, if K_0 is the maximal separable subextension of K over k, then $K = K_0K^G$ and $K_0 \cap K^G = k$.

Proof. Let's first show that K^G is purely inseparable over k. Suppose that $\alpha \in K$ is fixed by all $g \in G$, then consider the embedding $\tau : k(\alpha) \hookrightarrow k^a$, we know that this can be extended to an embedding of K to k^a over k, which is an automorphism since K is normal, therefore we know that α is mapped to α, thus τ is the identity on $k(\alpha)$, therefore $[k(\alpha) : k]_s = 1$, therefore α is purely inseparable over k, we are done. Then we know that the intersection of K^G with K_0 is both separable and purely inseparable, therefore is k.

To prove K is separable over K^G, let's assume first that K is finite, then we know that in this case since K is normal, then G is finite. Let $\alpha \in K$, let $\sigma_1, \cdots, \sigma_r$ be a maximal subset of elements of G such that $\sigma_1\alpha, \cdots, \sigma_r\alpha$ are distinct and such that σ_1 is the identity. Notice that in this case α is the root of:

$$f(x) = \prod_{i=1}^{r}(X - \sigma_i\alpha)$$

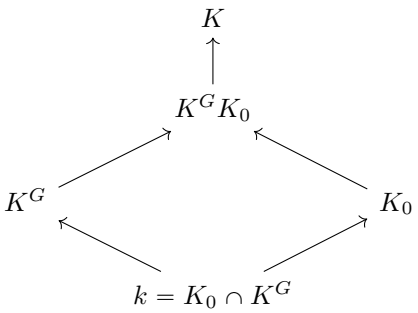
We know that $f^\tau = f$ for any $\tau \in G$ since we know that τ permutes $\sigma_1\alpha, \cdots, \sigma_r\alpha$ (because if there is some i such that $\tau\sigma_i\alpha$ is not in the original set of element, we can put $\tau\sigma_i\alpha$ in the orginal set and get a larger set, a contradiction.) Notice that $f = f^\tau$ is separable and $f \in K^G[x]$, therefore α is separable over K^G.

Now if K is infinite, let $\alpha \in K$, we know that if we let $p(x)$ be the minimal polynomial of α, since K/k is normal, we know that all the roots of $p(x)$ is contained in K, therefore suppose that they are $\alpha_1, \cdots, \alpha_n$, we notice that $k \subset k(\alpha_1, \cdots, \alpha_n)$ is normal since its the splitting field of $p(x)$ and we let $\alpha_1 = \alpha$. Then we know that any automorphism of K over k restricts to an automorphsim of $k(\alpha_1, \cdots, \alpha_n)$ over k. By the above discussion of the finite normal case, we know α is the root of:

$$f(x) = \prod_{i=1}^{r}(x - \sigma_j\alpha)$$

where $\sigma_1, \cdots, \sigma_r$ is a maximal set of automorphisms of $k(\alpha_1, \cdots, \alpha_n)$ such that $\sigma_i\alpha$ are distinct, then we know that for any $g \in G$, it's action on f is the same as it's restriction to $k(\alpha_1, \cdots, \alpha_n)$, therefore it fixes f, therefore $f \in K^G[x]$, thus α is separable.

Summarize what we prove above, we have:



We know that K is purely inseparable over K_0, therefore K is purely inseparable over K^GK_0. However, we know that K is separable over K^G, therefore separable over K^GK_0, therefore is equal to K^GK_0. □

In the next preliminary section, we will discuss this group G a lot, which is called the **Galois group** of K/k. Galois is mainly useful for extensions that are separable and normal, and such extensions are called **Galois extensions**. Notice that K_0/k is normal, because if $\alpha \in K_0$, then it's minimal polynomial $p(x)$ is a separable polynomial, since K/k is normal, then all the roots of $p(x)$ is in K. Moreover, each of the roots

has $p(x)$ as the minimal polynomial, therefore they are all separable, thus all in K_0. Therefore we know that K_0 is the splitting field for all minimal polynomials of $\alpha \in K_0$, thus it's normal. Then we know that K/k factors to a Galois extension and a purely inseparable extension.

Definition 6.16. Let k be a field, we say it's **perfect** if $k^p = k$ when $\mathrm{char}k = p > 0$ or when $\mathrm{char}k = 0$.

Corollary 6.17. If k is perfect, then every algebraic extension of k is separable and every algebraic extension is perfect.

Proof. Let's still focus on $\mathrm{char}k = p > 0$ since all the assertions is trivial for a characteristic 0 field.

Let K/k be an algebraic extension, we want to prove that if $\alpha \in K$, then it's separable over k. Consider the extension $k(\alpha)/k$, we know that it's contained in a normal finite extension, i.e. $k \subset k(\alpha) \subset k'$. Then we know that this extension decomposes into a purely inseparable extension $(k')^G$ followed by a separable extension. Since k is perfect, we know that for any $\alpha \in (k')^G$ there is an n such that $\alpha^{p^n} \in k$, however we can assume that $\alpha^{p^n} = \beta^{p^n}$ for some $\beta \in k$. Therefore $(\alpha - \beta)^{p^n} = 0$, therefore $\alpha - \beta = 0$, thus $\alpha = \beta$, therefore $K^G = k$, therefore we know that k' is separable over k, so is $k(\alpha)$.

Notice that perfect is equivalent to nonontrivial purely inseparable extensions. If $k^a \neq k$, then there is some $\alpha \in k$ such that $x^p - \alpha$ has no roots in k, therefore we consider the root to be β in k^a, then consider $k(\beta)/k$, since β is purely inseparable over k and not in k, $k(\beta)/k$ is a nontrivial purely inseparable extension. This is equivalent to the fact that every algebraic extension is separable.

Consider $k \subset F \subset E$, where E is an algebraic extension of F. Since k is perfect, E/k is separable, thus E/F is separable, therefore F is perfect. □

References