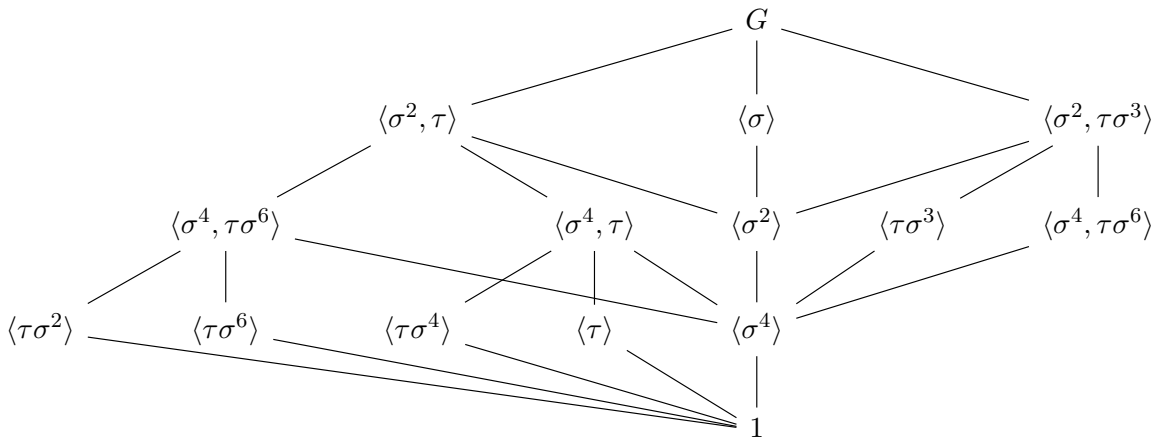
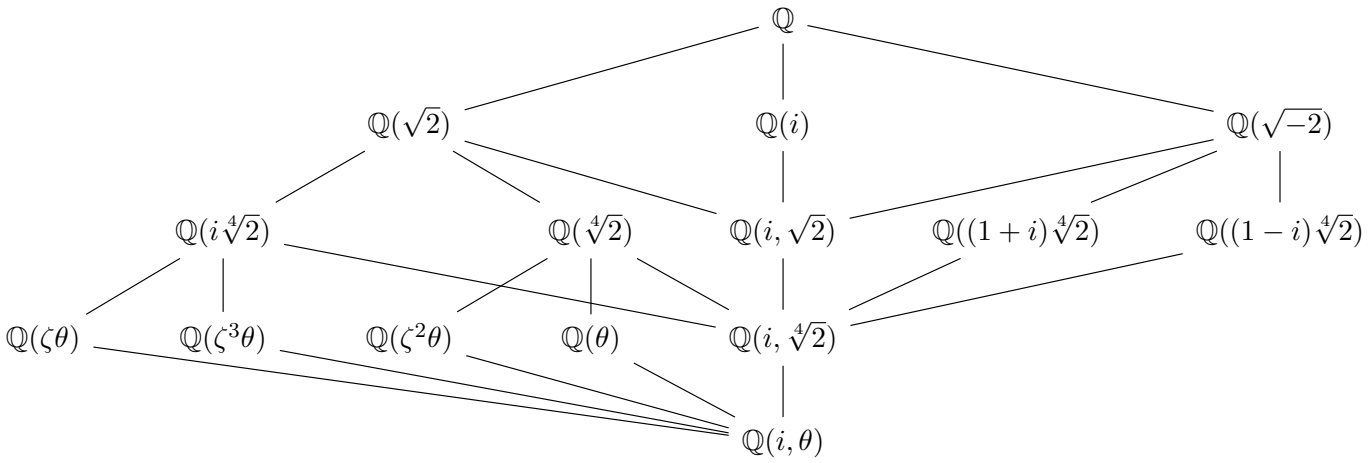
Field Extensions and Galois Theory

Tianyi





Abstract

Cover: The first lattice diagram shows the subgroup of the Galois group of the extension $\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q})$. The second lattice shows that intermediate extensions of the field extension $\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}$. The Fundamental Theorem of Galois Theory says that there is a bijective correspondence between these two lattice diagrams. More specifically, given a Galois extension K/F, there is a bijective correspondence between the subgroups of the Galois group $\mathrm{Gal}(K/F)$ and the intermediate extensions of K/F. This result is extremely elegant, and is perhaps one of the most important mathematical discoveries in the history of modern algebra. Galois ultimately proved the insolvability of the quintic and polynomial of higher degrees with the help of this observation. Galois' work was the key motivation of the development of modern algebra.

This notes covers the material of basic field theory and Galois theory, which is essentially a class notes for MATH 111C at UCSB. The offical textbook, and also the reference of this notes, is Dummit and Foote, Abstract Algebra, 3ed. Professor also posts lecture notes on the website, so some proofs are omitted in this notes, and we refer the readers to the lecture notes or the textbook.

Contents

1 Introduction

The main objects of interest in this note are fields and fields extensions. We first quickly recall some of the basic definitions and key results.

To start with, A field F is a commutative ring with $1 \neq 0$ in which every nonzero element has a multiplicative inverse. Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Or more formally,

Definition 1.1 (Field)**.** A field is a set F with two binary operations $+, \times$ satisfying

1. $(F, +)$ is an abelian group;
2. $(F \setminus \{0\}, \times)$ is an abelian group;
3. The distribution law holds. We have $(a + b) \times c = a \times c + b \times c$ for all $a, b, c \in F$.

Usually we will denote $F \setminus \{0\}$ by $F^\times$, called the units of F.

A subset S of a field F is called a subfield if it is a subring that is closed under taking multiplicative inverses.

Next, we define maps between fields.

Definition 1.2. Let F, K be fields. A map $\varphi : F \to K$ is a field homomorphism if it is a ring homomorphism. A bijective field homomorphism is called an isomorphism.

Proposition 1.3. Let F, K be fields. If $\varphi : F \to K$ is a nonzero field homomorphism, then φ is injective.

Proof. $\ker \varphi$ is an ideal of F. The only ideals in a field are $\{0\}$ and F. □

Hence we often call a nonzero field homomorphism a field embedding.

Definition 1.4 (Characteristic)**.** Let F be a field of 1_F being its identity. One can check that the map $\varphi : \mathbb{Z} \to F$ defined by

$$\varphi(n) = n \cdot 1_F := \begin{cases} 0 & n = 0 \\ \underbrace{1_F + \cdots + 1_F}_{n \text{ times}} & n \geq 1 \\ \underbrace{1_F + \cdots + 1_F}_{-n \text{ times}} & n \leq -1 \end{cases}$$

is a ring homomorphism. The characteristic of the field F, denoted by $\mathrm{ch}(F)$, is the non-negative integer that generates $\ker \varphi$.

Proposition 1.5. Let F be a field. Then either $\mathrm{ch}(F) = 0$ or $\mathrm{ch}(F) = p$ where p is a prime number.

Proof. Since $\mathbb{Z}/\ker \varphi \cong \mathrm{im}\, \varphi$ is a subring of F containing 1_F, it is an integral domain. Hence $\ker \varphi$ is a prime ideal of $\mathbb{Z}$, which is either 0 or generated by a prime number. □

Remark 1.6. If $\mathrm{ch}(F) = 0$, then it means that $1_F + \cdots + 1_F$ is never zero no matter how many times you add the identity to itself. Then if we identify $\mathbb{Z}$ with its isomorphic image in $\operatorname{im}\varphi$, we see that F contains a copy of $\mathbb{Z}$, hence also a copy of $\mathbb{Q}$.

If $\mathrm{ch}(F) = p$, then $p \cdot 1_F = 1_F + \cdots + 1_F = 0$ if you add identify to itself for p times. Then F contains a copy of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Definition 1.7. The prime subfield of a field F is the smallest subfield of F containing 1_F. From the remark above, we see that

$$\text{prime subfield of } F \cong \begin{cases} \mathbb{Q} & \mathrm{ch}(F) = 0 \\ \mathbb{F}_p & \mathrm{ch}(F) = p. \end{cases}$$

Example 1.8 (Frobenius Endomorphism)**.** Let $\mathrm{ch}(F) = p$. Then the map

$$\begin{aligned} \Phi : F &\longrightarrow F \\ a &\longmapsto a^p \end{aligned}$$

is a field homomorphism, called Frobenius endomorphism of F. First, it is clear that ψ preserves multiplication. That is, $\Phi(ab) = \Phi(a)\Phi(b)$. Now we show that $\Phi(a+b) = \Phi(a) + \Phi(b)$.

Let $a, b \in F$, we use the binomial expansion:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Now, for all $1 \le j \le p-1$, the binomial coefficient has the property

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} \qquad p | p! \quad \text{but} \quad p \not| j!(p-j)!$$

And since $\mathrm{ch}(F) = p$, we lnow that $p | \binom{p}{j}$. Hence all the term besides a^p and b^p are zero in the expansion above. This shows that

$$\Phi(a+b) = (a+b)^p = a^p + b^p = \Phi(a) + \Phi(b).$$

By induction, one can also see that the map

$$\begin{aligned} \Phi_n : F &\longrightarrow F \\ a &\longmapsto a^{p^n} \end{aligned}$$

is a field homomorphism for all integer $n \ge 1$.

Now we come to the key subject to this section.

Definition 1.9 (Field Extension)**.** Let F be a field. A field K containing F is called a field extension of F or an extension of F. We use the notation K/F or

$$\begin{array}{c} K \\ | \\ F \end{array}$$

to indicate that K is a field extension of F. The field F is sometimes called the base field.

Example 1.10. Every field of characteristic 0 is an extension of $\mathbb{Q}$. And every field of characteristic p is an extension of $\mathbb{F}_p$.

Let K/F be a field extension. Then K can be viewed as an F-vector space. To see this, all we need is to be able to add "vectors" in K (easy since K is equipped with an addition itself), and define a scalar multiplication

$$\bullet : F \times K \to K$$

which is also easy since $F \subseteq K$ and there is already a natural multiplication defined on K. Hence this gives rise to the following definition.

Definition 1.11 (Degree)**.** Let K/F be an extension. Then the degree of the extension K/F is the dimension of K as a vector space over F, denoted by

$$[K : F] = \dim_F K.$$

Example 1.12. Consider $\mathbb{C}/\mathbb{R}$. Clearly $[\mathbb{C} : \mathbb{R}] = 2$ since $1, i$ is a basis of $\mathbb{C}$ over $\mathbb{R}$.

Often, we are interested in polynomial ring $F[x]$ given that F is a field. Let $p(x) \in F[x]$ be an irreducible polynomial. Then the ideal generated by this polynomial $(p(x))$ is maximal since $F[x]$ is a PID. Hence $F[x]/(p(x))$ is a field. Then we have the following result.

Theorem 1.13. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Then:*

1. *$K = F[x]/(p(x))$ is a field extension of F;*
2. *$\theta = \bar{x} \in K$ is a root of $p(x)$ in K;*
3. *$[K : F] = \deg p(x)$. Let $n = \deg p(x)$, then $1, \theta, \cdots, \theta^{n-1}$ is a basis of K viewed as an F-vector space.*

Proof. (1) is already proved above. Note that F (its equivalence class, which we identify with F) is contained in K since $p(x)$ is nonconstant (irreducible elements are nonzero and nonunit). To prove (2), if we identify F with its isomorphic copy in K, as stated by (1), then

$$p(\theta) = p(\bar{x}) = p(\bar{x}) = 0.$$

To prove (3), notice that $F[x]$ is an Euclidean domain. So for every $f(x) \in F[x]$, we have $f(x) = p(x)q(x)+r(x)$ with $\deg r(x) < \deg p(x) = n$ or $r(x) = 0$. Hence K consists of the set of polynomials with degree at most $n-1$. which are F-linear combinations of $1, \theta, \cdots, \theta^{n-1}$.

Finally if $b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$, where $b_j \in F$, then $p(x)|b_0 + b_1x + \cdots + b_{n-1}x^{n-1} = 0$. But $\deg(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) < \deg p(x) = n$. Hence $b_j = 0$ for all j. Thus $1, \theta, \cdots, \theta^{n-1}$ are linearly independent. This proves (3). □

Remark 1.14. This is an important example of field extension. Before, we have $p(x) \in F[x]$, which is irreducible, thus has no roots in F. But then we can extend F to a larger field K in which $p(x)$ has a root. Then we can factor $f(x) = s(x)t(x)$, for $s(x), t(x) \in K[x]$, where $s(x)$ is a product of linear factors and $t(x)$ is irreducible in $K[x]$, and then we repeat this process, eventually we will get a field in which $p(x)$ becomes a product of linear factors.

Definition 1.15. Let K/F be an extension. Let $S \subseteq K$ be a collection of elements in K (which need not to be in F). Then the field generated by S over F, denoted by $F(S)$, is the smallest field containing both F and the elements S.

If $S = \{\alpha\}$ consists of only one element $\alpha \in K$, then we write $F(\alpha)$ instead of $F(\{\alpha\})$.

Theorem 1.16. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Suppose K/F is an extension with $\alpha \in K$ is a root of the polynomial $p(x)$ (i.e. $p(\alpha) = 0$). Then*

$$F(\alpha) \cong F[x]/(p(x)).$$

Proof. Consider the field homomorphism

$$\begin{aligned} \varphi : F[x] &\longrightarrow F(\alpha) \\ a(x) &\longmapsto a(\alpha). \end{aligned}$$

We know that $(p(x)) \subseteq \ker\varphi \subseteq F[x]$. But since $p(x)$ is irreducible and $F[x]$ is a PID, $(p(x))$ is maximal. Since φ is not the zero map, we have $\ker\varphi = (p(x))$. Also, we know that $\operatorname{im}\varphi$ contains both F and α, hence $\operatorname{im}\varphi = F(\alpha)$. Then apply the first isomorphism theorem and we are done. □

Corollary 1.17. *Assume that* $\deg p(x) = n$. *Then we see that from Theorem 1.13 and Theorem 1.16 we have*

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_j \in F\}.$$

We conclude this section with one last theorem.

Theorem 1.18. *Let $\varphi : F \to F'$ be an isomorphism of fields. Then φ induces a natural isomorphism $\varphi : F[x] \to F'[x]$ by $\varphi(a_0 + \cdots + a_n x^n) = \varphi(a_0) + \cdots + \varphi(a_n)x^n \in F'[x]$. Let $p(x) \in F[x]$ be irreducible and $p'(x) = \varphi(p(x)) \in F'[x]$ be the corresponding irreducible polynomial in $F'[x]$. Let α be a root of $p(x)$ and β be a root of $p'(x)$. Then there exists an isomorphism*

$$\sigma : F(\alpha) \to F'(\beta)$$

such that $\sigma|_F = \varphi$.

Proof. First, notice that $p'(x)$ is irreducible. Otherwise if $p'(x) = s'(x)t'(x)$, then $p(x) = s(x)t(x)$. Since φ maps the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$, then taking the quotient, and by Theorem 1.16, we have the following chain of isomorphisms:

$$F(\alpha) \xrightarrow{\cong} F[x]/(p(x)) \xrightarrow{\cong} F'[x]/(p'(x)) \xrightarrow{\cong} F'(\beta)$$

This is the desired σ. And clearly $\sigma|_F = \varphi$. □

Remark 1.19. The theorem above can also be reprensented by the following diagram:

$$\begin{array}{ccc} F(\alpha) & \xrightarrow[\sigma]{} & F'(\beta) \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

We will come back to this theorem later when we cover Galois extension.

2 Finite Extensions

Finite extension is the most standard form of extension we can imagine. Let us now study such extensions in detail.

Definition 2.1. The extension K/F is finite if $[K : F] < \infty$.

Easy enough. This definition allows us to convert finite extension problems to problems related to finite dimension vector spaces. For now, one of the most useful properties of finite extension is that the property of being finite is transitive.

Theorem 2.2 (Transitivity of Finite Extension)**.** *Let $F \subseteq K \subseteq L$ be fields. Then $[L : F]$ is finite if and only if $[L : K]$ and $[K : F]$ are both finite. And when they are finite,*

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

Proof. We first show that $[L : F] < \infty$ implies $[L : K]$ and $[K : F]$ are both finite. Let $\alpha_1, \cdots, \alpha_m \in K$ be linearly independent over F and $\beta_1, \cdots, \beta_n$ be linearly independent over F. Then if for $c_{ij} \in F$, we have

$$\sum_{ij} c_{ij}\alpha_j\beta_j = 0 \Rightarrow \sum_{j=1}^{n}\left(\sum_{i=1}^{m} c_{ij}\alpha_i\right)\beta_j = 0 \Rightarrow \sum_{i=1}^{m} c_{ij}\alpha_i = 0 \Rightarrow c_{ij} = 0$$

for all i, j. Hence $\alpha_i\beta_j$ are linearly independent over F. Therefore if $[L : K] \geq n$ and $[K : F] \geq m$, we have $[L : F] \geq nm$.

Conversely, we it suffices to prove the equality above directly. Let $\alpha_1, \cdots, \alpha_m \in K$ be a basis of K over F and $\beta_1, \cdots, \beta_n$ be a basis of L over K. Then it is easy to show that $\alpha_i\beta_j$ span L over F. Since they are linearly independent by the first part, $\alpha_i\beta_j$ is a basis of L over F. This concludes the proof. □

Remark 2.3. Actually, we can generalize this theorem. Let $F \subseteq K \subseteq L$ be fields. Then the degree is multiplicative: $[L : K] = [L : K][K : F]$. If one side of the equation is infinite, the other side is also infinite. So this relation also applies to infinite extensions.

3 Algebraic Extensions

Algebraic extension is the first of many important field extensions we will encounter. From now on, most of the proofs will be directly omitted. Otherwise, we will only provide some short sketch of how to proceed.

Definition 3.1. Let K/F be an extension. The element $\alpha \in K$ is said to be algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, we say it is transcendental over F. The extension K/F is said to be algebraic if every element of K is algebraic over F.

Proposition 3.2. Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ having α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)|f(x)$.

Proof. Let $m_{\alpha,F}(x)$ be the polynomial of minimal degree having α as a root in $F[x]$. By multiplication of a constant in $F^\times$ we may assume $m_{\alpha,F}(x)$ is monic. If $m_{\alpha,F}(x)$ is reducible then it would contradict the minimality of $m_{\alpha,F}(x)$. Hence $m_{\alpha,F}(x)$ is monic irreducible.

By the Euclidean algorithm, let $f(x) \in F[x]$ contains a root α. Then $f(x) = q(x)m_{\alpha,F}(x)+r(x)$ with $\deg r(x) < \deg m_{\alpha,F}(x)$ or $r(x) = 0$. By $f(\alpha) = r(\alpha) = 0$ and the minimality of $m_{\alpha,F}(x)$, we have $f(x) = q(x)m_{\alpha,F}(x)$, hence $f(x)|m_{\alpha,F}(x)$. The other direction is obvious. □

Corollary 3.3. *If L/F is a field extension and α is algebraic over both fields L and F, then $m_{\alpha,L}(x)|m_{\alpha,F}(x)$ in $L[x]$.*

Proposition 3.4. Let α be algebraic over F. Then

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$$

and in particular,

$$[F(\alpha) : F] = \deg m_{\alpha,F}(x).$$

Proof. Immediate from Theorem 1.16. □

Theorem 3.5. *An element α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.*

Proof. The "if" part is proven above. For the "only if" part, suppose $[F(\alpha) : F] = n < \infty$, then the $n + 1$ elements $1, \alpha, \cdots, \alpha^n$ of $F(\alpha)$ are F-linearly dependent. Hence there exists $b_j \in F$ such that

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$$

where b_j are not all zero. Then $f(x) = b_0 + \cdots + b_nx^n \in F[x]$ contains α as a root. Hence α is algebraic. □

Proposition 3.6. Finite extensions are algebraic.

Proof. Let K/F be a finite extension. Then consider the F-vector subspaces $F(\alpha)$ of K. We have $[F(\alpha) : F] \leq [K : F] < \infty$. Hence K/F is algebraic by the previous theorem. □

We already have some criteria to determine whether an element or a field extension is algebraic (the previous theorem and proposition). Now we give a necessary and sufficient condition to determine whether a field extension is finite/algebraic. To to this, we first need some preparation work on fields generated by subsets of elements.

Lemma 3.7. *The field generated over F by α, β is the field generated by β over $F(\alpha)$. In notation,*

$$F(\alpha, \beta) = F(\alpha)(\beta).$$

Proof. The inclusions in both directions are easy by definition. □

Form this lemma, we have that

$$K = F(\alpha_1, \cdots, \alpha_k) = F(\alpha_1, \cdots, \alpha_{k-1})(\alpha_k).$$

Now, suppose that $\alpha_1, \cdots, \alpha_k$ are algebraic elements over F. What can we say about $[K : F]$? Actually, by using Theorem 2.2 and the remarking following it, we notice that we have a chain of inclusion

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots F(\alpha_1, \cdots, \alpha_{j-1}) \subseteq F(\alpha_1, \cdots, \alpha_j) \subseteq \cdots \subseteq F(\alpha_1, \cdots, \alpha_{k-1}) \subseteq K.$$

Therefore

$$\begin{aligned}
[K : F] &= \prod_{j=1}^{k} [F(\alpha_1, \cdots, \alpha_{j-1})(\alpha_j) : F(\alpha_1, \cdots, \alpha_{j-1})] \\
&= \prod_{j=1}^{k} \deg m_{\alpha_j, F(\alpha_1, \cdots, \alpha_{j-1})}(x) \\
&\leq \prod_{j=1}^{k} \deg m_{\alpha_j, F}(x) \\
&= \prod_{j=1}^{k} [F(\alpha_j) : F].
\end{aligned}$$

The third inequality follows from the fact that $m_{\alpha_j, F(\alpha_1, \cdots, \alpha_{j-1})}(x) | m_{\alpha_j, F}(x)$ in $F(\alpha_1, \cdots, \alpha_{j-1})$, hence $\deg m_{\alpha_j, F(\alpha_1, \cdots, \alpha_{j-1})}(x) \leq \deg m_{\alpha_j, F}(x)$. Now, we are ready to present the following theorem, which gives sufficient and necessary conditions for an extension K/F to be finite or algebraic.

Theorem 3.8. *Let K/F be a field extension.*

1. *K/F is finite if and only if there exists a finite algebraic generating set: i.e. There exists a finite subset $S = \{\alpha_1, \cdots, \alpha_n\} \subseteq K$ such that each α_j is algebraic over F, and $K = F(S)$.*

2. *K/F is algebraic if and only if there exists an algebraic generating set (not necessarily finite): i.e. There exists a subset $S \subseteq K$ such that every element in S is algebraic over F and $K = F(S)$.*

Proof. For (1): Suppose K/F finite. Then if $[K : F] = n$, there exists $\alpha_1, \cdots, \alpha_n \in K$ such that $K = F\alpha_1 + \cdots + F\alpha_n$. Then $K = F(\alpha_1, \cdots, \alpha_n)$. Since K/F finite, K/F is algebraic by the previous proposition. Then $\alpha_j \in K$ is algebraic over F for all j. Conversely, suppose $K = F(\alpha_1, \cdots, \alpha_n)$ where each α_j is algebraic over F, then we have

$$[K : F] = [F(\alpha_1, \cdots, \alpha_n) : F] \leq \prod_{j=1}^{n} [F(\alpha_j) : F] = \prod_{j=1}^{n} \deg m_{\alpha_j, F}(x) < \infty.$$

For (2), take $S = K$ and we have proven the "if" part. Conversely, suppose $\alpha \in K = F(S)$, then it is generated by some element in S. i.e. $\alpha \in F(\alpha_1, \cdots, \alpha_n)$ for $\alpha_1, \cdots, \alpha_n \in S$. Then (1) implies that $F(\alpha_1, \cdots, \alpha_n)/F$ is finite, hence algebraic. Thus α is algebraic over F. □

We conclude the discussion of algebraic extension by presenting one last theorem. It is natural to ask whether we have a result similar to Theorem 2.2 for being algebraic. That is, is being algebraic transitive? The answer is yes.

Theorem 3.9. *Let $F \subseteq K \subseteq L$ be fields. Then K/F and L/K are both algebraic if and only if L/F is algebraic.*

Proof. Suppose K/F and L/K are both algebraic. We show that L/F is algebraic by showing every $\alpha \in L$ is algebraic over F. Since L/K is algebraic, there exists $a_0, \cdots, a_{n-1} \in K$ such that

$$\alpha^n + a_{n-1}\alpha_{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Hence α is algebraic over $F(a_0, \cdots, a_{n-1})$. Then by Theorem 3.5, we know that

$$[F(\alpha, a_0, \cdots, a_{n-1}) : F(a_0, \cdots, a_{n-1})] < \infty.$$

Since K/F is algebraic, we know $a_0, \cdots, a_{n-1}$ are algebraic over F. Then by Theorem 3.8 we know that $[F(a_0, \cdots, a_{n-1}) : F] < \infty$. Then

$$[F(\alpha, a_0, \cdots, a_{n-1}) : F] = [F(a_0, \cdots, a_{n-1})(\alpha) : F(a_0, \cdots, a_{n-1})][F(a_0, \cdots, a_{n-1}) : F] < \infty.$$

Then $F(\alpha, a_0, \cdots, a_{n-1})/F$ is finite, hence algebraic. Thus α is algebraic over F.

Conversely, suppose L/F is algebraic. Then for all $\alpha \in K$, $\alpha \in L$. Hence α is algebraic over F. Thus K/F algebraic. Next, for all $\alpha \in L$, since it is algebraic over F, there exists $f(x) \in F[x] \subseteq K[x]$ such that $f(\alpha) = 0$. Hence L/K algebraic. □

4 Splitting Fields

Given a polynomial $f(x) \in F[x]$, it may not have a root in F. Even if it does, it may not have all the roots in F. If $f(x)$ has all its roots in a extension field K/F, then it will split completely into linear factors, by that we mean

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

for some $a \in F$ and $\alpha_1, \cdots, \alpha_n \in K$. Notice that these roots $\alpha_1, \cdots, \alpha_n$ need not to be distinct. Nevertheless, it is still worth investigating that given a polynomial $f(x) \in F[x]$, in what extension K/F does it split completely? And what is the smallest such extension? This gives rise to the definition of splitting fields.

Definition 4.1. Let $f(x) \in F[x]$. A field extension K/F is called a splitting field of $f(x)$ if

- $f(x)$ splits completely in $K[x]$ (or splits completely over K);
- If $F \subseteq E \subseteq F$ and $f(x)$ splits completely over E, then $E = K$.

Notice that the second criterion requires a splitting field to be the smallest field in which $f(x)$ splits completely. Then one would suspect that the field generated by all the roots of $f(x)$ satisfies these two requirements and is a splitting field of $f(x)$. This is indeed correct.

Proposition 4.2. Let $f(x) \in F[x]$ and K/F is a field extension such that $f(x)$ splits completely in $K[x]$, i.e. $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ for some $a, \alpha_1, \cdots, \alpha_n \in K$. Then $F(\alpha_1, \cdots, \alpha_n)$ is a splitting field for $f(x)$.

Proof. Clearly $f(x)$ splits completely in $F(\alpha_1, \cdots, \alpha_n)$ by assumption. If $F \subseteq E \subseteq F(\alpha_1, \cdots, \alpha_n)$ and $f(x)$ splits completely in $E[x]$, say

$$f(x) = b(x - \beta_1) \cdots (x - \beta_n)$$

for $b, \beta_1, \cdots, \beta_n \in E$. Then in the UFD $F(\alpha_1, \cdots, \alpha_n)[x]$, we have

$$a(x - \alpha_1) \cdots (x - \alpha_n) = b(x - \beta_1) \cdots (x - \beta_n).$$

Then $\beta_j = \alpha_j$ up to reordering. Hence $E = F(\alpha_1, \cdots, \alpha_n)$. □

Actually, this is the most important theorem about splitting field that we should know. The following theorem gaurantees that splitting field exists and is a finite extension.

Theorem 4.3. *For any field F and $f(x) \in F[x]$, a splitting field of $f(x)$ exists and is a finite extension of F.*

The proof uses induction on the degree of $f(x)$. We will omit the proof and refer to the lecture notes of Professor Liu on Apr 8, Theorem 4. We now turn our attention to several interesting and important examples.

Example 4.4. Consider a splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. In order to find a splitting field, we first find the root of this polynomial. Over $\mathbb{C}$, the roots are given by

$$\theta_1 = \sqrt[3]{2} \qquad \theta_2 = \sqrt[3]{2}e^{2\pi i/3} \qquad \theta_3 = \sqrt[3]{2}e^{4\pi i/3}.$$

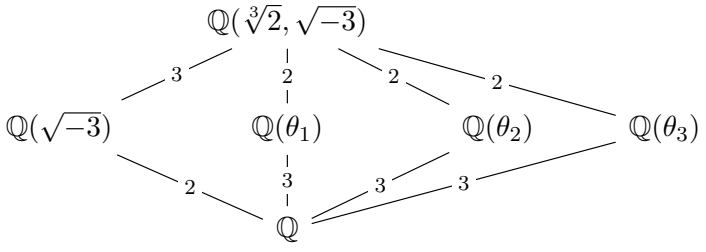
Hence our splitting field is $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$. Some simple work will show that $\mathbb{Q}(\theta_1, \theta_2, \theta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. It is not hard to show that

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

This is because

$$m_{\sqrt{-3}, \mathbb{Q}(\sqrt[3]{2})}(x) = x^2 + 3 \qquad m_{\sqrt[3]{2}, \mathbb{Q}}(x) = x^3 - 2.$$

Then $\mathbb{Q}(\theta_j)$ for $j = 1, 2, 3$ are all nontrivial extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. In fact, we can even calcualte all the nontrivial extensions and their degrees after we learn Galois theory, which is given by the following diagram:



Example 4.5. We consider a splitting field of $x^n - 1 \in \mathbb{Q}[x]$. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ be the nth roots of unity. Then ζ_n^j, where $j = 0, 1, \cdots, n-1$ are different roots of $x^n - 1$. Hence

$$\mathbb{Q}(\zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}) = \mathbb{Q}(\zeta_n)$$

is a splitting field of $x^n - 1$ over $\mathbb{Q}$. Then we ask, what is the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$? If $n = p$ is a prime number, then the cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is an irreducible polynomial in $\mathbb{Q}[x]$ by Eisenstein's criterion. And it is easy to see that $\Phi_p(\zeta_p) = 0$. Hence $\Phi_p(x) = m_{\zeta_p,\mathbb{Q}}(x)$. And we conclude that

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|.$$

Later, we will show that for general integer n, we have

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n),$$

where φ is Euler's Phi function.

Finally, we give one more result about the splitting field. We have been keep using the term "a splitting field", which may raise question about the uniqueness of splitting fields. The next theorem says that all splitting fields of $f(x)$ are isomorphic. In fact, it is even more general.

Theorem 4.6. *Let $\varphi : F_1 \to F_2$ be a field isomorphism. φ induces a natural isomorphism $\varphi : F_1[x] \to F_2[x]$ by*

$$\varphi : f_1(x) = a_n x^n + \cdots + a_0 \mapsto f_2(x) = \varphi(a_n)x^n + \cdots + \varphi(a_0).$$

Let E_1 be a splitting field of $f_1(x) \in F_1[x]$ and E_2 be a splitting field of $f_2(x) \in F_2[x]$. Then φ extends to an isomorphism $\sigma : E_1 \to E_2$ (i.e. $\sigma|_{F_1} = \varphi$) such that the following diagram commutes.

$$\begin{array}{ccc} F_1 & \xrightarrow{\varphi} & F_2 \\ \downarrow & & \downarrow \\ E_1 & \xrightarrow[\sigma]{} & E_2 \end{array}$$

Proof. The proof uses induction on $\deg f_1(x)$. Here we only sketch the basic idea of the proof, and refer the reader to lecture notes (April 13, Theorem 1) for details.

The base case: When $\deg f_1(x) = 1$, we have $E_1 = F_1$, $E_2 = F_2$, and we can simply take $\sigma = \varphi$.

Now, suppose the theorem is true for any F_1, F_2 with isomorphism $\varphi : F_1 \to F_2$, and $f_1(x) \in F_1[x]$ with $\deg f_1(x) \leq n - 1$.

By Theorem 1.18 and the remarking following it, let α be a root of $f_1(x)$ and β be a root of $f_2(x)$. Then φ extends to an isomorphism $\tau : F_1(\alpha) \to F_2(\beta)$ such that the following diagram commutes:

$$\begin{array}{ccc} F_1 & \xrightarrow{\varphi} & F_2 \\ \downarrow & & \downarrow \\ F_1(\alpha) & \xrightarrow[\tau]{} & F_2(\beta) \end{array}$$

Next, consider the extensions $E_1/F_1(\alpha)$ and $E_2/F_2(\beta)$. Write $f_1(x) = (x - \alpha)g_1(x)$ and $f_2(x) = (x - \beta)g_2(x)$, where $g_1 \in F_1(\alpha)[x]$ and $g_2 \in F_2(\beta)[x]$. Then one can check that

- E_1 is a splitting field of $g_1(x)$, and E_2 is a splitting field of $g_2(x)$.
- $g_2(x)$ is the polynomial obtained by applying τ to the coefficients of $g_1(x)$.
- $\deg g_1(x) = n - 1$.

Then we can apply induction hypothesis to $\tau : F_1(\alpha) \to F_2(\beta)$, $g_1(x), g_2(x)$ and E_1, E_2. Then τ extends to an isomorphism $\sigma : E_1 \to E_2$ such that the following diagram commutes:

$$\begin{array}{ccc} F_1 & \xrightarrow{\varphi} & F_2 \\ \downarrow & & \downarrow \\ F_1(\alpha) & \xrightarrow[\tau]{} & F_2(\beta) \\ \downarrow & & \downarrow \\ E_1 & \xrightarrow{\sigma} & E_2 \end{array}$$

And clearly $\sigma|_{F_1} = \varphi$. This proves the theorem. □

Remark 4.7. In the special case where $F_1 = F_2 = F$, and $\varphi = \mathrm{id}_F$, by the following theorem, we have that all the splitting fields of $f_1(x) = f(x) \in F[x]$ are isomorphic.

There is a nice result, which we will state without proving:

Proposition 4.8. The splitting field K of a polynomial of degree n over a field F is of degree at most $n!$. That is, $[K : F] \leq n!$.

For the proof, see the end of the lecture notes on Apr 13, proposition 2. We will end the discussion of splitting fields here.

5 Algebraically Closed Fields and Algebraic Closure

Now we consider another kind of extension that generalizes the notion of a splitting field. In the case of splitting field, we have one polynomial $f(x) \in F[x]$, and the splitting field of $f(x)$ is the extension of F containing all the roots of $f(x)$. Generalizing one step further, we ask, what is the field extension of F that contains all the roots of all polynomials in $F[x]$? This gives the definition of algebraic closure of F.

Definition 5.1 (Algebraic Closure)**.** Let F be a field. A field Ω containing F is called an algebraic closure of F if Ω/F is algebraic and every non-constant polynomial in $F[x]$ splits completely over Ω.

To study the algebraic closure of a field F, we need some preparation. In particular, we need to first study a family of fields that shares the property of being "algebraically closed".

Definition 5.2 (Algebraically Closed Fields)**.** Let Ω be a field. We say Ω is algebraically closed if every non-constant polynomial in $\Omega[x]$ has a root in Ω.

We give a set of equivalence conditions to determine whether a field is algebraically closed.

Proposition 5.3. Let Ω be a field. The following conditions are equivalent.

1. Every non-constant polynomial in $\Omega[x]$ splits completely over Ω;
2. Ω is algebraically closed (i.e. every non-constant polynomial in $\Omega[x]$ has a root in Ω);
3. The irreducible polynomials in $\Omega[x]$ are those of degree 1;
4. If K/Ω is a finite extension, then $K = \Omega$.

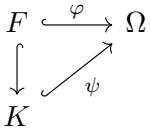
Proof. (1) $\Rightarrow$ (2) is obvious.

(2) $\Rightarrow$ (3): Let $f(x) \in \Omega[x]$ be an irreducible polynomial. Then if $\alpha \in \Omega$ is a root of $f(x)$, by the division algorithm we have $f(x) = (x - \alpha)g(x)$ where $g(x) \in \Omega[x]$. Since $f(x)$ is irreducible, $g(x) \in (\Omega[x])^\times = \Omega^\times$ must be constant. Hence $\deg f(x) = 1$.

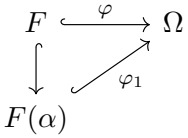
(3) $\Rightarrow$ (4): Let K/Ω be a finite extension. Then for all $\alpha \in K$, by assumption $m_{\alpha,\Omega}(x)$ is a monic irreducible polynomial in $\Omega[x]$. Hence $\deg m_{\alpha,\Omega}(x) = 1$ and $m_{\alpha,\Omega}(x) = x - \alpha$. Thus $\alpha \in \Omega$.

(4) $\Rightarrow$ (1): Let $f(x) \in \Omega[x]$ be a non-constant polynomial. Theorem 4.3 says there exists a splitting field K of $f(x)$ over Ω and K/Ω is finite. Then by assumption $K = \Omega$ and $f(x)$ splits completely over Ω. □

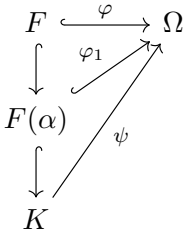
Proposition 5.4. Let K/F be an algebraic extension. Let Ω be an algebraically closed field. Then every field embedding $\varphi : F \to \Omega$ extends to K, i.e. there exists a field embedding $\psi : K \to \Omega$ such that the following diagram commutes.



Proof. We only sketch the proof here, and refer the reader to the end of the lecture notes on Apr 13. Assume $[K : F] < \infty$ first. Then we use induction on $[K : F]$. The base case $[K : F] = 1$ is easy. If $[K : F] > 1$, suppose that the statement holds for all integer less or equal to $n - 1$. Then take $\alpha \in K \setminus F$ and show there exists $\varphi_1 : F(\alpha) \to \Omega$ such that the following diagram commutes:



Then we have $[K : F(\alpha)] < [K : F]$. Apply induction hypothesis to $K/F(\alpha)$ and φ_1 shows that there exists $\psi : K \to \Omega$ extending φ_1. Then we have the follow diagram:



Then this completes the proof for the finite case. If $[K : F] = \infty$, we need to use Zorn's lemma. □

Proposition 5.5. Let Ω/F be an algebraic extension. Then Ω is an algebraic closure of F if and only if Ω is algebraically closed.

Proof. Suppose Ω is algebraically closed. Then by the equivalent considtions every nonconstant polynomial in $\Omega[x]$ splits completely over Ω. Then every nonconstant polynomial in $F[x]$ splits completely over Ω. Hence by definition, Ω is an algebraic closure of F.

Conversely, suppose Ω is an algebraic closure of F. We show that every nonconstant polynomial in $\Omega[x]$ splits completely over Ω. Given $f(x) \in \Omega[x]$, by Theorem 4.3, $f(x)$ has a splitting field Ω' and Ω'/Ω is finite. Hence Ω'/Ω is algebraic. Then both Ω'/Ω and Ω/F are algebraic implies that Ω'/F is algebraic (algebraic is transitive). Then given $\alpha \in \Omega'$, α is a root of some $g(x) \in F[x]$. Since Ω is the algebraic closure of F, $g(x)$ splits completely over Ω. Hence $\alpha \in \Omega$. This shows that $\Omega' = \Omega$ and $f(x)$ splits completely over Ω. □

Remark 5.6. The converse part of this proposition says that if K is algebraically closed, then itself is an algebraic closure of K. The if part of the proposition actually says the process of taking algebraic closure stops after one step: taking the algebraic closure of an algebraic closure does not give a larger field. Notationally:

$$\bar{\bar{F}} = \bar{F}.$$

Or we can simply summarize this as **algebraic closures are algebraically closed.**

Recall that when we were trying to find the splitting field of a polynomial $f(x) \in F[x]$. Then all we need is to find a field K in which $f(x)$ splits completely, and we take all the roots of $f(x)$ in K, say S, then $F(S)$ is the desired splitting field. The following proposition says that similar procedure can also be applied to finding the algebraic closure of F.

Proposition 5.7. Let Ω be an algebraically closed field containing F. And let

$$F' = \{\alpha \in \Omega |\ \alpha \text{ is algebraic over } F\}.$$

Then F' is an algebraic closure of F. Moreover, if $K \subseteq \Omega$ is an algebraic extension of F and

$$K' = \{\alpha \in \Omega |\ \alpha \text{ is algebraic over } K\},$$

then $K' = F'$.

Proof. It is easy to show that F' is a subfield of Ω [1] containing F. We directly verify the definition of algebraic closure. By its definition F'/F is algebraic. Let $f(x) \in F[x]$. Then since Ω is algebraically closed, we have

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n) \qquad a \in F^\times, \alpha_j \in \Omega.$$

Since α_js are clearly algebraic over F, by definition $\alpha_j \in F'$ for all j. Hence $f(x)$ splits completely over F'. Thus F' is the algebraic closure of F.

Next, clearly $F' \subseteq K'$. To show the converse inclusion, notice that $\alpha \in K'$ implies that α is algebraic over K. Hence $K(\alpha)/K$ is finite by Theorem 3.8, hence algebraic. Also since K/F is algebraic. Hence $K(\alpha)/F$ is algebraic, showing $\alpha \in F'$. This proves the claim. □

[1] Let K/F be a field extension and $E = \{\alpha \in K |\ \alpha \text{ algebraic over } F\}$, then E is a subfield of K. Since if we take $\alpha, \beta \in E$, we have $\alpha + \beta, -\alpha, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$. Since α, β is a finite algebraic generating set of this field, $F(\alpha, \beta)$ is finite and thus algebraic. Hence $F(\alpha, \beta) \subseteq E$.

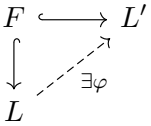
The next result ensures the existence of algebraic closure.

Proposition 5.8. Let F be a field, then F has an algebraic closure.

The proof uses Zorn's lemma and uses a very clever idea of Artin. For the proof we shall refer reader to Dummit and Foote, proposition 30 on page 544. The next result says that two algebraic closures of the same field is isomorphic.

Theorem 5.9. *If L and L' are both algebraic closures of F, then there exists a field isomorphism $\varphi : L \to L'$ such that $\varphi|_F = \mathrm{id}_F$.*

Proof. By definition of algebraic closure, we know L/F is algebraic and L' is algebraically closed. Then apply Proposition 5.4 and we know there exists a homomorphism $\varphi : L \to L'$ such that $\varphi|_F = \mathrm{id}_F$.



It remains to show that $\varphi(L) = L'$. Since L is an algebraic closure of F, it is algebraically closed. Then since $L \cong \varphi(L)$, we conclude that $\varphi(L)$ is also algebraically closed. For any $\alpha \in L'$, since α is algebraic over F, we know α is algebraic over $\varphi(L)$ since $F \subseteq \varphi(L)$. Then we have $[\varphi(L)(\alpha) : \varphi(L)] < \infty$. Then since $\varphi(L)$ is algebraically closed, by the equivalence condition (4) before, we know $\varphi(L)(\alpha) = \varphi(L)$. Thus $\alpha \in \varphi(L)$. This proves the theorem. □

Since any two algebraic closure of F is isomorphic, we usually do not make distinctions between them. We denote the algebraic closure of F as $\bar{F}$.

We end this section with one last proposition.

Proposition 5.10. If K/F is algebraic, then $\bar{K}$ is an algebraic closure of F.

Proof. Just verify the definition directly. Since $\bar{K}/K$ is algebraic and K/F is algebraic, we have $\bar{K}/F$ is algebraic. $\bar{K}$ is algebraically closed, so every nonconstan polynomial in $\bar{K}[x]$ (hence every nonconstant polynomial in $F[x]$) splits completely over $\bar{K}$. □

Remark 5.11. When K/F is algebraic and we need to use algebraic closures of K and F, we often take $\bar{F} = \bar{K}$.

6 Separable Extensions

When we were talking about splitting fields, we say a polynomial splits completely in a field K if

$$f(x) = a\,(x - \alpha_1) \cdots (x - \alpha_n)$$

for some $a \in F$ and $\alpha_1, \cdots, \alpha_n \in K$. However, we did not require the roots $\alpha_1, \cdots, \alpha_n$ to be distinct. There are some polynomials whose roots are not distinct (for example $x^2 + 2x + 1$). However, some polynomials have distinct roots (for example $x^2 - 2$). Thus we say a polynomial $f(x)$ is separable if it has no multiple roots (all roots are distinct). We first study this intrinsic property of polynomials, and then we generalize separability to field extensions.

Remark 6.1. There is no need to specify the field containing all the roots of $f(x)$. Since if $f(x)$ has distinct roots $\alpha_1, \cdots, \alpha_n$ a splitting field K, and we have $\alpha_1', \cdots, \alpha_n'$ are another set of roots of $f(x)$ in K', then since splitting fields are isomorphic, there exists a direct isomorphism $\varphi : K \to K'$. It is easy to check that if α_j is a root of $f(x)$, then $\varphi(\alpha_j)$ is also a root of $f(x)$. And φ maps distinct roots to distinct roots.

Definition 6.2 (Separable Extensions)**.** Let K/F be a field extension and $\alpha \in K$ be an algebraic element over F. Then α is separable over F if $m_{\alpha,F}(x)$ is separable. An algebraic extension K/F is separable if every element of K is separable over F.

We first ask, what criterion gaurantees a polynomial to be separable? To answer this, we define the derivative of a polynomial:

Definition 6.3. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$. Then define its derivative to be

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

This is exactly the same definition of derivative in analysis. However, since we are in a general field, the process of taking limit may not even be defined. So the best we can do is to associate each polynomial $f(x) \in F[x]$ to its derivative polynomial $f'(x) \in F[x]$. Then we have a criterion to determine whether a polynomial is separable:

Proposition 6.4. The following are true:

- α is a multiple root of $f(x) \in F[x]$ if and only if $f(\alpha) = f'(\alpha) = 0$.
- If $\gcd(f(x), f'(x)) = 1$, then $f(x) \in F[x]$ is separable.
- If $\mathrm{ch}(F) = 0$, then every irreducible polynomial in $F[x]$ is separable, and every algebraic extension of F is separable.

The proof is not hard. We refer to the lecture notes of April 15 (prop 6). Now that we have some criteria to determine the separability of polynomials, we turn our attention to separability of field extensions.

For the remaining of this section, our endeavor is to show the similarity between finite/algebraic extensions and separable extensions. Recall that the property of finite/algebraic are transitive, and an extension K/F is finite/algebraic if and only if there exists a finite algebraic/algebraic set S such that $K = F(S)$. Our attempt for the remaining of this section is the prove the following two analogous properties of separable extensions:

- Let K/F and L/K be algebraic extensions. Then L/F is separable if and only if K/F and L/K are separable.
- Let K/F be algebraic, then K/F is separable if and only if there exists a subset $S \subset K$ such that $K = F(S)$ and every element in S is separable over F.

Our first goal is to prove the claim that separability is transitive. However, to prove this, we need to do a lot of preparation which involves several propositions about F-embeddings.

Definition 6.5. Let K/F and L/F be field extensions. An F-embedding from K to L is a field embedding $\varphi : K \to L$ such that $\varphi|_F = \mathrm{id}_F$.

We denote the set of F-embeddings $\varphi : K \to L$ by $\mathrm{Emb}_F(K, L)$. The number of such embeddings will be denoted by $|\mathrm{Emb}_F(K, L)|$.

Proposition 6.6. Let $\alpha \in \bar{F}$. Then

1. $|\mathrm{Emb}_F(F(\alpha), \bar{F})|$ is equal to the number of roots of $m_{\alpha,F}(x)$ in $\bar{F}$.
2. $|\mathrm{Emb}_F(F(\alpha), \bar{F})| \leq [F(\alpha) : F]$, and the equality holds if and only if α is separable over F.

Proof. For (1), we consider the map

$$\begin{aligned} \mathrm{Emb}_F(F(\alpha), \bar{F}) &\longrightarrow \bar{F} \\ \varphi &\longmapsto \varphi(\alpha). \end{aligned} \tag{*}$$

We show that (*) is injective and the image of (*) is equal to the roots of $m_{\alpha,F}(x)$ in $\bar{F}$. For injectivity, notice that every elements in $F(\alpha)$ can be written as $c_n\alpha^n + \cdots + c_1\alpha + c_0$ for some $c_j \in F$. Then

$$\varphi : c_n\alpha^n + \cdots + c_1\alpha + c_0 \longmapsto c_n\varphi(\alpha)^n + \cdots + c_1\varphi(\alpha) + c_0.$$

Hence φ is completely determined by $\varphi(\alpha)$. i.e. if φ, φ' are in the source such that $\varphi(\alpha) = \varphi'(\alpha)$, then $\varphi = \varphi'$. This shows the injectivity of (*). Also, it is easy to verify that

$$m_{\alpha,F}(\varphi(\alpha)) = \varphi(m_{\alpha,F}(\alpha)) = 0.$$

Hence the image of (*) is a subset of all the roots of $m_{\alpha,F}(x)$ in $\bar{F}$. Now, we show the reverse inclusion. Let $\beta \in \bar{F}$ be another root of $m_{\alpha,F}(x)$. Then since $m_{\alpha,F}(\beta) = 0$ and $m_{\alpha,F}(x)$ is monic irreducible in $F[x]$, we conclude that

$$m_{\alpha,F}(x) = m_{\beta,F}(x).$$

There exists field isomorphisms $\sigma : F[x]/(m_{\alpha,F}(x)) \to F(\alpha)$, and $\tau : F[x]/(m_{\beta,F}(x)) \to F(\beta)$, i.e. $\tau : F[x]/(m_{\alpha,F}(x)) \to F(\beta)$. Let φ be the composition shown in the following commutative diagram:

$$\begin{array}{ccc} F[x]/(m_{\alpha,F}(x)) & \xrightarrow{\sigma} & F(\alpha) \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\varphi} \\ F(\beta) & \hookrightarrow & \bar{F} \end{array}$$

Recall what σ and τ do:

$$\begin{aligned} \sigma : F[x]/(m_{\alpha,F}(x)) &\longrightarrow F(\alpha) \\ a(\bar{x}) &\longmapsto a(\alpha) \\ \tau : F[x]/(m_{\beta,F}(x)) &\longmapsto F(\beta) \\ a(\bar{x}) &\longmapsto a(\beta). \end{aligned}$$

Clearly $\varphi|_F = \mathrm{id}_F$, and $\varphi : F(\alpha) \to \bar{F}$ is an F-embedding. Moreover, $\varphi(a(\alpha)) = a(\beta)$ for all $a(x) \in F[x]$. In particular $\varphi(\alpha) = \beta$. Hence β is in the image of all the roots of $m_{\alpha,F}(x)$, and the

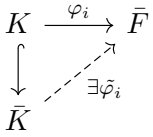
reverse inclusion holds. This shows that (*) is injective and its image is all the roots of $m_{\alpha,F}(x)$. This proves the first claim.

(2) is immediate since the number of roots of $m_{\alpha,F}(x)$ is less or equal to $\deg m_{\alpha,F}(x) = [F(\alpha) : F]$. And the equality holds if and only if $m_{\alpha,F}(x)$ has no repeated roots, i.e. α is separable over F. □

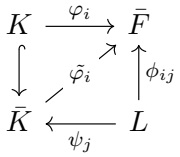
Proposition 6.7. Let L/K and K/F be finite extensions. Then

$$|\operatorname{Emb}_F(L, \bar{F})| = |\operatorname{Emb}_F(K, \bar{F})| \cdot |\operatorname{Emb}_K(L, \bar{K})|.$$

Proof. We sketch the proof here. Let $\varphi_1, \cdots, \varphi_n$ be all the F-embeddings from F to $\bar{K}$ and let $\psi_1, \cdots, \psi_m$ be all the K-embeddings from L to $\bar{K}$. Apply Proposition 5.4 and we have the diagram



and we see φ_i extends to $\tilde{\varphi}_i : \bar{K} \to \bar{F}$. Let $\phi_{ij} = \tilde{\varphi}_i \circ \psi_j : L \to \bar{F}$:



One can check that $\phi_{ij}|_F = \mathrm{id}_F$. And $\phi_{ij} = \phi_{kl}$ if and only if $i = k$ and $j = l$. And one can verify that ϕ_{ij}s are all the F-embeddings from L to $\bar{F}$. □

Proposition 6.8. Let K/F be a finite extension. Then $|\operatorname{Emb}_F(K, \bar{F})| \leq [K : F]$, and the equality holds if and only if K/F is separable.

Proof. Use induction on $[K : F]$. If $[K : F] = 1$, then the statement is obviously true. Assume the statement is true for all field extensions of degree less or equal to $n - 1$. Then take $\alpha \in K \setminus F$. Then by proposition 6.7, we have that

$$|\operatorname{Emb}_F(K, \bar{F})| = |\operatorname{Emb}_F(F(\alpha), \bar{F})| \cdot |\operatorname{Emb}_{F(\alpha)}(K, F\bar{(}\alpha))| = |\operatorname{Emb}_F(F(\alpha), \bar{F})| \cdot |\operatorname{Emb}_{F(\alpha)}(K, \bar{F})|.$$

since $F\bar{(}\alpha) = \bar{F}$. Then by Proposition 6.6, We have $|\operatorname{Emb}_F(F(\alpha), \bar{F})| \leq [F(\alpha) : F]$.

Next, since $[K : F(\alpha)] < [K : F]$, we can apply the induction hypothesis to $K/F(\alpha)$. Then $|\operatorname{Emb}_{F(\alpha)}(K, \bar{F})| \leq [K : F(\alpha)]$. Hence the inequality is proven.

If the equality in the statement hold, then $|\operatorname{Emb}_F(F(\alpha), \bar{F})| = [F(\alpha) : F]$. Henc every $\alpha \in K \setminus F$ is separable over F. Clearly then K/F is separable. Conversely, if K/F is separable, then the equality $|\operatorname{Emb}_F(F(\alpha), \bar{F})| = [F(\alpha) : F]$ holds. For all $\beta \in K$, since β is separable over F, and $m_{\beta,F(\alpha)}(x) | m_{\beta,F}(x)$, we see that β is separable over $F(\alpha)$. hence $K/F(\alpha)$ is separable and $|\operatorname{Emb}_{F(\alpha)}(K, \bar{F})| = [K : F(\alpha)]$. Hence the equality in the statement holds. □

Finally, we are ready to prove the big theorem of the day:

Theorem 6.9. *Let L/K and K/F be algebraic field extensions. Then L/F is separable if and only if K/F and L/K are both separable.*

Proof. ($\Rightarrow$):We first prove that L/K is separable. Since L/F is separable, for any $\alpha \in L$, we have that $m_{\alpha,F}(x)$ is separable. That is, all the roots of $m_{\alpha,F}(x)$ in $\bar{F}$ are simple. Now, consider the corresponding minimal polynomial $m_{\alpha,K}(x)$ over the field K. Since $m_{\alpha,K}(x)|m_{\alpha,F}(x)$ in $K[x]$, we see that $m_{\alpha,F}(x)$ contains all the roots of $m_{\alpha,K}(x)$, which are simple in $\bar{F}$. However, since $F \subseteq K \subseteq \bar{K}$, we know every nonconstant polynomial in $F[x]$ splits completely over $\bar{K}$. Hence we conclude that $\bar{F} \subseteq \bar{K}$. Hence if all the roots of $m_{\alpha,K}(x)$ are simple in $\bar{F}$, they are also simple in $\bar{K}$. This, by definition, proves that L/K is separable. Now we prove that K/F is separable. Since we know L/F is separable, for all $\alpha \in L$ we know $m_{\alpha,F}(x)$ is separable. But since $K \subseteq L$, clearly for all $k \in K$ we have $m_{k,F}(x)$ is separable. Hence K/F is also separable.

($\Leftarrow$): Conversely, we have two cases:

- Case I: $[L : F] < \infty$: We apply Proposition 6.7 and 6.8, we get

$$|\operatorname{Emb}_F(L, \bar{F})| = |\operatorname{Emb}_F(K, \bar{K})| \cdot |\operatorname{Emb}_K(L, \bar{K})| = [K : F][L : K] = [L : F].$$

  This shows that L/F is separable.

- $[L : F] = \infty$: See the details at the end of the lecture notes of Apr 20.

□

We conclude this section with one last theorem, which is also one of the key results of this section:

Theorem 6.10. *Let K/F be an algebraic extension. Then K/F is separable if and only if there exists $S \subseteq K$ such that $K = F(S)$ and every element in S is separable over F.*

Proof. ($\Rightarrow$): Simily take $S = K$.

($\Leftarrow$): When $[K : F] < \infty$, use induction on $[K : F]$. When $[K : F] = 1$ the statment obviously hold. Suppose the implication is true for all field extensions of fegree less than or equal to $n - 1$. Then suppose $[K : F] = n \geq 2$, $K = F(S)$ and every element in S is separable over F. Take $\alpha \in S$ such that $\alpha \notin F$. Since α is separable over F, from Proposition 6.6, we know that

$$|\operatorname{Emb}_F(F(\alpha), \bar{F})| = [F(\alpha) : F].$$

Then by Proposition 6.8, we know that $F(\alpha)/F$ is separable. Also, for $K/F(\alpha)$, we have that

- $[K : F(\alpha)] = \frac{[K:F]}{[F(\alpha):F]} < [K : F] = n$;
- $K = (F(\alpha))(S)$;
- Every element in S is separable over F, hence every element separable over $F(\alpha)$, since the minimal polynomial of that element in $F(\alpha)$ divides that in F.

Then we can apply the induction hypothesis to $K/F(\alpha)$, and we deduce that $K/F(\alpha)$ is separable. Since $K/F(\alpha)$ and $F(\alpha)/F$ are separable, we have that K/F is separable.

When $[K : F] = \infty$, given an element $\beta \in K = F(S)$, there exists finite $\alpha_1, \cdots, \alpha_n \in S$ such that $\beta \in F(\alpha_1, \cdots, \alpha_n)$. Since K/F algebraic, $\alpha_1, \cdots, \alpha_n \in S$ are algebraic over F. Hence $[F(\alpha_1, \cdots, \alpha_n) : F] < \infty$. Also, since $\alpha_1, \cdots, \alpha_n \in S$, they are separable over F. Then apply the first case to $F(\alpha_1, \cdots, \alpha_n)/F$ and we have that $F(\alpha_1, \cdots, \alpha_n)/F$ is separable. Thus $\beta \in F(\alpha_1, \cdots, \alpha_n)$ is separable over F. □

7 Finite Fields and Perfect Fields

We shall digress slightly now from field extensions to the study of finite and perfect fields. REASON: I lost (lots of) points on mitderm because of them. We first present a classification theorem of finite fields.

Theorem 7.1. *Let p be a prime number and n a positive integer.*

1. *Let $\mathbb{F}_{p^n} \subseteq \bar{\mathbb{F}}_p$ be the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$. Then $|\mathbb{F}_{p^n}| = p^n$ and $\mathbb{F}_{p^n}$ is the unique subfield of $\bar{\mathbb{F}}_p$ of cardinality p^n.*

2. *If F is a field with $|F| = p^n$, then $F \cong \mathbb{F}_{p^n}$.*

Proof. (1) Let $S \subseteq \bar{\mathbb{F}}_p$ be the subset of all the roots of $x^{p^n} - x$. Then since we are in a field of characteristic p, use Frobenius endomorphism we can check that S is a subfield of $\bar{\mathbb{F}}_p$. Thus $\mathbb{F}_p(S) = S$ since S clearly contains $\mathbb{F}_p$. Then S is a splitting field of $x^{p^n} - x$. Hence $\mathbb{F}_{p^n} = S$ (for details see lecture notes of Apr 22). Then $\mathbb{F}_{p^n}$ is all the roots of $x^{p^n} - x$ in $\bar{\mathbb{F}}_p$.

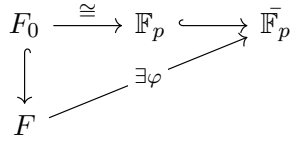
We still need to show that $|\mathbb{F}_{p^n}| = p^n$. Since $\gcd(x^{p^n} - x, (x^{p^n} - x)') = -1$, the polynomial $x^{p^n} - x$ has no multiple roots. Thus $|S| = \deg(x^{p^n} - x) = p^n = |\mathbb{F}_{p^n}|$.

For uniqueness, let F be a subfield of $\bar{\mathbb{F}}_p$ with $|F| = p^n$. Then $F^\times$ is an abelian group of order $p^n - 1$. Let $\alpha \in F$ be nonzero. Then by Lagrange's theorem $|\alpha||p^n - 1$. Hence $\alpha^{p^n - 1} = 1$, giving $\alpha^{p^n} - \alpha = 0$. Hence α is a root of $x^{p^n} - x$. Thus $F \subseteq S$ and they have the same cardinality. Hence $F = S = \mathbb{F}_{p^n}$.

(2) Let F be a field of cardinality p^n. Denote its prime subfield by F_0. Then since finite field has nonzero characteristic, we have $F_0 \cong \mathbb{F}_q$ for some prime number q. Then, viewing F as an F_0-vector space, we have that

$$p^n = |F| = |F_0|^{\dim_{F_0} F} = q^{\dim_{F_0} F}.$$

Then since $\mathbb{Z}$ is a UFD, we have $p = q$ and $n = \dim_{F_0} F$. Hence $F_0 \cong \mathbb{F}_p$. Then by Proposition 5.4 we have the following commutative diagram:



Since φ is a (nonzero) field homomorphism, it is injective. Thus $F \cong \varphi(F) \subseteq \bar{\mathbb{F}}_p$. Then $|\varphi(F)| = |F| = p^n$. Then by (1), we have $\varphi(F) = \mathbb{F}_{p^n}$. Hence $F \cong \mathbb{F}_{p^n}$. □

Here is one practice problem:

Midterm Problem. Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial.

(a) Show that if $\theta_1, \theta_2 \in \bar{\mathbb{F}_p}$ are both roots of $f(x)$, then $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_2)$.

(b) Let $K \subseteq \bar{\mathbb{F}_p}$ be the splitting field of $f(x)$. over $\mathbb{F}_p$. Show that $[K : \mathbb{F}_p] = \deg f(x)$.

Solution. (a) We can assume that $f(x)$ is monic. Then since θ_1, θ_2 are both roots of $f(x)$, we know that $m_{\theta_1,\mathbb{F}_p}(x) = f(x) = m_{\theta_2,\mathbb{F}_p}(x)$ since $f(x)$ is irreducible. Then let $\deg f(x) = n$. We have that

$$[\mathbb{F}_p(\theta_1) : \mathbb{F}_p] = [\mathbb{F}_p(\theta_2) : \mathbb{F}_p] = n.$$

Hence both $\mathbb{F}_p(\theta_1), \mathbb{F}_p(\theta_2)$ are subfields of $\bar{\mathbb{F}_p}$ of cardinality p^n. By the previous theorem, $\bar{\mathbb{F}_p}$ has a unique subfield of cardinality p^n. Hence $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_2)$.

(b) Let $\theta_1, \cdots, \theta_n$ be all the roots of $f(x)$ in $\bar{\mathbb{F}_p}$. Then by (a), we have $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_j)$ for all j. Hence $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_1, \cdots, \theta_n)$, which is exactly the splitting field K of $f(x)$ inside $\bar{\mathbb{F}_p}$. Thus

$$[K : \mathbb{F}_p] = [\mathbb{F}_p(\theta_1, \cdots, \theta_n) : \mathbb{F}_p] = [\mathbb{F}_p(\theta_1) : \mathbb{F}_p] = \deg f(x).$$

□

We conclude this section with a discussion of perfect field.

Definition 7.2. A field F is called perfect if every finite extension K/F is separable.

Proposition 7.3. The following are true:

1. Every field of characteristic 0 is perfect.
2. A field F of characteristic p is perfect if and only if $F = F^p$, i.e. every element in F is a pth power in F (for all $\alpha \in F$, there exists $\beta \in F$ such that $\alpha = \beta^p$).
3. Every finite field is perfect.

Proof. (1) Finite extensions are algebraic extensions, and every algebraic extensions of a field of characteristic 0 is separable.

(2) Suppose $\mathrm{ch}(F) = p$ and $F = F^p$. Let K/F be a finite extension with $\alpha \in K$. We use proof by contradiction to show that α is separable over F. Suppose that α inseparable over F, then $m_{\alpha,F}(x)$ is inseparable. Hence $\gcd(m_{\alpha,F}(x), m'_{\alpha,F}(x)) \neq 1$. But $m_{\alpha,F}(x)$ is irreducible in $F[x]$, hence $\gcd(m_{\alpha,F}(x), m'_{\alpha,F}(x)) = m_{\alpha,F}(x)$ and $m'_{\alpha,F}(x) = 0$. Then if we write $m_{\alpha,F}(x) = \sum_{j=0}^{n} a_j x^j$ where $a_n = 1$, then

$$m'_{\alpha,F}(x) = \sum_{j=0}^{n} j a_j x^{j-1} = 0 \Longrightarrow j a_j = 0 \quad \forall j \Longrightarrow a_j = 0 \quad \forall j \not| p.$$

Then we can write

$$m_{\alpha,F}(x) = x^{pk} + c_{k-1}x^{p(k-1)} + \cdots + c_1x^p + c_0$$

for some $c_j \in F$. Then there exists $d_j \in F$ such that $d_j^p = c_j$. Hence

$$m_{\alpha,F}(x) = x^{pk} + d_{k-1}^p x^{p(k-1)} + \cdots + d_1^p x^p + d_0^p = (x^k + d_{k-1}x^{k-1} + \cdots + d_1x + d_0)^p.$$

This contradict the irreduciblity of minimal polynomial. Hence α iis separable over F.

Conversely, again we prove by contradiction. Suppose that F is perfect, but $a \in F$ has no pth root. Let K be a splitting field of $f(x) := x^p - a$. Then $K = F(\theta_1, \cdots, \theta_p)$, where $\theta_1, \cdots, \theta_p$ are roots of $f(x)$. Now, $\theta_1, \cdots, \theta_p$ are obviously algebraic over F. Hence K/F is finite. Therefore by assumption K/F is separable. Then take $\theta_j \in K$, it should be separable over F. i.e. $m_{\theta_j,F}(x)$ has no multiple roots. Now, we claim that $f(x) = x^p - a \in F[x]$ is irreducible. Otherwise since $\theta_j^p - a = 0$ we have that

$$f(x) = x^p - a = x^p - \theta_j^p = (x - \theta_j)^p \in F[x].$$

If $f(x) \in F[x]$ is reducible, then there exists $1 \leq k \leq p$ such that $(x - \theta_j)^k \in F[x]$. Expanding this polynomial we find that $(x - \theta_j)^k = x^k - k\theta_j x^{k-1} + \cdots \in F[x]$. Hence $-k\theta_j \in F$ implies $\theta_j \in F$, which contradicts the assumption that a has no pth root. Hence $f(x)$ is irreducible and monic in $F[x]$ containing θ_j as a root. Thus

$$f(x) = m_{\theta_j,F}(x) = (x - \theta_j)^p.$$

But this contradicts the separability of θ_j. Hence we must have $F = F^p$ if F is perfect.

(3) Let F be a finite field of characteristic p. Then $|F| = p^n$ for some $n \geq 1$. Let $\alpha \in F^\times$, then $|\alpha|||F^\times| = p^n - 1$. Hence $\alpha^{p^n-1} = 1$ and this implies that $\alpha = \alpha^{p^n} = (\alpha^{p^{n-1}})^p$. Hence by (2) F is perfect. □

8 Automorphisms of Fields

From this point we have entered the study of Galois theory. The idea is to study the correspondence of the group permuting the root of a polynomial $f(x)$ and the splitting field of $F[x]$. We first establish the basic object of study in these first few sections (automorphisms and Galois extension), then we introduce the Fundamental Theorem of Galois Theory.

Definition 8.1. Let F be a field.

1. An automorphism of F is a field isomorphism from F to itself. The set of all automorphisms of F are denoted by $\operatorname{Aut} F$.

2. An automorphism σ of F is said to fix $\alpha \in F$ if $\sigma(\alpha) = \alpha$, and is said to fix a subset $S \subseteq F$ if $\sigma(\alpha) = \alpha$ for all $\alpha \in S$.

Example 8.2. Here are some examples of automorphisms:

1. Every field F has at least one automorphism: id_F.

2. If $\sigma \in \operatorname{Aut} F$, then $\sigma(1) = 1$ and $\sigma(1 + \cdots + 1) = 1 + \cdots + 1$. Hence any automorphism of F fixes the prime subfield of F.

3. Let $\operatorname{ch}(F) = p$. Then the Frobenius endomorphism $\Phi : a \mapsto a^p$ is injective. It is surjective if and only if every element is a p-th power, i.e. if and only if F is perfect.

Definition 8.3. Let K/F be a field extension. $\operatorname{Aut}(K/F)$ is defined to be the subset of $\operatorname{Aut} K$ consistung of all the automorphisms that fix F.

Hence by the last example, we clearly have that $\operatorname{Aut}(F/F_0) = \operatorname{Aut} F$.

Proposition 8.4. Let K/F be a field extension.

1. $\operatorname{Aut} K$ is a group under composition, and $\operatorname{Aut}(K/F)$ is a subgroup of $\operatorname{Aut} K$.

2. If $F \subseteq K \subseteq L$ are fields, then $\operatorname{Aut}(L/K) \leq \operatorname{Aut}(L/F)$.

3. For $H \leq \operatorname{Aut}(K/F)$, define

$$K^H = \{\alpha \in K |\ \sigma(\alpha) = \alpha\ \forall \sigma \in H\}$$

called the fixed field of H. Then as the name suggests, K^H is a subfield of K.

4. If $H_1 \leq H_2 \leq \operatorname{Aut}(K/F)$, then $K^{H_2} \leq K^{H_1}$.

More examples will come later.

9 Normal Extensions

Definition 9.1. An algebraic extension K/F is normal if for every $\alpha \in K$, $m_{\alpha,F}(x)$ splits completely over K.

There are many equivalent conditions for K/F to be normal, we present them here:

Proposition 9.2. Let K/F be an algebraic extension. The following are equivalent:

1. K/F is normal;

2. Any irreducible polynomial in $F[x]$ which has a root in K splits completely over K;

3. There exists $S \subseteq K$ such that $K = F(S)$ and $m_{\alpha,F}(x)$ splits completely over K for all $\alpha \in S$;

4. K is the splitting field for some $A \subseteq F[x]$;

5. Every F-embedding $\varphi : K \to \bar{F}$ satisfies $\varphi(K) = K$;

6. Every F-embedding $\varphi : K \to \bar{F}$ satisfies $\varphi(K) \subseteq K$.

Remark 9.3. Notice that in (4), an algebraic extension K/F is called a splitting field for $A \subseteq F[x]$ if every $f(x) \in A$ splits completely over K and if $F \subseteq E \subseteq K$ where every $f(x) \in A$ splits completely over E implies $E = K$.

Proof. Let K/F be an algebraic extension.

- (1) $\Rightarrow$ (2): Let $f(x) \in F[x]$ be irreducible with a root $\alpha \in K$. WLOG assume $f(x)$ monic, then $m_{\alpha,F}(x) = f(x)$, which splits completely over K.

- (2) $\Rightarrow$ (3): Take any $S \subseteq K$ such that $K = F(S)$. For all $\alpha \in S$, we have $m_{\alpha,F}(x)$ irreducible in $F[x]$ and $\alpha \in K$ is a root. Thus by assumption $m_{\alpha,F}(x)$ splits completely over K.

- (3) $\Rightarrow$ (4): Let $S \subseteq K$ such that $K = F(S)$ and $m_{\alpha,F}(x)$ splits completely over K for all $\alpha \in S$. Let
$$A = \{m_{\alpha,F}(x) |\ \alpha \in S\}.$$
Claim: K is the splitting field of A. Let S' be the set of roots in $\bar{F} = \bar{K}$ of polynomials in A. Then $F(S')$ is the splitting field for A. Since $K = F(S)$ and by definition of A and S', we have $S \subseteq S'$. Thus we have $F \subseteq K \subseteq F(S')$ and every polynomial in A splits completely over K. Hence $K = F(S')$ is the splitting field for A.

- (4) $\Rightarrow$ (5): Suppose that K is a splitting field for $A \subseteq F[x]$ and we have fixed an algebraic closure such that $F \subseteq K \subseteq \bar{F}$. Then $K = F(S)$ where S is the roots in $\bar{F}$ of polynomials in A. Let $\varphi : K \to \bar{F}$ be an F-embedding. Since $K = F(S)$, to show $\varphi(K) = K$ it suffices to check that $\varphi(S) = S$.

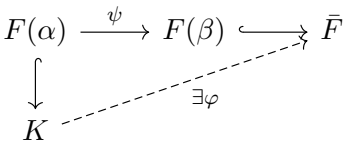
  $\varphi(S) \subseteq S$: $\alpha \in S$ implies α is a root of some $f(x) \in A$. Then $\varphi(\alpha) \in S$ is immediate.

  $\varphi(S) \supseteq S$: Given $\alpha \in S$, then α is a root of some $f(x) \in A$. Let R_f be the subsets of $\bar{F}$ consisting of all the roots of $f(x)$. Then $R_f \subseteq S$. One can check that the map
$$\begin{aligned} R_f &\to R_f \\ \beta &\mapsto \varphi(\beta) \end{aligned}$$
is bijective. Hence there exists $\beta \in R_f \subseteq S$ such that $\varphi(\beta) = \alpha$. Thus $\alpha \in \varphi(S)$. This proves the claim.

- (5) $\Rightarrow$ (6): Obvious.

- (6) $\Rightarrow$ (1): Given $\alpha \in K$, we need to show $m_{\alpha,F}(x)$ splits completely over K. It suffices to show K contains all the roots of $m_{\alpha,F}(x)$ in $\bar{F}$. Let $\beta \in \bar{F}$ be a root of $m_{\alpha,F}(x)$. We want to show that there exists an F-embedding $\varphi : K \to \bar{F}$ such that $\varphi(\alpha) = \beta$. Then (6) implies that $\beta = \varphi(\alpha) \subseteq K$.

  We know that
$$\begin{aligned} \psi : F(\alpha) &\to F(\beta) \\ a(\alpha) &\mapsto a(\beta) \end{aligned}$$
is a well defined isomorphism. Then by Proposition 5.4 we have the following diagram:



  Hence φ is an F-embedding. In particular $\varphi(\alpha) = \psi(\alpha) = \beta$. This completes the proof.

□

10 Galois Extensions

Proposition 10.1. Let K/F be an algebraic extension.

1. Fix an algebraic closure of F such that $F \subseteq K \subseteq \bar{F}$. Then we have the bijective map

$$\begin{aligned} \mathrm{Aut}(K/F) &\longrightarrow \{F\text{-embeddings } \varphi : K \to \bar{F} \text{ s.t. } \varphi(K) = K\} \\ \sigma &\longmapsto \varphi_\sigma \end{aligned}$$

   where

$$\varphi_\sigma : K \xrightarrow{\sigma} K \hookrightarrow \bar{F}.$$

2. If K/F is finite then $|\mathrm{Aut}(K/F)| \leq |\mathrm{Emb}_F(K, \bar{F})|$ and the equality holds if and only if K/F is normal.

Proof. (1) φ_σ is clearly an F-embedding. $\varphi_\sigma(K) = \sigma(K) = K$. The injectivity is easy to see: $\varphi_\sigma = \varphi_\tau$ implies $\sigma = \tau$. Given an F-embedding $\varphi : K \to \bar{F}$ with $\varphi(K) = K$, define $\sigma : K \to K$ with $\sigma(\alpha) = \varphi(\alpha)$. Then $\sigma \in \mathrm{Aut}(K/F)$ since $\sigma(K) = K$ and $\sigma|_F = \mathrm{id}_F$. One can check $\varphi_\sigma = \varphi$. Hence the map is a bijection.

(2) Clearly

$$\{F\text{-embeddings } \varphi : K \to \bar{F} \text{ s.t. } \varphi(K) = K\} \subseteq \{F\text{-embeddings } \varphi : K \to \bar{F}\}.$$

Hence

$$|\mathrm{Aut}(K/F)| = \#\{F\text{-embeddings } \varphi : K \to \bar{F} \text{ s.t. } \varphi(K) = K\} \leq \#\{F\text{-embeddings } \varphi : K \to \bar{F}\}.$$

The equality holds if and only if every φ satisfies $\varphi(K) = K$, which, according to the equivalent conditions in the last section, amounts to saying that K/F is normal. □

Definition 10.2. An algebraic extension K/F is called Galois if it is both separable and normal. If K/F is Galois, we call the group $\mathrm{Aut}(K/F)$ the Galois group of K/F and denoted it by $\mathrm{Gal}(K/F)$.

Proposition 10.3. Let K/F be a finite extension. Then $|\mathrm{Aut}(K/F)| \leq [K : F]$, and the equality holds if and only if K/F is Galois.

Proof. We know that

$$|\mathrm{Aut}(K/F)| \leq |\mathrm{Emb}_F(K, \bar{F})| \leq [K : F],$$

where the first inequality comes from the previous proposition, which is equality if and only if K/F is normal, and the second inequality comes from Proposition 6.8, which is equality if and only if K/F is separable. □

Hence an equivalent definition for K/F to be a Galois extension is that $|\mathrm{Aut}(K/F)| = [K : F]$. This is also the definition given in Dummit and Foote.

Corollary 10.4. *If K is the splitting field over F of a separable polynomial $f(x) \in F[x]$, then K/F is Galois.*

Proof. Let $K = F(\theta_1, \cdots, \theta_n)$ be the splitting field generated by roots of $f(x)$. Then K/F is normal since K is the splitting field of the subset $\{f(x)\} \subseteq F[x]$. Since $f(x)$ is separable and $m_{\theta_j,F}(x)|f(x)$, each $m_{\theta_j,F}(x)$ has no multiple root, hence is separable. Thus K is generated by a bunch of separable elements over F, which shows that K/F is separable. Hence K/F is Galois. □

We generalize this result by the following proposition.

Proposition 10.5. An algebraic extension K/F is Galois if and only if K is the splitting field for a subset of separable polynomials in $F[x]$.

Proof. Fix $\bar{F} = \bar{K}$. Then $F \subseteq K \subseteq \bar{F}$. First suppose that K/F is Galois. Then let

$$A = \{m_{\alpha,F}(x) |\ \alpha \in K\},$$
$$S = \{\text{ roots in } \bar{F} \text{ of polynomials in } A\}.$$

We make the following two observation:

- $K = F(S)$. Since K/F is normal, we have that every polynomial in A splits completely over K. Hence $S \subseteq K$. And also since by the definition of A and S, we see that $K \subseteq S$.
- The polynomials in A are all separable because K/F is separable.

This proves the first half of the claim. Conversely, suppose there exists $A \subseteq F[x]$, a subset of separable polynomials such that K is the splitting field of A. Since K is a splitting field of A, then K/F satisfies the equivalence condition (4) of being normal, hence K/F is normal. Let

$$S = \{\text{ roots in } \bar{F} \text{ of polynomials in } A\}.$$

Then $K = F(S)$. Let $\alpha \in S$, then α is a root of some separable polynomial $f(x)$. Since $m_{\alpha,F}(x)|f(x)$, we have α is separable over F. Hence K is generated by a bunch of separable elements over F. This shows that K/F is separable. Hence K/F is Galois. □

Thus the previous corollary is just a special case of this proposition.

Let us set up the stage before we enter some examples. Suppose that K/F is a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$. Hence $\mathrm{Aut}(K/F)$ permutes the roots of irreducible polynomials. If $f(x) = s(x)t(x)$ is reducible but $s(x), t(x)$ are irreducible, then σ also permutes the root of $f(x)$, in the sense that a root of $f(x)$ will still be a root of $f(x)$. However, since a root of $s(x)$ will be mapped to a root of $s(x)$ and similar for $t(x)$, then a root of $s(x)$ will not necessarily be mapped to a root of $t(x)$.

Also, if $K = F(S)$, then the behavior of σ will be completely determined by what σ maps the generators S to, since σ fixes F. Now we study two examples in detail.

Example 10.6. The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois since $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of the separable polynomial $(x^2 - 2)(x^2 - 3)$. Any automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Hence we have 4 possibilities:

$$\sigma : \left\{ \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array} \right. \left\{ \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array} \right. \left\{ \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array} \right. \left\{ \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array} \right. .$$

Since

$$|\operatorname{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4,$$

the these are actually all the elements in the automorphism group. We want to classify the group $\operatorname{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$, or $\operatorname{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. A group of order 4 is either isomorphic to the Klein four group or $\mathbb{Z}/4\mathbb{Z}$. We show that the former case is true. Let

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

Since

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = (-\sqrt{2})(\sqrt{3}) = -\sqrt{6},$$

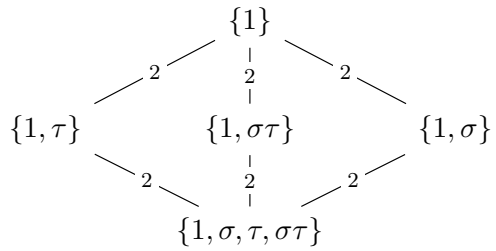
we can write down σ specifically. The basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ is $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. Hence we have

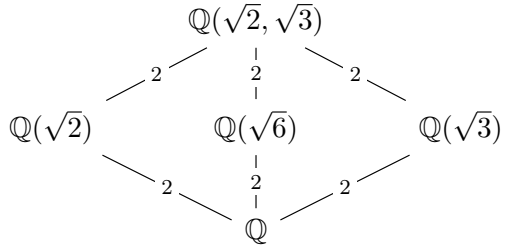
$$\begin{aligned} \sigma &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \tau &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}. \end{aligned}$$

Then it is easy to verify that $\sigma^2 = 1$, $\tau^2 = 1$, and

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{1,\sigma,\tau,\sigma\tau\} \cong V_4.$$

We can actually look at the subgroups of $\operatorname{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})$ and its correspondence with the fixed field determined by these subgroups, which are illustrated in the following two diagrams.





One can see that there is a correspondence between the diagram of subgroups of the Galois group and the diagram of the corresponding fixed field. This is our first (and one very elegant) example that illustrates the Fundamental theorem of Galois theory.

Example 10.7. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is Galois of degree 6. The roots of this equation are $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = \frac{-1+\sqrt{3}}{2}$. Hence the splitting field can be written as $\mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})$. Any automorphism maps each of these two elements to one of the roots of $x^3 - 2$ (irreducible by Eisenstein's criterion). Any automorphism maps each of these two elements to one of the roots of $x^3 - 2$, giving 9 possibilities. However, since the Galois group has order 9, not every such map is an automorphism of the field.

Intuitively, $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})/\mathbb{Q})$ is a group of order 6, which is isomorphic to either S_3 or $\mathbb{Z}/6\mathbb{Z}$. Since the automorphism group permutes three roots of $x^3 - 2$, it is isomorphic to a subgroup of S_3. But since they have the same cardinality, we expect the Galois group to be isomorphic to S_3. We prove this claim now.

To determine the Galois group, we use a more convenient set of generators. Notice that $\mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \rho)$. Now, any automorphism σ maps $\sqrt[3]{2}$ to one of $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$, since

$f(x) = m_{\sqrt[3]{2},\mathbb{Q}}(x)$. On the other hand, since $m_{\rho,\mathbb{Q}} = \Phi_3(x) = x^2 + x + 1$, we have σ maps ρ to $\rho, \rho^2 = -1 - \rho$, which are roots of the minimal polynomial of ρ. Hence this gives 6 possibilities and they are actually all the elements in the automorphism group. Let

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \quad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1 - \rho \end{cases}.$$

Then, we can find a basis of $\mathbb{Q}(\sqrt[3]{2}, \rho)$ over $\mathbb{Q}$, which is of degree 6. The basis is given by

$$\left\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\right\}.$$

Then, one can check that

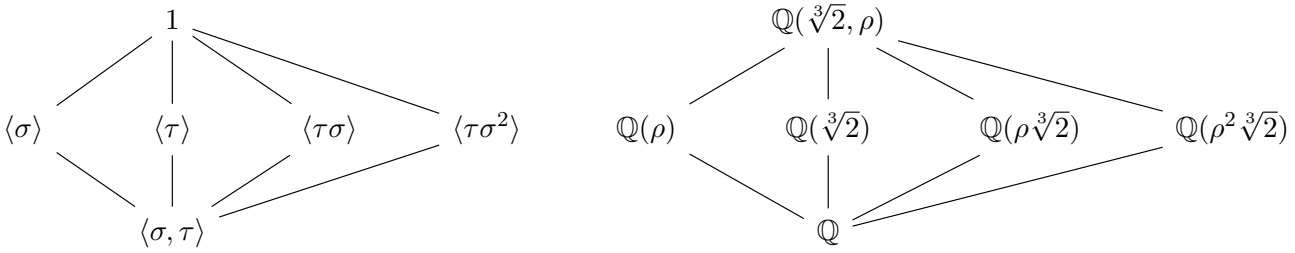
$$\sigma\tau = \tau\sigma^2$$

$$\sigma^3 = \tau^2 = 1$$

and

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3.$$

Similar to the previous example (but with a lot more computation), one can determine the fixed field for any of the subgroups of the Galois group. And the correspondence is shown below.



Hence it is reasonable to suspect that the relations observed in these two examples are not coincidental. Such correspondence holds for any Galois extension. This leads to the Fundamental Theorem of Galois Theory.

It has been proven that the properties of finite/algebraic/separable are transitive. Unfortunately, this does not hold for normal or Galois extension. We illustrate this with the following example.

Example 10.8. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois. This is because this extension is not normal: $m_{\sqrt[4]{2},\mathbb{Q}}(x) = x^4 - 2$ does not split completely over $\mathbb{Q}(\sqrt[4]{2})$. Since

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}),$$

but the roots $\pm i\sqrt[4]{2}$ are not contained in the field $\mathbb{Q}(\sqrt[4]{2})$ since they are complex. However, we have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$, and Both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are Galois, since they are both quadratic: Any extension K/F of degree 2 with $\mathrm{ch}(F) \neq 2$ is of the form $F(\sqrt{D})/F$ for some D, hence is the splitting field of $x^2 - D$, which is separable (See Dummit and Foote page 522, example after Corollary 13.13 for details).

We generalize this example with the following proposition. This proposition tells us that if we have a chain of fields $F \subseteq K \subseteq L$, and L/F is normal (Galois), then the best we can say is that L/K is normal (Galois).

Proposition 10.9. Let K/F and L/K be algebraic extensions with $F \subseteq K \subseteq L$. Then L/F is normal (Galois) implies L/K is normal (Galois).

Proof. Homework. □

11 The Story So Far: Review

This section is a brief (non-exaustive) summary of what we have discussed so far. The main objects we study are various field extensions. Here are a summary of all the field extensions we have encountered.

- Finite extensions: An extension K/F such that $[K : F] < \infty$. Notice that finite extensions are algebraic.
- Algebraic extensions: An extension K/F such that every element $\alpha \in K$ is a root of some nonzero polynomial $f(x) \in F[x]$.
- Splitting field of $f(x) \in F[x]$: An extension K/F such that K is the smallest field over which $f(x)$ splits completely.
- Algebraic Closure: An algebraic extension Ω/F such that every nonconstant polynomial in $F[x]$ splits completely over Ω (i.e. Ω contains all the roots of all polynomials in $F[x]$).
- Separable Extension: An algebraic extension K/F such that every element in K is separable over F (the minimal polynomial over F has no multiple root).
- Normal Extension: An algebraic extension K/F in which $m_{\alpha,F}$ splits completely for all $\alpha \in K$.
- Galois Extension: An algebraic extension K/F that is both separable and normal (i.e. $|\operatorname{Aut}(K/F)| = [K : F]$).

There are some criteria that tell us how to determine what kind of extension(s) is(are) K/F. For example, we only need to verify the properties of the generating sets:

Generating Set Criterion	
K/F **is...**	**iff** $\exists S \subseteq K$ **such that** $K = F(S)$ **and...**
algebraic	every element in S is algebraic over F
finite	every element in S is algebraic over F and S is finite
separable	every element in S is separable over F
normal	$m_{\alpha,F}(x)$ splits completely over K for every $\alpha \in S$

Also, we discussed whether these properties are transitive:

Transitivity	
K/F **and** L/K **have the property X**	**iff** L/F **has the property X**
X=algebraic	Yes
X=finite	Yes
X=separable	Yes
X=normal	No
X=Galois	No

Of course, there are also some numerical criteria to determine types of extensions. Some of them are listed below.

- K/F is finite if and only if $[K : F] < \infty$;
- K/F is normal if and only if $|\operatorname{Aut}(K/F)| = |\operatorname{Emb}_F(K, \bar{F})|$;
- K/F is separable if and only if $|\operatorname{Emb}_F(K, \bar{F})| = [K : F]$;
- K/F is Galois if and only if $|\operatorname{Aut}(K/F)| = |\operatorname{Emb}_F(K, \bar{F})| = [K : F]$.

There are some other criteria, which we list below.

- If $\operatorname{ch}(F) = 0$, then every algebraic extension of F is separable;
- If $|F| < \infty$, every algebraic extension of F is Galois;
- An algebraic extension K/F is normal if and only if K is the splitting field for a subset of $F[x]$;
- An algebraic extension K/F is Galois if and only if K is the splitting field for a subset of **separable polynomials** of $F[x]$.

We conclude this summary with the classification theorem of finite fields. Let F be a field with $|F| < \infty$ and $\operatorname{ch}(F) = p$. Then

- $|F| = p^n$, where $F_0 \cong \mathbb{F}_p$ is the prime subfield of F and $n = [F : F_0]$;
- $F \cong \mathbb{F}_{p^n}$, the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$;
- If $F \subseteq \bar{\mathbb{F}}_p$, then $F = \mathbb{F}_{p^n}$.

Introduction: Galois Theory

The material so far is covered roughly before midterm of 111C. Now we have come to the second half of this note. For the remaining part of this note, our focus will mainly be on the Fundamental Theorem of Galois Theory, which establishes the correspondence of the subgroups of the Galois group $\operatorname{Gal}(K/F)$ and subextensions of K/F.

Then, we will apply this key result to various situations and study the structure of the Galois group of some extensions (composite, cyclotomic, cyclic, radical, solvable extensions) in detail.

We will also study the solvability of polynomials, which is determined by the solvability of the Galois group of the polynomial. Finally, we will prove the famous result (and perhaps one of the most important work by Galois) of the insolvability of the quintic (degree 5 polynomial) or polynomials of higher degree.

12 The Fundamental Theorem of Galois Theory

Our goal is to prove the Fundamental Theorem of Galois Theory in this section. However, we will need some preparation work.

Definition 12.1. A character χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L: i.e. $\chi : G \to L^\times$ such that $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$ and $\chi(g) \neq 0$ for all $g \in G$.

Proposition 12.2. If $\chi_1, ..., \chi_n$ are distinct characters of G with values in L, then they are linearly independent as functions on G over L.

Proof. Suppose $\chi_1, ..., \chi_n$ are linearly dependent. Then there exists some coefficients over L, not all zero, such that the linear combination of them with $\chi_1, ..., \chi_n$ is 0. Among these coefficients, choose a set of coefficients $a_1, ..., a_n \in L$ such that the number m of nonzero coefficients a_i is minimal. Suppose these nonzero coefficients are $a_1, ..., a_m$, then we have

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_m\chi_m = 0.$$

Then for any $g \in G$ we have

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_m\chi_m(g) = 0. \tag{*}$$

Let $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_m(g_0)$, such g_0 exists since χ_1, χ_m are distinct. Hence

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \cdots + a_m\chi_m(g_0g) = 0.$$

That is,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0. \tag{**}$$

Multiply (*) by $\chi_m(g_0)$ and subtracting (**) from it:

$$\begin{aligned}[\chi_m(g_0) - \chi_1(g_0)]\, a_1\chi_1(g) + [\chi_m(g_0) - \chi_2(g_0)]\, a_2\chi_2(g) + \cdots \\ + [\chi_m(g_0) - \chi_{m-1}(g_0)]\, a_{m-1}\chi_{m-1}(g) = 0.\end{aligned}$$

This holds for all $g \in G$. But this is a relation with fewer nonzero coefficients, a contradiction. □

Now, let $\sigma : K \to L$ be an injective field homomorphism, called an embedding of K into L. Then σ is a homomorphism from the multiplicative group $K^\times$ to $L^\times \subseteq L$. Hence σ may be viewed as a character of $K^\times$ with values in L. This gives the following corollary.

Corollary 12.3. *If $\sigma_1, ..., \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular, distinct automorphisms of K are linearly independent as a function on K.*

Now we use this result to prove one of the following key preparation work for the Fundamental Theorem of Galois Theory:

Theorem 12.4. *Let $G = \{\sigma_1 = 1, \sigma_2, ..., \sigma_n\}$ be a subgroup of automorphisms group $\mathrm{Aut}(K/F)$, with K^G being its fixed field. Then*

$$[K : K^G] = |G| = n.$$

Proof. For the following arguments of this proof, let $F := K^G$ denote the fixed field and let $m = [K : K^G] = [K : F]$. We first prove that $n \leq [K : F] = m$.

Suppose that $n > [K : F] = m$. Let $\omega_1, ..., \omega_m$ be a basis for K over F. Then consider the system

$$\begin{gathered}\sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n = 0 \\ \vdots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \cdots + \sigma_n(\omega_m)x_n = 0.\end{gathered}$$

This is a system with m equations and n unknowns (more unknowns than equations). Hence there exists a nontrivial solution $(x_1, ..., x_n) = (\beta_1, ..., \beta_n)$ in K^n (i.e. $\beta_j \in K$). Now, let $a_1, ..., a_m \in F$ be m arbitrary elements. Then σ_j fixes $a_1, ..., a_m$ for all j by assumption. Hence multiply the first equation by a_1, the second by a_2..., the last by a_m gives

$$\begin{gathered}\sigma_1(a_1\omega_1)\beta_1 + \sigma_2(a_1\omega_1)\beta_2 + \cdots + \sigma_n(a_1\omega_1)\beta_n = 0 \\ \vdots \\ \sigma_1(a_m\omega_m)\beta_1 + \sigma_2(a_m\omega_m)\beta_2 + \cdots + \sigma_n(a_m\omega_m)\beta_n = 0.\end{gathered}$$

Adding these equations together we see there are $\beta_1, ..., \beta_n \in K$, not all zero, satisfying

$$\sigma_1(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_n = 0$$

for arbitrary choices of $a_1, ..., a_m \in F$. Since $\omega_1, ..., \omega_m$ is a F-basis for K, for every $\alpha \in K$ we can write it as an F-linear combination of ωs. This shows that

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0$$

for all $\alpha \in K$, and $\beta_1, ..., \beta_m$ nontrivial. But this contradicts the previous corollary that σ_js are linearly independent over K. Hence we conclude that $n \leq [K : F]$.

Now we again argue by contradiction to show that $n < [K : F]$ cannot happen. Suppose this is the case, then there are at least $n + 1$ F-linearly independent elements $\alpha_1, ..., \alpha_{n+1} \in K$. The system

$$\begin{gathered}\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0\end{gathered} \tag{I}$$

of n equations and $n+1$ unknowns. Hence there is a nontrivial solution $(x_1, \cdots, x_{n+1}) = (\beta_1, \cdots, \beta_{n+1}) \in K^n$. If all the elements $\beta_1, ..., \beta_{n+1}$ were elements of F, then since $\sigma_1 = 1$, the first equation would contradict the linear independence of σs. Hence at least one $\beta_j \notin F$. Among all the nontrivial solutions, choose one with the minimal number r of nonzero β_j. WLOG, we may assume that

$\beta_1, ..., \beta_r$ are nonzero. Dividing this set of solution by β_r we still have a solution. Hence we may assume $\beta_r = 1$. Since at least one of $\beta_1, ..., \beta_{r-1}, 1$ is not in F (in particular $r > 1$), we may assume WLOG that $\beta_1 \notin F$. Then our system reads

$$\begin{gathered} \sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0 \\ \vdots \\ \sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0 \end{gathered} \tag{II}$$

or more briefly

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0 \quad i = 1, 2, \ldots, n. \tag{III}$$

Since $\beta_1 \notin F$, there exists an automorphism σ_{k_0} with $k_0 \in \{1, 2, ..., n\}$ such that $\sigma_{k_0}\beta_1 \neq \beta_1$. Apply automorphisms to equations in (II), we get

$$\sigma_{k_0}\sigma_j(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_j(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_j(\alpha_r) = 0 \tag{IV}$$

for $j = 1, ..., n$. Since G is a group, left multiplication by an element in G is a group action, which amounts to a permutation. That is,

$$\{\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \ldots, \sigma_{k_0}\sigma_n\} = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}.$$

Hence, if we define index i by $\sigma_{k_0}\sigma_j = \sigma_i$, then (IV) can be written as

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0. \tag{V}$$

Now, if we subtract (V) from (III), we get

$$\sigma_i(\alpha_1)[\beta_1 - \sigma_{k_0}(\beta_1)] + \cdots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})] = 0$$

for $i = 1, ..., n$. But this is a solution to (I) with

$$x_1 = \beta_1 - \sigma_{k_0}(\beta_1) \neq 0$$

hence nontrivial but with fewer than r nonzero x_is. This is a contradiction. Hence we have shown that $n = [K : F]$. This proves the claim. □

Before we prove the Fundamental Theorem of Galois Theory, we give one more important result, which may not seem relevant at the moment, but will be important later.

Theorem 12.5. *Let K/F be a Galois extension. Suppose $\alpha \in K$. The the roots of $m_{\alpha,F}(x)$ are given precisely by the distinct Galois conjugates $\sigma(\alpha)$ of α, where $\sigma \in \mathrm{Gal}(K/F)$. That is,*

$$m_{\alpha,F}(x) = \prod_{\sigma \in \mathrm{Gal}(K/F),\ \sigma(\alpha)\ distinct} (x - \sigma(\alpha)).$$

Proof. First notice that K/F is normal, hence $m_{\alpha,F}(x)$ splits completely over K. Hence the equation above makes sense. Let $\mathrm{Gal}(K/F) = G = \{1, \sigma_2, ..., \sigma_n\}$. Then

$$\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \in K.$$

Let

$$\alpha, \alpha_2, \alpha_3, \ldots, \alpha_r$$

denote the distinct elements in the list above. If $\tau \in G$, by group action, $\{\tau, \tau\sigma_2, ..., \tau\sigma_n\} = \{1, \sigma_2, ..., \sigma_n\}$ up to reordering. Hence the coefficiens of the polynomial

$$f(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_r)$$

is fixed by τ for all $\tau \in G$. Thus $f(x) \in F[x]$. Since $\alpha, ..., \alpha_r$ are all distinct roots of $m_{\alpha,F}(x)$, we have that $f(x)|m_{\alpha,F}(x)$. Since $f(x)$ is in $F[x]$, containing α as a root, we have $m_{\alpha,F}(x)|f(x)$. This shows that $m_{\alpha,F}(x) = f(x)$ and the theorem follows. □

From this we have a simple corollary:

Corollary 12.6. *Let K/F be a finite extension. Then K/F is Galois if and only if K is the splitting of some separable polynomial in $F[x]$.*

Proof. If K is the splitting field of a separable polynomial, we proved that K/F is Galois. Suppose K/F is Galois. Let $\omega_1, \cdots, \omega_n$ be a basis for K/F. Then K/F is both separable and normal, hence for each j, we have $m_{\omega_j,F}(x)$ is separable and splits completely into linear factors over K (all roots are in K). Then let $g(x)$ be the polynomial obtained by removing any multiple factors in the product $\prod_{j=1}^{n} m_{\omega_j,F}(x)$. Then the splitting field of these two polynomials are the same. Since all roots are in K, so K contains the splitting field. But the splitting field contains $F(\omega_1, ..., \omega_n)$, hence contains K. Thus K is the splitting field of the separable polynomial $g(x) \in F[x]$. □

Compare this to Proposition 10.5, notice that when K/F is finite, the subset of separable polynomials in that proposition reduces to one.

Now we are ready to state the Fundamental Theorem of Galois Theory.

Theorem 12.7 (the Fundamental Theorem of Galois Theory)**.** *Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$. Then there is a bijective correspondence*

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \{\text{subfields } E \text{ of } K \text{ containing } F\} \xleftrightarrow{1:1} \{\text{subgroups } H \text{ of } G\} & H \\ | & & | \\ F & & G \end{array}$$

given by the maps

$$\begin{aligned} E &\longmapsto \mathrm{Gal}(K/E) \\ K^H &\longmapsfrom H \end{aligned}$$

which are inverses to each other. Under this correspondence, let the subextension E corresponds to the subgroup H.

1. *If the fields E_1, E_2 corresponds to the subgroups H_1, H_2, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$ (i.e. $\mathrm{Gal}(K/E_2) \leq \mathrm{Gal}(K/E_1)$).*

2. $[K:E] = |H|$ *and* $[E:F] = |G:H|$*, the index of* H *in* G*.*

3. K/E *is always Galois, with* $\mathrm{Gal}(K/E) = H$*.*

4. E/F *is Galois if and only if* H *is a normal subgroup in* G*. If this is the case, then we have*

$$\mathrm{Gal}(E/F) \cong G/H.$$

Proof. To prove the bijective correspondence, it suffices to prove that the given two maps are inverse to each other. That is, we want to prove

$$E = K^{\mathrm{Gal}(K/E)}, \quad H = \mathrm{Gal}(K/K^H). \tag{1}$$

It is clear that $E \subseteq K^{\mathrm{Gal}\ (k/E)}$. Hence we only need to show that $[K^{\mathrm{Gal}\ (K/E)} : E] = 1$. By Theorem 12.4, we have

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

And

$$[K:E] = [K : K^{\mathrm{Gal}(K/E)}][K^{\mathrm{Gal}\ K/E)} : E].$$

Combine these two equalities we see that $[K^{\mathrm{Gal}\ (K/E)} : E] = 1$. This proves the first equality in (1). Next, it is also easy to see that $H \leq \mathrm{Gal}\left(K/K^H\right)$. This is because the RHS is the Galois subgroup that fixes the subfield fixed by H, which obviously contain H. Hence our goal now is to Show $|H| = |\,\mathrm{Gal}\left(K/K^H\right)|$. Agin by Theorem 12.4, we have

$$|H| = [K : K^H] = |\,\mathrm{Gal}(K/K^H)|.$$

This proves the correspondence. Now we prove the subresults. Now, 1,2,3 are all straightforward to check under the correspondence, hence are left to the reader as exercise. The last statement takes a considerable amount of work.

This statement is equivalent to saying that K^H/F is Galois if and only if $H \trianglelefteq \mathrm{Gal}(K/F)$. If this is the case, then

$$\mathrm{Gal}(K^H/F) \cong \mathrm{Gal}(K/F)/H.$$

Now we shall prove this statement.

Consider $H \leq \mathrm{Gal}(K/F)$. Since K/F is Galois, it is separable, hence K^H/F is separable. We want to show that

$$K^H/F \textit{ is normal if and only if } H \textit{ is a normal subgroup of } \mathrm{Gal}(K/F).$$

Fix $\bar{F} = \bar{K}$. Then $F \subseteq K^H \subseteq K \subseteq \bar{F}$. By the equivalence condition, K^H/F is normal if and only if $\varphi(K^H) = K^H$ for all F-embeddings $\varphi : K^H \to \bar{F}$.

> Claim 1: $\varphi(K^H) = K^H$ for all F-embeddings $\varphi : K^H \to \bar{F}$ if and only if $\sigma(K^H) = K^H$ for all $\sigma \in \mathrm{Gal}(K/F)$.

We prove Claim 1. Given $\sigma \in \mathrm{Gal}(K/F)$, the map

$$\varphi : K^H \hookrightarrow K \xrightarrow{\sigma} K \hookrightarrow \bar{F}$$

is an F-embedding. Since $\varphi(K^H) = K^H$ by assumption, we have $\sigma(K^H) = \varphi(K^H) = K^H$. Conversely, given an F-embedding $\varphi : K^H \to \bar{F}$, apply Proposition 5.4 and we see that

$$\begin{array}{ccc} K^H & \xrightarrow{\varphi} & \bar{F} \\ \downarrow & \nearrow_{\exists\psi} & \\ K & & \end{array}$$

Hence φ extends to $\psi : K \to \bar{F}$. Since K/F normal, we have $\psi(K) = K$. Hence we can define $\sigma : K \to K$ by $\alpha \mapsto \psi(\alpha)$. Then we have $\sigma \in \mathrm{Gal}(K/F)$. Since by assumption $\sigma(K^H) = K^H$ we have $\varphi(K^H) = \sigma(K^H) = K^H$. This proves Claim 1.

Claim 2: $\sigma(K^H) = K^{\sigma H \sigma^{-1}}$.

We prove Claim 2. ($\subseteq$): Let $\alpha \in K^H$. Then for all $\tau \in H$, we have

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

The last step is because $\tau \in H$ and $\alpha \in K^H$. Hence $\sigma(\alpha)$ is fixed by $\sigma\tau\sigma^{-1}$ for all $\tau \in H$. This proves the inclusion. For ($\supseteq$): Let $\beta \in K^{\sigma H \sigma^{-1}}$. For all $\tau \in H$, we have

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

The last step is because $\beta \in K^{\sigma H \sigma^{-1}}$ and $\sigma\tau\sigma^{-1} \in \sigma H \sigma^{-1}$. Hence $\sigma^{-1}(\beta)$ is fixed by every $\tau \in H$. Hence $\sigma^{-1}(\beta) \in K^H$, therefore $\beta \in \sigma(K^H)$. This proves Claim 2.

Now, we have that

$$\begin{aligned} K/F \text{ is normal} &\iff \sigma(K^H) = K^H, \quad \forall \sigma \in \mathrm{Gal}(K/F) \\ &\iff K^{\sigma H \sigma^{-1}} = K^H, \quad \forall \sigma \in \mathrm{Gal}(K/F) && \text{[Claim 2]} \\ &\iff \sigma H \sigma^{-1} = H, \quad \forall \sigma \in \mathrm{Gal}(K/F) && \text{[Galois correspondence]} \\ &\impliedby H \trianglelefteq \mathrm{Gal}(K/F). \end{aligned}$$

Hence we have proved that K^H/F is normal if and only if H is a normal subgroup of $\mathrm{Gal}(K/F)$. Next, suppose $H \trianglelefteq \mathrm{Gal}(K/F)$, we have the following group homomorphism:

$$\begin{aligned} \Phi : \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(K^H/F) \\ \sigma &\longmapsto \sigma|_{K^H}. \end{aligned}$$

Notice that $\sigma(K^H) = K^H$ since H is normal in G. Now, $\sigma \in \ker\Phi$ of and only if σ fixes K^H, if and only if $\sigma \in \mathrm{Gal}(K/K^H)$ by the Galois correspondence. Hence we have $\ker\Phi = H$ and by the 1st isomorphism theorem

$$\mathrm{Gal}(K/F)/H \cong \mathrm{im}\,\Phi \leq \mathrm{Gal}(K^H/F).$$

Now, we have that

$$|\,\mathrm{im}\,\Phi| = |\,\mathrm{Gal}(K/F)/H| = \frac{|\,\mathrm{Gal}(K/F)|}{|H|} = \frac{[K:F]}{[K:K^H]} = [K^H:F] = |\,\mathrm{Gal}(K^H/F)|.$$

Hence Φ is surjective. And we have that

$$\mathrm{Gal}\left(K^H/F\right) \cong \mathrm{Gal}(K/F)/H.$$

Now, let $H = \mathrm{Gal}(K/E)$, then we have

$$\mathrm{Gal}(E/F) \cong G/H.$$

This concludes the proof of the Fundamental Theorem of Galois Theory. □

13 Finite Fields, Composite Extensions, Galois Closure, Primitive Element Theorem

In this section we discuss some applications of FTGT and how it is used to calculate Galois groups of finite fields extension and composite extension. We first briefly recall the existence and uniqueness of the finite field, which we discussed before.

We consider the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. It is separable since it is coprime to its derivative. Let α, β be two roots of $f(x)$, that is, $\alpha^{p^n} = \alpha$, and $\beta^{p^n} = \beta$. Then it is easy to see $(\alpha\beta)^{p^n} = \alpha\beta$, $(\alpha^{-1})^{p^n} = \alpha^{-1}, (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Hence all roots of $f(x)$ is a subfield $\mathbb{F}$ in its splitting field. But then $\mathbb{F}$ must be the splitting field, since $f(x)$ splits completely in $\mathbb{F}$ into linear factors. Since $|\mathbb{F}| = p^n$ and it is clear that $\mathbb{F}$ contains $\mathbb{F}_p$ (since $1 \in \mathbb{F}$ and raising to p^n power is a homomorphism), we have $[\mathbb{F} : \mathbb{F}_p] = n$. This shows the existence of finite field of degree n over $\mathbb{F}_p$.

Now suppose a finite field $\mathbb{F}$ of character p is of degree n over its prime subfield $\mathbb{F}_p$. Then this shows that $|\mathbb{F}| = p^n$. Hence $|\mathbb{F}^\times| = p^n - 1$. Let $\alpha \in \mathbb{F}^\times$, then by Lagrange's theorem $\alpha^{p^n-1} = 1$, that is $\alpha^{p^n} - \alpha = 0$. Thus all elements in $\mathbb{F}$ is a root of $f(x)$. Since $[\mathbb{F} : \mathbb{F}_p] = n$ is exactly the degree of the splitting field of $f(x)$ over $\mathbb{F}_p$, and we know $\mathbb{F}$ is contained in a splitting field of $f(x)$, it follows that $\mathbb{F}$ is a splitting field of $f(x)$, hence $\mathbb{F} \cong \mathbb{F}_{p^n}$.

Proposition 13.1. $\mathbb{F}_{p^n}/\mathbb{F}$ is Galois, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$, where $\sigma : \alpha \mapsto \alpha^p$ is the Frobenius endomorphism.

Proof. $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is obviously an injective homomorphism by the previous discussion, and is thus an isomorphism (automorphism) since its source and target has the same size. Then we have $\sigma^k(\alpha) = \alpha^{p^k}$. Then $\sigma^n(\alpha) = \alpha^{p^n} = \alpha$ is the identity map. And no other power lower than n can be the identity. Otherwise, say $l < n$ with σ^l being the identity, then $\alpha^{p^l} = \alpha$. Hence all elements of $\mathbb{F}_{p^n}$ are roots of $x^{p^l} - x$, which is impossible since the polynomial has only $p^l < p^n$ roots. Hence the claim follows. □

Now, we recap some peroperties of the cyclic group from 111A:

- All subgroup of a cyclic group is cyclic.
- Let $H = \langle x\rangle$. Then $|x^a| = \frac{n}{(n,a)}$. In particular, if $a|n$, then $|x^a| = \frac{n}{a}$.
- For every positive integer dividing $n = |H|$, there is a unique subgroup of H of order a, given by $\langle x^d\rangle$, where $d = \frac{n}{a}$.

- Subgroups of H corresponds bijectively with the positive divisors of $n = |H|$.

This shows that all subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$ is given by $\langle\sigma^d\rangle$, where $d|n$. And by the FTGT, all subextensions of $\mathbb{F}_{p^n}/\mathbb{F}_p$ are given by

$$\mathbb{F}_{p^n}^{\langle\sigma^d\rangle} = \{\alpha \in \mathbb{F}_{p^n} |\ \alpha^{p^d} = \alpha\} = \mathbb{F}_{p^d}$$

where $d|n$. Also, since $\langle\sigma^d\rangle \trianglelefteq \langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$, hence $\mathbb{F}_{p^d}/\mathbb{F}_p$ are Galois, for all $d|n$. And finally, by the FTGT, we have

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\langle\sigma^d\rangle = \langle\sigma\rangle/\langle\sigma^d\rangle \cong \mathbb{Z}/d\mathbb{Z},$$

as expected. This concludes our discussion of finite fields. Now we start our discussion of composite fields.

Definition 13.2. Let K_1, K_2 be subfields of K. Then their composite K_1K_2 is the smallest subfield of K containing both K_1 and K_2.

Proposition 13.3. It is not hard to check that:

1. $K_1K_2 = K_1(K_2) = K_2(K_1)$.
2. Let $F \subseteq K_1 \subseteq K$ and $F \subseteq K_2 \subseteq K$. Suppose $K_1 = F(S_1)$ for some $S_1 \subseteq K_1$ and $K_2 = F(S_2)$ for some $S_2 \subseteq K_2$. Then

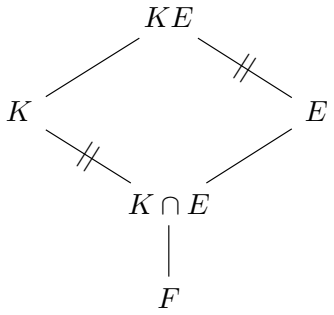
$$K_1K_2 = K_1(S_2) = K_2(S_1) = F(S_1 \cup S_2).$$

Proof. Exercise. □

Proposition 13.4. Let K/F be a Galois extension, and E/F be any finite extension. Then KE/E is galois and

$$\mathrm{Gal}(KE/E) \cong \mathrm{Gal}(K/K \cap E).$$

This can be expressed by the following diagram:



The two opposite sizes of the paralleogram of the diagram are Galois, and their Galois group are isomorphic.

Proof. Since $KE = E(K)$. Hence KE/E is normal if and only if $m_{\alpha,E}(x)$ splits completely over KE for all $\alpha \in K$. And KE/E is separable if and only if $m_{\alpha,E}(x)$ is separable for all $\alpha \in K$.

Now, since K/F is Galois, K/F is normal and separable. For normal, we get $m_{\alpha,F}(x)$ splits completely over K for all $\alpha \in K$. Thus $m_{\alpha,E}(x)$ splits completely over EK for all $\alpha \in K$ (since $m_{\alpha,E}(x)|m_{\alpha,F}(x)$ and $K \subseteq EK$). Hence EK/K is normal. Since K/F is separable, $m_{\alpha,F}(x)$ is separable for all $\alpha \in K$. Then $m_{\alpha,E}(x)$ is separable for all $\alpha \in K$ (again since $m_{\alpha,E}(x)|m_{\alpha,F}(x)$). Hence EK/E is separable. This shows that EK/E is Galois.

Now, given $\sigma \in \mathrm{Gal}(KE/E)$, the map

$$\varphi : K \hookrightarrow KE \xrightarrow{\sigma} KE \hookrightarrow \bar{F}$$

given by $\varphi : \alpha \mapsto \alpha \mapsto \sigma(\alpha) \mapsto \sigma(\alpha)$ is an F-embedding. Since K/F is Galois, $\sigma(K) = \varphi(K) = K$. Hence $\sigma|_K$ is an automorphism of K fixing $K \cap E$. Then we have the group homomorphism

$$\begin{aligned} \mathrm{Gal}(KE/E) &\longrightarrow \mathrm{Gal}(K/K \cap E) \\ \sigma &\longmapsto \sigma|_K. \end{aligned} \tag{*}$$

Suppose now σ is in the kernel of (*), then $\sigma|_K = 1_K$. Hence σ fixes both K and E, thus fixes KE. Thus $\sigma = 1_{KE}$. Thus (*) is injective.

Now we want to show (*) is surjective. Let H be the image of (*). Consider K^H. For all $\alpha \in K$, we have

$$\begin{aligned} \alpha \in K^H &\iff \sigma(\alpha) = \alpha, \quad \forall \sigma \in \mathrm{Gal}(KE/E) \\ &\iff \alpha \in (KE)^{\mathrm{Gal}(KE/E)} \\ &\iff \alpha \in E. \end{aligned}$$

In the second step, we used FTGT, which says $\mathrm{Gal}(KE/E) = E$. Hence $K^H = K \cap E$. Hence by FTGT, we have

$$H = \mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/K \cap E).$$

Hence (*) is surjective. Hence is an isomorphism. This proves the claim. □

Corollary 13.5. *If K/F is a Galois extension and E/F is any finite extension, then*

$$[KE : F] = \frac{[K : F][E : F]}{[K \cap E : F]}.$$

Proof. By the isomorphism of Galois group $[KE : E] = [K : K \cap E]$. □

Proposition 13.6. Let K_1, K_2 be Galois extensions of F. Then

1. $K_1 \cap K_2/F$ is Galois.
2. K_1K_2/F is Galois, with

$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) |\ \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\} \subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Proof. (1) Suppose $p(x) \in F[x]$ is an irreducible polynomial with a root $\alpha \in K_1 \cap K_2$. Since $\alpha \in K_1$ and K_1/F is normal, all roots of $p(x)$ lie in K_1 and similar for K_2. Hence all roots of $p(x)$ lies in $K_1 \cap K_2$. Hence $K_1 \cap K_2/F$ is normal by the equivalence conditions, and it is clearly separable, hence is Galois.

(2) Consider the map

$$\begin{aligned} \varphi : \mathrm{Gal}(K_1K_2/F) &\longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ \sigma &\longmapsto (\sigma|_{K_1}, \sigma|_{K_2}). \end{aligned}$$

This is a homomorphism. $\sigma \in \ker \varphi$ if and only if σ is trivial on both K_1, K_2, which is true if and only if σ fixes K_1K_2. Hence φ is injective. Now, the image clearly lies in the subgroup $H = \{(\sigma, \tau) |\ \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$, since

$$\left(\sigma|_{K_1}\right)\big|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2} = \left(\sigma|_{K_2}\right)\big|_{K_1 \cap K_2}.$$

Now we compute the order of H. Notice that for every $\sigma \in \mathrm{Gal}(K_1/F)$ there are $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ elements $\tau \in \mathrm{Gal}(K_2/F)$ whose restriction to $K_1 \cap K_2$ is the same as σ. The reason is: Suppose we have found one $\tau \in \mathrm{Gal}(K_2/F)$ such that $\sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$. Then $\tau' \in \mathrm{Gal}(K_2/F)$ such that $\tau'|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$ if and only if $\tau(\tau')^{-1} = 1_{K_1 \cap K_2}$, if and only if $\tau(\tau')^{-1} \in \mathrm{Gal}(K_2/K_1 \cap K_2)$, if and only if $\tau' = \tau h$ for some $h \in \mathrm{Gal}(K_2/K_1 \cap K_2)$. Thus there are $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ for τ'. Hence

$$|H| = |\mathrm{Gal}\,(K_1/F)| \cdot |\mathrm{Gal}\,(K_2/K_1 \cap K_2)| = |\mathrm{Gal}\,(K_1/F)| \, \frac{|\mathrm{Gal}\,(K_2/F)|}{|\mathrm{Gal}\,(K_1 \cap K_2/F)|}.$$

By the previous corollary

$$|H| = |\,\mathrm{Gal}(K_1K_2/F)| = [K_1K_2 : F] = \frac{[K_1 : F]\,[K_2 : F]}{[K_1 \cap K_2 : F]}.$$

Hence φ is surjective and the proof is completed. □

Our final goal in this section is to prove the so called primitive element theorem. To do that, we need some preparation. Recall that an extension K/F is simple if $K = F(\theta)$ for some element θ, where θ is called a primitive element for K.

Proposition 13.7. The finite field $\mathbb{F}_{p^n}$ is simple over $\mathbb{F}_p$. In particular, there is an irreducible polynomial of degree n over $\mathbb{F}_p$ for every $n \geq 1$.

Proof. $\mathbb{F}_{p^n}^{\times}$ if a finite subgroup of the multiplicative group of a field, hence is cyclic (from 111B, proposition 9.18 in the book). If θ is the generator then $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. □

Proposition 13.8. Let K/F be a finite extension. Then $K = F(\theta)$ if and only if there exist only finitely many subfields of K containing F.

Proof. Suppose $K = F(\theta)$ is simple. Let E/F be a subextension of K/F. Then $m_{\theta,E}(x) | m_{\theta,F}(x)$ in $E[x]$. Let E' be the field generated over F by the coefficients of $m_{\theta,E}(x)$. Then $E' \subseteq E$ and clearly $m_{\theta,E'}(x) = m_{\theta,E}(x)$, since $m_{\theta,E}(x) \in E'[x]$ and has θ as a root, which is monic and irreducible. Now, $K = F(\theta) = E(\theta) = E'(\theta)$. Hence

$$[K : E] = \deg m_{\theta,E}(x) = [K : E'].$$

This implies that $E = E'$. Hence subfields of K containing F are generated by the coefficients of monic factors of $m_{\theta,F}(x)$. Hence there are finitely many such subextensions.

Conversely, there are finitely many subextensions of K/F. If F is a finite field then the previous proposition proves the claim. Otherwise, suppose F is infinite. Then since K/F is finite, $K = F(S)$ with S being a set of finitely many algebraic elements over F. Hence it suffices to show that $F(\alpha, \beta)$ is generated by a single element over α. Consider the subfields

$$F(\alpha + c\beta) \qquad c \in F.$$

Since there are infinitely many choices of $c \in F$ and only finitely many subfields, there exists $c, c' \in F$ with $c \neq c'$ such that

$$F(\alpha + c\beta) = F(\alpha + c'\beta).$$

Hence $\alpha + c\beta, \alpha + c'\beta \in F(\alpha + c\beta)$. Thus $(c - c')\beta \in F(\alpha + c\beta)$. Hence $\beta \in F(\alpha + c\beta)$. Therefore we also have $\alpha \in F(\alpha + c\beta)$. Hence $F(\alpha, \beta) \subseteq F(\alpha + c\beta)$. The reverse containment is obvious hence this proves that

$$F(\alpha, \beta) = F(\alpha + c\beta).$$

And the claim follows. □

Corollary 13.9. *Let E/F be any finite separable extension. Then E/F is contained in a Galois extension K/F, and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K. We call such K a Galois closure of F.*

Proof. Such K exists. Let $\omega_1, ..., \omega_n$ be an F-basis for E. Then $m_{\omega_1,F}(x), ..., m_{\omega_n,F}(x)$ are all separable since E/F is separable. Then let $K_1', ..., K_n'$ be the splitting field of $m_{\omega_1,F}(x), ..., m_{\omega_n,F}(x)$. Hence they are all Galois over F since they are splitting fields of separable polynomials over F. Then the composition $K' = K_1'K_2' \cdots K_n'$ is Galois over F. Then K is the intersection of all Galois extensions F containing E. □

Theorem 13.10 (The Primitive Element Theorem)**.** *If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.*

Proof. Let L be the Galois closure of K/F. Then any subextension of K/F corresponds to a subgroup of $\mathrm{Gal}(L/F)$. Since there are only finitely many subgroups, by the previous proposition, K/F is simple. Finally, any finite extension of fields in characteristic 0 is separable. □

We end this section with one last proposition of Galois closure, the proof is omitted. See the lecture notes for detail.

Proposition 13.11. Let K/F be a separable extension and $F \subseteq K \subseteq \bar{F}$. Suppose $K = F(S)$ with $S \subseteq K$. Let $S' \subseteq \bar{F}$ be the subset consisting of all roots of $m_{\alpha,F}(x)$ for all $\alpha \in S$. Then

1. $F(S')$ is a Galois closure of K/F.
2. If L is a Galois closure of K/F then $L \cong F(S')$. If $L \subseteq \bar{F}$ then $L = F(S')$.
3. $F(S') = \bigcap_{L/F \text{ Galois }, L \subseteq \bar{F}} L$.

14 Cyclotomic Extension

In this section, we are concerned with extensions involving roots of unity. We first make some quick definitions and observations about roots of unity.

- As we have already seen, $\mu_n = \{1, \zeta_n, ..., \zeta_n^{n-1}\}$ is a multiplicative group and is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ given by the isomorphic $\zeta_n^k \mapsto \bar{k}$.
- We see that $|\zeta_n^k| = \frac{n}{(n,k)}$. Hence $|\zeta_n^k| = n$ if and only if $(n,k) = 1$. If ζ is an nth root of unity of order n, then we call it a *primitive nth root of unity*. Hence the number of primitive nth roots of unity is $|(\mathbb{Z}/n\mathbb{Z})^\times|$, where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} |\ (a,n) = 1\}.$$

- If $d|n$, and ζ is a dth root of unity, then ζ is also an nth root of unity, since $\zeta^n = (\zeta^d)^{n/d} = 1$. Hence $\mu_d \subseteq \mu_n$ for all $d|n$.

Definition 14.1. Define the nth cyclotomic polynomial $\Phi_n(x)$ be the polynomial whose roots are the primitive nth roots of unity:

$$\Phi_n(x) = \prod_{\zeta \text{ primitive in } \mu_n} (x - \zeta) = \prod_{1 \le a \le n,\ (a,n)=1} (x - \zeta_n^a).$$

Now we show how to calculate the cyclotomic polynomials. Notice that

$$x^n - 1 = \prod_{\substack{\zeta^n = 1 \\ \text{i.e. } \zeta \in \mu_n}} (x - \zeta).$$

We can group together $(x - \zeta)$ where ζ is of order d in μ_n, that is, ζ is a primitive dth root of unity. Then we get

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta) = \prod_{d|n} \Phi_d(x).$$

Hence we can calculate Φ_d recursively.

Lemma 14.2. *$\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.*

Proof. Clearly $\Phi_n(x)$ is is monic and has degree $\varphi(n)$. It is clear that $\Phi_1(x) = x - 1$ has coefficients in $\mathbb{Z}$. Suppose $\Phi_d(x) \in \mathbb{Z}[x]$ for $1 \le d < n$. Then $x^n - 1 = f(x)\Phi_n(x)$ where $f(x) = \prod_{d|n, d<n} \Phi_d(x)$ is monic and has coefficients in $\mathbb{Z}$. Since $f(x)$ divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$, and both $f(x), x^n - 1$ has coefficients in $\mathbb{Q}$. But the uniqueness of the quotient and remainder in the division algorithm of polynomials, we see that $\Phi_n(x) \in \mathbb{Q}[x]$. Then by Gauss' Lemma, there exists $r, s \in \mathbb{Z}$ such that $rf(x), s\Phi_n(x) \in \mathbb{Z}$ and $x^n - 1 = rsf(x)\Phi_n(x)$. It is clear that $r = s = 1$ due to monicity. This proves that $\Phi_n(x) \in \mathbb{Z}[x]$. □

Theorem 14.3. *$\Phi_n(x)$ is irreducible.*

Proof. If not, then we have a factorization

$$\Phi_n(x) = f(x)g(x) \quad \text{with } f(x), g(x) \text{ monic in } \mathbb{Z}[x].$$

We can take $f(x)$ to be an irreducible factor of $\Phi_n(x)$. Let ζ be a primitive nth root of of unity which is a root of $f(x)$ (so f is the minimal polynomial for ζ over $\mathbb{Q}$). Let p denote any prime not dividing n, then ζ^p is again a primitive nth root of unity, hence is a root of either $f(x)$ or $g(x)$.

Suppose $g(\zeta^p) = 0$. Then ζ is a root of $g(x^p)$ and since $f(x)$ is the minimal polynomial of ζ, we have $f(x)|g(x^p)$ in $\mathbb{Z}[x]$. Say

$$g\left(x^p\right) = f(x)h(x), \quad h(x) \in \mathbb{Z}[x].$$

We can reduce this equation mod p and get

$$\bar{g}\left(x^p\right) = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x].$$

Since $\bar{g}\left(x^p\right) = (\bar{g}(x))^p$, we have

$$(\bar{g}(x))^p = \bar{f}(x)\bar{h}(x)$$

in the UFD $\mathbb{F}_p[x]$. Hence $\bar{f}(x)$ and $\bar{g}(x)$ have a factor in common in $\mathbb{F}_p[x]$. And by reducing $\Phi_n(x) = f(x)g(x)$ in $\mathbb{F}_p[x]$ we see that $\bar{\Phi}_n(x)$ has a multiple root, hence $x^n - 1$ would have a multiple root in $\mathbb{F}_p[x]$, which is a contradiction.

Hence ζ^p must be a root of $f(x)$. Since this applies to every root ζ of $f(x)$, it follows that ζ^a is a root of $f(x)$ for every $(a, n) = 1$. We can write $a = p_1 p_2 \cdots p_k$ as a product of primes not dividing n. So ζ^{p_1} is a root of $f(x)$, and $(\zeta^{p_1})^{p_2}$ is also a root... hence ζ^a is also a root of $f(x)$. But since raising to ath power only permutes primitive roots of unity, it follows that every primitive roots of unity is a root of $f(x)$. Hence $f(x) = \Phi_n(x)$ is irreducible. □

Theorem 14.4. *$\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, and* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. We see that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. The isomorphism is given explicitly by

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right) \\ a(\mathrm{mod} n) &\longmapsto \sigma_a \end{aligned}$$

where

$$\sigma_a\left(\zeta_n\right) = \zeta_n^a.$$

□

Example 14.5. In this section we study the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, where p is an odd prime. It is clear that the elements

$$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}, \zeta_p^{p-1}$$

form a basis of $\mathbb{Q}(\zeta_p)$. Every element is the Galois group simply permutes these basis elements since these are precisely the pth root of unity.

Let H be a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. We want to find the subfield of $\mathbb{Q}(\zeta_p)$ fixed by H. Consider the element

$$\alpha_H = \sum_{\sigma \in H} \sigma\zeta_p.$$

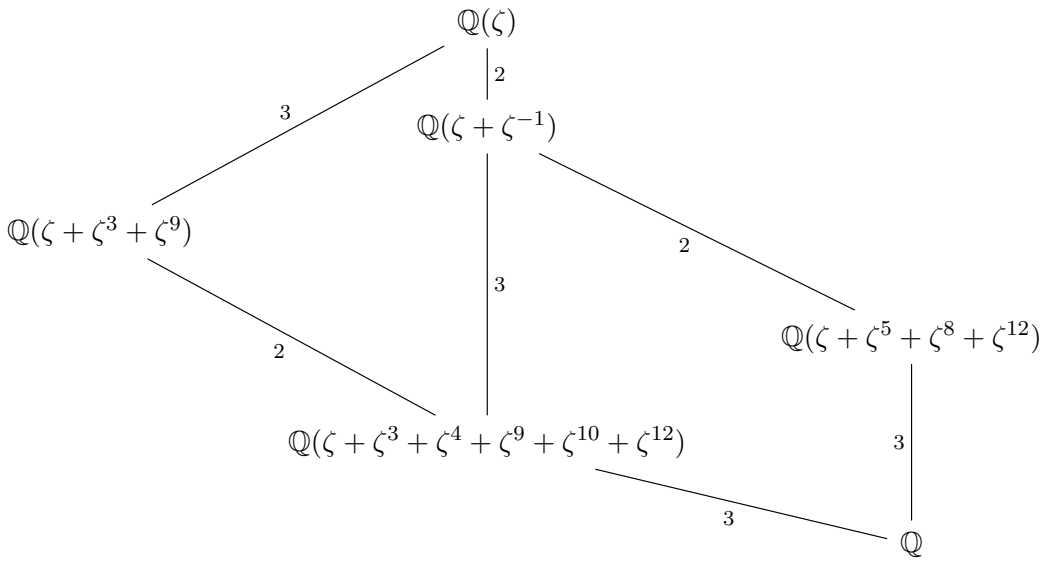
We will denote it by α from now on, since the subgroup is clear. For any $\tau \in H$, the element $\tau\sigma$ run over the elements of H as σ runs over the elements of H. It follows that $\tau(\alpha) = \alpha$. So α lies in the fixed field of H. Thus $\mathbb{Q}(\alpha)$ is fixed by H.

We claim that $\mathbb{Q}(\alpha)$ is precisely the fixed field of H. By the FTGT, $\mathbb{Q}(\alpha)$ is the fixed field of H if and only if $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha) = H$. Suppose this is not the case and denote $K = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha)$. Then $H < K$ (H is a proper subgroup of K). Hence there exists $\tau \in K$ such that $\tau \notin H$. Now, if $\tau \notin H$, then $\tau\alpha$ is the sum of basis elements, one of which is $\tau(\zeta_p)$. If we had $\tau\alpha = \alpha$ then since these elements are a basis, we must have $\tau(\zeta_p) = \sigma(\zeta_p)$ for one of the terms $\sigma\zeta_p$ in α. But this implies that $\tau\sigma^{-1}(\zeta_p) = \zeta_p$ and therefore $\tau\sigma^{-1} = 1$, then $\tau = \sigma \in H$, a contradiction. Hence $\mathbb{Q}(\alpha)$ is precisely the fixed field of H.

For a specific example, consider $\mathbb{Q}(\zeta_{13})$, whose Galois group is $(\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/12\mathbb{Z}$. A generator for this cyclic group is $\sigma = \sigma_2$ which maps $\zeta_{13} \mapsto \zeta_{13}^2$. The nontrivial subgroups corresponds to divisors of 12, which are 2,3,4,6 whose corresponding generators are $\sigma^6, \sigma^4, \sigma^3, \sigma^2$. The corresponding fixed fields will be degrees 6,4,3,2 over $\mathbb{Q}$. Let $\zeta = \zeta_{13}$, then the corresponding generators of the fixed field is

$$\begin{aligned}
\zeta + \sigma^6\zeta &= \zeta + \zeta^{2^6} = \zeta + \zeta^{-1} \\
\zeta + \sigma^4\zeta + \sigma^8\zeta &= \zeta + \zeta^{2^4} + \zeta^{2^8} = \zeta + \zeta^3 + \zeta^9 \\
\zeta + \sigma^3\zeta + \sigma^6\zeta + \sigma^9\zeta &= \zeta + \zeta^8 + \zeta^{12} + \zeta^5 \\
\zeta + \sigma^2\zeta + \sigma^4\zeta + \sigma^6\zeta + \sigma^8\zeta + \sigma^{10}\zeta &= \zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}.
\end{aligned}$$

The corresponding lattice is given by:



We end this section with one more corollary, whose proof is given in the book (pg.598):

Corollary 14.6. *Let $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ be the prime factorization of the positive integer n. Then the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ for $i = 1, ..., k$ intersects only in $\mathbb{Q}$ and their composite is the cyclotomic field $\mathbb{Q}(\zeta_n)$. We have*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}}))$$

and under the isomorphism is the Chinese Remainder Theorem:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^\times \times \cdots \times \left(\mathbb{Z}/p_k^{a_k}\mathbb{Z}\right)^\times.$$

15 Solvable Groups, Radical Extensions, Insolvability of the Quintic

In this section, we discuss the solvability of polynomials and how they are associated with the Galois group of the polynomial. The symbol $\sqrt[n]{a}$ for $a \in F$ will denote any root of the polynomial $x^n - a \in F[x]$. We say an extension K/F is cyclic if it is Galois and its Galois group is a cyclic group.

Proposition 15.1. Let F be a field of characteristic not dividing n and $\zeta_n \in F$. Then $F(\sqrt[n]{a})/F$ is cyclic with degree dividing n for $a \in F$. We call such an extension a simple radical extension.

Proof. $K = F(\sqrt[n]{a})/F$ is Galois since $F(\sqrt[n]{a})$ is the splitting field of the separable polynomial $x^n - a \in F[x]$. Then for any $\sigma \in \mathrm{Gal}(K/F)$ we have $\sigma(\sqrt[n]{a})$ is another root of $x^n - a$. Hence $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some nth root of unity ζ_σ. Then the homomorphism is given by

$$\begin{aligned} \mathrm{Gal}(K/F) &\to \mu_n \\ \sigma &\mapsto \zeta_\sigma. \end{aligned}$$

Since F contains μ_n, every element in μ_n is fixed by elements in the Galois group. Hence

$$\sigma\tau(\sqrt[n]{a}) = \sigma\left(\zeta_\tau \sqrt[n]{a}\right) = \zeta_\tau\sigma(\sqrt[n]{a}) = \zeta_\tau\zeta_\sigma \sqrt[n]{a} = \zeta_\sigma\zeta_\tau \sqrt[n]{a}.$$

Hence the map is indeed an homomorphism. It is injective, since the kernel is precisely the automorphism fixing $\sqrt[n]{a}$, hence is the identify. This gives an injective homomorphism and $\mathrm{Gal}(K/F)$ is isomorphic to a cyclic group with order dividing n. □

Proposition 15.2. Any cyclic extension of degree n over a field F of characteristic not dividing n which contains ζ_n is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

Proof. Let the Galois group $G = \mathrm{Gal}(K/F) = \{1, \sigma, ..., \sigma^{n-1}\}$. Then by the linear independence of $1, \sigma, ..., \sigma^{n-1}$, there exists $\alpha \in K$ such that

$$\beta = \alpha + \zeta_n\sigma(\alpha) + \zeta_n^2\sigma^2(\alpha) + \cdots + \zeta_n^{n-1}\sigma^{n-1}(\alpha) \neq 0.$$

Then applying σ to it we find that

$$\begin{aligned} \sigma(\beta) &= \sigma\alpha + \zeta_n\sigma^2(\alpha) + \zeta_n^2\sigma^3(\alpha) + \cdots + \zeta_n^{n-1}\sigma^n(\alpha) \\ &= \sigma\alpha + \zeta_n\sigma^2(\alpha) + \zeta_n^2\sigma^3(\alpha) + \cdots + \zeta_n^{-1}\alpha \\ &= \zeta_n^{-1}\left(\alpha + \zeta_n\sigma(\alpha) + \zeta_n^2\sigma^2(\alpha) + \cdots + \zeta_n^{n-1}\sigma^{n-1}(\alpha)\right) \\ &= \zeta_n^{-1}\beta. \end{aligned}$$

Thus we have

$$\sigma\left(\beta^n\right) = \sigma(\beta)^n = \left(\zeta_n^{-1}\beta\right)^n = \beta^n.$$

Hence β^n is fixed by σ. Therefore, $\beta^n \in F$. Since K/F is Galois, $K/F(\beta)$ is Galois. And

$$\mathrm{Gal}(K/F(\beta)) = \{\sigma^j \mid \sigma^j(\beta) = \beta\} = \{\sigma^j \mid \zeta_n^{-j}\beta = \beta\} = \{1\}.$$

Therefore,

$$[K : F(\beta)] = |\,\mathrm{Gal}(K/F(\beta))| = 1.$$

Hence $F(\beta) = K$. Let $a = \beta^n \in F$. Then $K = F(\sqrt[n]{a})$. □

Now we digress from field extensions and introduce the notion of solvable groups from group theory.

Definition 15.3. A finite group G is called solvable if there exists a chain of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_k = \{1\}$$

such that $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is cyclic form all $0 \leq i \leq k-1$.

Example 15.4. Here are some examples of solvable groups:

1. Any finite abelian group is solvable, since every finite abelian group is a direct product of cyclic groups.
2. The dihedral group D_{2n} is solvable, since the subgroup $G_1 = \langle r \rangle$ is cyclic and the quotient group D_{2n}/G_1 is also cyclic (it has order 2 and is generated by s).
3. The symmetric group S_4 is solvable, via the chain $S_4 \geq A_4 \geq V_4 \geq \langle (12)(34) \rangle \geq \{1\}$, where $V_4 = \langle (12)(34), (13)(24) \rangle$.
4. Any non-cyclic simple group is not solvable, because it has no nontrivial normal subgroups (and thus there is no way to start the chain).
5. Finite p-groups are solvable, as are finite nilpotent groups, and direct and semidirect products of solvable groups.

Proposition 15.5. We exhibit some fundamental properties of solvable groups without proofs:

1. If G is solvable, then any subgroup H is solvable and any quotient group G/N is solvable.
2. If N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.
3. G is solvable if and only if there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{1\}$ such that $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian form all $0 \leq i \leq k-1$.

Now that we have characterized the extensions obtained by adjoining nth roots of individual elements, we can give a precise definition for solving an equation in radicals:

Definition 15.6. If $\alpha \in F$, we say α can be expressed in radicals if α is an element of some tower of simple radical extensions: Namely, if there exists extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_d = K$$

such that $\alpha \in K$ and K_{i+1}/K_i is a simple radical extension for all i. We call K/F a root extension. A polynomial can be solved by radicals if all its roots can be solved in terms of radicals.

If α is in a root extension, then α can be obtained by successive algebraic operations $(+, -, \times, \cdot/\cdot, \sqrt{\cdot})$. For example, consider the element

$$\alpha = -1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}.$$

Then α belongs to an root extension given by

$$\begin{aligned}
&K_0 = \mathbb{Q} \\
&K_1 = K_0(\sqrt{a_0}) && a_0 = 17 \\
&K_2 = K_1(\sqrt{a_1}) && a_1 = 2(17 - \sqrt{17}) \\
&K_3 = K_2(\sqrt{a_2}) && a_2 = 2(17 + \sqrt{17}) \\
&K_4 = K_3(\sqrt{a_3}) && a_3 = 17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}.
\end{aligned}$$

We first make some observation about root extensions:

- The composite of two root extensions of F is also a root extension of F. specifically, if $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$ and $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$ are two towers of simple radical extensions, then

  $$F = K_0L_0 \subseteq K_1L_0 \subseteq K_2L_0 \subseteq \cdots \subseteq K_dL_0 \subseteq K_dL_1 \subseteq \cdots \subseteq K_dL_k = KL$$

  is again a tower of simple radical extensions.

- Also, if α can be expressed in radicals and $\sigma(\alpha)$ is any Galois conjugate, then $\sigma(\alpha)$ can also be expressed in radicals, because

  $$F = K_0 \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_d) = \sigma(K)$$

  is a tower of simple radical extensions. This is because $\sigma K_{i+1}/\sigma K_i$ is a simple radical extension, since it is generated by the element $\sigma(\sqrt[n_i]{a_i})$, which is a root of the equation $x^{n_i} - \sigma(a_i)$.

Lemma 15.7. *If α is contained in a root extension K in the definition above (expressable by radicals), it is then contained in a root extension which is Galois over F and where each intermediate extension is cyclic.*

Proof. Let L be the Galois closure of K/F. For any $\sigma \in \mathrm{Gal}(L/F)$, we have the chain of subfields

$$F = \sigma K_0 \subset \sigma K_1 \subset \cdots \subset \sigma K_i \subset \sigma K_{i+1} \subset \cdots \subset \sigma K_s = \sigma K,$$

which is a root extension by the observation above. And since the composition of two root extensions is again a root extension, we have that the compositions of all the conjugate fields $\sigma(K)$ is again a root extension. And we have proved in HW7 that

$$L = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(K) = \sigma_1(K) \cdots \sigma_n(K).$$

Hence L is a Galois root extension containing α.

Now, adjoin F with all n_ith roots of unity with n_i defined by $L_{i+1} = L_i(\sqrt[n_i]{a_i})$. This gives a field F'. Now composite this field with the obtained Galois root extension:

$$F \subseteq F' = F'L_0 \subseteq F'L_1 \subseteq \cdots \subseteq F'L_i \subseteq F'L_{i+1} \subseteq \cdots \subseteq F'L_s = F'L.$$

The field $F'L$ is Galois since it is the composition of two Galois extensions L and F' (F' is the splitting field of the separable polynomial $x^{n_1 n_2 \cdots n_s} - 1$) over F. Then extension F'/F can be written as a chain of cyclic extension (Any abelian extension can be given as a chain of cyclic extension, since every abelian group has a chain of subgroups such that the adjacent quotient is cyclic). And each $F'L_{i+1}/F'L_i$ is a simple radical extension with all roots of unity in the base field, so is a cyclic extension by the proposition in the beginning. Hence this is the desired extension. □

Theorem 15.8. *A polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.*

Proof. Suppose $f(x)$ can be solved by radicals. Then each root of $f(x)$ is contained in an extension as in the lemma. The composition L of such extension is again the same type.

> Reason: By induction, we only need to show that if $F = K_0 \subset K_1 \subset ... \subset K_n$ and $F = L_0 \subset ... \subset L_m$ are two chains such that $K_{j+1}/K_j, L_{i+1}/L_i$ are Galois with cyclic Galois group, then there is such a chain for K_nL_m.
>
> One can consider the chain $F = K_0 \subset K_1 ... \subset K_n = K_nL_0 \subset K_nL_1 \subset K_nL_2 \subset ...K_nL_m$. Then K_nL_{i+1}/K_nL_i is Galois with Galois group a subgroup of $\mathrm{Gal}(L_{i+1}/L_i)$ because $K_nL_{i+1} = (K_nL_i)L_{i+1}$ and L_{i+1}/L_i is Galois. (Apply Prop 19 to $K = L_{i+1}, F = L_i, F' = K_nL_i$.)

Let G_i be the subgroups corresponding to the subfields K_i, $i = 0, 1, ..., s-1$. Since

$$\mathrm{Gal}\,(K_{i+1}/K_i) = G_i/G_{i+1} \quad i = 0, 1, \ldots, s-1$$

it follows that the Galois group $G = \mathrm{Gal}(L/F)$ is a solvable group. The field L contains the splitting field of $f(x)$ so the Galois group of $f(x)$ is a quotient group of the solvable group G, hence is solvable.

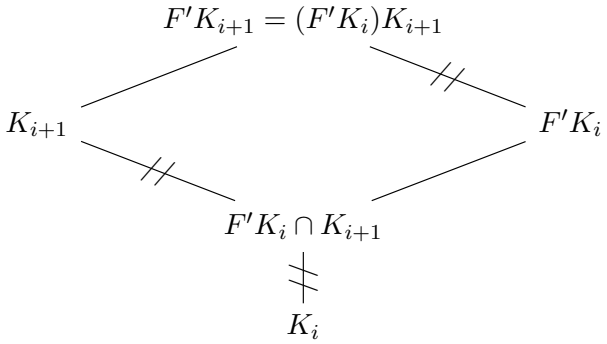
Suppose now that the Galois group G of $f(x)$ is a solvable group and let K be the splitting field for $f(x)$. Taking the fixed field of the subgroup for G gives a chain

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K$$

where $K_{i+1}/K_i, i = 0, 1, \ldots, s-1$ is a cyclic extension of degree n_i. Again let F' be the cyclotomic field over F adjoining all roots of unity of order n_i. And denote $K_i' = F'K_i$. We obatina sequence of extensions

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_i \subseteq F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K.$$

The extension $F'K_{i+1}/F'K_i$ is cyclic of degree dividing n_i. We can see this from the following diagram:



Since K_{i+1}/K_i is cyclic, hence so is any intermediate extension. Then by the proposition on composite field, we have that $F'K_{i+1}/F'K_i$ is cyclic of degree dividing n_i. Then it follows that each of these cyclic extension is a simple radical extension, and $f(x)$ can be solved by radicals. □

Now we discuss the solvability of the general polynomial of degree n. Our discussion culminate in the insolvability of the quintic. Before that, we need a lemma:

Lemma 15.9. *Let K be the splitting field of a degree n polynomial $f(x) \in F[x]$. Then $[K : F] \leq n!$.*

Proof. See lecture note 5 (Apr 13). □

Definition 15.10. Let $x_1, ..., x_n$ be indeterminates. The elementary symmetric functions $s_1, ..., s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

That is, s_i is the sum of all products of x_j's taken i at a time.

Definition 15.11. The general polynomial of degree n is the polynomial

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

whose roots are the indeterminates $x_1, ..., x_n$. It is easy to check that the coefficients of the general polynomial of degree n are given by elementary symmetric functions in the roots:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n.$$

Theorem 15.12. *Let $F(x_1, ..., x_n)$ be the splitting field of the general polynomial whose roots are $x_1, ..., x_n$. Let $F(s_1, ..., s_n)$ be the field generated by $s_1, ..., s_n$ over F. Then the extension $F(x_1, ..., x_n)/F(s_1, ..., s_n)$ is Galois with*

$$\mathrm{Gal}(F(x_1, ..., x_n)/F(s_1, ..., s_n)) \cong S_n.$$

Proof. For any field F, the extension $F(x_1, ..., x_n)/F(s_1, ..., s_n)$ is Galois, since it is the splitting field of the general polynomial of degree n.

Let $\sigma \in S_n$. Then σ acts on $F(x_1, ..., x_n)$ by permuting the subscripts of the variables $x_1, ..., x_n$. Clearly this gives an automorphism of $F(x_1, ..., x_n)$. Identifying $\sigma \in S_n$ with this automorphism of $F(x_1, ..., x_n)$ identifies S_n as a subgroup of $\mathrm{Aut}(F(x_1, ..., x_n))$.

It is obvious from the definition that elementary symmetric functions $s_1, ..., s_n$ are fixed under any permutation of their subscripts. Hence $F(s_1, ..., s_n)$ is contained in the fixed field of S_n. By the FTGT, the fixed field of S_n has index precisely $n!$ in $F(x_1, ..., x_n)$. Then combining this observation with the previous lemma we have

$$n! = [F(x_1, ..., x_n) : F(x_1, ..., x_n)^{S_n}] \leq [F(x_1, ..., x_n) : F(s_1, ..., s_n)] \leq n!$$

and therefore $F(s_1, ..., s_n)$ is precisely the fixed field of S_n in $F(x_1, ..., x_n)$. Also, this shows that $[F(x_1, ..., x_n) : F(s_1, ..., s_n)] = n!$ which is precisely the order of S_n. Hence we conclude that

$$\mathrm{Gal}(F(x_1, ..., x_n)/F(s_1, ..., s_n)) \cong S_n.$$

□

Theorem 15.13. *A_n is simple for all $n \geq 5$.*

We omit the proof since this is a technical result from group theory which distracts us from our main goal. Instead, we refer reader to Dummit and Foote, section 4.6, pg. 149.

Corollary 15.14. *The general equation of degree n cannot be solved by radicals for $n \geq 5$.*

Proof. The general polynomial of degree n has Galois group isomorphic to S_n. If S_n is solvable, then every subgroup of S_n is solvable. In particular, A_n is solvable. Since A_n is simple and noncyclic for all $n \geq 5$, by Example 15.4 we see that A_n is not solvable. Hence S_n is not solvable for $n \geq 5$. Thus the claim follows from Theorem 15.8. □

Remark 15.15. We have seen that the Galois group of a general polynomial of degree n is isomorphic to S_n. But given an arbitrary specific polynomial, like $x^8 - 2$, this is not the case. All we know is that the Galois group is a subgroup of S_n (in this case a subgroup of S_8). This is because there are certain algebraic relations among the generators of the splitting field. In this case, the splitting field is $\mathbb{Q}(\sqrt[8]{2}, \zeta_8)$. And notice that

$$(\sqrt[8]{2})^4 = \sqrt{2} = \zeta_8 + \zeta_8^7.$$

Such algebraic relation suggests that one cannot specify the images of the generators independenly, their images must again satisfy the same algebraic relation. Hence many elements of S_n are no longer qualified as automorphisms since they do not repsect this algebraic relation, hence not a homomorphism.

What we are saying here is that if there are no relations among the roots of a polynomial of degree n (in other words, we are searching for a general formula of roots of polynomials of degree n), then the Galois group is exactly S_n.