Field and Galois Theory

Labix

May 9, 2025

Abstract

References

- Abstract Algebra by David S. Dummit and Richard M. Foote
- Field and Galois Theory by P. Morandi

Contents

1 Field Extensions **3**
- 1.1 Basics of Field Extensions . . . 3
- 1.2 Finitely Generated Field Extensions . . . 3
- 1.3 Algebraic Elements . . . 4
- 1.4 Algebraic Extensions . . . 6

2 More on Field Homomorphisms **8**
- 2.1 Homomorphisms that Fixes Subfields . . . 8
- 2.2 The Norm and Trace Map . . . 10

3 Special Field Extensions **12**
- 3.1 Splitting Extensions . . . 12
- 3.2 Algebraically Closed Fields . . . 14
- 3.3 Normal Extensions . . . 14
- 3.4 Separable Extensions . . . 16

4 The Galois Correspondence **17**
- 4.1 The Fixed Field of Automorphisms . . . 17
- 4.2 Galois Extensions . . . 18
- 4.3 The Inclusion Reversing Bijection . . . 19
- 4.4 Application: Biquadratic Extensions . . . 20

5 Finite Field Theory **23**
- 5.1 Existence and Uniqueness of Finite Fields . . . 23
- 5.2 Galois Theory for Finite Fields . . . 23

6 Cyclotomic Fields and Polynomials **26**
- 6.1 Cyclotomic Polynomials . . . 26
- 6.2 Cyclotomic Fields . . . 26

7 Radial and Soluble Extensions **27**
- 7.1 Radical Extensions . . . 27

8 Transcendental Extensions **28**
- 8.1 Transcendence Basis . . . 28
- 8.2 Transcendence Degree . . . 29
- 8.3 Linear Disjointness . . . 29

1 Field Extensions

1.1 Basics of Field Extensions

Definition 1.1.1: Field Extensions

Let F, K be fields such that K contains F as a subfield. Then we say that K is a field extension of F and we write it as $F < K$.

If $F < L < K$ are field extensions then we say that L is the intermediate field of the extension $F < K$.

Proposition 1.1.2

If K is an extension of F, then K is a vector space over F.

Proof. Define the action of F on K by simply left multiplication. Then the axioms of a vector space is satisfied through properties of F as a field. □

Definition 1.1.3: Degree of an Extension

Let K/F be a field extension. The degree of K/F, denoted

$$[K : F]$$

is the dimension of K as a vector space over F. It is said to be finite if $[K : F]$ is finite and infinite otherwise.

Proposition 1.1.4: The Tower Law

Let $F < K < E$ be field extensions. Then

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

Moreover, if $\{a_i | i \in I\}$ is a basis for E over K and $\{b_j | j \in J\}$ is a basis for K over F then

$$\{a_i b_j | i \in I, j \in J\}$$

is a basis for E over F.

Definition 1.1.5: Finite Extensions

Let K/F be a field extension. We say that K/F is a finite extension if $[K : F]$ is finite.

1.2 Finitely Generated Field Extensions

Recall the evaluation map $\phi_a : F[x] \to K$ given by $f \mapsto f(a)$ for each $a \in K$.

Definition 1.2.1: Simple Extensions

Let $F < K$ be a field extension. Let $a \in K$. Define

$$F(a) = \left\{ \frac{\phi_a(f(x))}{\phi_a(g(x))} \middle| f, g \in F[x], g(a) \neq 0 \right\} = \left\{ \frac{f(a)}{g(a)} \middle| f, g \in F[x], g(a) \neq 0 \right\}$$

We say that a field extension $F < L$ is a simple extension if $L = F(a)$ for some $a \in L$.

Definition 1.2.2: Finitely Generated Field Extensions

Let K/F be a field extension. Let $\{a_1, \dots, a_n\} \subset K$. Define

$$F(a_1, \dots, a_n) = \left\{ \frac{\phi_a(f(a_1, \dots, a_n))}{\phi_a(g(a_1, \dots, a_n))} \;\middle|\; f, g \in F[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0 \right\}$$

to be the field extension finitely generated by $a_1, \dots, a_n$.

In particular, finitely generated extensions is just the simple extension applied finitely many times.

Lemma 1.2.3

Let $F < K$ be fields. Let $a, b \in K$, then $F(a, b) = F(a)(b)$.

Proposition 1.2.4

Let K/F be a field extension. Let $X = \{a_1, \dots, a_n\} \subset K$. Then

$$F(a_1, \dots, a_n) = \bigcap_{\substack{R \text{ is a field} \\ F \cup X \subseteq R \subseteq K}} R$$

Namely, it is the smallest field extension of F containing X.

Proposition 1.2.5

Every finite field extension is finitely generated.

Proof. Let K/F be a finite field extension, say $n = [K : F]$. Then by definition, $K = \text{span}\{k_1, \dots, k_n\}$ where $k_i \in K$ for each i. Hence every element of K can be written as a finite linear combination of $k_1, \dots, k_n$ over F. Thus $K \subseteq F(x_1, \dots, x_n)$. Since K is a field that contains F and $\{k_1, \dots, k_n\}$, by proposition 9.4.6, we have that $F(k_1, \dots, k_n) \subseteq K$ and so we conclude. $\square$

There is a great relation between the polynomial ring and finitely generated field extensions. Notice that a polynomial ring over a field is not a field while finitely generated field extensions are a field.

Proposition 1.2.6

Let K/F be a field extension. Let $X = \{a_1, \dots, a_n\} \subset K$. Then

$$F[a_1, \dots, a_n] = \bigcap_{\substack{R \text{ is a ring} \\ F \cup X \subseteq R \subseteq K}} R$$

Proposition 1.2.7

Let K/F be a field extension. Let $X = \{a_1, \dots, a_n\} \subset K$. Then

$$F(a_1, \dots, a_n) = \text{Frac}\left(F[a_1, \dots, a_n]\right)$$

1.3 Algebraic Elements

Recall the notion of algebraic elements and the minimal polynomials from groups and rings.

Definition 1.3.1: Algebraic and Transcendental Elements

Let $F < K$ be fields. Then $a \in K$ is said to be algebraic over F if there exists a non zero polynomial $f \in F[x]$ such that $f(a) = 0$. Otherwise it is said to be transcendental.

Definition 1.3.2: Minimal Polynomial

Let $F < K$ be field extensions and $a \in K$ be algebraic over F. Then the minimal polynomial of a over F is the monic irreducible polynomial $p(x) \in F[x]$ of least degree such that $p(a) = 0$. It is often denoted $\min(F, a)$.

A polynomial can be the minimal polynomial for one of its roots, but not for its other roots. For example, the minimal polynomial of $2^{1/3}$ is $x^3 - 2$, but it is not the minimal polynomial for $2^{1/3}e^{2\pi i/3}$ even though it is a root of $x^3 - 2$. On the other hand, $x^2 + 1$ is the minimal polynomial of both i and $-i$.

Proposition 1.3.3

Let $F < K$ be fields and $a \in K$ be algebraic over F. Then the following are true.

- $\min(F, a)$ exists and is unique.
- If a is a root of $g \in F[x]$, then $f|g$.

Proposition 1.3.4

Let $F < K$ be a field extension and $a \in K$ algebraic over F. Let $\deg(\min(F, a)) = n$. Then $[F(a) : F] = n$ and $1, a, \dots, a^{n-1}$ is a basis for $F(a)$ over F.

Proof. Suppose that f is the minimum polynomial. We prove that $L : F[x]_{<n} \to F[x]/(f)$ defined by $L(g) = g + (f)$ is a field isomorphism. It is easy to check that it is a F-linear map. For injectivity, suppose that $L(v) = 0$. Then $v \in (f)$ as well as $\deg(v) < \deg(f)$ by construction forces v to be 0. For sujectivity, suppose that $r + (f) \in F[x]/(f)$ and $\deg(r) < \deg(f)$. Then we can just choose $r \in F[x]_{<n}$ and we are done. Thus L is an isomorphism.

Using the fact that $F[x]/(f) \cong F(a)$, we can construct a basis for $F(a)$ from L. But L has the basis $\{1, x, \dots, x^{n-1}\}$. Transporting it through the field isomorphisms, we get $\{1, a, \dots, a^{n-1}\}$ is a basis of $F(a)$.

□

Lemma 1.3.5

Let F be a field. Let $f \in F[x]$ be a polynomial. Then there exists a field extension $F < K$ such that f has a root α in K.

Proof. Consider the field $K = F[x]/(f)$. K is a field since f is irreducible in $F[x]$. Moreover, the composition $F \to F[x] \to F[x]/(f) = K$ is a field homomorphism and so is injective. Let $a = x + (f) \in K$. Any element of K is of the form $h(x) + (f)$, but that is exactly $h(a)$, so a generates K over F. It is clear that $f(a) = f(x) + (f) = 0 + (f)$ is zero in K. □

Corollary 1.3.6

Let F be a field. Let $f \in F[x]$ be a monic irreducible polynomial. Suppose that $F < K$ is a field extension such that $\alpha \in K$ is a root of F. Then $\min_F(\alpha) = f$.

Proof. f is by definition monic and irreducible, and so is the minimal polynomial of α over F. □

Proposition 1.3.7

Let $F < K$ be fields. Let $a \in K$. Then a is algebraic over F if and only if $F(a) = F[a]$.

1.4 Algebraic Extensions

Every field extension can be classified into an algebraic extension or a transcendental extension or a mixture of both. Since $\mathbb{R}$ contains both algebraic elements and transcendental elements of $\mathbb{Q}$, it is the prototypical example of such a field extension. Algebraic extensions will be studied briefly here, while more is said on transcendental extensions in field and Galois theory.

Definition 1.4.1: Algebraic Extensions

Let K/F be a field extension. We say that K/F is an algebraic extension if every element of K is algebraic over F.

In particular, notice that $a \in K$ is an algebraic element over F if and only if $F(a)$ is an algebraic extension.

Lemma 1.4.2

If $F < K$ is a finite extension of fields, then K is algebraic over F.

Proof. Suppose that $[K : F] = n$. If $a \in L$, consider the elements $1, a, \dots, a^n$. Since they lie in an n dimensional vector space, there exists $c_0, \dots, c_n \in F$ not all 0 such that $\sum_{i=0}^n c_i a^i = 0$. Thus a satisfies a non-trivial polynomial relation over F. □

Theorem 1.4.3

If K is algebraic over L and L is algebraic over F then K is algebraic over F.

Proposition 1.4.4

Let K be a field extension of F. If each $a_1, \dots, a_n \in K$ is algebraic over F, then $F(a_1, \dots, a_n)$ is a finite dimensional vector space with

$$[F(a_1, \dots, a_n) : F] \leq \prod_{k=1}^n [F(a_k) : F]$$

Corollary 1.4.5

Let $F < K$ be fields. Then $a \in K$ is algebraic over F if and only if $[F(a) : F] < \infty$.

Since finitely generated field extensions is a finite concatenation of simple extensions, we can ask the question of whether the simplicity criteria can be relaxed to finitely generated extensions. The following proposition shows that it is possible.

Proposition 1.4.6

Let K/F be a finitely generated field extension. Then K/F is a finite extension if and only if K/F is an algebraic extension.

If one know of colimits, then it is easy to see that algebraic extension are just colimits of finite extensions. This means that algebraic extensions are just finite extensions applied a countable number of times.

2 More on Field Homomorphisms

2.1 Homomorphisms that Fixes Subfields

Recall that K/F is a field extension if K contains F as a subfield. Since every field homomorphism is necessarily injective, this amounts to saying that there is a field homomorphism from F to K. We now have notion of a particular homomorphism that fixes the subfield.

Definition 2.1.1: F-Homomorphism

Let K/F and L/F be field extensions. We say that $\phi : K \to L$ is a F-homomorphism if ϕ is a ring homomorphism such that $\phi(a) = a$ for all $a \in F$.

Denote the set of all F-homomorphisms between K and L to be

$$\text{Emb}_F(K, L) = \{\phi : K \to L \mid \phi(a) = a \text{ for all } a \in F\}$$

Proposition 2.1.2

Let K/F and L/F be field extensions. Let $\tau : K \to L$ be an F-homomorphism.

- τ is a homomorphism between F-vector spaces
- τ is surjective if $[K : F] = [L : F] < \infty$

Proof.

- Let $a, b \in K$. Then $\tau(a + b) = \tau(a) + \tau(b)$ by property of a ring homomorphism. Similarly, for $\lambda \in F$, we have $\tau(\lambda a) = \tau(\lambda)\tau(a) = \lambda\tau(a)$ by property of ring homomorphism.
- Since τ is a linear transformation between vector spaces, if the two vector spaces are finite dimensional, then τ is injective if and only if τ is surjective. But τ is a field homomorphism and so is injective.

And so we conclude. □

Lemma 2.1.3

Let $\tau : K \to L$ be an F-homomorphism. Let $a \in K$ be algebraic over F. If $f \in F[x]$ is a polynomial such that $f(a) = 0$, then $f(\tau(a)) = 0$.

Proof. Write $f(x) = \sum_{k=1}^{n} c_k x^k$ for $c_k \in F$. Then since τ fixes F, we have

$$\begin{aligned}
\tau(f(a)) &= \tau(0) \\
\tau\left(\sum_{k=1}^{n} c_k a^k\right) &= 0 \\
\sum_{k=1}^{n} \tau(c_k)\tau(a)^k &= 0 && (\tau \text{ is a field homomorphism}) \\
f(\tau(a)) &= 0
\end{aligned}$$

and so we conclude. □

In particular, this means that F-homomorphisms $\tau : K \to K$ permute the roots of f. We also have a converse given by the following proposition. It shows that any two roots can be mapped by an F-homomorphism.

Proposition 2.1.4

Let L/K be a field extension. Let $f \in K[x]$ is an irreducible polynomial and that $\alpha, \beta \in L$ are roots of f. Then there exists a K-isomorphism $\phi : K(\alpha) \to K(\beta)$ such that $\phi(\alpha) = \beta$.

Proof. From groups and rings we know that both $K(\alpha)$ and $K(\beta)$ are isomorphic to $K[x]/(f)$ with $x \mapsto \alpha$ and $x \mapsto \beta$ respectively, so composing the inverse of the first with the second gives our isomorphism as required. □

Corollary 2.1.5

Let L/K be a field extension. Let $f \in K[x]$ be irreducible. Let α be a root of f. Then

$$|\text{Emb}_K(K(\alpha), L)| = |\{\beta \in L \mid f(\beta) = 0\}|$$

Proof. Any K-homomorphism $\varphi : K(\alpha) \to L$ is determined be the image $\beta = \varphi(\alpha)$. Also $\beta \in L$ is a root of f by lemma 1.1.3. Conversely, the above proposition implies that for any root β, $\alpha \mapsto \beta$ determines a K-homomorphism. □

Theorem 2.1.6

Let L/K be a finite extension and M/K any extension. Then

$$|\text{Emb}_K(L, M)| \leq [L : K]$$

Proof. If $L = K(\alpha)$ is a simple extension with minimal polynomial f, then $\deg(f) = [L : K]$ is an upper bound on the number of roots of f, and thus by the above corollary we conclude.

The above case for simple extension serves as our base case for induction. Now we work by induction on $[L : K]$. Let $\alpha \in L \setminus K$ and consider $K < K(\alpha) < L$. There is a map of sets

$$\text{Emb}_K(L, M) \xrightarrow{\rho} \text{Emb}_K(K(\alpha), M)$$

just by restriction of a map from L to a map from $K(\alpha)$. Let $\varphi \in \text{Emb}_K(K(\alpha), M)$. Then the preimage $\rho^{-1}(\varphi)$ is the set of K-homomorphisms L to M that restricts to φ. In particular, $\rho^{-1}(\varphi)$ is just the set of $K(\alpha)$ homomorphisms L to M. Since $[L : K(\alpha)] < [L : K]$, we have by induction that $\left|\rho^{-1}(\varphi)\right| \leq [L : K(\alpha)]$. Thus we have that

$$\begin{aligned}
|\text{Emb}_K(L, M)| &= \max\left\{\left|\rho^{-1}(\varphi)\right| \;\middle|\; \varphi \in \text{Emb}_K(K(\alpha), M)\right\} \times |\text{Emb}_K(K(\alpha), M)| \\
&\leq [L : K(\alpha)][K(\alpha) : K] \\
&= [L : K]
\end{aligned}$$

by the tower law and so we conclude. □

Definition 2.1.7: Field Automorphisms

Let K/F be a field extension. Define the set of automorphisms of K fixing F to be

$$\text{Aut}_F(K) = \text{Emb}_F(K, K) = \{\varphi : K \to K \mid \varphi \text{ is a bijective field homomorphism that fixes } F\}$$

Lemma 2.1.8

Let K/F be a field extension. Then $\text{Aut}_F(K)$ is a group with composition of functions.

2.2 The Norm and Trace Map

Definition 2.2.1: The Multiplication Map

Let K be a field. Let $\alpha \in K$. Define the multiplication map by α to be the map $M_\alpha : K \to K$ where $\beta \mapsto \alpha\beta$ for all $\beta \in K$.

Proposition 2.2.2

Let K/F be a field extension. Then the characteristic polynomial χ_{M_α} of the multiplication map $M_\alpha : K \to K$ is equal to the minimal polynomial $\min_{K,\alpha}$.

Proof. Let $\chi_{M_\alpha} = \sum_{k=0}^{n} a_n x^n$ be the characteristic polynomial of M_α. In particular we must have $a_n = 1$ because characteristic polynomials are monic. By the Cayley-Hamilton theorem, $\chi_{M_\alpha}(M_\alpha) = 0$, where both sides of the equation is considered as functions $K \to K$. Now evaluate the function at 1_K to obtain $\sum_{k=0}^{n} a_n \alpha^n = 0$. Thus $\min_{K,\alpha}$ divides χ_{M_α}. Now $\min_{K,\alpha}$ is monic and has degree $\deg(\min_{K,\alpha}) = [K : F]$. But also $\deg(\chi_{M_\alpha}) = [K : F]$. Thus we conclude that $\min_{K,\alpha} = \chi_{M_\alpha}$. $\square$

Proposition 2.2.3

Let L/K be an extension of number fields. Let $\alpha \in K$. Then

$$\chi_{L,M_\alpha} = \chi_{K,M_\alpha}^{[L:K]}$$

Definition 2.2.4: The Trace Map

Let L/K be a field extension. Define the trace map $\text{Tr}_{L/K} : L \to K$ to be the map

$$\text{Tr}_{L/K}(\alpha) = \text{tr}(M_\alpha)$$

where $M_\alpha : L \to L$ is the multiplication map defined by $\beta \mapsto \alpha\beta$.

Lemma 2.2.5

Let L/K be a field extension. Then the trace map $\text{Tr}_{L/K}$ is K-linear.

Definition 2.2.6: The Norm Map

Let L/K be a field extension. Define the trace map $N_{L/K} : L \to K$ to be the map

$$N_{L/K}(\alpha) = \det(M_\alpha)$$

where $M_\alpha : L \to L$ is the multiplication map defined by $\beta \mapsto \alpha\beta$.

Lemma 2.2.7

Let L/K be a field extension. Then for all $\alpha, \beta \in L$, we have that

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

Moreover, we have that $N_{L/K}(L) \subseteq K^\times$.

Corollary 2.2.8

Let $L/K/F$ be an extension of number fields. Then the following are true.

- $\text{Tr}_{L/F} = [L : K]\text{Tr}_{K/F}$
- $N_{L/F} = N_{K/F}^{[L:K]}$

3 Special Field Extensions

In order to work towards Galois theory, we will need more technical definitions so that the theory could work in its sufficient conditions. Hence we will see 3 important types of field extensions.

3.1 Splitting Extensions

Intuitively, splitting fields for a polynomial in a base field is the smallest field extension so that f splits into linear factors. Hence the name splitting fields.

Definition 3.1.1: Splitting Fields

Let F be a field and $f \in F[x]$. A splitting field of F is a field extension $F < K$ such that the following are true.

- f factors completely into linear factors in $K[x]$: there exists $a_1, \dots, a_n, c \in K$ such that $f(x) = c \cdot (x - a_1) \cdots (x - a_n)$
- f does not factor completely into linear factors over any proper subfield of K containing F

Since $K(a_1, \dots, a_n)$ is the minimal field containing $a_1, \dots, a_n$, the second condition implies that $K = F(a_1, \dots, a_n)$.

In other words, it is the smallest field extension of F such that $f(x)$ splits completely in it. Notice that in depends on what base field we are working on, because K has to be a field extension of F.

Notice that if K/F is a splitting field for $f \in F[x]$, K can still be a splitting field for other polynomials in $F[x]$.

Theorem 3.1.2

Let $f \in F[x]$ be a polynomial of degree n. Then there exists a splitting field K/F of f of degree $[L : K] \leq n!$.

Proof. If f splits into linear factors in $F[x]$ then we are done. Suppose f does not split linearly over F. Let g_1 be a non-linear irreducible factor of f. Then $K_1 = \frac{F[x]}{(g_1)} = F(a)$ is an extension that contains a root a of g_1. Moreover, we must have $[K_1 : F] = \deg(g) \leq n$. Now the factorization of f into irreducible factors over $F(a)$ has factors strictly less than that of the factorization in F. The maximum degree of an irreducible factor is now $n - 1$.

Repeating this process inductively, at the ith step adding at least one root $K_{i+1} = K_i(a_i)$ of an irreducible factor g_i of degree less than $n - i$, so $[K_{i+1} : K_i] \leq n - i$. If there are s steps, then the tower law implies that

$$\begin{aligned}
[K : F] &= [K_1 : F][K : K_1] \\
&= [K : K_{s-1}][K_{s-1} : K_{s-2}] \cdots [K_1 : K] \\
&\leq (n - (s-1))(n - (s-2)) \cdots n \\
&\leq n!
\end{aligned}$$

and so we conclude. □

The proof of the above existence theorem yields the following corollary. In particular, the splitting field of f is obtained by adjoining some subset of the roots of f. So certainly by adjoining all roots of f, we result in the splitting field of f, albeit the presentation being less tidy.

Corollary 3.1.3

Let $f \in F[x]$ be a polynomial of degree n. Let $\{a_1, \dots, a_n\}$ be the roots of f. Then the splitting field of f is of the form $F(a_{k_1}, \dots, a_{k_s})$ for $a_{k_i} \in \{a_1, \dots, a_n\}$ and $s \leq n$.

Proof. The above proof demonstrates the result. □

Theorem 3.1.4

Let K/F be a splitting field for $f \in F[x]$. Let $g \in F[x]$ be irreducible and that it has at least one root in K. Then g has all its roots in K.

Proof. Regard g as a polynomial in $K[x]$ instead and let L/K be a splitting field of g. Our goal is to show that $L = K$. Suppose that $a \in L$ is a root of g. Consider the following commutative diagram:

$$\begin{tikzcd}
F(a) \arrow[r, hook] & K(a) \arrow[dr, hook] & \\
F \arrow[u, hook] \arrow[r, hook] & K \arrow[u, hook] \arrow[r, hook] & L
\end{tikzcd}$$

Notice that $K(a)/F(a)$ is a splitting field for f (consider f as a polynomial in $K(a)[x]$). By the tower law, we have

$$[K(a) : K][K : F] = [K(a) : F] = [K(a) : F(a)][F(a) : F]$$

If b is another root of g, then we have the same equation:

$$[K(b) : K][K : F] = [K(b) : F(b)][F(b) : F]$$

By proposition 1.4.4, we know that $F(a) \cong F(b)$ via an F-homomorphism. Combining the fact that $K(a)/F(a)$ is a splitting field for f, we have that $F(a) \overset{\cong}{\to} F(b) \to K(b)$ is also a splitting field of f. Since splitting fields are unique up to isomorphism, we have that $K(a) \cong K(b)$. This means that $[K(a) : F(a)] = [K(b) : F(b)]$ and $[F(a) : F] = [F(b) : F]$ and thus

$$[K(a) : K] = [K(b) : K]$$

We know that at least one root of g lies in K, say a, then $[K(a) : K] = 1$. By the above calculations, for any other root b of g, we must also have $[K(b) : K] = 1$ and thus g splits in K. □

The following theorem characterizes splitting fields as the smallest field that splits a polynomial.

Theorem 3.1.5

Let K/F be a spitting field for $f \in F[x]$. If L/F is a field extension such that f splits into linear factors, then there exists a F-homomorphism $K \to L$.

Proof. Suppose that $K = F(a_1, \dots, a_s)$. Where $a_1, \dots, a_s$ are some of the roots of f. We induct on s.

Suppose that m is the minimal polynomial of a_1. Then $m|f$ by definition. Thus m splits into linear factors in L. Let b_1 be any root of m in L. Then by proposition 1.4.4, there exists an F-isomorphism from $F(a_1) \subset K$ to $F(b_1) \subset L$.

Now $K/F(a)$ is a splitting field for $\frac{f(x)}{(x-a_1)} \in F(a_1)[x]$, and $K = F(a_1)(a_2, \dots, a_s)$ is generated

by fewer than s elements over $F(a_1)$. By induction, there is a $F(a_1)$-homomorphism $K \to L$. That map is in particular, an F-homomorphism and we are done. □

Corollary 3.1.6

Let F be a field and $f \in F[x]$. Then any two splitting fields of f are isomorphic.

Proof. Let K and L both be splitting fields of the polynomial f. By the above theorem, there exists injective field homomorphism going from K to L and from L to K. Both K and L are of finite dimension by theorem 2.1.2 and so they must have the same dimension. Therefore both maps are bijections. □

Note that the splitting field is not unique to one polynomial. For example, $\mathbb{Q}(\sqrt{2})$ is the splitting field of both $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ and $g(x) = x^2 - 8 \in \mathbb{Q}(x)$.

3.2 Algebraically Closed Fields

Definition 3.2.1: Algebraically Closed Fields

Let K be a field. We say that K is algebraically closed if there are no algebraic extensions for K other than K itself.

Lemma 3.2.2

The following are equivalent for a field K.
- K is algebraically closed
- There are no finite extensions for K other than K itself
- Every $f \in K[x]$ splits in K
- Every $f \in K[x]$ has a root in K
- Every irreducible polynomial over K has degree 1.

Definition 3.2.3: Algebraic Closure

Let K/F be a field extension. We say that K is the algebraic closure of F if K is algebraically closed.

Proposition 3.2.4

Let F be a field. Then F has an algebraic closure.

3.3 Normal Extensions

Theorem 2.1.7 demonstrates that as long as at least one root of an irreducible polynomial lands on a field extension, then all its other roots will also lie in the field extension. But what if we relax this condition? Namely, there could be some field extension that does not have this property (obviously we just show that splitting fields have this property). Fields extensions that have this type of property is called normal fields.

Definition 3.3.1: Normal Fields

Let K be a field extension of F. We say that K/F is normal if every irreducible $g \in F[x]$ that has a root in K, has all its roots in K.

In the case of finite extensions, the notion of normality and splitting are exactly the same.

Lemma 3.3.2

Let K/F be a finite extension. Then K/F is a normal extension if and only if K/F is the splitting field of some $f \in F[x]$.

Proof. If K/F is the splitting field of $f \in F[x]$, then by theorem 2.1.7, we are done. Now suppose that K/F is a finite normal extension. Then $K = F(a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in K$. Let $m_i \in F[x]$ be the minimal polynomial of a_i. Since K is normal and m_i has a root in K, m_i has all its roots in K. Thus K is the splitting field for $f = m_1 \cdots m_n$. □

In particular, we show the existence of a normal field extension for finite field extensions.

Corollary 3.3.3

Let $F < K$ be a finite field extension. Then there exists a finite extension $K < L$ such that it is normal. Moreover, $F < L$ is also normal.

Proof. Write $K = F(a_1, \dots, a_n)$, with $m_i \in F[x]$ the minimal polynomial of a_i. Write $f = m_1 \cdots m_n$. Then let N be a splitting field for $f \in K[x]$. It is normal over K be the above theorem. □

Definition 3.3.4: Normal Closure

Let $F < K$ be a finite extension. We say that $K < L$ is a normal closure of $F < K$ if $F < L$ is normal, and that L does not contain any subfield that is normal.

We will see how subfields behave with respect to automorphisms of normal extensions.

Corollary 3.3.5

Let $F < K < L$ be a field extension such that $F < L$ is a finite normal extension. For any $\phi : K \to L$ an F-homomorphism, there exists an F-automorphism $\varphi \in \text{Aut}_F(L)$ such that $\phi = \varphi|_K$.

Proof. Suppose L is the splitting field over F, so in particular L is also the splitting field for f over K. Since ϕ fixes F, $\phi(f) = f$. This means that L is also a splitting field for $\phi(f) \in \phi(K)[x]$. Now $K \cong \phi(K)$, and L/K and $L/\phi(K)$ are splitting fields for f and $\phi(f)$. By uniqueness of splitting fields, there is an isomorphism $L \to L$ that restricts to ϕ. □

Corollary 3.3.6

Let K/F be a finite normal extension. Suppose $f \in K[x]$ is irreducible and a, b are roots of $f \in K$. Then there exists $\varphi \in \text{Aut}]_F(K)$ such that $f(a) = b$.

Proof. There is an F-homomorphism $F(a) \to F(b)$ since a and b has the same minimal polynomial. The above corollary implies that this lifts to an F-automorphism of K since K/F is a finite normal extension. □

Now we will also see what happens to automorphisms of a field extension of a normal extension.

Proposition 3.3.7

Let K/F be a finite normal extension. Suppose L/K is a finite extension. Then the following are true.

- If $\varphi : K \to L$ is an F-homomorphism, then $\varphi(K) = K$
- If $\tau \in \text{Aut}_F(L)$, then $\tau(K) = K$

Proof. Let $a \in K$ and let m be its minimal polynomial over F. Then we know that $\varphi(a)$ is also a root of m so that $\varphi(a) \in K$ since K/F is normal. Thus $\varphi(K) \subseteq K$. But K/F is a finite dimensional F-vector space and φ is injective. Thus φ is an isomorphism and $\varphi(K) = K$.

The second part follows by applying the first part to τ_K. □

3.4 Separable Extensions

Definition 3.4.1: Separable Polynomials

Let F be a field. An irreducible polynomial $f \in F[x]$ is separable over F if f has no repeated roots in any splitting fields.

A polynomial $g \in F[x]$ is separable over F if all irreducible factors of g are separable over F.

Definition 3.4.2: Separable Elements and Fields

Let L/K be a field extension. An element $\alpha \in L$ is separable over K if its minimal polynomial is separable over K.

The extension L/K is separable if every $\alpha \in L$ is separable over K.

Proposition 3.4.3

Let $f \in K[x]$ be an irreducible polynomial. Then f is inseparable over K if and only if $\text{char}(K) = p > 0$ and f is of the form

$$f(x) = \sum_{k=0}^{n} a_k x^{kp}$$

Proposition 3.4.4

Let L/K be a finitely generated field extension given by $L = K(\alpha_1, \dots, \alpha_n)$. If each α_i is separable over K, then the extension L/K is separable.

Lemma 3.4.5

Let K be a field and $f \in K[x] \setminus \{0\}$. Then f is separable over K if and only if f and $\frac{df}{dx}$ are coprime in $K[x]$.

Theorem 3.4.6: Primitive Element Theorem

Let K/F be field extension. If K/F is finite and separable, then it is simple.

4 The Galois Correspondence

4.1 The Fixed Field of Automorphisms

Definition 4.1.1: Fixed Fields

Let K be a field. Let $S \subseteq \text{Aut}(K)$ be a subset of automorphisms. Define the fixed field of S to be

$$\text{Fix}_K(S) = \{a \in K \mid \tau(a) = a \text{ for all } \tau \in S\}$$

Lemma 4.1.2

Let K be a field. Let $S \subseteq \text{Aut}(K)$. Then $\text{Fix}_K(S) < K$ is a subfield.

Proposition 4.1.3

Let K be a field and let $G \leq \text{Aut}(K)$ be a finite subgroup. Then

$$[K : \text{Fix}_K(G)] = |G|$$

Proof. Let $G = \{\sigma_1, \dots, \sigma_n\}$. Suppose that $a_1, \dots, a_{n+1} \in K$. Set $L = K^G < K$, the fixed field of G. Let

$$v_i = \begin{pmatrix} \sigma_1(a_i) \\ \vdots \\ \sigma_n(a_i) \end{pmatrix} \in K^n$$

for $i = 1, \dots, n+1$. Since K^n is a vector field over K with dimension n, $v_1, \dots, v_{n+1}$ are linearly dependent with

$$c_1 v_1 + \cdots + c_k v_k = 0$$

the shortest linear independence relation for $c_i \in K \setminus \{0\}$. Without loss of generality suppose that $x_1 = 1$ and $\sigma_1 = \text{id}_K$. Write the relation as

$$\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

This means that $(x_1, \dots, x_k)^T$ is a non-trivial solution of the n simultaneous linear equations. For any $\sigma \in G$, applying σ to the system of linear equation only permutes the rows of the matrix so it leaves exactly the same set of equations, but the solution is now $(\sigma(x_1), \dots, \sigma(x_k))^T$. But this must be the same solution as before. If not, then $\sigma(x_1) = \sigma(1) = 1 = x_1$ implies that we can get a shorter linear dependence relation which is a contradiction. Thus we have that $\sigma(x_i) = x_i$ for each $i = 1, \dots, k$ and for every $\sigma \in G$. So each $x_i \in K^G = L$ together with the first row of the system of linear equations give a non-trivial L-linear relation among the a_i.

Thus every K^G-linearly independent set of elements of K has size less than $|G|$, proving that $[K : K^G] \leq |G|$.

By theorem 1.1.6, we have that

$$|G| \leq |\text{Aut}_{K^G}(K)| = |\text{Emb}_{K^G}(K, K)| \leq [K : K^G]$$

and so we conclude. □

4.2 Galois Extensions

Definition 4.2.1: Galois Extension

Let K/F be a field extension. We say that K/F is a Galois extension if K is the splitting field of a separable polynomial with coefficients in F.

Proposition 4.2.2: Equivalent characterization of Galois Extension

Let K/F be a field extension. Then the following are equivalent.
- K/F is a Galois extension.
- K/F is a normal and separable extension.
- $[K : F] = |\text{Aut}_F(K)|$.
- $\text{Fix}_F(\text{Aut}_F(K)) = F$.

Proof.
- (1) $\iff$ (3): Let $n = [K : F]$. We induct on n.

  When $n = 1$, then $K = F$ and there is exactly one F-automorphism. So suppose that $n > 1$. Let K be the splitting field of $f \in F[x]$ with $\deg(f) = d > 1$.

  Let $a \in K \setminus F$ a root of f. Let $m \in F[x]$ be the minimal polynomial of a. This is an irreducible factor of f by definition. Break up the field extension into $F < F(a) < K$. We handle $K/F(a)$ by induction and $F(a)/F$ by hand.

  Step 1: $K/F(a)$ is Galois by lemma 4.1.3. So by induction, we have

  $$[K : F(a)] = |\text{Gal}(K/F(a))|$$

  Step 2: Since f is separable, it has distinct roots in K. Thus the minimal polynomial m also has distinct roots in L as its divides f. By property of the minimal polynomial, we have that $[F(a) : F] = \deg(m)$. By corollary 2.1.5, we have that $\deg(m) = |\text{Emb}_F(F(a), K)|$.

  Step 3: For every automorphism $\phi : K \to K$, the restriction to $F(a)$ gives a map of sets

  $$\text{res}_a : \text{Gal}(K/F) \to \text{Emb}_F(F(a), K)$$

  defined by $\phi \mapsto \phi|_{F(a)}$. I claim that this map is surjective. Let $\iota : F(a) \to K \in \text{Emb}_F(F(a), K)$. Since K/F is normal, by corollary 3.3.5 there exists an F-automorphism σ of K that restricts to ι. Let $\tau \in \text{Gal}(L/K)$ be any other map that restricts to ι. The map $\tau^{-1} \circ \sigma : K \to K$ is the identity on $F(a)$, and thus $\tau^{-1} \circ \sigma \in \text{Gal}(K/F(a))$. Thus τ and σ lie in the same coset, and thus

  $$\frac{|\text{Gal}(K/F)|}{|\text{Gal}(K/F(a))|} = \left|\frac{\text{Gal}(K/F)}{\text{Gal}(K/F(a))}\right| = |\text{Emb}_F(F(a), K)|$$

  Step 4: Putting the equalities together, we have that

  $$\begin{aligned} |\text{Gal}(K/F)| &= |\text{Gal}(K/F(a))| \cdot |\text{Emb}_F(F(a), K)| \\ &= [K : F(a)] \cdot [F(a) : F] \\ &= [K : F] \end{aligned}$$

  Thus we are done.

$\square$

Lemma 4.2.3

If L/F is a Galois extension and $F < K < L$ an intermediate field, then L/K is a Galois extension.

Proof. Let L be the splitting field of a separable polynomial $f \in F[x]$. Then L is also a splitting field of f regarded as a polynomial in $K[x]$. The factorization of f clearly does not change since f splits over L which K is a subfield of. □

Beware that while L/K is a Galois extension in the above lemma, K/F may not be a Galois extension.

4.3 The Inclusion Reversing Bijection

Theorem 4.3.1: The Fundamental Theorem of Galois Theory

Let L/K be a Galois extension. Then there is an inclusion reversing bijection

$$\left\{\begin{matrix}\text{Subgroups of}\\ \text{Aut}_K(L)\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Intermediary subfields}\\ K<M<L\end{matrix}\right\}$$

given as follows.

- For a subgroup $H \leq \text{Aut}_K(L)$, $H \mapsto \text{Fix}_K(H)$.
- For an intermediary subfield M, $M \mapsto \text{Aut}_M(L)$.

Note: We sometimes write $\text{Gal}(L/K) = \text{Aut}_K(L)$ when L/K is a Galois extension.

Proposition 4.3.2

Let L/K be a Galois extension. Then the above bijection restricts to a bijection

$$\left\{\begin{matrix}\text{Normal Subgroups}\\ \text{of Aut}_K(L)\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Normal Extensions}\\ K<M\end{matrix}\right\}$$

Proof. Suppose that M/K is a normal extension. Then by proposition 2.3.7, we have that $\sigma(M) = M$ for any $M \in \text{Gal}(L/K)$. Suppose that $h \in \text{Gal}(L/M)$. Let $a \in M$ and $b = \sigma^{-1}(a)$. Notice that

$$\sigma h \sigma^{-1}(a) = \sigma(h(b)) = \sigma(b) = a$$

so that $\sigma h \sigma^{-1}$ fixes M. This means that $\sigma h \sigma^{-1} \in \text{Gal}(L/M)$.

Conversely, suppose that $\text{Gal}(L/M) \trianglelefteq \text{Gal}(L/K)$. Let $a \in M$ has minimal polynomial $g \in K[x]$. We want to prove that g splits in M. Let b be a root of g. Then there exists some $\sigma \in \text{Gal}(L/K)$ such that $b = \sigma(a)$. For any $h \in \text{Gal}(L/M)$, we have that

$$\sigma h \sigma^{-1}(b) = \sigma h(a) = \sigma(a) = b$$

By normality, we have that $\sigma H \sigma^{-1} = H$ so that b is fixed by every element of H and so $b \in L^{\text{Gal}(L/M)}$. Since L/M is Galois by lemma 3.1.3, proposition 3.2.3 implies that $b \in L^{\text{Gal}(L/M)} = M$, and so g splits over M, and M/K is normal. □

Proposition 4.3.3

Let $K < M < L$ be field extensions such that L/K is Galois and M/K is normal. Then we have

$$\text{Aut}_K(M) \cong \frac{\text{Aut}_K(L)}{\text{Fix}_M(\text{Aut}_K(L))}$$

Moreover, the following are true.

- $[L : M] = |\text{Fix}_M(\text{Aut}_K(L))|$
- $[M : K] = \left|\frac{\text{Aut}_K(L)}{\text{Fix}_M(\text{Aut}_K(L))}\right|$

Let L/K be a Galois extension. We summarize what we know about $\text{Gal}(L/K) = \text{Aut}_K(L)$.

- $|\text{Aut}_K(L)| \leq [L : K]$.
- $[L : \text{Fix}_K(H)] = |H|$ where $H \leq= \text{Aut}_K(L)$.

4.4 Application: Biquadratic Extensions

As an immediate application of the fundamental theorem of Galois theory, we apply the inclusion reversing bijection to biquadratic extensions. The set up is as follows:

Let K be a field such that $\text{char}(K) \neq 2$. Let $a, b \in K$ such that $b(a^2 - b) \neq 0$ and b is not a square in K. Consider

$$f(x) = x^4 - 2ax^2 + (a^2 - b) \in K[x]$$

Write $\beta^2 = b$. Then it is easy to see that $x^2 - a = \pm\beta$ so that the roots of f are $\alpha, -\alpha, \alpha', -\alpha' \in L$ the splitting field of K by taking quadratic extensions (degree 2 extensions) where $\alpha^2 = a + \beta$ and $(\alpha')^2 = a - \beta$. In particular, $L = K(\alpha, \alpha')$. It is easy to see that the four roots are four distinct elements. Together with the fact that $\deg(f) = 4$ shows that L/K is a Galois extension (It may be easier to show that $Df = 4x(x^2 - a)$ is coprime with f). We can see L/K in a tower:

$$\begin{tikzcd}
 & L = K(\alpha, \alpha') \arrow[dl, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[dr, dash] & & K(\alpha') \arrow[dl, dash] \\
 & K(\beta) \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Notice that β is omitted in the bigger fields since $\beta = \alpha^2 - a = a - (\alpha')^2$. Each inclusion in the tower is either an equality or a degree 2 extension. Thus $[L : K] = 2, 4$ or 8. We need a lemma.

Lemma 4.4.1

Let K be a field. Let $u, v \in M$. If u is a square in $M(\sqrt{v})$ then either u or uv is a square in M.

Proof. This follows since

$$(c^2 + d^2v) + 2cd\sqrt{v} = (c + d\sqrt{v})^2 = u \in M$$

would imply that $cd = 0$. If $d = 0$, then $u = c^2$. If $c = 0$, then $u = d^2v$ so that $uv = (dv)^2$ and we are done. $\square$

Proposition 4.4.2

Let K be a field such that $\text{char}(K) \neq 2$. Let $a, b \in K$ such that $b(a^2 - b) \neq 0$ and b is not a square in K. Consider

$$f(x) = x^4 - 2ax^2 + (a^2 - b) \in K[x]$$

Write $\beta^2 = b$. Let L/K be the splitting field of f. Denote the four distinct roots of f by $\alpha, -\alpha, \alpha', -\alpha' \in L$ for $\alpha^2 = a + \beta$ and $(\alpha')^2 = a - \beta$.

- If $a^2 - b$ is not a square in K, then $[K(\alpha) : K] = [K(\alpha') : K] = 4$
- If neither $a^2 - b$ nor $b(a^2 - b)$ is a square in K, then $[L : K] = 8$.

Proof. Suppose that $a^2 - b$ is not a square in K. Since $b \in K$ is not a square, we have $[K(\beta) : K] = 2$. It remains to show that $[K(\alpha) : K(\beta)] = 2$. Suppose for a contradiction that $\alpha = c + d\beta \in K(\beta)$ for some $c, d \in K$. Then we have that

$$a + \beta = \alpha^2 = (c + d\beta)^2 = (c^2 + d^2 b) + 2cd\beta$$

and so $a - \beta = (c - d\beta)^2$ is also a square in $K(\beta)$. Thus

$$a^2 - b = (a + \beta)(a - \beta) = ((c + d\beta)(c - d\beta))^2$$

is a square in K, a contradiction. Thus we have that $\alpha \notin K(\beta)$ and $[K(\alpha) : K] = 4$. Similarly, we have that $\alpha' \notin K(\beta)$ and thus $[K(\alpha') : K] = 4$.

Now suppose further that $b(a^2 - b)$ is not a square in K. We need to show that $\alpha' \notin K(\alpha)$. Suppose for a contradiction that $\alpha' \in K(\alpha)$. Writing $\alpha' = c + d\alpha$ with $c, d \in K(\beta)$, we have that

$$a - \beta = (\alpha')^2 = (c^2 + d^2(a + \beta)) + 2cd\alpha$$

Thus $cd = 0$ since $\{1, \alpha\}$ is a basis for $K(\alpha)/K(\beta)$. Since $\alpha' \in K(\beta)$ by the first part of the proof, we have $d \neq 0$. Thus $c = 0$ and $a - \beta = d^2(a + \beta)$. Therefore

$$a^2 - b = (a - \beta)(a + \beta) = (d(a + \beta))^2$$

is a square in $K(\beta)$. By the above lemma, either $a^2 - b$ or $b(a^2 - b)$ is a square in K, both of which are contradictions and so we conclude. $\square$

Lemma 4.4.3

Let K be a field such that $\text{char}(K) \neq 2$. Let $a, b \in K$ such that $b(a^2 - b) \neq 0$ and b is not a square in K. Consider

$$f(x) = x^4 - 2ax^2 + (a^2 - b) \in K[x]$$

Write $\beta^2 = b$. Let L/K be the splitting field of f. Denote the four distinct roots of f by $\alpha, -\alpha, \alpha', -\alpha' \in L$ for $\alpha^2 = a + \beta$ and $(\alpha')^2 = a - \beta$.

Suppose further that $[K(\alpha) : K] = [K(\alpha') : K] = 4$.

- $q(x) = x^2 - (a + \beta)$ is the minimal polynomial of α over $K(\beta)$, and $q'(x) = x^2 - (a - \beta)$ is that of α'
- Any $\sigma \in \text{Gal}(L/K)$ can only map β, α, α' in one of the following 8 ways:

	1	2	3	4	5	6	7	8
$\sigma(\beta)$	β	β	β	β	$-\beta$	$-\beta$	$-\beta$	$-\beta$
$\sigma(a)$	α	α	$-\alpha$	$-\alpha$	α'	α'	$-\alpha'$	$-\alpha'$
$\sigma(\alpha')$	α'	$-\alpha'$	α'	$-\alpha'$	α	$-\alpha$	α	$-\alpha$

(No claim in existence of these maps)

Proof.

- The assumption on degree implies that each step in the tower has degree 2, so that it ensures the irreducibility of both.
- By corollary 1.1.5, either $\sigma(\beta) = \beta$ or $-\beta$. If $\sigma(\beta) = \beta$, then σ fixes $K(\beta)$ so that by the same corollary, σ must permute the roots of q and the roots of q' respectively. If instead $\sigma(\beta) = -\beta$, then notice that $\sigma(q) = q'$ and so σ must exchange the roots of q and q' in some order.

And so we are done. □

Theorem 4.4.4

Let K be a field such that $\text{char}(K) \neq 2$. Let $a, b \in K$ such that $b(a^2 - b) \neq 0$ and b is not a square in K. Consider

$$f(x) = x^4 - 2ax^2 + (a^2 - b) \in K[x]$$

Let L/K be the splitting field of f. Then the following completely classifies $\text{Aut}_K(L)$.

- If $[L : K] = 8$, then $\text{Aut}_K(L) \cong D_8$
- If $\sqrt{b(a^2 - b)} \in K$, then $[L : K] = 4$ and $\text{Aut}_K(L) \cong C_4$
- If $\sqrt{a^2 - b} \in K$ and $[L : K] = 4$ then $\text{Aut}_K(L) \cong C_2 \times C_2$
- Otherwise, $[L : K] = 2$ and $\text{Aut}_K(L) \cong C_2$

Proof. Write $\beta^2 = b$. Denote the four distinct roots of f by $\alpha, -\alpha, \alpha', -\alpha' \in L$ for $\alpha^2 = a + \beta$ and $(\alpha')^2 = a - \beta$.

-
- Notice that $(\beta\alpha\alpha')^2 = b(a^2 - b)$ so that $\beta\alpha\alpha' \in K$ by the case assumption. Thus $\alpha' \in K(\alpha, \beta) = K(\alpha)$, where $L = K(\alpha) = K'(\alpha)$. Since b is not a square implies that $a^2 - b$ is not a square, we have $[L : K] = 4$ by proposition 3.4.2.

  Now f is irreducible in K. Indeed, it has no roots in K and so we just have to check that f is not a product of two irreducible quadratics. By a computation, we can show that all pairwise products of linear factors $x - \alpha$, $x - \alpha'$, $x + \alpha$ and $x + \alpha'$ are not factors of f in K. Since f is irreducible, there exists some $\sigma \in \text{Gal}(L/K)$ with $\sigma(\alpha) = \alpha'$. Lemma 3.4.3 implies that $\sigma(\beta) = -\beta$ and since $\beta\alpha\alpha' \in K$ is fixed by σ, it follows that $\sigma(\alpha') = -\alpha$. Thus σ has order 4.

  But we also know that $\text{Gal}(L/K) = 4$ since L/K is Galois. So $\text{Gal}(L/K) = \langle \sigma \rangle$ is a cyclic group of order 4.
- If $\sqrt{a^2 - b} \in K$, then $a^2 - b = (\alpha\alpha')^2 \in K$ so that $\alpha\alpha' \in K$. Then we have $\alpha' \in K(\alpha)$ so that $L = K(\alpha) = K(\alpha')$. By the Galois correspondence, we have that $\text{Gal}(L/K) = 4$ since L/K is Galois. There is an element $\nu \in \text{Gal}(K(\beta)/K)$ such that $\nu(\alpha) = -\alpha$ and $\nu(\beta) = \beta$ by lemma 3.4.3. Since $\alpha\alpha'$ is fixed by ν, we also have $\nu(\alpha') = -\alpha'$. There is also an element of $\text{Gal}(K(\beta)/K)$ that maps β to $-\beta$. This must lift to an element $\rho \in \text{Gal}(K(\beta)/K)$. This automorphism takes α to one of the roots of $\rho(q(x)) = q'(x)$ as in lemma 3.4.3. If $\rho(\alpha) = \alpha'$, then we have 4 distinct automorphisms

  $$\text{id}, \nu, \rho, \nu\rho \in \text{Gal}(L/K)$$

  where $\nu\rho(\alpha) = -\alpha'$ and so is distinct from the first three. If instead $\rho(\alpha) = -\alpha'$ then we will still get the four automorphisms. So fix notation with $\rho(\alpha) = \alpha'$ so that

  $$\text{Gal}(L/K) = \langle \nu \rangle \times \langle \rho \rangle \cong C_2 \times C_2$$

□

5 Finite Field Theory

5.1 Existence and Uniqueness of Finite Fields

Proposition 5.1.1

If K is a finite field, then it has $\text{char}(K) = p$ a prime, and $|K| = p^n$ for some $n \in \mathbb{N} \setminus \{0\}$.

Proof. Since K is finite, there is no field homomorphism $\mathbb{Z} \to K$ since such a homomorphism must be injective. This means that the prime subfield of K must be $\mathbb{F}_p$ for some prime p. So K is a finite dimensional vector space over $\mathbb{F}_p$, and after choosing any basis, its elements are simply vectors $(a_1, \dots, a_n)$ where $a_i \in \mathbb{F}_p$, where $n = [K : \mathbb{F}_p]$, and there are obviously p^n of these vectors. □

Lemma 5.1.2

Let $\mathbb{F}$ be any field. A finite subgroup of $\mathbb{F}^\times$ is cyclic.

Proposition 5.1.3

Every finite field is isomorphic to $\frac{\mathbb{F}_p[x]}{(f)}$ where p is a prime number and $f \in F_p[x]$ is an irreducible polynomial.

5.2 Galois Theory for Finite Fields

Theorem 5.2.1

Let p be a prime number and $n \geq 1$. Let $q = p^n$. Then the splitting field L of

$$f(x) = x^q - x \in \mathbb{F}_p[x]$$

is a field with p^n elements. Moreover, $L/\mathbb{F}_p$ is a Galois extension.

Proof. Let $L/\mathbb{F}_p$ be the splitting field for f. Since the formal derivative of f is $Df = -1$, f is separable over L with n distinct roots. Thus $L/\mathbb{F}_p$ is a Galois extension. Let $M \subset L$ be the set of roots of f in L, then $M = \{\alpha \in L \mid \alpha^q = \alpha\}$ and $|M| = q$. It is easy to check that M is a field in its own right so that $M = L$ by minimality of the splitting field. □

Proposition 5.2.2

Any two fields of order p^n are isomorphic.

Proof. By the above theorem, one such field of order n is the splitting field L of the polynomial $f(x) = x^q - x \in \mathbb{F}_p[x]$. Suppose $N/\mathbb{F}_p$ is another field of $q = p^n$ elements. Consider the set N^* of non-zero elements as a finite group under multiplication. We must have $\beta^{q-1} = 1$ for any $\beta \in N^*$ by Lagrange's theorem. Multiplying by β, we have that $\beta^q = \beta$ for all $\beta \in N$. That is, f splits in N. Since $|N|$ is the number of roots of f in any splitting field, N is the splitting field for f over $\mathbb{F}_p$. Since splitting fields are unique up to isomorphism, we conclude. □

We denote this unique field up to isomorphism $\mathbb{F}_{p^n}$

Definition 5.2.3: Frobenius Map

Let K be a field of characteristic $p > 0$. The Frobenius map is the homomorphism

$$\varphi_p : K \to K$$

defined by $\alpha \mapsto \alpha^p$.

Lemma 5.2.4

The Frobenius map is a field homomorphism.

Proof. We have that

$$\begin{aligned}\varphi(a+b) &= (a+b)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \\ &= a^p + b^p \\ &= \varphi(a) + \varphi(b)\end{aligned}$$

and

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

and so we conclude. □

Proposition 5.2.5

Let K be a field of characteristic $p > 0$. Let $\varphi_p : K \to K$ be Frobenius map. Then the following are true.

- $F_p = \{a \in K \mid \varphi_p(a) = a\}$
- If K is a finite field, then φ_p is surjective and $\varphi_p \in \text{Aut}_{F_p}(K)$. In this case, it has fixed field $K^{\varphi_p} = \mathbb{F}_p$

Proof. The set of elements on which φ is the identity is certainly a subfield of K since φ is a field homomorphism which contains the prime subfield. At the same time, elements such that $\varphi_p(a) = a$ can be interpreted as the roots in K of the polynomial $x^p - x \in \mathbb{F}_p[x]$. This is not the zero polynomial and has at most p roots. $\mathbb{F}_p$ has p roots and so they must be all of them.

If K is a finite field, then it is a finite dimensional vector space over $\mathbb{F}_p$, and φ_p is an injective linear map, thus φ_p is an isomorphism. In particular, the first part of the proposition shows that φ_p fixes $\mathbb{F}_p$, so it is an $\mathbb{F}_p$-automorphism. It fixed field is given precisely by the set $\{a \in K \mid \varphi_p(a) = a\}$. By the first part of the proof, this is exactly $\mathbb{F}_p$. □

Theorem 5.2.6

Let p be prime. Denote $\varphi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ the Frobenius map. Then

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

is a cyclic group of order n generated by the Frobenius map.

Proof. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois by theorem 4.1.2, so

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

by theorem 3.2.2. When $n = 1$, the case is trivial. Suppose that $n > 1$. $\varphi_p \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a non trivial element by the above proposition. φ_p has order at most n. We show that the order is exactly n. If $\varphi_p^m = \text{id}$ for some $m \leq n$, then for every $\alpha \in K$,

$$\alpha^{p^m} = \varphi_p^m(\alpha) = \alpha$$

and so $g(x) = x^{p^m} - x$ has p^n solutions in $\mathbb{F}_{p^n}$. Then $p^m = \deg(g) \geq p^n$, so that $m = n$. $\square$

Notice that it follows that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n.

6 Cyclotomic Fields and Polynomials

6.1 Cyclotomic Polynomials

Lemma 6.1.1

Let $d, n \in \mathbb{N} \setminus \{0\}$ where $d|n$. Then $x^d - 1$ divides $x^n - 1$ as elements of the polynomial ring $\mathbb{Z}[x]$.

Lemma 6.1.2

Let $n > 0$ be an integer and for $0 \leq i < n$, define $d_i = \gcd(n, i)$. Then the following are true regarding the n-th roots of unity $\{\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}\}$.

- ζ_n^i has order n/d_i
- ζ_n^i is a primitive (n/d_i)th root of unity
- ζ_n^i is a primitive nth root of unity if and only if $d_i = 1$

Definition 6.1.3: Cyclotomic Polynomials

Let $n \in \mathbb{N} \setminus \{0\}$. Define the nth cyclotomic polynomial as

$$\Phi_n(x) = \prod_{\substack{0 \leq i < n \\ \gcd(n,i)=1}} (x - \zeta_n^i)$$

In other words the polynomial is the product over all linear factors of primitive nth roots of unity.

Proposition 6.1.4

The cyclotomic polynomials factorizes in $\mathbb{C}[x]$ into

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Proposition 6.1.5

For each $n \in \mathbb{N}$, $\Phi_n(x)$ is monic and has coefficients in $\mathbb{Z}$.

6.2 Cyclotomic Fields

Definition 6.2.1: n-th Cyclotomic Field

Let $n \in \mathbb{N}$ and let $\zeta_n = e^{2\pi i/n}$ denote the nth root of unity. Define the n-th cyclotomic field to be $\mathbb{Q}(\zeta_n)$.

Proposition 6.2.2

Let p be a prime number. Then the minimal polynomial of ζ_p is the nth cyclotomic polynomial Φ_n. In particular, we have that

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

This is exactly the Euler totient function $\phi(n)$ in number theory.

7 Radial and Soluble Extensions

7.1 Radical Extensions

Roughly speaking, a polynomial is soluble by radicals if its roots can be expressed using nth roots. This motivates the definition of radical extensions and soluble extensions.

Definition 7.1.1: Radical Extensions

A field extension L/K is radical if there is a sequence of subfields

$$K = F_0 < F_1 < \cdots < F_n = L$$

such that $F_k = F_{k-1}(\alpha_i)$ where $\alpha_i^{n_i} \in F_{k-1}$ for some $n_i > 0$.

Proposition 7.1.2

Suppose that $\text{char}(K) = 0$. If L/K is a radical extension, then there exists a finite extension M/L so that M/K is both radical and Galois.

Definition 7.1.3: Soluble Extensions

A field extension L/K is soluble if L is contained in a field M with M/K radical. A polynomial $f \in K[x]$ is soluble by radicals if its splitting field L is soluble.

Thus, if f is soluble by radicals, every element of its splitting field has an expression that involves only nth roots, field operations and elements of K.

Proposition 7.1.4

Let K be a field such that $\text{char}(K) = 0$. If L/K is a radical extension, then there is a finite extension M/L so that M/K is both radical and Galois.

8 Transcendental Extensions

8.1 Transcendence Basis

Definition 8.1.1: Algebraically Independent

Let K/F be a field extension. We say that a set $S \subset K$ is algebraically independent if for any finite set $\{a_1, \dots, a_n\} \subseteq S$, there exists no $f \in F[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) = 0$. We say that S is algebraically dependent otherwise.

An algebraically independent set of elements behave similarly to variables in a polynomial ring. The following statement demonstrates this.

Lemma 8.1.2

Let K/F be a field extension and let $\{a_1, \dots, a_n\} \subset K$ be an algebraically independent set of elements. Then $F[a_1, \dots, a_n]$ is F-isomorphic to $F[x_1, \dots, x_n]$. Moreover $F(a_1, \dots, a_n)$ is F-isomorphic to $F(x_1, \dots, x_n)$.

Proposition 8.1.3

Let K/F be a field extension. Let $t_1, \dots, t_n \in K$. Then the following statements are equivalent.

- $\{t_1, \dots, t_n\}$ is algebraically independent over F
- For each i, t_i is transcendental over $F(t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_n)$
- For each i, t_i is transcendental over $F(t_1, \dots, t_n)$.

Definition 8.1.4: Transcendence Basis

Let K/F be a field extension. A subset S of K is a transcendence basis for K/F if S is algebraically independent over F and if K is algebraic over $F(S)$.

Lemma 8.1.5

Let K be a field extension of F. Let $S \subseteq K$ be algebraically independent over F. If $t \in K$ is transcendental over $F(S)$, then $S \cup \{t\}$ is algebraically independent over F.

We can now prove that every field extension has a transcendence basis.

Proposition 8.1.6

Every field extension has a transcendence basis.

Similar to bases in vector spaces, the cardinality of any two transcendence basis is the same.

Theorem 8.1.7

Let K be a field extension of F. If S and T are transcendence bases for K/F, then $|S| = |T|$.

Again, recall that linearly independent sets can be extended to a basis and spanning sets can be reduced to a basis in vector spaces. There is similar analogue for transcendence basis.

Theorem 8.1.8

Let K/F be a field extension. Then the following are true.

- If $T \subseteq K$ is such that $K/F(T)$ is algebraic, then T contains a transcendence basis.
- If $S \subseteq K$ is algebraically independent, then S is contained in a transcendence basis of K/F.

8.2 Transcendence Degree

The following definition is well defined since the cardinality of transcendence basis is an invariant of field extensions.

Definition 8.2.1: Transcendence Degree

Let K/F be a field extension. Define the transcendence degree $\text{trdeg}(K/F)$ of K/F to be the cardinality of any transcendence basis of K/F.

Proposition 8.2.2

Let K/F and L/K be field extensions. Then

$$\text{trdeg}(L/F) = \text{trdeg}(L/K) + \text{trdeg}(K/F)$$

8.3 Linear Disjointness