# Field Theory

Donghyun Park

January 21, 2026

## 1 Splitting Field and Simple extension

$f \in F[X]$, the field $E$ splitting field of $F$ then $E = F[\alpha_1, \cdots, \alpha_n]$ so not always equal to the $F[\alpha]$ for some root. Understanding following fundamental theorem is important

**Proposition 1** ([Mil22] Proposition 2.1)**.** *Let $F(\alpha)$ a simple extension of $F$ and $\Omega$ a second extension of $F$.*
*(a) Suppose $\alpha$ is transcendental over $F$. Then the **$F$-homomorphism** $\varphi : F(\alpha) \to \Omega$ and **Elements in** $\Omega$ **transcendental over** $F$ has one-to-one correspondence.*

$$F\textbf{-}\textbf{\textit{homomorphisms}}\ F(\alpha) \to \Omega \longleftrightarrow \textbf{\textit{Elements of}}\ \Omega\ \textbf{\textit{transcendental over}}\ F$$
$$\varphi \longleftrightarrow \varphi(\alpha)$$

*(b) Suppose $\alpha$ is algebraic over $F$. Then there exists a one-to-one correspondence **$F$-homomorphisms** $\varphi : F[\alpha] \to \Omega$ and **Roots of $f$ in** $\Omega$*

$$F\textbf{-}\textbf{\textit{homomorphisms}}\ \varphi : F[\alpha] \to \Omega \longleftrightarrow \textbf{\textit{Roots of}}\ f\ \textbf{\textit{in}}\ \Omega$$
$$\varphi \longleftrightarrow \varphi(\alpha)$$

I think this proposition as some **Number of Freeness for extending fields**. We'll recover later.

Next, I want to mention **the** Splitting field. $f \in F[X]$, $E$ is a splitting field if $f$ splits in $E$ and $E$ is generated by roots of $f$.
By [Mil22] Proposition 2.1, the following holds.

**Proposition 2** ([Mil22] Proposition 2.12)**.** *$f \in F[X]$, $E$ be an extension of $F$ generated by roots of $f$ in $E$ and $\Omega$ be an extension of $F$ splitting $f$. There exists at most $[E : F]$ numbers of $F$-homomorphism $\varphi : E \to \Omega$ and it equals to $[E : F]$ if $f$ has distinct roots in $\Omega$*

Proof is by inductively defining image of the roots of $f$. $E = F[\alpha_1, \cdots, \alpha_m]$ then we choose minimal polynomial of $\alpha_1$ in $F$. Then $F[\alpha_1] \to \Omega$ has degree of freedom $\deg f_1 = [F[\alpha_1] : F]$. Precede with $F[\alpha_1]$ instead of $F[\alpha]$... we have

$$[F[\alpha_1, \cdots, \alpha_n] : F[\alpha_1, \cdots, \alpha_{n-1}]] \cdots [F[\alpha_1, \alpha_2] : F[\alpha_1]][F[\alpha_1] : F] = [E : F]$$

As a Corollary (Corollary 2.13 of [Mil22]), there exists an $F$-isomorphism between two splitting fields, by the above process. It is remarkable that **an isomorphism is not canonical**
Also we cannot just say $F[\alpha]$ generated by root of $f$. This only make sense when $f$ is irreducible by Proposition 2.1 of [Mil22]. Also we cannot just say $F[\alpha, \beta]$ generated by two roots of $f$ even if irreducible, because in $F[\alpha]$, $f$ might be not irreducible and the choice of $\beta$ might be subtle.

Some examples provides good toy models.
- Example 2.8 of [Mil22]: $f(X) = (X^p - 1)/(X - 1) \in \mathbb{Q}[X]$ then splitting field of $f$ is just $\mathbb{Q}[\zeta]$ since the other roots are $\zeta^2, \cdots, \zeta^{p-1}$
- Example 2.9 of [Mil22]: $F$ has characteristic $p \neq 0$, $f(X) = X^p - X - a$ where $a \in F$. If there exists some extension of $F$ which root is $\alpha$, the other roots are $\alpha + 1, \cdots, \alpha + p - 1$ so Splitting field is $F[\alpha]$

## 2 Separability

Separability of the polynomial $f \in F[X]$ is amazingly, can be determined in $F$! (Since the definition contains root of $f$ in splitting field, more natural is separability determined in the splitting field)
Moreover, very brief criteria exists.

**Proposition 3** ([Mil22] Proposition 2.20). *For a nonconstant irreducible polynomial $f$ in $F[X]$, FSAE*
*(a) $f$ has a multiple root*
*(b) $gcd(f, f') \neq 1$*
*(c) $F$ has nonzero characteristic p and $f$ is a polynomial in $X^p$*
*(d) all the roots of $f$ are multiple*

The fact that $gcd(f, g)$ defined on $F[X]$ where $f, g \in F[X]$ is invariant over field extensions.

# 3 The Fundamental Theorem of Galois Theory

The gist of the Galois theory is, for the galois extension $E/F$ of field, all the subextensions $E \supset M \supset F$ is encoded by the subgroup of Galois group $Gal(E/F)$.
We call the extension $E/F$ is Galois if it is finite (so must be algebraic), normal, and separable.
$Gal(E/F) = Aut(E/F)$, the automorphisms of $E$ fixing $F$.

**Theorem 1** ([Mil22] Theorem 3.10). *For an extension $E/F$, FSAE*
*(a) $E$ is the splitting field of a separable polynomial $f \in F[X]$*
*(b) $E$ is finite over $F$ and $F = E^{Aut(E/F)}$*
*(c) $F = E^G$ for some finite group $G$ of automorphisms of $E$*
*(d) $E$ is Galois over $F$*

As an Corollary, if $E/F$ is Galois with Galois group $G$ then

$$[E : F] = (G : 1)$$

Now the gist of the Galois theory is in the next theorem

**Theorem 2** (Fundamental Theorem of Galois Theory). *Let $E$ be a Galois extension of $F$ with Galois group $G$. There exists a bijection between*

$$\textbf{\textit{subgroups of }} H \textbf{\textit{ of }} G \longleftrightarrow \textbf{\textit{subextensions }} F \subset M \subset F$$
$$H \leftrightarrow E^H$$
$$Gal(E/M) \leftrightarrow M$$

*Moreover,*
*(a) $H_1 \supset H_2 \Leftrightarrow E^{H_1} \subset E^{H_2}$*
*(b) $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$*
*(c) $\sigma H \sigma^{-1} \leftrightarrow \sigma M$*
*(d) $H$ normal in $G \Leftrightarrow E^H$ is Galois over $F$.*

$$Gal(E^H/F) \simeq G/H$$

Now we can translate the problem on field extension to the group theory.

## 3.1 Examples

[Mil22] includes remarkable examples. First one is analyzing $\mathbb{Q}[\zeta]/\mathbb{Q}$ where $\zeta$ is a primitive 7th root of unity.
$\mathbb{Q}[\zeta]$ is the splitting field of $X^7 - 1$. So $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 6$, Galois of degree 6.
$\sigma \in Gal(\mathbb{Q}[\zeta]/\mathbb{Q})$ sends $\zeta$ to the root of minimal polynomial; $\zeta^i$. So let $\sigma : \zeta \mapsto \zeta^3$ then it generates the Galois group. Galois group is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.
There are two intermediate subfields, each corresponding to $\{0, 3\}$ and $\{0, 2, 4\}$. To determine these fields, it is just $\mathbb{Q}[\zeta]^H$ where $H$ is a subgroup.
(1) $H = \{0, 3\}$. $\sigma^3\zeta = \zeta^{27} = \bar{\zeta}$ so one fixed element is $\zeta + \bar{\zeta}$.

$$\mathbb{Q}[\zeta] \supset \mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} \supset \mathbb{Q}[\zeta + \bar{\zeta}] \supsetneq \mathbb{Q}$$

By degree analysis, $\mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} = \mathbb{Q}[\zeta + \bar{\zeta}]$. And since $H$ is normal, this extension is Galois
(2) $H = \{0, 2, 4\}$. $\sigma^2\zeta = \zeta^2$ and $\sigma^4\zeta = \zeta^4$ so

$$\mathbb{Q}[\zeta] \supset \mathbb{Q}[\zeta]^{\langle\sigma^2\rangle} \supset \mathbb{Q}[\zeta + \zeta^2 + \zeta^4] \supsetneq \mathbb{Q}$$

By the degree analysis, $\mathbb{Q}[\zeta]^{\langle\sigma^2\rangle} = \mathbb{Q}[\zeta + \zeta^2 + \zeta^4]$ and since $(\beta - \sigma\beta)^2 = -7$, $\mathbb{Q}[\beta] \supset \mathbb{Q}[\sqrt{-7}]$ but by degree analysis, it is $\mathbb{Q}[\sqrt{-7}]$

See also the [Mil22] Example 3.23.

Another example: $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}]$ is Galois over $\mathbb{Q}$ with Galois group the quaternion group.

# 4 Galois Groups of Polynomials

## 4.1 Discriminant

For $f \in F[X]$ separable and the splitting field $F_f$ over $F$. $G_f = Gal(E_f/F)$
In $E_f$, if $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

$$D(f) = \Delta(f)^2$$

As each Galois group permuting the roots of $f$, $\sigma\Delta(f) = sgn(\sigma)\Delta(f)$ and $\sigma D(f) = D(f)$ (Proposition 4.1 of [Mil22]).
Thus by the fundamental theorem of Galois theory, $D(f) \in F$ and if $char(F) \neq 2$, $G_f \subset A_n$ if and only if $\Delta(f) \in F$ or $D(f) \in F^2$

## 4.2 Transitivity

Each Galois element permutes the roots of irreducible parts. Conversely, $f(X) \in F[X]$ separable, irreducible then Galois group permutes roots transitively (Proposition 4.5 of [Mil22])

## 4.3 Degree 2 polynomial

$F$ a field of odd characteristic and $f$ not a square. Then

$$f \text{ irreducible} \Leftrightarrow D(f) \text{ not a square} \Leftrightarrow G_f = S_2$$

## 4.4 Degree 3 polynomial

$F$ a field of $char(F) \neq 3$ and $f$ irreducible, separable.
$G_f = A_3$ or $S_3$, determined by whether $D(f)$ is a square or not.
- $X^3 - 3X + 1$, $D(f) = 9^2$, $G_f = A_3$
- $X^3 + 3X + 1$, $D(f) = -135$, $G_f = S_3$

## 4.5 Degree 4 polynomial

Read [Mil22] Chapter 4. Quartic polynomials. It classifies all possible Galois group.

## 4.6 Existence of polynomial in $\mathbb{Q}[X]$ having Galois group $S_p$

Read [Mil22] Chapter 4. Examples of polynomials with $S_p$ as Galois group over $\mathbb{Q}$

## 4.7 Dedekind's Theorem

Dedekind theorem provides Galois group of polynomial viewed as permuting roots must contain some element.

**Theorem 3** ([Mil22] Theorem 4.28)**.** *$f(X) \in \mathbb{Z}[X]$ monic degree $m$. If $p$ is a prime, $f$ modulo $p$ has only simple roots and $\bar{f} = \prod_{i=1}^{r} f_i$ which are irreducible with degree $m_i$ in $\mathbb{F}_p[X]$. Then $G_f$ contains $\sigma_f$ represented by cycle $\sigma_1 \cdots \sigma_r$ with each cycle of length $m_i$*

This proof is very beautiful, constructing **Frobenius Automorphism**
For $E$ a finite Galois extension of $\mathbb{Q}$ with Galois group $G$ and $\mathcal{O}_E$ be the ring of integers in $E$. $P$ be a prime ideal of $\mathcal{O}_E$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$. Then there exists a unique element $\sigma_P \in G$ such that $\sigma_P P = P$ and $\sigma_P(a) \equiv a^p (mod\ P)$ for all $a \in \mathcal{O}_E$. We call $\sigma_P$ a Frobenius automorphism.
Why is this Frobenius automorphism important? Currently, I cannot give a full answer.

## 5 Finite Fields

$E$ be a field of characteristic $p$. It contains subfield $\mathbb{F}_p = \{m1_E | m \in \mathbb{Z}\}$. If $E$ is a field of degree $n$ over $\mathbb{F}_p$, $q = p^n$ elements. Then $E$ is a splitting field for $X^q - X$.
In other words **Any two field with $q = p^n$ elements are isomorphic**

**Proposition 4** ([Mil22] Proposition 4.19)**.** *Every extension of finite fields is simple*

*Proof.* Using that for the finite field $E$, $E^\times$ is a cyclic group. For field extension $E/F$, the generator of $E^\times$, $\zeta$ satisfies $E = F[\zeta]$ □

Next, we can find the Galois group $Gal(\mathbb{F}_q/\mathbb{F}_p)$.

**Proposition 5** ([Mil22] Proposition 4.20)**.** *$Gal(\mathbb{F}_q/\mathbb{F}_p)$ is a cyclic group generated by the Frobenius automorphism $\sigma(a) = a^p$*

*Proof.* $a \in \mathbb{F}_q$ fixed by $\sigma$ is $a^p = a$ which are roots of $X^p - X = 0$ is exactly $\mathbb{F}_p$. By Galois theorem.

$$\langle \sigma \rangle = Gal(\mathbb{F}_q/\mathbb{F}_p)$$

$$|Gal(\mathbb{F}_q/\mathbb{F}_p)| = |\langle \sigma \rangle| = n = [\mathbb{F}_q : \mathbb{F}_p]$$

□

So we can generate subgroup of $Gal(\mathbb{F}_q/\mathbb{F}_p)$ by $\langle \sigma^{n/m} \rangle$ which gives a subfield of $p^m$ elements.

**Corollary 1** ([Mil22] Corollary 4.21)**.** *$E$ be a field with $p^n$ elements. For every $m|n$, $E$ contains exactly one field with $p^m$ elements.*

**Corollary 2** ([Mil22] Corollary 4.22)**.** *$f \in \mathbb{F}_p[X]$ be a monic irreducible of degree $d$. If $d|n$ then $f$ occurs exactly once as a factor of $X^{p^n} - X$*

This gives us to find all the monic irreducible polynomials of $\mathbb{F}_p$. We can just look at factoring of $X^{p^n} - X$. From this, we can prove the existence of algebraic closure.

**Proposition 6** ([Mil22] Proposition 4.24)**.** *The field $\mathbb{F}_p$ has an algebraic closure $\mathbb{F}$*

*Proof.* Motivation is Proposition 4.23 of [Mil22]. If such algebraic closure exists, then there exists only one copy of each $\mathbb{F}_{p^n}$ and the relationship

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$$

holds.
So defining $\mathbb{F}_{p^{n!}}$ inductively by arguing $\mathbb{F}_{p^{n!}}$ be a splitting field of $X^{p^{n!}} - X$ over $\mathbb{F}_{p^{(n-1)!}}$

$$\mathbb{F} = \bigcup \mathbb{F}_{p^{n!}}$$

□

## 6 Primitive Element Theorem

**Theorem 4** ([Mil22] Theorem 5.1)**.** *$E = F[\alpha_1, \cdots, \alpha_r]$ be a finite extension of $F$ and assume $\alpha_2, \cdots, \alpha_r$ are separable over $F$. Then there exists $\gamma \in E$ such that $E = F[\gamma]$*

We call this $\gamma$ a primitive element.
From this, we can see that there are only finitely many intermediate fields.

**Proposition 7** ([Mil22] Proposition 5.3)**.** *$E = F[\gamma]$ simple algebraic extension of $F$. Then there exists only finitely many intermediate fields $M$,*

$$F \subset M \subset E$$

*Proof.* The minimal polynomial of $\gamma$ on $M[X]$ divides minimal polynomial on $F[X]$ □

## 7 The normal basis theorem

**Theorem 5** ([Mil22] Theorem 5.18)**.** *Every Galois extension has a normal basis. That is, there exists a basis of form $\{\sigma\alpha \mid \sigma \in Gal(E/F)\}$ for $\alpha \in E$*

Proof is quite complicated. Read [Mil22] Chapter 5. The normal basis theorem section.

# 8 Fundamental Theorem of Algebra

**Theorem 6** ([Mil22] Theorem 5.6)**.** *$\mathbb{C}$ is algebraically closed.*

# 9 Cyclotomic extensions, Cyclic extensions, Kummer theorem

## 9.1 Cyclotomic extension

We consider the roots of unity.

**Proposition 8** ([Mil22] Proposition 5.8)**.** *$F$ be a field of characteristic not dividing $n$, $E$ a splitting field of $X^n - 1$*
*(a) There exists a primitive $n$th root of 1 in $E$.*
*(b) $E = F[\zeta]$ for primitive $n$th root of unity $\zeta$*
*(c) $E/F$ is Galois, and there exists an injective homomorphism*

$$Gal(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

But $Gal(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is not always surjective. But it is true in $F = \mathbb{Q}$. The key is **cyclotomic polynomial** $\Phi_n(X) = \prod(X - \zeta)$.

**Lemma 1** ([Mil22] Lemma 5.9)**.** *$F$ be a field of characteristic not dividing $n$, $\zeta$ a primitive $n$th root of uninty in some extension of $F$. FSAE*
*(a) $\Phi_n$ irreducible*
*(b) $[F[\zeta] : F] = \varphi(n)$*
*(c) $Gal(F[\zeta]/F) \xrightarrow{\simeq} (\mathbb{Z}/n\mathbb{Z})^\times$*

In $\mathbb{Q}[X]$, the cyclotomic polynomial is really irreducible.

## 9.2 Cyclic extensions

We want to classify all cyclic extensions of $F$. We assume $F$ **contains primitive $n$-th root of unity**
Then every degree $n$ extension is of following form.

**Proposition 9** ([Mil22] Proposition 5.27)**.** *In the above setting, if $E = F[\alpha]$ where $\alpha^n \in F$ and no smaller power of $\alpha$ is in $F$. Then $E/F$ is Galois with cyclic Galois group of order $n$.*
*Conversely, if $E$ is a cyclic extension of $F$ of degree $n$, then $E = F[\alpha]$ for $\alpha^n \in F$*

*Proof.* The key idea and the importance of the condition: $F$ **containing primitive root of unity** is,
(in converse direction) $\sigma$ generating $G$ and $\zeta$ primitive $n$-th root of unity,

$$\sum_{i=0}^{n-1} \zeta^i \sigma^i$$

is nonzero function (Dedekind's character theorem) so

$$\alpha = \sum_{i=0}^{n-1} \zeta^i \sigma^i \gamma \neq 0$$

satisfies $\sigma\alpha = \zeta^{-1}\alpha$ □

And these extensions are differ by

**Proposition 10** ([Mil22] Proposition 5.28)**.** *Two cyclic extensions of degree $n$, $F[a^{\frac{1}{n}}], F[b^{\frac{1}{n}}]$ in common field $\Omega$ are equal iff $a, b$ generates the same subgroup of $F^\times/F^{\times n}$*

## 9.3 Kummer theory

More generally, we want to classify all extensions of $F$ (containing primitive $n$-th root of unity) whose Galois group is abelian of exponent $n$. (i.e. Every $g \in Gal(E/F)$, $g^n = 1$ and $n$ is the smallest number satisfying. So this group is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^r$)
By the Hilbert's Theorem 90 (Read [Mil22] Chapter 5. Hilbert's theorem 90)

**Theorem 7** ([Mil22] Theorem 5.30)**.** *The map $E \mapsto F^\times \cap E^{\times n}$ defines 1-1 correspondence*
*(a) Finite abelian extensions of $F$ of exponent $n$ contained in some fixed algebraic closure $\Omega$ of $F$*
*(b) Subgroups $B$ of $F^\times$ containing $F^{\times n}$ as a subgroup of finite index.*
*The inverse map is $B \mapsto F[B^{\frac{1}{n}}]$ which is the smallest subfield of $\Omega$ containing $F$ and an $n$-th root of every element of $B$. Moreover*

$$[E : F] = (B : F^{\times n})$$

This again inherits **Galois philosophy**. We can find abelian extensions of exponent $n$ by finding groups. Main idea is the isomorphism

$$F^\times \cap E^{\times n}/F^{\times n} \xrightarrow{\simeq} Hom(Gal(E/F), \mu_n)$$

established by the Hilbert's Theorem 90. If $E/F$ is abelian extension of exponent $n$,

$$(F^\times \cap E^{\times n} : F^{\times n}) = |Hom(G, \mu_n)| = |(G : 1)| = [E : F]$$

# 10 Galois Solvability Theorem

Another central theorem : that the solvable by radicals in field can be move on to solvability of group is Galois's solvability theorem. Read [Mil22] Chapter 5, Proof of Galois's solvability theorem.

# References

[Mil22] James S. Milne. *Fields and Galois Theory (v5.10)*. Available at www.jmilne.org/math/. 2022.