13.4

Splitting Fields AND Algebraic Closures

(8.15)

Splitting Fields

Def. (Splitting Fields)

If the extension K of field F has the property such that: for $f(x) \in F[x]$, $f(x)$ factors completely into linear factors over K and $f(x)$ doesn't factor completely into linear factors over any proper subfield of K containing F,

Then K is called the splitting field of $f(x)$.

#1 Th. (Splitting Field exists.)

For any field F, if $f(x) \in F[x]$, then there exists an extension K of F which is a splitting field for $f(x)$.

Proof. (by induction)

We will prove #1 Th. by casework on the degree n of $f(x)$: let the field extension of F in which $f(x)$ splits completely into linear factors be E.

Case #1 $n = 1$. $\Rightarrow$ Take $E = F$.

Case #2. $n > 1$.

- If the irreducible factors of $f(x)$ over F are all of degree 1, then take $E = F$.

- Otherwise, there exists an irreducible factor $p(x)$ of $f(x)$ that has at least degree 2. Then there exists E_1 / F such that $p(x)$ has a root in E_1.

Consider $F(x)$ over E_1: $f(x)$ has a linear factor $(x-\alpha)$. The degree of the remaining factor $f_1(x)$ is $n-1$, and by induction ☺ there exists an extension E of E_1 that contains all the roots of $f_1(x)$. Since $\alpha \in E_1$, E is an extension of F that contains all the roots of $f(x)$. Let K be the intersection of all the subfields of E containing F and all the roots of $f(x)$ ☺. Then K is the splitting field of $f(x)$.

😐 Induction process: (really abstract)

Take any irreducible factor $p(x)$ of $f(x)$ that has degree $m \geq 2$.

① E_1 is an extension of F with a root (α) of $p(x)$. Over E_1, $p(x)$ has the factor $(x-\alpha)$. $p(x)/(x-\alpha)$ now has degree $m-1$.

If p has any other linear factors over E_1, then the roots given by these factors are also in E_1. Suppose p has k linear factors over E_1 $(x-\alpha_1), (x-\alpha_2), \ldots, (x-\alpha_k)$. Then define

$p_1(x) = p(x) / (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$, which is irreducible over E_1 and has degree $(m-k)$.

② Take any irreducible factor $g_1(x)$ of $p_1(x)$ that has degree $l \geq 2$. Then there exists E_2 / E_1 with a root (β) of $g_1(x)$. Over E_2, $g_1(x)$ has the factor $(x-\beta)$.

If $g_1(x)$ has any other linear factors over E_2, then the roots given by these factors are also in E_2. Suppose $g_1(x)$ has k_1 linear factors over E_2: $(x-\beta_1), (x-\beta_2), \ldots, (x-\beta_{k_1})$. Define

$p_2(x) = g_1(x) / (x-\beta_1)(x-\beta_2)\ldots(x-\beta_{k_1})$, which is irreducible over E_1 into linear factors, and has degree $(m-k-k_1)$.

③ Since the degree of the polynomial in question decreases with each iteration, at some point it will factor completely into linear factors, which is the base case $n=1$.

Perform this induction process on every choice of $p(x), g_1(x), \ldots, g_s(x)$ and we are done.

☺ Because we want the splitting field to be the smallest.

Def (Normal Extensions)

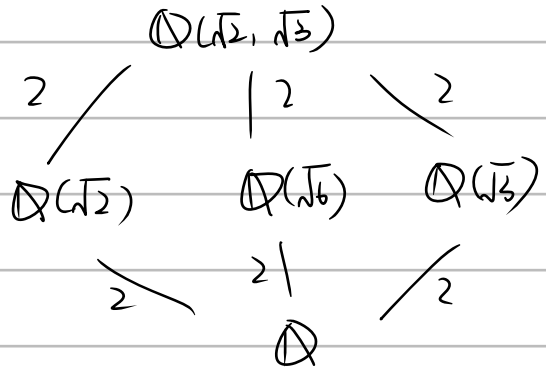
If K is an algebraic extension of F which is the splitting field over F for a collection of $f(x) \in F[x]$,

Then K is called a <u>normal extension</u> of F.

Ex. (1) The splitting field of x^2-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$.

(2) The splitting field of $(x^2-2)(x^2-3)$ is the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

The diagram of known subfields:



※ $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{6})(\sqrt{2})$
$= \mathbb{Q}(\sqrt{6})(\sqrt{3})$.

(8.16)

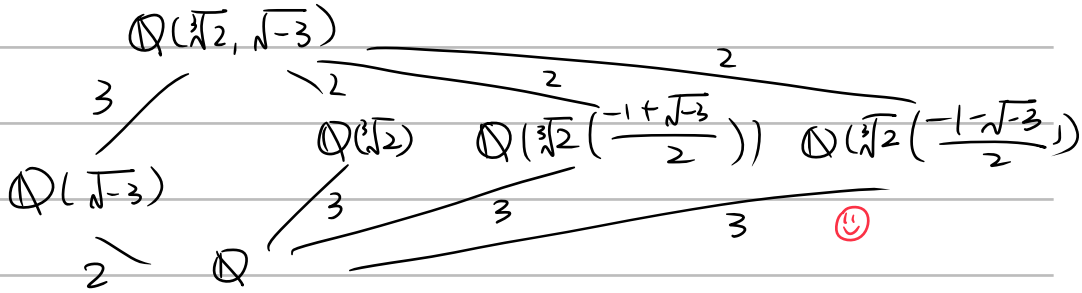
(3) Splitting Field of x^3-2 over $\mathbb{Q}$:

The roots of x^3-2 in $\mathbb{C}$ are

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\left(\frac{-1+\sqrt{3}i}{2}\right), \quad \sqrt[3]{2}\left(\frac{-1-\sqrt{3}i}{2}\right)$$

We will form the splitting field by adjoining the roots to $\mathbb{Q}$: first adjoin $\sqrt[3]{2}$ to obtain $\mathbb{Q}(\sqrt[3]{2})$. Note that the 2 complex roots are both linear combinations of $\sqrt{3}i$ with rational coefficients, so the splitting field is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$.

It follows that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = 6$:



☺ Since x^3-2 is the minimal polynomial of all 3 roots over $\mathbb{Q}$, adjoining a root to $\mathbb{Q}$ gives an extension of degree 3.

(4) Splitting field of x^4+4 over $\mathbb{Q}$:

At first sight, it seems like the splitting field is a degree 4 extension of $\mathbb{Q}$. but

$$x^4+4 = (x^4+4x^2+4) - 4x^2$$
$$= (x^2+2)^2 - (2x)^2 = (x^2+2x+2)(x^2-2x+2).$$

Solving for the roots of factors gives us $\pm 1, \pm i$. So the splitting field is $\mathbb{Q}(i)$, an extension of degree 2.

#1 Prop. (degree of splitting field)
A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

Reasoning. If $f(x) \in F[x]$ is a polynomial of degree n, then adjoining a root of $f(x)$ to F creates a field extension of at most degree n over F (the extension is of degree n if $f(x)$ is irreducible). Then the remaining polynomial $f_1(x)$ has degree $n-1$. Adjoining a root of $f_1(x)$ to F creates a field extension of degree at most $n-1$, so on and so forth.

$\Rightarrow$ The splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

#1 Ex. (Splitting Fields of $x^n - 1$: Cyclotomic Fields)
Consider the splitting field of $x^n - 1$ over $\mathbb{Q}$. The roots of the polynomial $x^n - 1$ are the nth roots of unity.

Over $\mathbb{C}$, there are n distinct solutions of the equation $x^n = 1$:

$$e^{\frac{2\pi k}{n} i} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right).$$

For any splitting field $K/\mathbb{Q}$ of $x^n - 1$, the nth roots of unity form a group since for $\alpha^n = 1$, $\beta^n = 1$, $(\alpha\beta)^n = 1$, so they're closed under multiplication. In addition:

Lemma. The nth roots of unity form a cyclic group under multiplication.

Reasoning. Here's a handy theorem: a finite subgroup of the multiplicative subgroup of a field is cyclic.

Def. (Primitive root of unity)
A generator of the cyclic group of nth roots of unity is called a primitive nth root of unity.

Let ζ_n denote a primitive nth root of unity. The other primitive nth roots of unity are therefore ζ_n^a with $1 \le a < n$ coprime to n. Therefore there are $\varphi(n)$ primitive nth roots of unity

An easy example is taking the nth root of unity

$$\zeta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Then all the other nth roots of unity are $\zeta_n^k = e^{2\pi ik/n}$, indicating that ζ^r is a primitive nth root of unity.

The splitting field of $x^n - 1$ over $\mathbb{Q}$ is therefore $\mathbb{Q}(\zeta_n)$ and it has a fancy name.

Def. (Cyclotomic Field)

The field $\mathbb{Q}(\zeta_n)$ is called the cyclotomic field of nth roots of unity.

The degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$:

Special Case Consider the case when $n = p$ is a prime. Then we have the factorization

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

Since $\zeta_p \neq 1$, ζ_p is a root of the (Irreducible) polynomial ← Assume this.

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

$\Phi_p(x)$ is irreducible, so it's the minimal polynomial of ζ_p over $\mathbb{Q}$, so

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

General Case! See 13.6.

(Hint: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.)

☺ Recall this property of cyclic groups:

An element $g \in U_n$ is a generator if and only if $|g| = n$. This requires that g is a power of a known generator coprime with n.

eg. if $g = g_0^k$ where $k \mid n$, then $|g| = \frac{n}{k}$ which implies that g is not a generator.

Ex. (Splitting Field of $x^p - 2$)

Consider the splitting field of $x^p - 2$. If α is a root of $x^p - 2$, then $\zeta\alpha$ is also a root of $x^p - 2$, where ζ is any pth root of unity:

If $\alpha^p = 2$, then $(\zeta\alpha)^p = 1 \cdot \alpha^p = 2$.

Therefore the solutions of $x^p - 2$ are

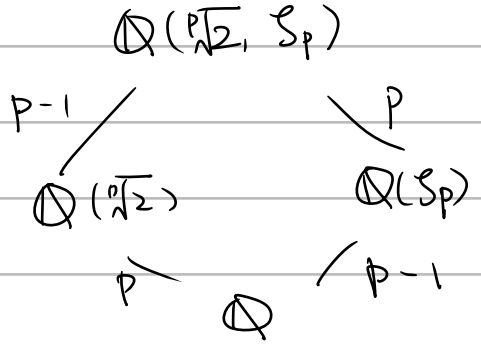
$\zeta \sqrt[p]{2}$, where ζ is any pth root of unity.

It is then easy to see that the splitting field of $x^p - 2$ is precisely $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ for any primitive pth root of unity ζ_p.

Degree of splitting field:

Since $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is generated over $\mathbb{Q}(\zeta_p)$ by $\sqrt[p]{2}$, $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}(\zeta_p)] \leq p$. Also $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, so $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \leq p(p-1)$. In addition, since $\mathbb{Q}(\sqrt[p]{2})$ and $\mathbb{Q}(\zeta_p)$ are subfields, $p \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]$ and $p-1 \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]$. Therefore $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$.

Diagram of subfields:



#2 Th. (Splitting Fields & Isomorphism)

Let $\varphi: F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial & let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma: E \to E'$, i.e. σ restricted to F is the isomorphism φ:

$$\begin{array}{ccc} \sigma: & E & \xrightarrow{\sim} E' \\ & | & | \\ \varphi: & F & \xrightarrow{\sim} F' \end{array}$$

Proof (Strong Induction)

Preregs. Recall that any isomorphism $F \xrightarrow{\sim} F'$ induces a natural isomorphism $F[x] \xrightarrow{\sim} F'[x]$. In particular, if $f(x) \to f'(x)$ under this isomorphism, then the irreducible factors of $f(x)$ in F correspond to the irreducible factors of $f'(x)$ in F.

Base Case. ($f(x)$ splits completely over F)

If $f(x)$ has all its roots in F then $f'(x)$ has all its roots in F', i.e. $f'(x)$ splits completely over F', take splitting fields $E = F$ & $E' = F'$. Then $\sigma = \varphi$, and the statement is proved for

- $n = \deg(f(x)) = 1$;
- $f(x)$ factors completely into linear factors over F.

Induction Hypothesis. Suppose that the statement is already proved for any field F, isomorphism φ, and $\deg f(x) < n$.

Let $p(x)$ be an F-irreducible factor of $f(x)$ of degree ≥ 2, and $p'(x)$ be the corresponding factor of $f'(x)$. If $\alpha \in E$ is a root of $p(x)$ and $\beta \in E'$ is a root of $p'(x)$, then we can extend φ to isomorphism $\sigma': F(\alpha) \xrightarrow{\sim} F'(\beta)$:

$$\begin{array}{ccc} \sigma': & F(\alpha) & \xrightarrow{\sim} F'(\beta) \\ & | & | \\ \varphi & F & \xrightarrow{\sim} F' \end{array}$$

Write $F_1 = F(\alpha)$, $F_1' = F'(\beta)$, so we have $F_1 \hookrightarrow F_1'$. We have $f(x) = (x-\alpha) f_1(x)$ over F_1 where $f_1(x)$ has degree $(n-1)$ and $f'(x) = (x-\beta) f_1'(x)$ where $f_1'(x)$ has degree $(n-1)$. The field E is a splitting field for $f(x)$ over F_1: all the roots of $f_1(x)$ are in E and if there exists a smaller field $L \subset F$ also containing all the roots of $f_1(x)$, since $\alpha \in F_1$, L contains all the roots of $f(x)$, contradicting the minimality of the splitting field of $f(x)$. Similarly, E' is the splitting field of $f_1'(x)$ over F_1'.

By the induction hypothesis, we can extend σ' to isomorphism σ:

$$\begin{array}{ccc} \sigma: & E & \hookrightarrow & E' \\ & | & & | \\ \sigma': & F_1 & \hookrightarrow & F_1' \\ & | & & | \\ \varphi & F & \hookrightarrow & F' \end{array}$$

Then σ is an extension of isomorphism φ, proving the statement for $\deg(f(x)) = n$. Q.E.D. □

#1 Cor. (Uniqueness of Splitting Field)

Any 2 splitting fields of polynomial $f(x) \in F[x]$ over F are isomorphic.

Proof: Refer to the proof of #2 Th. Set $F = F'$ and $f(x) = f'(x)$. This induces the identity isomorphism of F to itself.

☺ Recall this theorem in 13.2:

$$\begin{array}{ccc} \sigma: & F(\alpha) & \hookrightarrow & F'(\beta) \\ & | & & | \\ \varphi: & F & \hookrightarrow & F' \end{array}$$

Algebraic Closures

Def. (Algebraic Closures)

The Field $\bar{F}$ is called an <u>algebraic closure</u> of F if:

- $\bar{F}$ is algebraic over F;
- Every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$.

Def (Algebraically Closed Fields)

A field F is said to be algebraically closed if every polynomial $f(x) \in F[x]$ has a root in F.

#2 Prop. (Algebraic Closures are algebraically closed.)

Let $\bar{F}$ be an algebraic closure of F. Then $\bar{F}$ is algebraically closed.

Proof Let $f(x) \in \bar{F}[x]$ and α be a root of $f(x)$. Then α generates an algebraic extension $\bar{F}(\alpha)$ over $\bar{F}$. Since $\bar{F}$ is algebraic over F, $\bar{F}(\alpha)$ is algebraic over F. Then $\alpha \in \bar{F}$, so $\bar{F}$ is algebraically closed.

※ Note that if K is algebraically closed, then any $f(x) \in K[x]$ has <u>all</u> its roots in K. Consider a root α of $f(x)$ in K. Then $f(x) = (x-\alpha)f'(x)$ ($f'(x) \in K[x]$), so $f'(x)$ also has a root in K, so on and so forth. Eventually we arrive at the point where every root of $f(x)$ is in K.

#3 Th. (Algebraically closed field extensions)

For any field F there exists an algebraically closed field containing F.

Proof I took one look at the proof and decided yeah, I'm not doing that.

#3 Prop (Construction of Algebraic Closures)

Let K be an algebraically closed field & F be a subfield of K. Then the collection of elements $\bar{F}$ of K that are algebraic over F is an algebraic closure of F.

An algebraic closure of F is unique up to isomorphism.

Proof

Part #1 By definition, $\bar{F}$ is an algebraic extension of F. Every polynomial $f(x) \in F[x]$ factors completely into linear factors of the form $(x-\alpha)$ over K with α as a root of $f(x)$. Therefore α is algebraic over F and therefore already belongs to $\bar{F}$.

It follows that every linear factor $(x-\alpha)$ has coefficients in $\bar{F}$, i.e. $f(x)$ splits completely over $\bar{F}$, so $\bar{F}$ is an algebraic closure of F.

Part #2 Too complicated for my brain to comprehend. (Spoiler: it contains ideals.)

FTA & Stuff Essential for Galois Theory.

#4 Th (Fundamental Theorem of Algebra.)

The field $\mathbb{C}$ is algebraically closed.

Proof Will be proven in Chap 14. Galois Theory.

#2 Cor $\mathbb{C}$ contains an algebraic closure for any of its subfields ($\mathbb{Q}$, $\mathbb{R}$, etc.)