Normal extensions

Recall: Let F be a field and $f(x) \in F[x]$ be irreducible

$\rightsquigarrow K := F[x]/(f(x))$ is a finite extension of F

- $f(x)$ has a zero in K, namely $\theta := x \bmod (f(x))$

Definition. Given a field F and a polynomial $f(x) \in F[x]$ of degree n, a field extension K/F is called a splitting field (分裂域) of $f(x)$, if

did not say $f(x)$ is irreducible.

(1) $f(x)$ splits completely in $K[x]$: $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_1, \dots, \alpha_n \in K$, and

(2) $K = F(\alpha_1, \dots, \alpha_n)$

Remark: If E is an intermediate field of K/F, then K is a splitting field of $f(x) \in E[x]$ over E.

Theorem. For any field F and $f(x) \in F[x]$ of degree n, a splitting field K of F exists.

Moreover, $[K:F] \leq n!$

Proof: Use induction on $\deg f(x) = n$.

$n=1$. ✓ Suppose the theorem is proved for $<n$.

(If $f(x)$ factors already completely, ✓)

Let $p(x)$ be an irreducible factor of $f(x)$.

Then $E := F[x]/(p(x))$ is a field extension of F of $\deg p(x) \leq \deg f(x) = n$,

over which $p(x)$ has a zero.

$\rightsquigarrow p(x) = (x-\theta) \cdot ?$ in $E[x]$

$\Rightarrow f(x) = (x-\theta) \cdot g(x) \rightsquigarrow$ reduces to $g(x) \in E[x]$

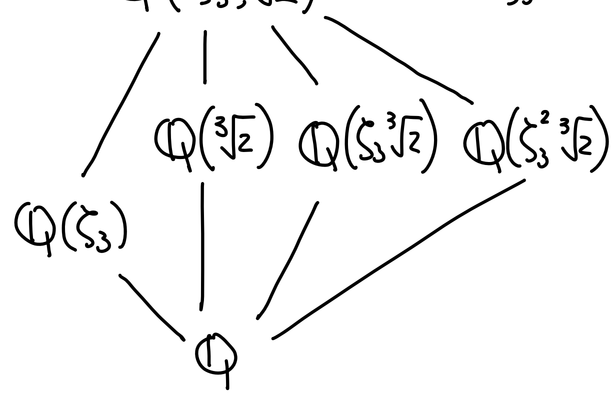
$$\left.\begin{array}{c} K \\ | \\ E \end{array}\right) \leq (n-1)!$$

By inductive hypothesis, $g(x)$ factors completely over some K/E with $[K:E] \leq (n-1)!$

$\left.\begin{array}{c} | \\ F \end{array}\right) \leqslant n \qquad \Rightarrow [K:F] \leqslant n! \qquad \square$

<u>Examples</u> ① splitting field of x^2-2 is $\mathbb{Q}(\sqrt{2})$

② splitting field of x^3-2 is $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ $\qquad \zeta_3 = e^{2\pi i/3}$



③ Splitting field of $x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$ is $\mathbb{Q}(\zeta_n) \leftarrow n^{\text{th}}$ cyclotomic field

Will see later $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

e.g. $x^p - 1 = (x-1)\,\Phi_p(x)$. So $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$

<u>"Uniqueness" of splitting field</u>?

<u>Lemma</u>. If $\eta : F \xrightarrow{\sim} \tilde{F}$ is an isomorphism of fields and $p(x) \in F[x]$ is irreducible, then $\tilde{p}(x) := \eta(p(x))$ is irreducible in $\tilde{F}[x]$.

Moreover $F[x]/(p(x)) \xrightarrow{\eta} \tilde{F}[x]/(\tilde{p}(x))$

<u>Example</u>: $\eta : \mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2}) \qquad a+b\sqrt{2} \longmapsto a-b\sqrt{2}$

$\rightsquigarrow \mathbb{Q}\left(\sqrt{5+\sqrt{2}}\right) \simeq \mathbb{Q}(\sqrt{2})[x]/(x^2-5-\sqrt{2}) \overset{\eta}{\simeq} \mathbb{Q}(\sqrt{2})[x]/(x^2-5+\sqrt{2}) \simeq \mathbb{Q}\left(\sqrt{5-\sqrt{2}}\right)$

<u>Lemma</u>. Let $\eta : F \longrightarrow \tilde{F}$ be an isomorphism and $f(x) \in F[x] \rightsquigarrow \tilde{f}(x) := \eta(f(x)) \in \tilde{F}[x]$

If E is a splitting field of $f(x)$ over F and $\tilde{E}$ is a splitting field of $\tilde{f}(x)$ over $\tilde{F}$, then $\exists$ isomorphism $\sigma : E \xrightarrow{\sim} \tilde{E}$ restricting to $\eta : F \longrightarrow \tilde{F}$

exists but may not be unique.

So splitting fields are (noncanonically) isomorphic to each other.

Proof: We will prove that, for the splitting field K of $f(x)$ constructed in the previous theorem, we have the following diagram

$$\begin{tikzcd} E & K \arrow[l, "\sim"'] \arrow[r, "\sim"] & \tilde{E} \\ F \arrow[u, dash] \arrow[r, equal] & F \arrow[u, dash] \arrow[r, "\sim"] & \tilde{F} \arrow[u, dash] \end{tikzcd}$$

Suffices to construct $K \xrightarrow{\sim} \tilde{E}$, the other isomorphism is similar.

Will prove something stronger:

<u>Claim</u>: If $\eta: F \xrightarrow{\sim} \tilde{F}$ is an isomorphism, and $\tilde{E}$ an extension of $\tilde{F}$ on which $\eta(f(x))$ splits completely, then η extends to

$$\begin{tikzcd} K \arrow[r, dashed, "\sigma"'] & \tilde{E} \\ F \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\sim", "\eta"'] & \tilde{F} \arrow[u, dash] \end{tikzcd}$$

As in the above proof, we make an induction on $\deg(f)$

At each step, we considered

$$\begin{tikzcd} L = F[x]/(p(x)) \arrow[r, dashed, "?"'] & \tilde{E} \\ F \arrow[u, dash] \arrow[r, "\sim"] & \tilde{F} \arrow[u, dash] \end{tikzcd}$$

As $\eta(p(x)) =: \tilde{p}(x)$ has a zero in $\tilde{E}$, say $\alpha \in \tilde{E}$

$\exists$ a homomorphism $\sigma_L : L = F[x]/(p(x)) \longrightarrow \tilde{E}$

$$x + (p(x)) \longmapsto \alpha$$

At the end of the induction, we get $\sigma: K \longrightarrow \tilde{E}$ compatible with $\eta: F \xrightarrow{\sim} \tilde{F}$

This proves the claim. $\square$

If $\tilde{E}$ is a splitting field of $\eta(f(x))$, note $\eta(f(x))$ already splits over $\sigma(K) \Rightarrow \sigma(K) = \tilde{E}$ $\square$

Observation 1. If
$$\begin{tikzcd} & K \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & \tilde{E} \arrow[dl, dash] \\ & F & \end{tikzcd}$$
are field extensions, such that both E and $\tilde{E}$ are splitting fields of some polynomial $f(x) \in F[x]$

Then $E = \tilde{E}$

(b/c $f(x)$ splits in E as $c(x-\alpha_1)\cdots(x-\alpha_n)$
and splits in $\tilde{E}$ as $c(x-\tilde{\alpha}_1)\cdots(x-\tilde{\alpha}_n)$ $\Big\} \Rightarrow$ Viewed in $K[x]$, $\{\alpha_1,\cdots,\alpha_n\} = \{\tilde{\alpha}_1,\cdots,\tilde{\alpha}_n\}$

So $E = \tilde{E}$ as subfield of K.)

Observation 2
$$\begin{tikzcd} K \arrow[d, dash] \\ E \arrow[d, dash] \\ F \end{tikzcd}$$
If E is a splitting field over F of some polynomial $f(x) \in F[x]$, then $\forall$ automorphism $\sigma : K \to K$ s.t. $\sigma|_F = \mathrm{id}$,

$$\sigma(E) = E$$

(b/c $\sigma(E)$ is the splitting field of $\sigma(f) = f$. By Observation 1 $\Rightarrow \sigma(E) = E$.)

Intrinsic definition of splitting fields

no finiteness assumption needed

An algebraic extension K/F is called normal (正规扩张) if

* for any irreducible polynomial $f(x) \in F[x]$ that has a zero in F, $f(x)$ splits completely in K.

Theorem. A finite extension K/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.

Proof: "$\Rightarrow$" $K = F(\alpha_1, \cdots, \alpha_r)$ for some $\alpha_1, \cdots, \alpha_r \in K$

$\rightsquigarrow$ minimal polynomial $m_{\alpha_i}(x) \in F[x]$ splits in $K[x]$

$\Rightarrow$ K is the splitting field of $m_{\alpha_1}(x) \cdots m_{\alpha_r}(x)$.

"$\Leftarrow$" K/F is the splitting field of $f(x) \in F[x]$

If $p(x) \in F[x]$ is an irreducible polynomial that has a zero α in K.

L Let $L :=$ splitting field over K of $p(x)$ (WTS $L = K$)

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

Clearly, L is the splitting field of $f(x)p(x)$ over F

Let β be a zero of $p(x)$ in L

$$\Rightarrow \exists \; F(\alpha) \xrightarrow{\sim} F(\beta) \text{ isomorphism fixing } F$$

$$\alpha \longmapsto \beta$$

This isomorphism extends to an automorphism σ of L, as L is the splitting field of $f(x)p(x)$ over $F(\alpha)$ and over $F(\beta)$

By Observation 2 $\Rightarrow \sigma(K) = K$

But $\alpha \in K \Rightarrow \sigma(\alpha) = \beta \in K \Rightarrow L = K$. $\square$

<u>Corollary</u>. If K/F is finite and normal, for any intermediate field E, K/E is normal.

↑ true for K/F algebraic

(<u>not</u> true for E/F)

b/c K is the splitting field of some $f(x) \in F[x] \subseteq E[x]$

<u>Definition</u> If K/F is an algebraic extension, a <u>normal closure</u> of K/F (正规闭包) is a field extension L/K s.t. (1) L/F is normal

(2) If $L \subseteq L' \subseteq K$ is such that L'/F is normal, then $L = L'$

<u>Lemma</u>. A normal closure of a finite extension K/F exists and is unique up to (some) isomorphism.

Proof: <u>Existence</u>: Say $K = F(\alpha_1, \cdots, \alpha_r)$ and $f(x) = \prod_i m_{\alpha_i, F}(x) \in F[x]$

Take L = a splitting field of f over K

$\Rightarrow L$ is a splitting field $/F \Rightarrow L/F$ normal

(2) is clear as L is generated by zeros of $f(x)$.

"<u>Uniqueness</u>": If L' is another normal closure of K/F

$$\Rightarrow \exists \text{ splitting field of } f \text{ over } K \hookrightarrow L'$$
$$\underset{L}{\shortparallel}$$

By minimality of normal closure $\Rightarrow L = L'$

* **Example**: Splitting field of $x^p - t$ over $\mathbb{F}_p(t)$

$$\begin{array}{c} \mathbb{F}_p(t^{1/p}) \\ | \\ \mathbb{F}_p(t) \end{array} \qquad x^p - t = \underbrace{(x - t^{1/p})^p}$$

This factorization looks strange

Origin of the pathology: Let F be a field

If $\mathrm{char}\, F = 0$, no pathology

If $\mathrm{char}\, F = p > 0$, define the Frobenius endomorphism (Frobenius 自同态) on F to be

$\sigma : F \longrightarrow F \qquad \sigma(x) = x^p$ (automatically injective)

Note $\sigma(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{1} x y^{p-1} + y^p \overset{\text{b/c } p=0 \text{ in } F}{=} x^p + y^p = \sigma(x) + \sigma(y)$

$\sigma(xy) = \sigma(x)\sigma(y)$

Say F is perfect (完全域) if σ is an isomorphism

$\iff$ any element $a \in F$ is a p^{th} power (of a unique element of F)

Examples $F = \mathbb{F}_p$ is a perfect field (so is any finite field)

b/c $\sigma : F \to F$ is injective $\Rightarrow$ surjective by counting.

$F = \mathbb{F}_p(t)$ is not a perfect field,

$\sigma(\mathbb{F}_p(t)) = \mathbb{F}_p(t^p)$

$F = \mathbb{F}_p(t, t^{1/p}, t^{1/p^n};\, n \in \mathbb{N})$ is a perfect field

Lemma Algebraic extensions of perfect fields are still perfect.

Proof: K/F algebraic and F perfect $\overset{?}{\Longrightarrow}$ K perfect

Say $\mathrm{char}(F) = p > 0$. For $\alpha \in K$, suffices to show that α has a p^{th} root in $E = F(\alpha)$

$E = F(\alpha)$ View this as field extensions:

$$\begin{tikzcd}[arrows=dash]
\sigma(E) \arrow[dd] & \\
& F \\
\sigma(F) \arrow[ur] &
\end{tikzcd}$$

$$[E:\sigma(E)][\sigma(E):\sigma(F)] = [E:F]\cdot[F:\sigma(F)]$$

But σ induces isomorphisms $E \xrightarrow{\sim} \sigma(E)$, $F \xrightarrow{\sim} \sigma(F)$

$\Rightarrow [\sigma(E):\sigma(F)] = [E:F]$ (is finite)

$\Rightarrow [E:\sigma(E)] = [F:\sigma(F)] = 1.$ $\square$

<u>Corollary</u>: K/F finite, K perfect $\Leftrightarrow$ F perfect

(<u>Caveat</u>: not true that K/F algebraic, K perfect $\Rightarrow$ F perfect.

<u>Example</u>: $K = \mathbb{F}_p(t, t^{1/p}, \dots)$, $F = \mathbb{F}_p(t)$.)

<u>Remark</u>: Can define $[F:\sigma(F)] = p^{\lambda(F)}$ to be a measurement of imperfectness of F

Then E/F finite $\Rightarrow \lambda(E) = \lambda(F)$

but E/F algebraic $\Rightarrow \lambda(E) \leq \lambda(F)$.