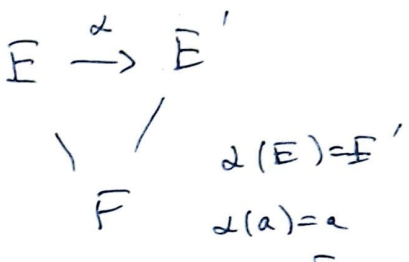
$f(x) \in F[x]$, E/F - splitting field of f is f factors into linear terms in E, $f = c(x-\alpha_1)\cdots(x-\alpha_n)$, and $E = F(\alpha_1, \ldots \alpha_n)$.

Last time:

Thm: Any two splitting fields of F, E/F, E'/F are isomorphic over F.

$\#$ of isomorphisms $\leq [E:F]$



If f is <u>separable</u> $/F$, then

$\#$ of isomorphisms $= [E:F] =$ degree $\dim_F(E)$

$f = f_1 \cdot \ldots \cdot f_r$ (irreducible $/F$)

<u>separable</u>: each f_i has only simple roots in any extension K/F

$\Leftrightarrow (f_i, f_i') = 1 \Leftrightarrow Df_i \neq 0$

Df_i

<u>Inseparable</u>: need char p and infinite field F.

$\mathrm{Gal}(E/F) = \alpha : E \to E$ isom, $\alpha(a) = a \ \forall a \in F$ $\quad \alpha|_F = id$

$\| \quad G(E/F)$

α restricted to F is identity.

<u>Remark</u>: If E is splitting field of $f(x)$

$\alpha_1 \ldots \alpha_n$ roots of f in E.

$g \in \mathrm{Gal}(E/F) \Rightarrow g(\alpha_i) = \alpha_j$ some α_j

A root of f goes to a root of f under $g \in \mathrm{Gal}(E/F)$.

$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad f(\alpha_i) = 0$

$a_0 + a_1 \alpha_i + \cdots + a_n \alpha_i^n = 0 \xrightarrow{g} a_0 + a_1 g(\alpha_i) + \cdots + a_n g(\alpha_i)^n = 0$

Prop Given E/F, $\{\alpha_1 .. \alpha_n\}$ roots of $f(x) \in F[x]$ in $\bar{F}$, there is a homomorphism $\mathrm{Gal}(E/F) \longrightarrow$ permutation group of $\{\alpha_1 .. \alpha_n\}$

$\mathrm{Gal}(E/F) \longrightarrow S_n = S\{\alpha_1 .. \alpha_n\}$.

Symmetric group on n elements.

Prop if E is a splitting field of $f \in F[x]$ and $\alpha_1 .. \alpha_n$ roots of f in F, homomorphism $\mathrm{Gal}(E/F) \longrightarrow S_n$ is injective

An automorphism $E \xrightarrow{\sigma} E$ is determined by its values on the roots.

Principle (informal) Galois groups for finite field extensions are not large.

Best-case scenario: E/F is a splitting field of separable $f \Rightarrow$

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

Otherwise, $|\mathrm{Gal}(E/F)| < [E:F]$ (an extension of Thm from last lecture).

Examples E/F, $[E:F]=2$. Take $\alpha \in E \setminus F$. Then $\{1, \alpha\}$ is a basis of E as F-vect. space. $\Rightarrow \alpha^2 + b\alpha + c = 0$ some $b, c \in F$.

$\Rightarrow \alpha$ is a root of $f(x) = x^2 + bx + c \in F[x]$.

If $\operatorname{char} F \neq 2$, can use familiar method to understand F.

$$x^2+bx+c = \left(x+\frac{b}{2}\right)^2 + c - \frac{b^2}{4} = \left(x+\frac{b}{2}\right)^2 - \left(\frac{b^2-4c}{4}\right) =$$

↑ need 2 to be invertible in F

Let $\mathcal{D} = b^2-4c \in F$ Discriminant of f

$$= \frac{1}{4}\left((2x+b)^2 - \mathcal{D}\right)$$

Let $y = 2x+b$ linear change of variables, $x = \frac{1}{2}(y-b)$ ↕

$$= \frac{1}{4}\left(y^2 - \mathcal{D}\right)$$

Exercise: $F[x]/(x^2+bx+c) \simeq F[y]/(y^2-\mathcal{D})$ $\operatorname{char} F \neq 2$

21
E.

In $\operatorname{char} \neq 2$, a quadratic extension reduces to $F[y]/(y^2-\mathcal{D})$

$\mathcal{D}$ not a square in F

$E = F[y]/(y^2-\mathcal{D}) \simeq F[\alpha]/(\alpha^2-\mathcal{D})$ $\quad x^2-\mathcal{D} = (x-\alpha)(x+\alpha)$

$\{\alpha, -\alpha\}$ roots of $x^2-\mathcal{D}$ in E

$\operatorname{Gal}(E/F)$: $\alpha \longleftrightarrow -\alpha$

$\simeq C_2$: identity, and permutation $\alpha \leftrightarrow -\alpha$ of the

$\sqrt{\mathcal{D}} \notin F$ ↑ $y^2-\mathcal{D}$ ↑ irreducible x^2+bx+c ← roots separable polynomial

$a+b\sqrt{\mathcal{D}} \xrightarrow{g} a-b\sqrt{\mathcal{D}}$ ↑ only nontrivial Galois symmetry

Note: $\operatorname{Gal}(E/F) \simeq C_2$ $|C_2| = 2 = [E:F]$

Case $F = \mathbb{Q}$. $\mathcal{D} = \frac{n}{m}$ $\sqrt{\frac{n}{m}} = \frac{1}{m}\sqrt{nm}$ ← integer. $\sqrt{k^2 n} = k\sqrt{n}$

$\Rightarrow$ can reduce to $n = p_1 \cdots p_r$ ← product distinct primes.

↑ ↑

Exercise: Degree 2 extensions $E/\mathbb{Q}$ are classified by

$n = \pm p_1 \cdots p_r$ - a finite collection of prime numbers.

$E = \mathbb{Q}[x]/(x^2 - n)$ splitting field of $x^2 - n$ $x^2-2, x^2-3, x^2-5, x^2-6, x^2-7, x^2-10, \ldots$

or

$E = \mathbb{Q}[x]/(x^2 + n)$ — // — of $x^2 + n$ $x^2+2, x^2+3, \ldots$

Note each such $E \subset \mathbb{C}$. There are 2 field homomorphisms

$E = \mathbb{Q}[\alpha]/(\alpha^2 - n)$

$E \to \mathbb{C}$ $\quad \mathbb{Q} \to \mathbb{C}$ only one homomorphism

$\alpha \mapsto \sqrt{n} \in \mathbb{R}_+$ 2 different embeddings

$\alpha \mapsto -\sqrt{n} \in \mathbb{R}_-$

$\mathrm{Gal}(E/\mathbb{Q}) \simeq C_2$ $\quad id,\ \alpha \mapsto -\alpha.$

Example $E = \mathbb{Q}[\alpha]/(\alpha^2 + \alpha + 1)$ $\quad D = 1 - 4 = -3$ $\quad y = 2\alpha + 1$

$\mathbb{Q}[y]/(y^2+3) \xrightarrow{2:1} \mathbb{C}$

$y \mapsto \pm\sqrt{-3}$

2 homomorphisms (field embeddings)

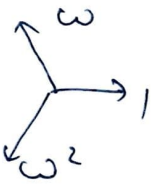
$\alpha = \frac{y-1}{2} = \frac{-1 \pm \sqrt{-3}}{2}$

$E \simeq \mathbb{Q}(\sqrt{-3}) \subset \mathbb{C}$.

$\mathrm{Gal}(E/\mathbb{Q}) \simeq C_2 : id,$

$y_1 \mapsto \sqrt{-3}$

$\alpha_1 \mapsto \frac{-1+\sqrt{-3}}{2} = \omega$



ω - 3rd root of unity

In this example, $6 \in C_2$, $6 \neq id$

extends to complex conjugation of $\mathbb{C}$.

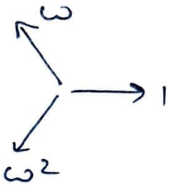
$F=\mathbb{Q}$, Splitting field of $f(x)=x^3-2$ irr. by Eisenstein. crit

take $\mathbb{C}$ and inside take splitting field of f

$E=\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ $\qquad \omega=e^{2\pi i/3}$

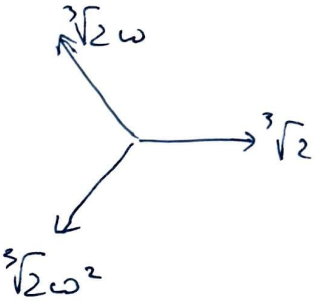
$\alpha_1 \quad \alpha_2 \quad \alpha_3$

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



$\mathbb{Q}(\sqrt[3]{2}) \simeq F(\alpha)/(\alpha^3-2)$ - not all of E.

only added 1 roots



$\mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$, $\mathbb{Q}(\alpha_3)$

3 different subfields of E

$[\mathbb{Q}(\alpha_i):\mathbb{Q}]=3$ basis $\{1, \alpha_i, \alpha_i^2\}$ $\qquad \alpha_i^3=2$

$\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2}\omega) \not\subset \mathbb{R}$ $\Rightarrow$ different subfields

$\mathbb{Q}(\omega)$ - subfield $\qquad \mathbb{Q}(\omega) \subset E \qquad \mathbb{Q}(\omega) \simeq \mathbb{Q}[\beta]/(\beta^2+\beta+1)$

$\omega = \alpha_2 \alpha_1^{-1} \in E$

$\mathbb{Q}(\alpha_1) \simeq \mathbb{Q}(\alpha_2) \simeq \mathbb{Q}(\alpha_3)$ same $\operatorname{irr}(\alpha_i, \mathbb{Q}) = x^3-2$.

have symmetries that permute them

$E \supset^{2} \mathbb{Q}(\alpha_i) \supset^{3} \mathbb{Q}$

$\uparrow$ add ω

$\omega \notin \mathbb{Q}(\sqrt[3]{2})$, $\Rightarrow \operatorname{irr}(\omega, \mathbb{Q}(\sqrt[3]{2})) = x^2+x+1$

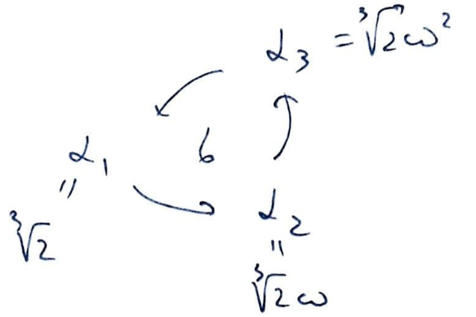
once add ω, α_2, α_3 are included too.

$[E:\mathbb{Q}]=6$, splitting field,

$\operatorname{Gal}(E/\mathbb{Q}) \longrightarrow S_3$ = permutations of $\{\alpha_1, \alpha_2, \alpha_3\}$

subgroup

$|\operatorname{Gal}(E/\mathbb{Q})| = 6$ (since separable) $\Rightarrow$ $\boxed{\operatorname{Gal}(E/\mathbb{Q}) = S_3.}$



one example of Galois symmetry ↑ for this σ

basis of E

$(1, \sqrt[3]{2}, \sqrt[3]{4})$ $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

$(1, \omega)$

$\Rightarrow$ multiply bases

$(1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega)$ basis $E/\mathbb{Q}$

$\sigma(\alpha_1) = \alpha_2,\ \sigma(\alpha_2) = \alpha_3,\ \sigma(\alpha_3) = \alpha_1$

$\Rightarrow \sigma(\alpha_2/\alpha_1) = \alpha_3/\alpha_2$

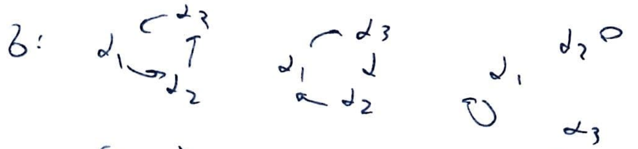
$\alpha_2/\alpha_1 = \omega$, $\alpha_3/\alpha_2 = \omega$

$\Rightarrow \sigma(\omega) = \omega$

Note that x^2+x+1 has 2 roots in E, $\omega, \omega^{-1} = \omega^2$

$\Rightarrow \sigma \in Gal(E/\mathbb{Q})$ $\sigma(\omega) = \omega$ or $\sigma(\omega) = \omega^2$

σ:

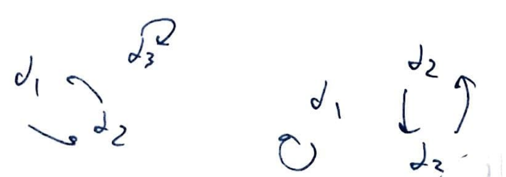


(123) (132) (1)(2)(3) = id

even permutations $\Rightarrow \sigma(\omega) = \omega$

σ: (12), (13), (23) ← this σ is induced by complex conjugation

$\mathbb{C} \to \mathbb{C}$ $z \mapsto \bar{z}$



$Gal(\mathbb{C}/\mathbb{R}) = C_2$

id, conjugation

$\mathbb{R}[\alpha]/(\alpha^2+1)$

$\alpha \to \alpha$

$\alpha \mapsto -\alpha$

odd permutations of roots $(\alpha_1, \alpha_2, \alpha_3)$ $\omega \to \bar{\omega} = \omega^2$

$E \supset \mathbb{Q}(\omega) \supset \mathbb{Q}$ ← preserved by all $\sigma \in Gal(E/\mathbb{Q})$.

↑ splitting field of x^2+x+1

E ← splitting field

$\cup$

B ← may or may not be a splitting field.

$\cup$ if

F

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ - trivial. No other roots of x^3-2 are in $\mathbb{Q}(\sqrt[3]{2})$ $\Rightarrow$ and σ takes $\sqrt[3]{2}$ to itself $\Rightarrow$ σ is identity

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$

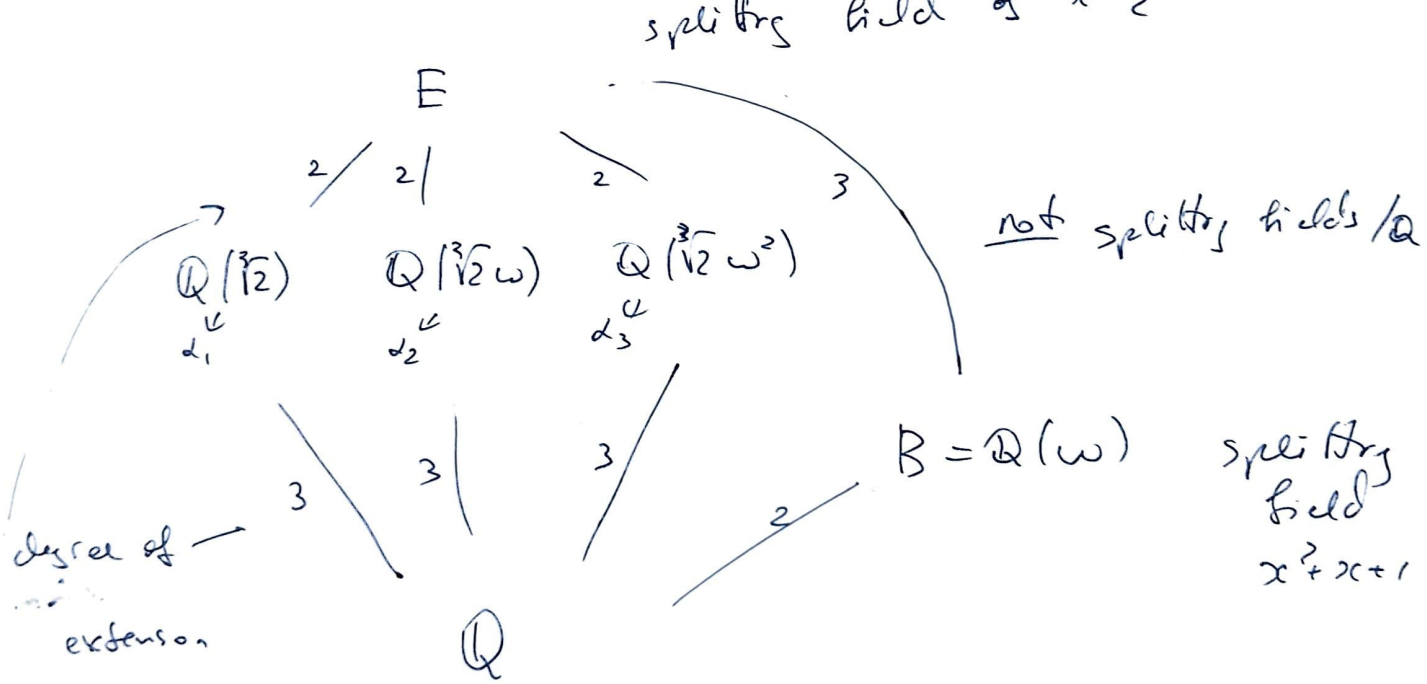
Same for $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\omega^2)/\mathbb{Q})$

$\mathrm{Gal}(E/B)$ $B=\mathbb{Q}(\omega)$ E is still splitting field of B for $P(x)=x^3-2$

only even permutations of $(\alpha_1,\alpha_2,\alpha_3)$ fix ω.

$\mathrm{Gal}(E/B) \cong C_3 \cong A_3$ - alternating group, cyclic group

Exercise: $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{2})) \cong C_2$



these are the only subfields of E.

$\mathbb{F}_p \subset \mathbb{F}$ $\quad F$ finite $\Rightarrow |F| = p^n \quad n = [F:\mathbb{F}_p]$

Remark el's of $\mathbb{F}_p$ are roots of $x^p - x = x(x-1)\cdots(x-(p-1))$ Fermat's little thm

$x^p - x = x(x^{p-1}-1)$, $|\mathbb{F}_p^*| = p-1 \Rightarrow \forall a \in \mathbb{F}_p^*,\ a^{p-1}=1$

$\Rightarrow \forall a \in \mathbb{F}_p,\ a^p = a.$

$q = p^n$

Consider polynomial $f(x) = x^{p^n} - x = x^q - x$

take splitting field $E/\mathbb{F}_p$ of $f(x)$. E - finite field

Ex if α, β are roots of $f(x)$ in $E \Rightarrow \alpha+\beta$ are roots, $\alpha\beta$ roots, α^{-1} root if $\alpha \neq 0$

$(\alpha+\beta)^q = \alpha^q + \beta^q$, iterate $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ $\quad (\alpha\beta)^q = \alpha^q\beta^q$

$\Rightarrow$ set of roots is an $\mathbb{F}_p$ - vector subspace of E., subfield of $E \Rightarrow$

E consists of all roots of $x^q - x$.

$f = x^q - x \quad f' = qx^{q-1} - 1 = -1 \quad \gcd(f, f') = 1 \Rightarrow f$ has no multiple roots $\Rightarrow$

f has q roots in splitting field $\Rightarrow |E| = q$.

Thm For each prime p, $n \geq 1$ there exists a

field of order p^n. Any two fields of order p^n are isomorphic.

$\mathbb{F}_q = \mathbb{F}_{p^n}$

$\mathbb{F}_q^* \cong C_{q-1}$ cyclic. Choose a generator α of $C_{q-1} \Rightarrow$

$\mathbb{F}_q \cong \mathbb{F}_p(\alpha)$ simple extension $\quad \mathrm{irr}(\alpha, \mathbb{F}_p) = g(x) \quad \deg g(x) = n$

$\Rightarrow \forall n \ \exists$ irr. polyn over $\mathbb{F}_p$ of deg n.

If $g(x)$ - irr $/\mathbb{F}_p$, $\deg g(x) = n \Rightarrow \mathbb{F}_p[x]/(g(x)) \cong \mathbb{F}_q \quad q = p^n$.

Any 2 irreducibles of the same degree define isomorphic fields $/\mathbb{F}_p$

Example $p=2$ $n=3$ $\mathbb{F}_8$

x^3+x^2+1, x^3+x+1 two irreps deg 3 / $\mathbb{F}_2$

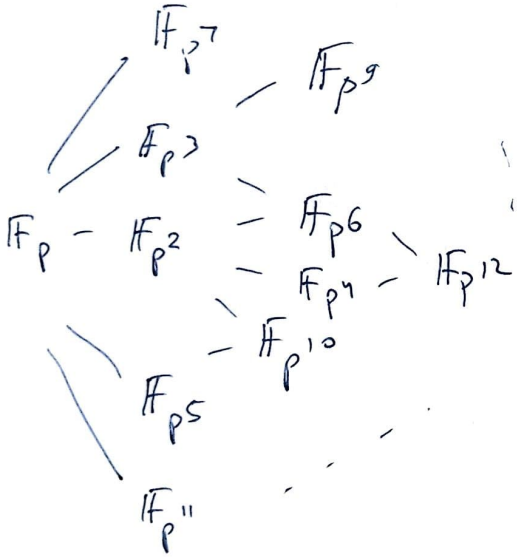
$\mathbb{F}_8 \simeq \mathbb{F}_2[\alpha]/(\alpha^3+\alpha^2+1) \simeq \mathbb{F}_2[\beta]/(\beta^3+\beta+1)$

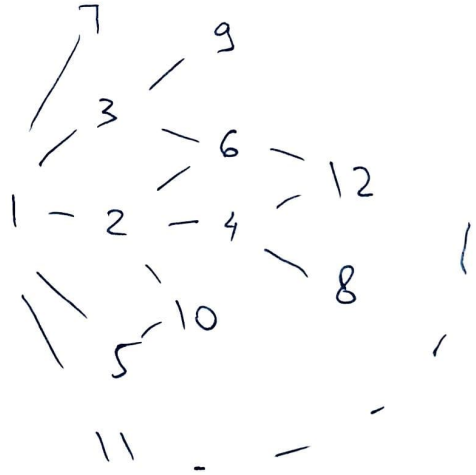
Prop $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$ iff $k \mid n$

$\mathbb{F}_4 \not\subset \mathbb{F}_8$ not a subfield

Since $\mathbb{F}_{p^n}$ must be a vect. space of dim m / p^k

$p^n = (p^k)^m = p^{km} \Rightarrow n = km \Rightarrow k \mid n$





$\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ Frobenius automorphism.

$\alpha \xrightarrow{\sigma_p} \alpha^p \xrightarrow{\sigma_p} (\alpha^p)^p = \alpha^{p^2} \xrightarrow{\sigma_p} \alpha^{p^3} \to \dots \xrightarrow{\sigma_p} \alpha^{p^n} = \alpha^q$

$(\sigma_p)^n \alpha = \alpha^q = \alpha$

Prop σ_p is an automorphism of order n on $\mathbb{F}_q$, $q = p^n$.

order cannot be smaller.

$\Rightarrow$ $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \mathrm{Aut}(\mathbb{F}_q) \simeq C_n$ generated by σ_p
Frobenius automorphism