Math 8202 Spring 2020 (Mar. 22+)

More on normal field extensions...

Recall

DEF'N $\mathbb{K}/\mathbb{F}$ is a normal extension if $\mathbb{K} = \text{split}_{\mathbb{F}}(\{f_i\}_{i\in I})$ for some $f_i \in \mathbb{F}[x]$

---

e.g. $\mathbb{Q}(\omega, \sqrt[3]{2}) = \text{split}_{\mathbb{Q}}(x^3-2)$ $\quad \omega = e^{2\pi i/3}$

$\mathbb{Q}(i, \sqrt[4]{7}) = \text{split}_{\mathbb{Q}}(x^4-7)$

are both normal over $\mathbb{Q}$,

but we claimed

$\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{7})$ are not.

How do we know?

(see Morandi Prop 3.28)

PROP. For $\mathbb{K}/\mathbb{F}$ algebraic, TFAE:

(i) $\mathbb{K}/\mathbb{F}$ normal, i.e. $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(\{f_i\})$ for some $\{f_i\}_{i \in I}$

(ii) Every nonzero field homom. $\mathbb{K} \xrightarrow{\varphi} \overline{\mathbb{F}}$ extending $1_{\mathbb{F}}$ has same image $\varphi(\mathbb{K})$

(iii) Every irred. $f(x) \in \mathbb{F}[x]$ with one root in $\mathbb{K}$ splits completely in $\mathbb{K}$ (has all its roots)

NON-EXAMPLES

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since $\mathbb{F}$

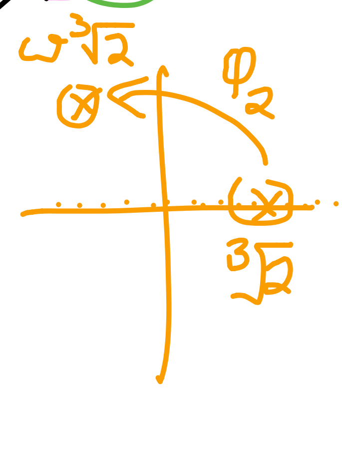
x^3-2 doesn't split completely

---

or because it has these two embeddings with different images

$$\overline{\mathbb{K}} = \overline{\mathbb{F}}$$

$$\begin{array}{ccccc}
\mathbb{K}=\mathbb{Q}(\sqrt[3]{2}) & \xhookrightarrow{\varphi_1} & \mathbb{Q}(\sqrt[3]{2}) & \hookrightarrow & \\
\sqrt[3]{2} & \longmapsto & \sqrt[3]{2} & & \overline{\mathbb{Q}} \subset \mathbb{C} \\
\sqrt[3]{2} & \longmapsto & \omega\sqrt[3]{2} & & \\
\mathbb{K}=\mathbb{Q}(\sqrt[3]{2}) & \xhookrightarrow{\varphi_2} & \mathbb{Q}(\omega\sqrt[3]{2}) & \nearrow &
\end{array}$$



$$\boxed{\varphi_1(\mathbb{K}) \neq \varphi_2(\mathbb{K})}$$

proof: (i) $\Rightarrow$ (ii)

$\left(\mathbb{K}/\mathbb{F} \text{ normal} \Rightarrow \text{all } \mathbb{K} \overset{\varphi}{\hookrightarrow} \overline{\mathbb{F}} \text{ extending } 1_{\mathbb{F}} \text{ have same image} \right)$

$$\mathbb{K} = \mathrm{split}_{\mathbb{F}}(\{f_i\}) = \mathbb{F}\Big(\{\underset{\text{within } \mathbb{K}}{\text{roots of } \{f_i\}\text{'s}}\}\Big)$$

$\Downarrow$ φ a field embedding

$$\boxed{\varphi(\mathbb{K})} = \mathbb{F}\Big(\{\underset{\text{within } \overline{\mathbb{F}}}{\text{roots of } \{\varphi(f_i)\}_{i\in I}}\}\Big)$$

$\{\varphi(f_i)\}_{i\in I} = \{f_i\}_{i\in I}$

φ extends $1_{\mathbb{F}}$

This RHS doesn't depend on φ ∎

(ii) $\Rightarrow$ (iii)

(all $\mathbb{K} \overset{\varphi}{\hookrightarrow} \overline{\mathbb{F}}$ have same image
$\Longrightarrow$ irred. $f(x) \in \mathbb{F}[x]$ with one root $\alpha \in \mathbb{K}$
has all roots $\alpha' \in \mathbb{K}$)

Given $\alpha \in \mathbb{K}$ a root of $f(x)$ irred. in $\mathbb{F}[x]$
and α' any other root of $f(x)$ in $\overline{\mathbb{K}}, = \overline{\mathbb{F}}$
Iso. Ext. Thm. gives

$$\begin{tikzcd}
\overline{\mathbb{K}} \arrow[r, dotted, "\exists \varphi"] & \overline{\mathbb{K}} \\
\mathbb{F} \arrow[u, hook] \arrow[r, "1_{\mathbb{F}}"] \arrow[ur, phantom, "\alpha \longmapsto \alpha'"] & \mathbb{F} \arrow[u, hook]
\end{tikzcd}$$

But then (ii) implies $1_{\mathbb{K}}$ and φ here

$$\begin{tikzcd}
 & \overline{\mathbb{K}} \\
\mathbb{K} \arrow[r, "1_{\mathbb{K}}"] & \mathbb{K} \arrow[u, hook] \\
\mathbb{F} \arrow[u, hook] \arrow[r, "1_{\mathbb{F}}"] & \mathbb{F} \arrow[u, hook]
\end{tikzcd}
\quad \text{versus} \quad
\begin{tikzcd}
 & \overline{\mathbb{K}} \\
\mathbb{K} \arrow[r, "\varphi"] & \varphi(\mathbb{K}) \arrow[u, hook] \\
\mathbb{F} \arrow[u, hook] \arrow[r, "1_{\mathbb{F}}"] & \mathbb{F} \arrow[u, hook]
\end{tikzcd}$$

have same image.

So $\varphi(\mathbb{K}) = \mathbb{K}$ and $\alpha' \in \varphi(\mathbb{K}) = \mathbb{K}$

(iii) $\Rightarrow$ (i)

(every irred. $f(x) \in \mathbb{F}[x]$ with one root $\alpha \in \mathbb{K}$ has all roots $\alpha' \in \mathbb{K}$
$\longrightarrow$ $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(\{f_i\})$ for some $\{f_i\}$)

This is easy since

$$(iii) \Rightarrow \mathbb{K} = \mathrm{split}_{\mathbb{F}}\left(\{m_{\mathbb{F},\alpha}(x) : \alpha \in \mathbb{K}\}\right)$$

minimal poly of α over $\mathbb{F}$

$\blacksquare$

MORAL: splitting fields $\mathbb{K}/\mathbb{F}$ = normal extensions are root-closed for irreducibles $f(x) \in \mathbb{F}[x]$

§13.5 Separability

Galois extensions are splitting fields for polynomials $\{f_i\}$ that avoid a certain pathology.

DEF'N: Say $f(x) \in \mathbb{F}[x]$ is separable if when we split it in some $\mathbb{K}$ (e.g. $\mathbb{K}=\overline{\mathbb{F}}$) it has distinct roots i.e.

$$f(x) = \alpha \prod_{i=1}^{n} (x-\alpha_i) \text{ with } \alpha_i \neq \alpha_j \text{ in } \mathbb{K} \text{ for } 1 \leq i < j \leq n$$

Say $f(x)$ is inseparable otherwise.

pathology!

EXAMPLES

① x^4+x^2+1 in $\mathbb{F}_2[x]$ is inseparable,
but for silly reasons:

$$x^4+x^2+1 = (x^2+x+1)^2$$

but x^2+x+1 is irreducible and separable

since in $\mathbb{K}=\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$ $\boxed{\alpha^2+\alpha+1=0}$

it splits as $(x+\alpha)(x+\alpha+1)$

so its roots are $\alpha, \alpha+1$

$\alpha \neq \alpha+1$

Can irreducibles $f(x) \in \mathbb{F}[x]$ ever be inseparable ??

Yes, but we need
$\left\{ \begin{array}{l} \text{prime characteristic} \\ \quad\quad \text{AND} \\ \text{transcendentals in } \mathbb{F} \end{array} \right.$

e.g.

---

② In $\mathbb{F}_p(t)[x]$,

→ $f(x) = x^p - t$ is both

irreducible (Eisenstein at (t)) and inseparable, !

because once we extend

$\mathbb{F}_p(t) \subset \mathbb{F}_p(t^{1/p}) = \mathbb{K}$ so $\alpha := t^{1/p}$

is a root of $f(x)$,

in $\mathbb{K}[x]$, $\boxed{f(x) = x^p - t = x^p - \alpha^p = (x-\alpha)^p}$

i.e. α is the only root, repeated p times!

Separability is easily predicted, before splitting to find roots.

PROP: $f(x) \in \mathbb{F}[x]$ is separable

$$\iff \gcd_{\mathbb{F}[x]}(f(x), f'(x)) = 1$$

[where $f(x) = a_0 + a_1 x + \dots + a_n x^n$
has $f'(x) := a_1 + 2a_2 x + 3a_3 x^2 + \dots + n a_n x^{n-1}$]

proof: We proved something more general in discussing Eisenstein ∎

COR: $f(x) \in \mathbb{F}[x]$ irreducible is separable $\iff f'(x) \neq 0$ in $\mathbb{F}[x]$.

proof: $\deg f' < \deg f$, f irred. $\Rightarrow$

$$\gcd(f, f') = \begin{cases} 1 & \text{if } f' \neq 0 \\ f(x) \neq 1 & \text{if } f' = 0. \end{cases}$$ ∎

EXAMPLES:

(1) $f(x) = x^4 + x^2 + 1$ in $\mathbb{F}_2[x]$

has $f'(x) = 4x^3 + 2x \equiv 0$ in $\mathbb{F}_2[x]$

so $\gcd(f, f') = f \neq 1$

and $f(x)$ is inseparable,

but $g(x) = x^2 + x + 1$ is irreducible

and has $g'(x) = 2x + 1 = 1 \not\equiv 0$ in $\mathbb{F}_2[x]$

so is separable.

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

has $f'(x) = \frac{d}{dx} f(x) = px^{p-1} \equiv 0$

so $\gcd(f, f') = f \neq 1$ and f is inseparable.

DEF'N: Say that a field $\mathbb{F}$ is **perfect** if every irreducible $f(x) \in \mathbb{F}[x]$ is separable, i.e. $f'(x) \neq 0$ $\forall$ irred. $f(x) \in \mathbb{F}[x]$.

PROP: (i) $\mathrm{char}(\mathbb{F}) = 0 \Rightarrow \mathbb{F}$ perfect

(ii) When $\mathrm{char}(\mathbb{F}) = p$ a prime p,

$\mathbb{F}$ is perfect $\iff \mathbb{F} = \mathbb{F}^p$ meaning that every $\alpha \in \mathbb{F}$ has a p^{th} root $\beta = \sqrt[p]{\alpha}$ in $\mathbb{F}$

$\iff$ the Frobenius endomorphism

$$\mathbb{F} \xrightarrow{F} \mathbb{F}$$
$$\beta \longmapsto \beta^p$$

surjects

(iii) Finite fields $\mathbb{F}$ are always perfect.

proof. (i) If $\mathrm{char}(\mathbb{F})=0$ then

$f(x)$ irred. in $\mathbb{F}[x] \Rightarrow \deg(f)\geq 1$

$\Rightarrow f'(x)\neq 0$

$\Rightarrow f(x)$ separable.

(ii) Assuming $\mathrm{char}(\mathbb{F})=p$ and $\mathbb{F}=\mathbb{F}^p$, let's show $\mathbb{F}$ is perfect (converse on HW).

Given $f(x)=a_0+a_1x+\dots+a_nx^n$ irred in $\mathbb{F}[x]$, if $0=f'(x)=\sum_{i=1}^{n} ia_ix^{i-1}$ then $\boxed{a_i=0 \text{ unless } i\equiv 0 \bmod p.}$

So $\boxed{f(x)=a_0+a_px^p+a_{2p}x^{2p}+\dots+a_{mp}x^{mp}}$

$= b_0^p+b_1^px^p+(b_2x^2)^p+\dots+(b_mx^m)^p$ where $\boxed{b_i=\sqrt[p]{a_{ip}}}$

$$\boxed{=(b_0+b_1x+b_2x^2+\dots+b_mx^m)^p}$$

not irreducible; contradiction

(iii) Note that Frobenius $\mathbb{F} \xrightarrow{F} \mathbb{F}$
$\beta \longmapsto \beta^p$

really is a ring endomorphism for a ring $\mathbb{F}$ of characteristic p,

since
$$\begin{cases} F(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = F(\alpha)F(\beta) \\ F(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p. \end{cases}$$

And when $\mathbb{F}$ is a field, it is injective since $F(1) = 1^p = 1 \neq 0$ implies $F \not\equiv 0$.

So if $\mathbb{F}$ is finite, $\mathbb{F} \xrightarrow{F} \mathbb{F}$ must also be surjective, and thus $\mathbb{F}$ is perfect. $\blacksquare$

We'll come back to finite fields later.

ASIDE | $\alpha \in \mathbb{K} \cong \mathbb{F}^n$ if $[\mathbb{K}:\mathbb{F}] = n$

for EXER 13.6.9
14.2.31

$=$ $\quad$ $\mathbb{F}$ $\quad$ as $\mathbb{F}$-vector spaces

$$\left(m_{\alpha,\mathbb{F}}(x) \right) = \ker\left(\begin{array}{ccc} \mathbb{F}[x] & \xrightarrow{ev_\alpha} & \mathbb{K} \\ x & \longmapsto & \alpha \end{array} \right)$$

defines $m_{\alpha,\mathbb{F}}(x)$

Given $A \in \mathbb{F}^{n\times n}$

the minimal poly $m_{A,\mathbb{F}}(x)$

is similarly defined

$$\left(m_{A,\mathbb{F}}(x) \right) = \ker\left(\begin{array}{ccc} \mathbb{F}[x] & \xrightarrow{ev_A} & \mathbb{F}^{n\times n} \\ x & \longmapsto & A \end{array} \right)$$

$\ni$

$\det(xI - A) \in \mathbb{F}[x]$

Chap. 12 FACT:

A diagonalizable $\iff$ $m_{A,\mathbb{F}}(x)$ has no repeated roots

$$A = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}$$

char poly

$$\det(xI - A) = (x-\lambda)^4$$

= min poly

$$(x-\lambda)^4$$

$$A = \left[\begin{array}{c|ccc} \lambda & 0 & 0 & 0 \\ \hline 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{array}\right]$$

char poly

$$= (x-\lambda)^4$$

but

min poly

$$(x-\lambda)^3$$

$$A = \begin{bmatrix} \lambda & & & \\ & \lambda & & \\ & & \lambda & \\ & & & \lambda \end{bmatrix}$$

char poly

$$(x-\lambda)^4$$

but

min poly $(x-\lambda)^1$

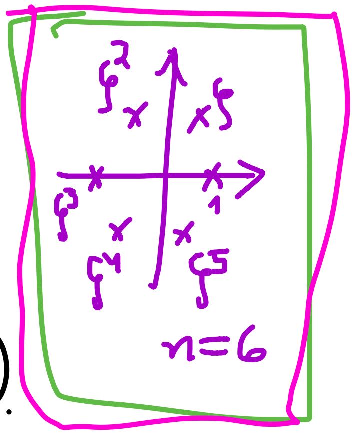
END ASIDE

§13.6 Cyclotomic extensions

We know x^n-1 has n distinct roots in $\mathbb{C}$,

namely $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$

$\zeta_n = e^{2\pi i/n}$



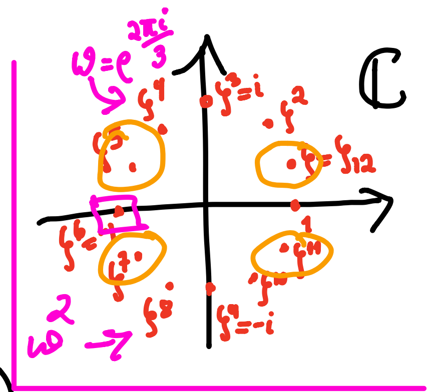
so $\mathbb{Q}(\zeta_n) = \text{split}_{\mathbb{Q}}(x^n-1)$

= the n^{th} cyclotomic extension of $\mathbb{Q}$

But what is $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$?

And $m_{\mathbb{Q},\zeta_n}(x)$?

EXAMPLE $n=12$



Factor $x^{12}-1 = (x^6-1)(x^6+1)$

$$= (x^3-1)(x^3+1)(x^2+1)(x^4-x^2+1)$$

$$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1)$$ in $\mathbb{Q}[x]$

roots: 1 | ζ^4, ζ^8 | $-1 = \zeta^6$ | ζ^2, ζ^{10} | $i, -i$ ($i = \zeta^3$, $-i = \zeta^9$) | $\zeta, \zeta^5, \zeta^7, \zeta^{11}$

$$= \Phi_1(x)\Phi_3(x)\Phi_2(x)\Phi_6(x)\Phi_4(x)\underbrace{\Phi_{12}(x)}_{= m_{\mathbb{Q},\zeta_{12}}(x)}$$

$\{1,2,3,4,6,12\} = \{d : d \mid 12\}$

DEF'N: n^{th} cyclotomic polynomial

$$\Phi_n(x) := \prod_{\substack{\text{primitive } n^{th} \\ \text{roots } \alpha \text{ of } 1 \text{ in } \mathbb{C}}} (x-\alpha) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$$

$$\left(\in \mathbb{Q}(\zeta_n)[x] \subset \mathbb{C}[x] \right)$$

PROP: (i) $x^n - 1 = \prod_{d \text{ dividing } n} \Phi_d(x)$ in $\mathbb{Q}[x]$

(ii) $\Phi_n(x)$ lies in $\mathbb{Z}[x]$, and is monic of degree $\varphi(n)$ (:= Euler phi function $= \#(\mathbb{Z}/n\mathbb{Z})^\times$)

EXAMPLES

① $\Phi_{12}(x) = (x-\zeta)(x-\zeta^5)(x-\zeta^7)(x-\zeta^{11})$
$= x^4 - x^2 + 1$ is monic of d $4 = \varphi(12)$)

② p prime $\Rightarrow$
$$\Phi_p(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

REMARK: Not all coefficients of $\Phi_n(x)$ are $+1, -1$
but n needs 3 odd prime factors to see it,

e.g. $\Phi_{3\cdot5\cdot7}(x) = \Phi_{105}(x)$ has a ± 2 coefficient

proof: (i) $x^n - 1 = \prod_{n^{th} \text{ roots } \alpha \text{ of } 1} (x-\alpha) = \prod_{d|n} \underbrace{\prod_{\text{prim. } d^{th} \text{ roots } \alpha \text{ of } 1} (x-\alpha)}_{\Phi_d(x) :=}$

(ii) Induction on n, using

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

e.g.

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)}$$

A product of monic polys in $\mathbb{Z}[x]$, so itself a monic poly in $\mathbb{Z}[x]$, hence same for the quotient, via division algorithm.

$\deg \Phi_n(x) = \#\{\text{primitive } n^{th} \text{ roots of } 1\}$
$= \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$

∎

THEOREM:

$\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$, and hence
- $\Phi_n(x) = m_{\mathbb{Q},\zeta_n}(x)$
- $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$

$\mathbb{Q}(i)/\mathbb{Q}$ has basis $\{1, i\}$ not $\{i, -i\}$

REMARK: When $n=p$ is a prime, we proved $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x^2 + x + 1$ was irreducible via a tricky usage of Eisenstein applied to $\Phi_p(x+1)$.

The proof for general n is surprisingly tricky to remember, although not hard to follow step-by-step; read it on pp 553-4 in §13.6 of D&F.

Chapter 14 Galois Theory

Understand $\mathbb{K}/\mathbb{F}$ with $[\mathbb{K}:\mathbb{F}]<\infty$

now via <u>symmetries</u>,

<u>DEF'N:</u> $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) := \left\{ \text{automorphisms of } \mathbb{K} \text{ over } \mathbb{F} \right.$

i.e.
$$\left.\begin{array}{ccc} \mathbb{K} & \xrightarrow[\sim]{\sigma} & \mathbb{K} \\ \uparrow & & \uparrow \\ \mathbb{F} & \xrightarrow{1_{\mathbb{F}}} & \mathbb{F} \end{array}\right\}$$

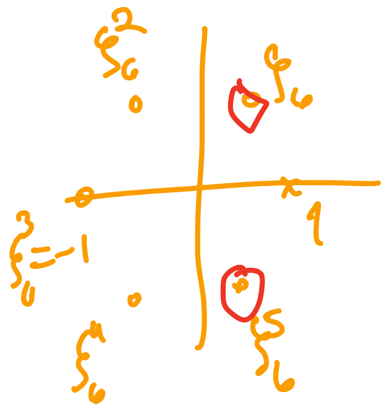
$= \mathrm{Gal}(\mathbb{K}/\mathbb{F})$

<u>EXAMPLES:</u>

① $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ is in $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$

(and in $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ but doesn't generate it)

② $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = ?$



$\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_6)/\mathbb{Q})$

is completely determined

by $\sigma(\zeta_6) \in \{\zeta_6^1, \zeta_6^5\}$

i.e. $\mathrm{Aut}(\mathbb{Q}(\zeta_6)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$

$= \{1, \zeta_6 \overset{\sigma}{\longmapsto} \zeta_6^5\}$

$\sigma =$ restrict $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \bar{z}$ to $\mathbb{Q}(\zeta_6)$

In general,

as abel. groups

$$\mathrm{Aut}(\boxed{\mathbb{Q}(\zeta_n)/\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\left(\mathbb{Q}(\zeta_n) \xrightarrow{\sigma_a} \mathbb{Q}(\zeta_n)\right) \longleftarrow\!\shortmid \ \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\underline{\zeta_n} \overset{\sigma_a}{\longmapsto} \underline{\underline{\zeta_n^a}}$$

another root of $\Phi_n(x)$

NEXT TIME

③ $\mathbb{K} := \mathrm{Split}_{\mathbb{Q}}(x^3-2) = \mathbb{Q}(\underset{e^{2\pi i/3}}{\underset{\shortparallel}{\omega}}, \sqrt[3]{2})$

has $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \cong S_3$

+ MAIN THMS

of

GALOIS THEORY

Analyze $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ where

$\mathbb{K} = \mathrm{Split}_{\mathbb{Q}}(x^3-2) = \mathbb{Q}(\omega, \underbrace{\sqrt[3]{2}}_{= \alpha})$, $\omega = e^{2\pi i/3}$

$$\begin{tikzcd}
 & & \mathbb{K} \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\alpha) \arrow[drr, dash, "3"'] & \mathbb{Q}(\omega\alpha) \arrow[dr, dash, "3"] & \mathbb{Q}(\omega^2\alpha) \arrow[d, dash, "3"] & \mathbb{Q}(\omega) = \mathrm{Split}_{\mathbb{Q}}(x^2+x+1) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

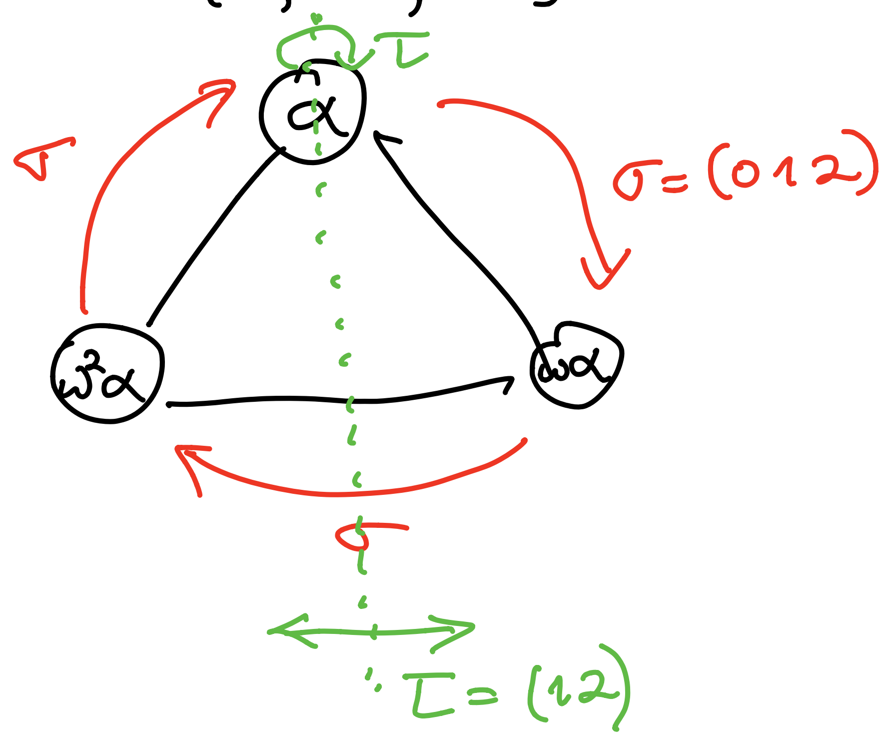
Every $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ is determined by

$$\begin{cases} \sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\} = \text{roots of } m_{\mathbb{Q},\alpha}(x) = x^3-2 \\ \quad \text{and} \\ \sigma(\omega) \in \{\omega, \omega^2\} = \text{roots of } m_{\mathbb{Q},\omega}(x) = x^2+x+1 \end{cases}$$

and Iso. Ext. Thm. gives us ...

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "\sigma"', "\omega \mapsto \omega" below] & \mathbb{K} \\
\mathbb{Q}(\alpha) \arrow[u, dash] \arrow[r, "\sigma"', "\alpha \mapsto \omega\alpha" below] & \mathbb{Q}(\alpha) \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[r, "1_{\mathbb{Q}}"] & \mathbb{Q} \arrow[u, dash]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{K} \arrow[r, "\tau"', "\alpha \mapsto \alpha" below] & \mathbb{K} \\
\mathbb{Q}(\omega) \arrow[u, dash] \arrow[r, "\tau"', "\omega \mapsto \omega^2" below] & \mathbb{Q}(\omega) \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[r, "1_{\mathbb{Q}}"] & \mathbb{Q} \arrow[u, dash]
\end{tikzcd}$$

Any $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ will permute the three roots $\{\alpha, \omega\alpha, \omega^2\alpha\}$ of x^3-2



This lets us identify

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \cong S_{\{\alpha, \omega\alpha, \omega^2\alpha\}} = S_{\{0,1,2\}}$$
$$\cong S_3$$

For every subgroup $H < \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ we get a tower

$$\begin{array}{c} \mathbb{K} \\ | \\ \text{fixed field of } H = \mathbb{K}^H := \{\alpha \in \mathbb{K} : h(\alpha) = \alpha \ \forall h \in H\} \\ | \\ \mathbb{F} \end{array}$$

For every intermediate subfield

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

we get a subgroup $\mathrm{Aut}(\mathbb{K}/\mathbb{L})$

$$< \mathrm{Aut}(\mathbb{K}/\mathbb{F})$$

---

e.g. above $\mathbb{K}^{\langle \tau \rangle}$ and $\mathbb{K}^{\langle \sigma \rangle}$

$\mathbb{K}^{\langle \sigma \rangle} = \mathbb{K}^{\langle (012) \rangle} \supseteq \mathbb{Q}(\omega)$ since $\underline{\sigma(\omega) = \omega}$

$(\sigma(\alpha) = \omega\alpha)$

and this turns out be an $\underline{\text{equality}}$:

$\mathbb{K}$ has $\mathbb{Q}$-basis $\{1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}$

$$1 \overset{\sigma}{\circlearrowleft} \qquad \alpha^2 \xrightarrow{\sigma} \omega^2\alpha^2 = -(\omega+1)\alpha^2 \qquad \omega \overset{\sigma}{\circlearrowleft} \qquad \omega\alpha \xrightarrow{\sigma} \omega^2\alpha = -(\omega+1)\alpha$$

typical element

$$\gamma = a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2$$

$$\gamma = a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2$$

$$\|$$

$$\sigma(\gamma) = a - e\alpha + (b-c+f)\alpha^2 + (d-e)\omega - e\omega\alpha - c\omega\alpha^2$$

$$= a + b\alpha^2 - c(\omega+1)\alpha^2 + d\omega - e(\omega+1)\alpha + f\alpha^2$$

requires

$$\boxed{\begin{array}{l} e = 0 \\ b = 0 \\ \left.\begin{array}{l} c = -f \\ c = -c+f \end{array}\right\} \Rightarrow c = f = 0 \\ \text{i.e. } \gamma = a\cdot 1 + d\cdot\omega \in \mathbb{Q}(\omega) \end{array}}$$

$$\mathbb{K}^{\langle \underset{\sigma}{(012)} \rangle} = \mathbb{Q}(\omega)$$

Similarly,

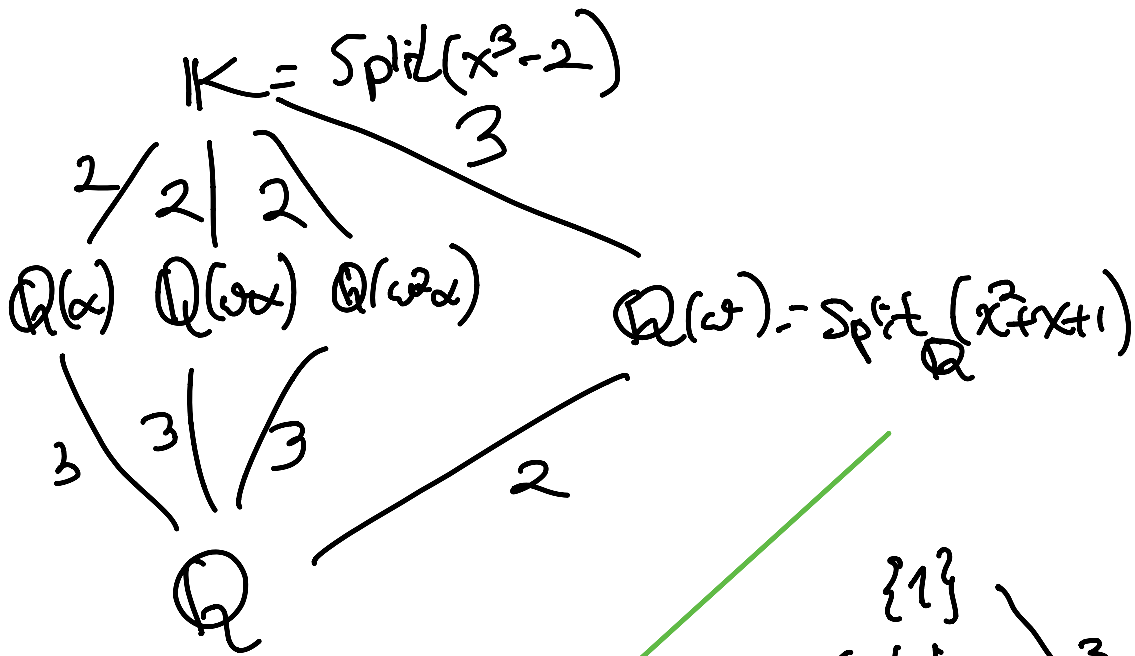
$$\mathbb{K}^{\langle \tau \rangle} \supseteq \mathbb{Q}(\alpha)$$

$$= \text{via linear algebra}$$

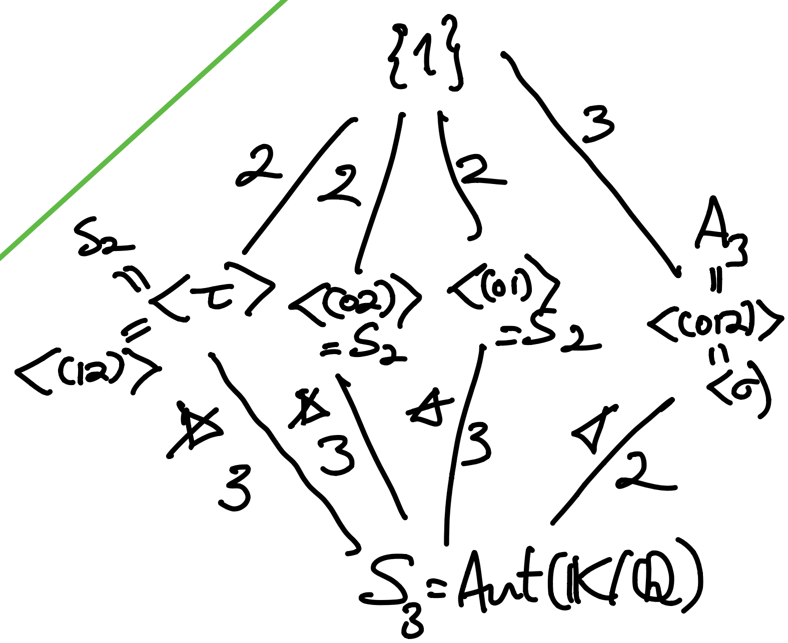
$\tau(\alpha) = \alpha$

$\tau(\omega) = \omega^2$

Get this picture...



$\mathbb{K}$
|
$\mathbb{F}$
|
$\mathbb{Q}$



1
|
H
|
$G = S_3$

TWO MAIN THMS OF GALOIS THEORY!

<u>THM 1:</u> $\mathbb{K}/\mathbb{F}$ finite

$\Rightarrow$ (i) $\mathbb{F} \subseteq \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$ (silly!)

(ii) $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$

and TFAE:

(a) equality in (i): $\mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

(b) $\exists$ <u>some</u> group $G \leq \mathrm{Aut}(\mathbb{K})$ for which $\mathbb{F} = \mathbb{K}^G$

(c) equality in (ii): $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$

(d) $\mathbb{K} = \mathrm{Split}_{\mathbb{F}}(f(x))$ where $f(x)$ is any <u>separable</u> polynomial in $\mathbb{F}[x]$

All of these (a) – (d) can be used to define <u>$\mathbb{K}/\mathbb{F}$ Galois</u>

$\underline{\text{THM 2}}$: When $\mathbb{K}/\mathbb{F}$ is Galois, with $G := \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ one has a bijection

$$\left\{ \begin{matrix} \mathbb{K} \\ | \\ \mathbb{L} \\ | \\ \mathbb{F} \end{matrix} \text{ subfields} \right\} \longleftrightarrow \left\{ \begin{matrix} 1 \\ | \\ H \\ | \\ G \end{matrix} \text{ subgroups} \right\}$$

$$\mathbb{L} \longmapsto H := \{\sigma \in G : \sigma|_{\mathbb{L}} = 1_{\mathbb{L}}\} = \mathrm{Aut}(\mathbb{K}/\mathbb{L})$$

$$\mathbb{L} := \mathbb{K}^H \longleftarrow H < G$$

with

$$\begin{matrix} \mathbb{K} \\ | \\ \mathbb{L} = \mathbb{K}^H \\ | \\ \mathbb{F} \end{matrix}$$

always Galois, $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) = H$

degree $[G:H]$, and Galois $\Leftrightarrow H \triangleleft G$ in which case, $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = G/H$

NEXT TIME:

- can easily compute $m_{\alpha,\mathbb{F}}(x)$ for $\alpha \in \mathbb{K}$
- $\mathbb{L}_1\mathbb{L}_2$, $\mathbb{L}_1 \cap \mathbb{L}_2$ corr. $H_1 \cap H_2$, $\langle H_1, H_2 \rangle$