§14.3 Finite fields

Let's play with an...

EXAMPLE

$$\mathbb{F}_{2^3} = \mathbb{F}_8 \cong \mathbb{F}_2[x] \big/ (x^3+x+1) \quad \text{with } \beta := \overline{x}$$

$\beta^3+\beta+1=0$

(or x^3+x^2+1 would work)

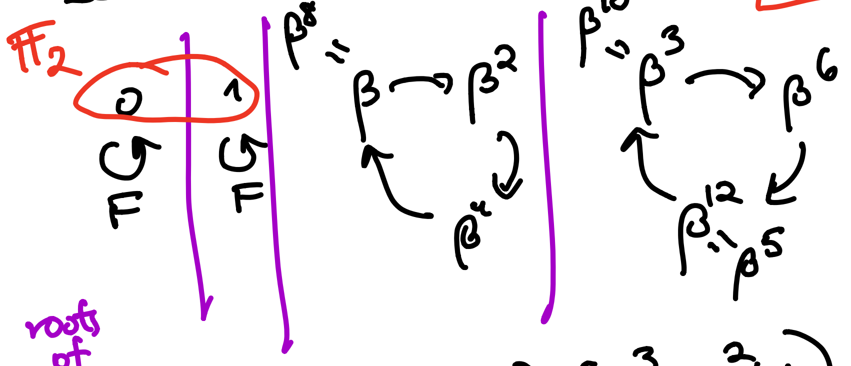
= an $\mathbb{F}_2$-vector space on basis $\{1, \beta, \beta^2\}$

Inside

$$\mathbb{F}_8^\times = \{ \underset{\underset{\beta^7}{\parallel}}{\overset{\overset{\beta^0}{\parallel}}{1}}, \overset{\overset{\beta}{\parallel}}{\beta^1}, \beta^2, \underset{\underset{\beta+1}{\parallel}}{\beta^3}, \underset{\underset{\beta^2+\beta}{\parallel}}{\beta^4}, \underset{\underset{\underset{\beta+1+\beta^2}{\parallel}}{\beta^3+\beta^2}}{\underset{\parallel}{\beta^5}}, \underset{\underset{\underset{\beta^2+1}{\parallel}}{\beta^2+\beta+\beta^3}}{\underset{\parallel}{\beta^6}} \}$$

Let's look at the orbits of $\boxed{\text{Frobenius } \mathbb{F}_8 \xrightarrow{F} \mathbb{F}_8, \ \alpha \mapsto \alpha^2}$

$F \in \mathrm{Aut}(\mathbb{F}_8 / \mathbb{F}_2)$



roots of ...

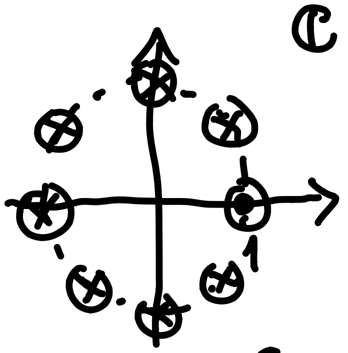
$$\underbrace{x\,(x+1)}_{\text{linear}} \underbrace{(x^3+x+1)\underbrace{(x^3+x^2+1)}_{\text{check: } = (x-\beta^3)(x-\beta^6)(x-\beta^5)}}_{\text{cubics}} = x^{2^3}-x = x^8-x \quad \text{in } \mathbb{F}_2[x]$$

PROP: Every finite subgroup $A \subset \mathbb{F}^\times$ for a field $\mathbb{F}$ is cyclic $A = \langle \alpha \rangle$.
In particular, if $\mathbb{F}$ is finite then $\mathbb{F}^\times$ is cyclic (so if $|\mathbb{F}| = q = p^d$ then $\mathbb{F}^\times \cong (\mathbb{Z}/(q-1)\mathbb{Z})^+$)

EXAMPLE: ① $\mathbb{F}_8^\times = \{\underset{\beta^7}{\underset{\|}{1}}, \beta, \beta^2, \dots, \beta^6\} \cong (\mathbb{Z}/7\mathbb{Z})^+$

---

② Inside $\mathbb{F}^\times = \mathbb{C}^\times$, every finite subgroup $A = \mu_n = \left\{ n^{th} \text{ roots of } 1 \right\}$



$\mu_8 \cong (\mathbb{Z}/8\mathbb{Z})^+$

PROP: Every finite subgroup $A \subset \mathbb{F}^\times$ for a field $\mathbb{F}$ is cyclic $A = \langle \alpha \rangle$.

proof: Let's assume for the moment a fin. abel. group..

LEMMA: In a finite abelian group A, if $L := \operatorname{lcm}\left\{ \begin{matrix} \text{orders} \\ \text{of } g \in A \end{matrix} \right\}$ then $\exists\, g \in A$ with order L.

Then we're done since

$$\underset{\mathbb{Z}/L\mathbb{Z}}{\underset{\cong}{\langle g \rangle}} \le A \quad (\subset \mathbb{F}^\times)$$

has $L = |\langle g \rangle| \le |A| \le L$

every $a \in A$ is a root in $\mathbb{F}$ of $x^L - 1$, which has $\le L$ roots in $\mathbb{F}$.

LEMMA: In a finite abelian group A, if $L := \operatorname{lcm}\left\{\begin{matrix}\text{orders}\\ \text{of } g \in A\end{matrix}\right\}$ then $\exists\, g \in A$ with order L.

proof 1 (cheating!)

In Chap 12, show every fin. abel. group A has $A = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_t\mathbb{Z}$

with $d_1 \mid d_2 \mid \ldots \mid d_t = \operatorname{LCM}\left(\begin{matrix}\text{orders}\\ \text{of } g \in A\end{matrix}\right)$

so take $g \in \{0\} \times \{0\} \times \ldots \times \left\{\begin{matrix}\text{generator}\\ \text{of } \mathbb{Z}/d_t\mathbb{Z}\end{matrix}\right\}$. ∎

proof 2: **SUBLEMMA:**

If A abel. and $g, h \in A$ have orders m, n with $\gcd(m,n)=1$ then gh has order mn.

FALSE if A nonabelian e.g. $(12), (123) \in S_3$

proof: $1 = (gh)^i \overset{A \text{ abelian}}{=} g^i h^i$

$\iff \underset{\text{order dividing } m}{g^i} = \underset{\text{order dividing } n}{h^{-i}} \iff 1 = g^i = h^{-i}$

$\iff$ i is a multiple of m and of n, so of mn ∎

SUBLEMMA:

If A abel. and $g, h \in A$ have orders m, n with $\gcd(m,n)=1$ then gh has order mn

Now, if A fin. abel. and $L = \mathrm{lcm}\left(\begin{matrix}\text{orders}\\ \text{of } g \text{ in } A\end{matrix}\right)$,

let $L = p_1^{d_1} \cdots p_r^{d_r}$ (p_i distinct primes)

find g_1 of order divisible by $p_1^{d_1}$

$\vdots$

g_r of order divisible by $p_r^{d_r}$

then h_1 of order exactly $p_1^{d_1}$

$\vdots$

h_r of order exactly $p_r^{d_r}$

and then $h_1 h_2 \cdots h_r$ has order

$$p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} = L \quad \blacksquare$$

EXAMPLE: $q=2,\ n=4$

$\mathbb{F}_{2^4} = \mathbb{F}_{16}$, $\quad \mathbb{F}_{16}^{\times} = \langle \gamma \rangle = \{1, \gamma, \gamma^2, \dots, \gamma^{14}\}$

$$\begin{tikzcd}
\mathbb{F}_{2^4} \arrow[d, dash] \\
\mathbb{F}_2
\end{tikzcd}$$

$1 \shortparallel \gamma^{15}$

$\cong (\mathbb{Z}/15\mathbb{Z})^{+}$

Frobenius orbits $\mathbb{F}_{16} \xrightarrow{F} \mathbb{F}_{16}$

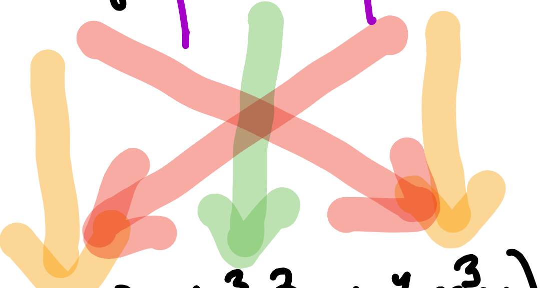
$\alpha \longmapsto \alpha^2$

$$\begin{tikzcd}
\mathbb{F}_{2^4} \arrow[d, dash] \\
\mathbb{F}_{2^2} \arrow[d, dash] \\
\mathbb{F}_2
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[loop below, "F"] & 1 \arrow[loop below, "F"] & \gamma^5 \arrow[r, bend left, "F"] & \gamma^{10} \arrow[dl, bend left, "F"] & \gamma \arrow[r] & \gamma^2 \arrow[d] & \gamma^3 \arrow[r] & \gamma^6 \arrow[d] & \gamma^7 \arrow[r] & \gamma^{14} \arrow[d] \\
 & & \gamma^{20} \arrow[u, phantom, "\shortparallel"] & & \gamma^8 \arrow[u] & \gamma^4 \arrow[l] & \gamma^9 \arrow[u] & \gamma^{12} \arrow[l] & \gamma^{11} \arrow[u] & \gamma^{13} \arrow[l]
\end{tikzcd}$$

$\mathbb{F}_2$

$\mathbb{F}_4$



roots of

$$\underbrace{x\,(x+1)}_{\text{deg } 1}\ \underbrace{(x^2+x+1)}_{\text{deg } 2}\ \underbrace{(x^4+x+1)\underbrace{(x^4+x^3+x^2+x+1)}_{\text{roots have order 5, not 15}}(x^4+x^3+1)}_{\text{deg } 4}$$

$$= x^{16} - x$$

$$= x^{2^4} - x \quad \text{in } \mathbb{F}_2[x]$$

THM: If $\begin{tikzcd} \mathbb{K} \arrow[d, dash] \\ \mathbb{F} \end{tikzcd}$ has $\mathbb{K}$ finite, then...

(i) $|\mathbb{F}| = q = p^d$ for some prime p and power $d \geq 1$

and $|\mathbb{K}| = q^n$ for some $n \geq 1$.

(ii) $\mathbb{K}^\times = \langle \alpha \rangle$ is cyclic.

(iii) $\mathbb{K} = \text{Split}_{\mathbb{F}}(x^{q^n} - x)$ $\left(\underset{\substack{\uparrow \\ \text{unique up to iso.}}}{=:} \mathbb{F}_{q^n} \right)$

$= \left\{ \begin{array}{c} \text{all roots of} \\ x^{q^n} - x \end{array} \right\}$

(iv) $\underset{\mathbb{F}_{q^n}}{\underset{\shortparallel}{\mathbb{K}}} / \underset{\mathbb{F}_q}{\underset{\shortparallel}{\mathbb{F}}}$ is <u>Galois</u>, with $\underset{\text{Gal}}{\text{Aut}}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \overset{\text{Frobenius}}{F} \rangle \cong (\mathbb{Z}/n\mathbb{Z})^+$

where $\mathbb{K} \xrightarrow{F} \mathbb{K}$
$\beta \mapsto \beta^q$

(v) The only intermediate fields are

$$\begin{tikzcd} & \mathbb{F}_{q^n} \arrow[d, dash] \\ (\mathbb{F}_{q^n})^{F^d} = \left\{ \begin{array}{c} \text{roots} \\ \text{of } x^{q^d} - x \end{array} \right\} = & \mathbb{F}_{q^d} \arrow[d, dash] \\ & \mathbb{F}_q \end{tikzcd}$$

where d divides n

(vi) $$x^{q^n} - x = \prod_{d \mid n} \prod_{\substack{\text{irred.} \\ f(x) \text{ in } \mathbb{F}_q[x] \\ \text{of degree } d}} f(x) \quad \text{in } \mathbb{F}_q[x]$$

---

proof (i) $\mathbb{K}$ finite, so $\mathbb{F}$ finite so $\operatorname{char}(\mathbb{F}) = p$

$$\begin{tikzcd} \mathbb{K} \arrow[d, dash, "\deg n = {[\mathbb{K}:\mathbb{F}]}"] \\ \mathbb{F} \arrow[d, dash, "\deg d = {[\mathbb{F}:\mathbb{F}_p]}"] \\ \mathbb{F}_p \end{tikzcd}$$

$\Longrightarrow$ $\mathbb{K} = \mathbb{F}^n$ so $|\mathbb{K}| = |\mathbb{F}|^n = q^n$

$\mathbb{F} \cong (\mathbb{F}_p)^d$ so $|\mathbb{F}| = p^d = q$

(ii) ✓

(iii) $$\boxed{\mathbb{K} = \operatorname{split}_{\mathbb{F}}\left(x^{q^n} - x\right) = \left\{ \begin{matrix} \text{all roots} \\ \text{of } x^{q^n} - x \end{matrix} \right\}}$$

since every $\beta \in \mathbb{K}^\times$ has order dividing

$|\mathbb{K}^\times| = q^n - 1$, so $\beta^{q^n - 1} = 1$

$$\beta^{q^n - 1} - 1 = 0$$

i.e. β is a root of $x^{q^n - 1} - 1$

and of $x^{q^n} - x$

and $x^{q^n} - x$ only has q^n root, so no more.

EXAMPLE

If we build

$$\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$$

$\omega := \bar{x}$ so ω satisfies

$$\omega^4 + \omega^3 + 1 = 0$$

then $\tau = \omega^7$ satisfies $\tau^4 + \tau + 1 = 0$

i.e. it's a root of

$$x^4 + x + 1$$

(iv) $\underset{\mathbb{F}_{q^n}}{\overset{}{\mathbb{K}}} \, / \, \underset{\mathbb{F}_q}{\overset{}{\mathbb{F}}}$ is Galois, with $\underset{\text{Gal}}{\text{Aut}}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \overset{\text{Frobenius}}{F} \rangle \cong (\mathbb{Z}/n\mathbb{Z})^+$

$\mathbb{K} = \mathbb{F}_{q^n}$, $\mathbb{F} = \mathbb{F}_q$

where $\mathbb{K} \xrightarrow{F} \mathbb{K}$, $\beta \mapsto \beta^q$

(v) The only intermediate fields are

$$\begin{tikzcd}
\mathbb{F}_{q^n} \arrow[d, dash] \\
\mathbb{F}_{q^d} \arrow[d, dash] \\
\mathbb{F}_q
\end{tikzcd}$$

$(\mathbb{F}_{q^n})^{F^d} = \{\text{roots of } x^{q^d} - x\} = \mathbb{F}_{q^d}$ where d divides n

To prove (iv), note that $\mathbb{K} \xrightarrow{F} \mathbb{K}$, $\beta \longmapsto \beta^q$

does fix $\mathbb{F} = \mathbb{F}_q$ pointwise (since they are roots of $x^q - x$)

and $F^n = 1_{\mathbb{K}}$ since $F^n(\beta) = (((\beta^q)^q)\underbrace{\cdots)^q}_{n \text{ times}} = \beta^{q^n} = \beta$

but $F^d \neq 1_{\mathbb{K}}$ for $d < n$ since $F^d(\underset{\text{cyclic generator of } \mathbb{K}^\times}{\alpha}) = \alpha^{q^d} \neq \alpha$ since $q^d < q^n$

Hence $\langle F \rangle$ generates a cyclic subgroup of $\text{Aut}(\mathbb{K}/\mathbb{F})$ of size n.

Since $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(\underbrace{x^{q^n}-x})$ $\hookleftarrow$ separable, q^n distinct roots $(\in \mathbb{K})$

so $\mathbb{K}/\mathbb{F}$ is Galois,

$$\begin{array}{c} |\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}] = n \\ \cup\!| \\ \langle F \rangle \end{array} \quad \Rightarrow \quad \langle F \rangle = \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

For (c), the intermediate subfields are

$\mathbb{K} = \mathbb{F}_{q^n} = \{\text{roots of } x^{q^n}-x\}$

$|$ $\longleftarrow$ name $[\mathbb{K}:\mathbb{L}]=e$

$\mathbb{L} = \mathbb{F}_{q^d}$ and $q^n = |\mathbb{K}| = |\mathbb{L}|^e = (q^d)^e = q^{de}$

$|$ i.e. d is a divisor of $n (=de)$

$\mathbb{F} = \mathbb{F}_q$

and $\mathbb{F}_{q^d} = \{\text{roots of } x^{q^d}-x\} \subset \{\text{roots of } x^{q^n}-x\}$ if d divides n

since if β is a root of $x^{q^d}-x$

that says $F^d(\beta) = \beta \Rightarrow F^n(\beta) = (\cdots(\underbrace{F^d(\beta))^d\cdots)^d}_{n/d \text{ times}}$

$= \beta$

For (vi) $$x^{q^n} - x = \prod_{d \mid n} \prod_{\substack{\text{irred.} \\ f(x) \text{ in } \mathbb{F}_q[x] \\ \text{of degree } d}} f(x) \quad \text{in } \mathbb{F}_q[x] \quad ,$$

note that any such $f(x)$ divides $x^{q^n} - x$ since if it has β as a root in some splittingfield, then

$$\begin{array}{l} \mathbb{F}(\beta) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} = \{\text{roots of } x^{q^n} - x\} \\ \quad | \ \deg d \text{ dividing } n \\ \mathbb{F} = \mathbb{F}_q \end{array}$$

Conversely, every irred. factor $f(x)$ of $x^{q^n} - x$ is $m_{\mathbb{F}_q,\beta}(x)$ for some root β of $f(x)$,

and
$$\begin{array}{ll} \mathbb{F}_{q^n} & \\ | & \\ \mathbb{F}_q(\beta) & \Rightarrow \mathbb{F}_q(\beta) = \mathbb{F}_{q^d} \text{ with } d \text{ dividing } n \\ | & \\ \mathbb{F}_q & \Rightarrow \deg m_{\mathbb{F}_q,\beta}(x) = d \\ & \qquad \| \\ & \qquad \deg f(x). \qquad \blacksquare \end{array}$$

§14.4 Simple extensions ($\mathbb{K}_1, \mathbb{K}_2$ later...]

For $\mathbb{K}/\mathbb{F}$ any algebraic extension (possibly infinite $[\mathbb{K}:\mathbb{F}]$)

define its <u>normal closure</u>

$\mathbb{N} :=$ splitting field over $\mathbb{F}$ for $\{m_{\alpha,\mathbb{F}}(x) : \alpha \in \mathbb{K}\}$

---

e.g. $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$

$\mathbb{F} = \mathbb{Q}$

has $\mathbb{N} = \mathbb{Q}(\omega, \sqrt[3]{2}) = \mathrm{split}_{\mathbb{Q}}(x^3-2)$

$\hookleftarrow$ not clear yet

<u>PROP</u>: (i) $\mathbb{N}/\mathbb{F}$ is normal, and the <u>smallest</u> in the sense that if

$$\begin{tikzcd}
\mathbb{L} \arrow[dd, dash] \arrow[dr, dotted, dash] & \\
& \mathbb{N} \\
\mathbb{K} \arrow[ur, dotted, dash] \arrow[d, dash] & \\
\mathbb{F} &
\end{tikzcd}$$

with $\mathbb{L}/\mathbb{F}$ normal, then $\mathbb{L} \supseteq \mathbb{N}$

PROP: (i) $\mathbb{N}/\mathbb{F}$ is normal, and the **smallest** in the sense that if

$$\begin{tikzcd} \mathbb{L} \arrow[d, dash] \arrow[r, dash, dotted] & \mathbb{N} \\ \mathbb{K} \arrow[ur, dash, dotted] \arrow[d, dash] & \\ \mathbb{F} & \end{tikzcd}$$

with $\mathbb{L}/\mathbb{F}$ normal, then $\underline{\mathbb{L} \supseteq \mathbb{N}}$

(ii) $\mathbb{K}/\mathbb{F}$ finite $\Longrightarrow \mathbb{N}/\mathbb{F}$ finite

---

(iii) $\mathbb{K}/\mathbb{F}$ finite & separable

$\Longrightarrow \mathbb{N}/\mathbb{F}$ Galois

---

e.g.

$$\begin{tikzcd} \mathbb{N} \arrow[d, dash, dotted] \\ \mathbb{K} = \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] \\ \mathbb{F} = \mathbb{Q} \end{tikzcd}$$

has $\mathbb{N} = \mathbb{Q}(\omega, \sqrt[3]{2})$

$= \mathrm{split}_{\mathbb{Q}}(x^3-2)$

$\omega = e^{2\pi i/3}$

---

proof of PROP:

(i) Since $\mathbb{N} := \mathrm{split}_{\mathbb{F}} \{ m_{\mathbb{F},\alpha}(x) : \alpha \in \mathbb{K} \}$,

$\mathbb{N}$ is normal.

If

$$\begin{tikzcd}[row sep=small]
\mathbb{L} \arrow[d, dash] & \\
 & \mathbb{N} \arrow[ul, dotted, dash] \arrow[dl, dotted, dash] \\
\mathbb{K} \arrow[d, dash] & \\
\mathbb{F} &
\end{tikzcd}$$

… with $\mathbb{L}$ normal, then every $\alpha \in \mathbb{K} \subset \underline{\mathbb{L}}$ so every root of $m_{\alpha,\mathbb{F}}(x)$ is also in $\mathbb{L}$, so $\mathbb{N} \underline{\subseteq \mathbb{L}}$.

For (ii),

$\mathbb{K}/\mathbb{F}$ finite $\Longleftrightarrow \mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, α_i alg./$\mathbb{F}$

$\Longrightarrow \mathbb{L} := \mathrm{split}_{\mathbb{F}}\{m_{\mathbb{F},\alpha_i}(x)\}_{i=1,\ldots,n}$ is finite, normal, containing $\mathbb{K}$

$\Longrightarrow \underline{\mathbb{L}} \supseteq \mathbb{N}$, so $[\mathbb{N}:\mathbb{F}] < \infty$. ($\leq [\mathbb{L}:\mathbb{F}] < \infty$).

For (iii), if $\mathbb{K}/\mathbb{F}$ is finite and $\underline{\text{separable}}$

every $\alpha \in \mathbb{K}$ has $m_{\alpha,\mathbb{F}}(x)$ a separable poly.

$\Longrightarrow \mathbb{N} := \mathrm{split}_{\mathbb{F}}(\{m_{\alpha,\mathbb{F}}(x) : \alpha \in \mathbb{K}\})$ is Galois $\boxed{}$

Passing to normal closure is useful...

<u>THEOREM</u> (on the primitive element)

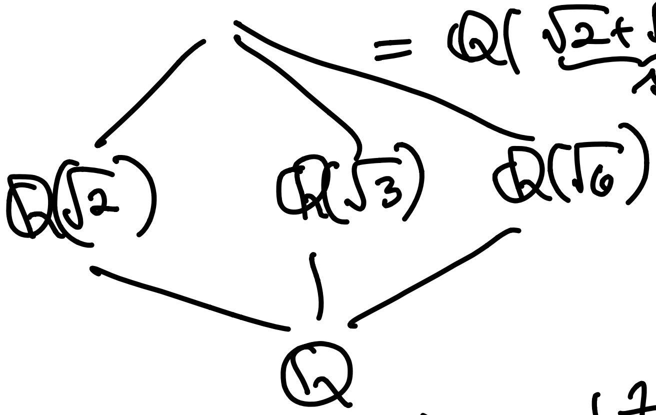
$\mathbb{K}/\mathbb{F}$ finite, separable

$\implies \mathbb{K}/\mathbb{F}$ is <u>simple</u>, i.e. $\mathbb{K}=\mathbb{F}(\alpha)$ for some $\alpha\in\mathbb{K}$, called a <u>primitive element</u>.

---

e.g. $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathrm{split}_{\mathbb{Q}}\left((x^2-2)(x^2-3)\right)$

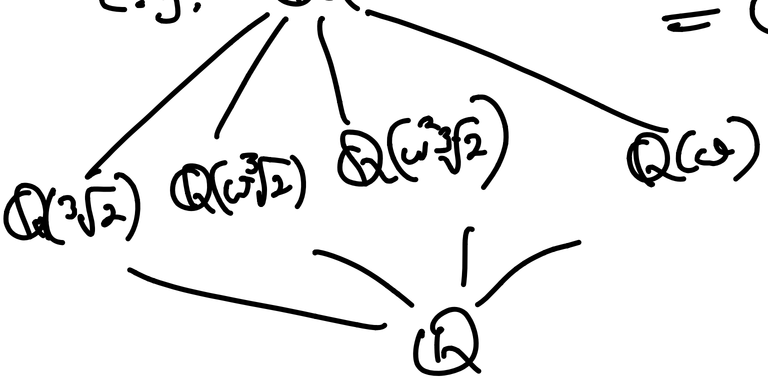
$= \mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha})$



---

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

$= \mathbb{Q}(\underbrace{\omega+\sqrt[3]{2}})$



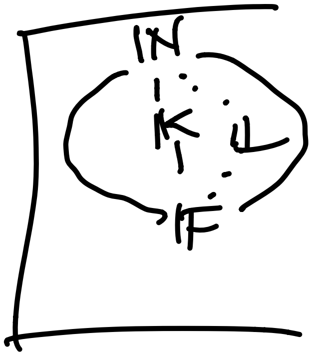
e.g.
$$\begin{tikzcd}\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha) \arrow[d, dash] \\ \mathbb{F}_q\end{tikzcd}$$

any α such that $\mathbb{F}_{q^n}^\times = \langle \alpha \rangle$
$= \{1, \alpha, \alpha^2, \dots, \alpha^{q^n-2}\}$

proof: $\mathbb{K}/\mathbb{F}$ separable, finite has normal closure $\mathbb{N}/\mathbb{F}$ Galois, so $\mathrm{Aut}(\mathbb{N}/\mathbb{F})$ is finite, so only has finitely many subgroups, and hence $\exists$ only finitely many subfields $\mathbb{L}$

in $\mathbb{F} \subset \mathbb{L} \subset \mathbb{N}$

or in $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K}$



Surprisingly, this property characterizes simple extensions $\mathbb{K}/\mathbb{F}$ ...

LEMMA: Let $\mathbb{K}/\mathbb{F}$ be finite.
Then $\mathbb{K}/\mathbb{F}$ is simple $\Longleftrightarrow$ $\exists$ only finitely many intermediate extensions
i.e. $\mathbb{K} = \mathbb{F}(\alpha)$

$$\begin{tikzcd}
\mathbb{K} \arrow[d, dash] \\
\mathbb{L} \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

proof: $(\Leftarrow)$: If $\mathbb{F}$ is finite, then $\mathbb{K}$ is finite so $\mathbb{K} = \mathbb{F}_{q^n} / \mathbb{F}_q = \mathbb{F}$, so α with $\mathbb{F}_{q^n}^{\times} = \langle \alpha \rangle$ works.

So $|\mathbb{F}| = \infty$. Since $\mathbb{K}/\mathbb{F}$ finite, $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in \mathbb{K}$. By induction on n, it suffices to show $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$ for every $\alpha, \beta \in \mathbb{K}$ and some $\gamma \in \mathbb{K}$.

There are only finitely many intermediate subfields between $\mathbb{K}$ & $\mathbb{F}$ or $\mathbb{F}(\alpha,\beta)$ & $\mathbb{F}$, so since $|\mathbb{F}| = \infty$, $\exists$ ∞ many subfields $\mathbb{F}(\alpha + c\beta)$, $\mathbb{F}(\alpha + c'\beta)$ with $c, c' \in \mathbb{F}$, and two must coincide.

$\exists\, c, c'$ in $\mathbb{F}$ with $\mathbb{F}(\alpha+c\beta) = \mathbb{F}(\alpha+c'\beta)$
$c \neq c'$

Then
$$\begin{aligned} \alpha+c\beta &\in \mathbb{F}(\alpha+c\beta) \\ \alpha+c'\beta &\in \mathbb{F}(\alpha+c\beta) = \mathbb{F}(\alpha+c'\beta) \end{aligned}$$

$$\Longrightarrow (c-c')\beta \in \mathbb{F}(\alpha+c\beta)$$

$$\Longrightarrow \beta \in \mathbb{F}(\alpha+c\beta)$$

$$\Longrightarrow \alpha \in \mathbb{F}(\alpha+c\beta)$$

$$\Longrightarrow \mathbb{F}(\alpha,\beta) = \mathbb{F}(\underbrace{\alpha+c\beta}_{\overset{\shortparallel}{\gamma}})$$

$(\Longrightarrow)$: If $\mathbb{K} = \mathbb{F}(\alpha)$, then note that for any $\mathbb{L}$ with

$$\begin{tikzcd} \mathbb{K} = \mathbb{F}(\alpha) \arrow[d, dash] \\ \mathbb{L} \arrow[d, dash] \\ \mathbb{F} \end{tikzcd}$$

one has

$m_{\alpha,\mathbb{L}}(x)$ divides $m_{\alpha,\mathbb{F}}(x)$ in $\mathbb{L}[x]$.

Setting $\mathbb{L}' := \mathbb{F}(\text{coefficients of } m_{\alpha,\mathbb{L}}(x))$

Then
$$\begin{tikzcd} \mathbb{K} = \mathbb{F}(\alpha) = \mathbb{L}'(\alpha) = \mathbb{L}(\alpha) \arrow[d, dash, "\text{degree} = \deg m_{\alpha,\mathbb{L}}(x)"] \arrow[dd, dash, bend right=60, "\text{degree} = \deg m_{\alpha,\mathbb{L}'}(x)"'] \\ \mathbb{L} \arrow[d, equal] \\ \mathbb{L}' \arrow[d, dash] \\ \mathbb{F} \end{tikzcd}$$

but $\boxed{m_{\alpha,\mathbb{L}}(x) = m_{\alpha,\mathbb{L}'}(x)}$

Think about it!

So $\mathbb{L} = \mathbb{L}'$.

Conclusion: every $\mathbb{L}$ with

$$\begin{tikzcd}
\mathbb{K} = \mathbb{F}(\alpha) \arrow[d, dash] \\
\mathbb{L} \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

is of form

$$\mathbb{L} = \mathbb{F}\left(\overset{\text{coeffs of}}{m(x)} \right)$$

where $m(x)$ is some factor of $m_{\alpha,\mathbb{F}}(x)$ in $\mathbb{K}[x]$.

There are only finitely many such $m(x)$'s $\blacksquare$

... ending proof of the lemma

$\mathbb{K}/\mathbb{F}$ simple $\iff$ fin. many $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$.

and hence also the THM

$\mathbb{K}/\mathbb{F}$ finite, separate $\Rightarrow$ $\mathbb{K}/\mathbb{F}$ simple.

EXERCISE for §14.4 and $\mathbb{K}/\mathbb{F}$ simple $\Leftrightarrow$ fin. many $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$.

Consider two normal, but inseparable extensions in characteristic p prime :

$$\begin{tikzcd} \mathbb{K}_1 = \mathrm{Split}_{\mathbb{F}_p(t)}(x^p-t) = \mathbb{F}_p(t^{1/p}) \arrow[d, dash] \\ \mathbb{F}_1 = \mathbb{F}_p(t) \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{K}_2 = \mathrm{Split}_{\mathbb{F}_p(s,t)}((x^p-t)(x^p-s)) = \mathbb{F}_p(s^{1/p}, t^{1/p}) \arrow[d, dash] \\ \mathbb{F}_2 = \mathbb{F}_p(s,t) \end{tikzcd}$$

Explain why

(a) $\mathbb{K}_1/\mathbb{F}_1$ is simple, i.e. $\mathbb{K}_1 = \mathbb{F}_1(\alpha)$ for some $\alpha \in \mathbb{K}_1$ and there are no strictly intermediate subfields $\mathbb{L}$ with $\mathbb{F}_1 \subsetneqq \mathbb{L} \subsetneqq \mathbb{K}_1$,

---

(b) whereas $\mathbb{K}_2/\mathbb{F}_2$ is not simple, i.e. show directly that $\mathbb{F}_2(\alpha) \subsetneqq \mathbb{K}_2$ for every $\alpha \in \mathbb{K}_2$

(and we already saw a while ago that $\exists$ ∞ many subfields $\mathbb{F}_2 \subsetneqq \mathbb{F}_2(s+ct) \subsetneqq \mathbb{K}_2$ for $c \in \mathbb{F}_p$

§14.6 Galois groups of polynomials

PROP: $\mathbb{K}/\mathbb{F}$ finite, Galois

say $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x))$ with roots $\alpha_1, \ldots, \alpha_n$ for $f(x)$ in $\mathbb{K}$.

Then

(i) $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \overset{\varphi}{\hookrightarrow} S_n = S_{\{\alpha_1, \ldots, \alpha_n\}}$ = permutations of $\{\alpha_1, \ldots, \alpha_n\}$

(ii) $G \cong \varphi(G) < S_n$ acts transitively (with a single orbit) on the roots within a given irreducible factor of $f(x)$.
Hence if $f(x)$ is irreducible in $\mathbb{F}[x]$, then $\varphi(G)$ is a transitive subgroup of S_n, i.e. $\{1, 2, \ldots, n\}$ lie in a single $\varphi(G)$-orbit.

Proof: (i): Any $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ permutes $\{\alpha_1, \ldots, \alpha_n\}$ and is determined if we know $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$ since $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

(ii): Isomorphism Extension Thm! $\boxed{\Xi}$

What can $\overset{G=}{\text{Aut}}(\mathbb{K}/\mathbb{Q})$ for $\mathbb{K} = \text{split}_{\mathbb{Q}}(f(x))$ with $\deg(f)$ small?

$\deg(f(x)) = 2$, $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$

- If $f(x)$ splits in $\mathbb{Q}[x]$, $\mathbb{K} = \mathbb{Q}$

  $(G = \{1\} < S_2)$

- If $f(x)$ is irreducible in $\mathbb{Q}[x]$, which happens if and only if $D = b^2 - 4c$ is not a perfect square in $\mathbb{Q}$, and then $\mathbb{K} = \mathbb{Q}(\sqrt{D})$:

$$0 = x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$$

$$x + \frac{b}{2} = \pm\sqrt{\frac{b^2}{4} - c} = \pm\frac{1}{2}\sqrt{D}$$

so $G = S_2 = S_{\{\alpha_1, \alpha_2\}}$

$\underline{\deg(f(x))=3}$, $f(x)=x^3+ax^2+bx+c$

- If $f(x)$ is reducible in $\mathbb{Q}[x]$,

either $\mathbb{K}=\mathbb{Q}$ (if $f=(\text{linear})(\text{linear})(\text{linear})$)

or it splits $f=(\overset{(x-\alpha_1)}{\text{linear}})(\underset{\text{irred.}}{\overset{(x-\alpha_2)(x-\alpha_3)}{\text{quadratic}}})$

and we're back in the previous case

with $G = \underset{\langle\sigma\rangle}{\underset{\|}{S_2}} < S_3 = S_{\{\alpha_1, \underset{\sigma}{\underbrace{\alpha_2, \alpha_3}}\}}$

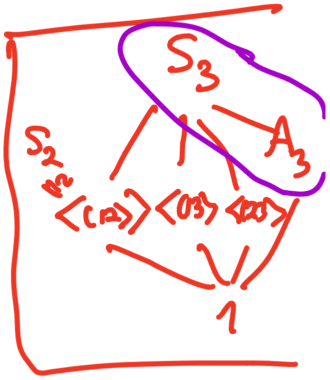
- If $f(x)$ is irreducible in $\mathbb{Q}[x]$,

then any root α of $f(x)$

has $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. But

$G=\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \hookrightarrow S_3$,

so either $G=A_3$ or S_3



this case occurs $\iff$ the discriminant $D=a^2b^2-4b^3-4a^3c-27c^2+18abc$ is a perfect square in $\mathbb{Q}$!

Then $\mathbb{K}=\mathbb{Q}(\alpha)$

Use on HW!

In this case, $\mathbb{K}=\mathbb{Q}(\alpha,\omega)$

$\omega = e^{2\pi i/3}$

$\deg f(x) = 4$

- If $f(x)$ is reducible, either
  - $\mathbb{K} = \mathbb{Q}$ $(4 = 1+1+1+1)$
  - $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ for $\sqrt{D}$ is a root of an irred. quadratic factor $(4 = 2+1+1)$
  - back on the irreducible cubic case $(4 = 3+1)$
  - $\mathbb{K} = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ for $\sqrt{D_i}$ roots of two irred. factors $(4 = 2+2$ case$)$ with discriminants D_1, D_2.

    If it happens $D_1 D_2$ is a perfect square in $\mathbb{Q}$, then $\mathbb{K} = \mathbb{Q}(\sqrt{D_1}) \ni \sqrt{D_2}$

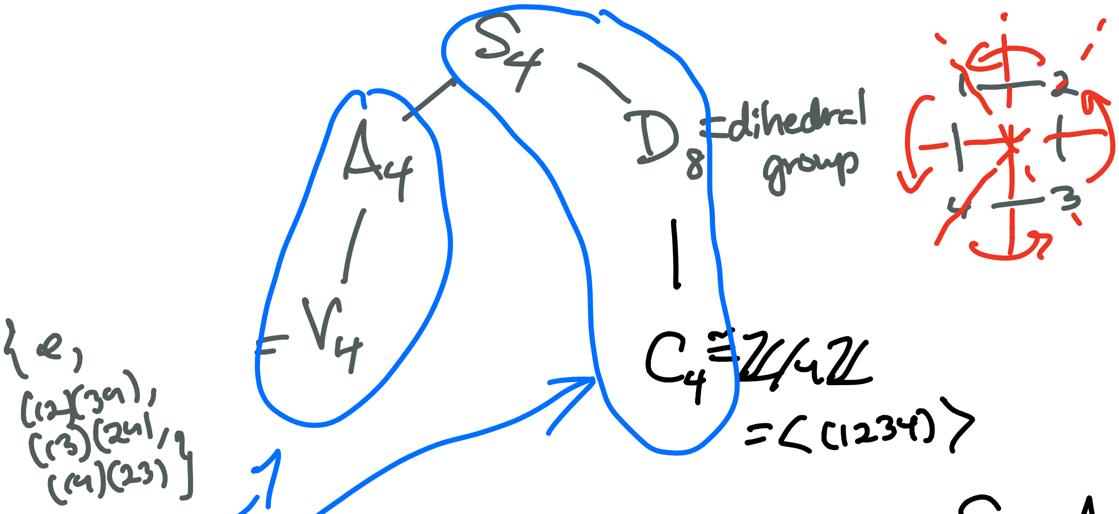
    and $G = S_2 = \mathbb{Z}/2\mathbb{Z}$,

    else $G = V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} < S_4$

    $$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}, \quad S_4 = S_{\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}}$$

- irreducible case on next page...

- If $f(x)$ is irred. in $\mathbb{Q}[x]$, the possible transitive subgroups of S_4 are



(but not transitive are S_3, A_3
S_2
$S_2 \times S_2$)

There is again a polynomial D in the coefficients of $f(x) = x^4 + ax^3 + bx^2 + dx + c$

"$D(a,b,c,d)$" $\in \mathbb{Q}$, still called the discriminant,

and
- D vanishes $\iff$ $f(x)$ inseparable
- D is a perfect square $\iff$ $G = V_4$ or A_4

  not a perfect square $\iff$ $G = S_4$ or D_4 or C_4

Discriminants

- detecting separability and $\mathrm{Aut}(K/\mathbb{Q}) < A_n < S_n$ or not.

Let $\alpha_1, \dots, \alpha_n$ be indeterminates (variables)

so $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ = rational functions $\dfrac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$

Consider $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

$$\in \mathbb{Q}(\alpha_1, \dots, \alpha_n)[x]$$

$$\in \mathbb{Z}[\alpha_1, \dots, \alpha_n][x]$$

$$= x^n - \underbrace{(\alpha_1 + \dots + \alpha_n)}_{\substack{s_1 := \\ 1^{st} \text{ elementary} \\ \text{symmetric} \\ \text{function}}} x^{n-1} + \underbrace{\begin{matrix}(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ + \dots + \alpha_{n-1}\alpha_n)\end{matrix}}_{s_2} x^{n-2}$$

$$- \dots + (-1)^n \underbrace{\alpha_1\alpha_2 \cdots \alpha_n}_{s_n}$$

$$\in \mathbb{Q}(\alpha_1, \dots, \alpha_n)^{S_n}[x]$$