How to determine $f(x)$ irreducible or not in $\mathbb{Q}[x]$?

Useful facts:

① $f(x) = c f_0(x)$ → $\in \mathbb{Z}[x]$ primitive.

$f_0(x)$ irreducible in $\mathbb{Z}[x]$

$\Leftrightarrow$ $f_0(x)$ irreducible in $\mathbb{F}_p[x]$

② $\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$

Prop: $f(x) \in \mathbb{Z}[x]$,

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$.

$p \nmid a_n$. If $\psi_p(f(x)) = \bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$, then

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

Pf: Assume $f(x)$ is reducible.

then $f(x) = g(x) \cdot h(x)$.

with $g, h \in \mathbb{Z}[x]$, and

$\deg g \geq 1$. $\deg h \geq 1$.

$\bar{f} = \bar{g} \cdot \bar{h}$, $\deg \bar{f} = n$ $(\not\equiv a_n)$

$\Rightarrow$ $\deg \bar{g} + \deg \bar{h} = n$

$\deg g + \deg h = n$.

$\deg \bar{g} \leq \deg g$, $\deg \bar{h} \leq \deg h$.

so $\deg \bar{g} = \deg g$, $\deg \bar{h} = \deg h$

≥ 1 ≥ 1.

so $\bar{f} = \bar{g}\bar{h}$ is a proper factorization.

$\bar{g}$ is a proper divisor of $\bar{f}$.

(on tradition with $\bar{f}$ being irreducible.

Ex: $f(x) = x^3 + x + 1$.

$\bar{f}(x)$ is irreducible in $\mathbb{F}_2[x]$.

How to find irreducible polynomials in $\mathbb{F}_p[x]$??

List all of them. (Sieve method)

$\mathbb{F}_2[x]$.

deg 1. x, $x+1$

deg 2. ~~x^2~~, ~~x^2+1~~, x^2+x+1.

deg 3. ~~x^3~~. ~~x^3+1~~. x^3+x+1,

x^3+x. x^3+x^2+x+1.

x^3+x^2+1. ~~x^3+x^2~~. ~~x^3+x^2+x~~.

deg 4. . - .

Key point to use the proposition:

Select the correct prime p.

Eisenstein criterion:

$f(x) \in \mathbb{Z}[x]$. primitive.

① $p \nmid a_n$

② $p \mid a_i$, $i = n-1, \cdots, 1, 0$

③ $p^2 \nmid a_0$.

Then $f(x)$ is irreducible.

Pf: Assume $f(x) = g(x) \cdot h(x)$

$$\bar{f}(x) = a_n x^n = \bar{g}(x) \cdot \bar{h}(x)$$

then $\bar{g}(x) = c \cdot x^m$.

$\bar{h}(x) = d\, x^{n-m}$.

So $g(x) = (x^{m_1} + \cdots + c_0$

$h(x) = d_x^{n-m} + \cdots + d_0$.

$p \mid c_0$, $p \mid d_0$.

So $p^2 \mid a_0 = c_0 d_0$.

Contradiction!

Ex: $f(x) = x^5 + 20x^4 + 5x^3 + 15$.

choose $p = 5$

Ex: (cyclotomic polynomial)

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

$= \dfrac{x^p - 1}{x - 1}$ is irreducible.

$\Phi_p(x) \cdot (x-1) = x^p - 1$

change of variable

$$y = x - 1$$

$$\mathfrak{F}_p(y+1) \cdot y = (y+1)^p - 1$$

$$= y^p + \binom{p}{1} y^{p-1} + \cdots \binom{p}{i} y^{p-i} + py$$

$$\mathfrak{F}_p(y+1) = y^{p-1} + p\, y^{p-2} + \cdots \binom{p}{i} y^{p-i-1} + \cdots + p$$

Also

$$p \mid \binom{p}{i} \text{ for } 1 \le i \le p-1.$$

because $\binom{p}{i} = \dfrac{p(p-1)\cdots(p-i+1)}{i \cdot (i-1) \cdots 1}$

$$\binom{p}{i} \cdot i(i-1)\cdots 1 = p(p-1)\cdots(p-i+1)$$

$p \nmid i$, $p \nmid i-1$, ...

so $p \mid \binom{p}{i}$

Apply Eisenstein criterion $\Rightarrow$

$\Phi_p(y+1)$ is irreducible.

The proof also helps you to do factorization in $\mathbb{Z}[x]$.

$f(x) = g(x)\,h(x) \Rightarrow \bar{f}(x) = \bar{g}(x)\cdot\bar{h}(x)$

This gives some hint how to find $g(x), h(x)$

Gauss primes:

Q: When is p prime in $\mathbb{Z}$ equal to sum of two squares?

$$p = m^2 + n^2 \qquad (p \text{ odd prime})$$

Prop: p is sum of two squares iff p is reducible in $\mathbb{Z}[i]$.

pf: $p = m^2 + n^2$

$$\Rightarrow p = (m+ni)(m-ni).$$

$m, n \neq 0$.

If $p = (a+bi)(c+di)$

$$p^2 = (a^2+b^2)(c^2+d^2)$$

$\Rightarrow a^2+b^2 = 1, p, p^2$.

But $a+bi, c+di$ are not units.

p is not $\equiv 1 \pmod 4$ $\iff$ -1 is not a square in $\mathbb{Z}/(p)$

$\iff$ x^2+1 has a root in $\mathbb{F}_p$

$\iff$ p is not a prime $\equiv 3 \pmod 4$

$\iff$ p is not a prime element in $\mathbb{Z}[i]$

Thm: p is a prime element in $\mathbb{Z}[i]$

$\iff$ $p \equiv 3 \pmod 4$

$\mathbb{Z}[i]/(p) = \mathbb{Z}[x]/(x^2+1, p)$

$= \mathbb{F}_p[x]/(x^2+1)$

So $a^2+b^2=p$ is not solvable when $p \equiv 3 \pmod 4$.

If $p \equiv 1 \pmod 4$. then

$(\mathbb{F}_p)^\times \cong (\mathbb{Z}/p-1\mathbb{Z})$ has

a subgroup $\cong \mathbb{Z}/4\mathbb{Z}$

choose $x \in \mathbb{Z}/4\mathbb{Z}$ as a generator

$x^4 = 1$. $x \neq 1$, $x^2 \neq 1$. $x^3 \neq 1$

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

If $x^2+1 = 0$. $x^2 = -1$

If $\exists\ x \in \mathbb{F}_p$, $x^2 = -1$,

then $x \neq 1$. $x^2 \neq 1$. $x^3 = -x \neq 1$.

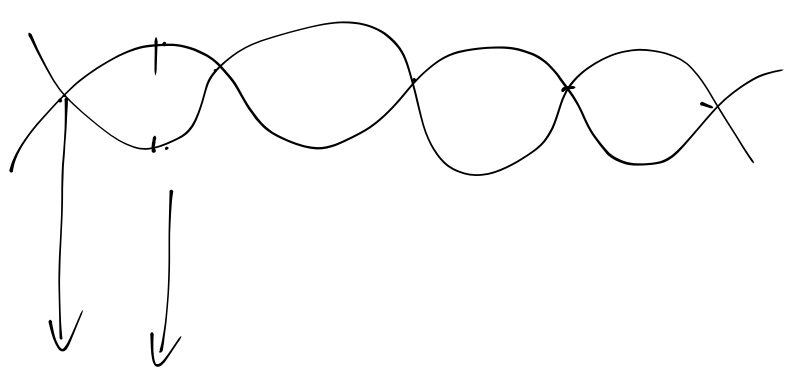
$x^4 = 1$.

$\langle x \rangle$ has order 4, so $4 \mid p-1$

Conclusion: $p = m^2 + n^2$ has solutions $m, n \in \mathbb{Z}$ iff

$$p \equiv 1 \pmod 4.$$

Prime elements in $\mathbb{Z}[i]$.



$p \equiv 1 \pmod 4$

$p' \equiv 3 \pmod 4$

$p' \in \mathbb{Z}$. $p' \equiv 3 \pmod 4$. then p' is still prime in $\mathbb{Z}[i]$

$p \in \mathbb{Z}$. $p \equiv 1 \pmod 4$. then $p = a^2 + b^2$

$= (a+bi)(a-bi)$

Such $a+bi$ are prime elements.

$(a+bi) = (c+di)(e+fi)$

$\Rightarrow \quad a^2+b^2 = (c^2+d^2)(e^2+f^2)$

$\Rightarrow \quad c^2+d^2$, or $e^2+f^2 = 1$

((aim:

If $a+bi$ is a prim element.

then a^2+b^2 must be a prime number.

$a^2+b^2 = p_1 p_2 \cdots p_m$

$(a+bi)(a-bi) = p_1 p_2 \cdots p_m$.

$a+bi$ prime $\Rightarrow$ $a-bi$ prime in $\mathbb{Z}[i]$.

So $m = 1$ or 2.

$m=1$, then $(a+bi)(a-bi) = p_1 \Rightarrow a^2+b^2 = p_1$.

$m=2$. then $(a+bi)(a-bi) = p_1 p_2$.

$a+bi$ associate with p_1.

so $a+bi = \pm p_1 \cdot \pm p_1 i$.

or $a+bi = \pm p$

$\pm pi$.

$p \equiv 3 \pmod 4$

Field extension.

$\varphi: F \to F'$. F, F' fields.

φ hom. φ is inj or 0. (why?!)

So the only interesting ring homs between fields are injective.

In which we can view F as a subring of F'.

Field extension. $F \subset F'$ subfield. F'/F.

F'/F

F' is an extension of F.

Ex: $\mathbb{Q} \hookrightarrow \mathbb{Q}(i)/(x^2+1)$.

Ex: $\mathbb{Q} \hookrightarrow \mathbb{C}$.

$\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$

Ex: $G \hookrightarrow G(\bar{f}) = \left\{ \frac{f(\bar{f})}{g(\bar{f})} \mid f, g \in F(\bar{f}), g \neq 0 \right\}$

Two different extensions.

Transcedental.

Algebraic element.

Algebraic element α over F.

$\exists f(x) \neq 0 \in F(x)$. s.t. $f(\alpha) = 0$.

then α is algebraic. otherwise transcedental

relation to: $\varphi: F(\bar{x}) \to K$.

$x \mapsto \alpha$.

Two possibility. $\ker \varphi = (0)$.

or $\ker \varphi = (f(x))$

$F(\bar{x})/(f(x)) \hookrightarrow K$ is a subring in K.

So it has no zero divisor

So $F(\bar{x})/(f(x))$ is an integral domain

$f(x)$ is prime element, irreducible polynomial

Such monic $f(x)$ is called the irreducible polynomial of α in F.

(1) $f(\alpha) = 0$

(2) If $g(\alpha) = 0$, $g(x) \in F[x]$, then $f(x) | g(x)$

Corollary:

$F(\alpha) = \{ g(\alpha) \mid g \in F[x] \} \hookrightarrow K$

is a subfield

Defn. K/F is algebraic iff $\forall \alpha \in K$, α is algebraic over F.

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in F[x],\ g(\alpha) \neq 0 \right\}$$

If α is algebraic, then

$$F(\alpha) = F[\alpha].$$

Prop: $f(x)$ is irreducible polynomial of α in F, then $F[\alpha] = F(\alpha)$ and has a basis $(1, \alpha, \ldots \alpha^{n-1})$ as a vector space over F.

pf: $F[\alpha]$ is already a field, so $g(\alpha) \neq 0$.

$$(g(\alpha))^{-1} \in F[\alpha].$$

$$F[\alpha] = F(\alpha).$$

basis from the statement about adjoining elements in a ring.

Defn deg of extension. K/F

$[K:F] = \dim_F K$

Prop: If $[K:F]$ is finite, then K is algebraic extension over F.

Pf: $\forall \alpha \in K$,

$1, \alpha, \alpha^2, \cdots \alpha^{n-1}, \alpha^n$

must be linear dependent for large n.

So $a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$.

for some $(a_0, \cdots a_n) \in F^n$

$\neq (0, \cdots 0)$

$f(x) = a_0 + a_1 x \cdots a_n x^n$ has a root $x = \alpha$.

① K/F field extension.

② $\alpha \in K$ algebraic

Irreducible polynomial of α over F.

$f(\alpha)=0$ and f irreducible in $F[x]$.

If $g(\alpha)=0$, $g \in F[x]$, then $f(x) \mid g(x)$

③ degree of extension $[K:F] = \dim_F K$.

④ $[F(\alpha):F]$ = deg of α over F.

= deg of $f(x)$

basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

⑤ If $[K:F] < +\infty$, then K/F is algebraic

Thm: (Degree is multiplicative)

$F \subset K \subset L$. or K/F, L/K.

$[L:F] = [L:K][K:F]$

Pf: $[K:F] = n$, $[L:K] = m$.

L as a K-vector space has a basis

$\alpha_1 \cdots \alpha_m$.

K as a F-vector space has a basis

$\beta_1 \cdots \beta_n$.

Claim. $\alpha_i \beta_j$ $1 \le i \le m$
$1 \le j \le n$.

form a basis of L as a F-vector space.

(1) $\mathrm{Span}_F(\alpha_i \beta_j) = L$.

$\forall v \in L$, $v = \sum a_i \alpha_i$. $a_i \in K$.

$$\alpha_i = \sum_j a_{ij} \beta_j . \qquad a_{ij} \in F$$

$$v = \sum_i \underline{a_{ij}} \alpha_i \beta_j .$$

(2) Linear independent.

If $\sum_{ij} \alpha_{ij} \alpha_i \beta_j = 0$

$$\Rightarrow \sum_j \underbrace{\left(\sum_i (\alpha_{ij} \alpha_i) \right)}_{K} \beta_j = 0$$

basis

$$\Rightarrow \sum_i \alpha_{ij} \alpha_i = 0 \Rightarrow \alpha_{ij} = 0 .$$

Corollary: a) $[K:F]=n$.

$\alpha \in K$. $\deg \alpha \mid n$.

b) $F \subset F' \subset K$.

$[K:F'] \mid [K:F]$

c) $\alpha_1, \alpha_2 \cdots \alpha_m$ algebraic

$\Rightarrow F(\alpha_1, \alpha_2 \cdots \alpha_m)$ is algebraic

simple example. α algebraic

β algebraic

$\alpha+\beta$ algebraic

$\alpha\beta$ algebraic

$\alpha = \sqrt{2}$. $\beta = \sqrt{3}$.

$t = \sqrt{2}+\sqrt{3}$. $t^4 - 10t^2 + 1 = 0$.

d) K/F, set of elements which are algebraic $/F$ is a subfield of K

Lemma: If $[K:F]$ prime p, $\alpha \in K$. $\alpha \notin F$, then $F(\alpha) = K$.

Corollary: L/F. K_1/F. K_2/F.
L/K_1, L/K_2.
$[K_1:F] = m$, $[K_2:F] = n$.
$\tilde{K}$ = subfield generated by K_1, K_2
$[\tilde{K}:F] \leq mn$, and $m \mid [\tilde{K}:F]$
$n \mid [\tilde{K}:F]$

$K_1 = F[\alpha_1 \cdots \alpha_m]$

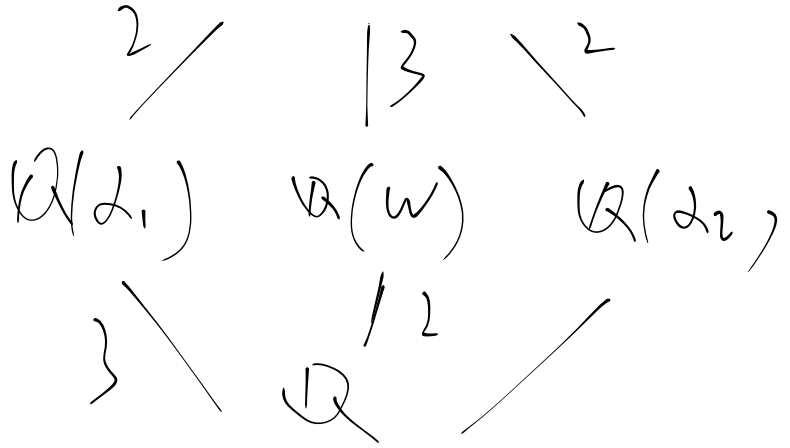
$\overline{K} = K_2[\alpha_1 \cdots \alpha_m)$.

Ex: has roots $\alpha_1, \alpha_2, \alpha_3$

$x^3 - 2$. $\alpha_1 = \sqrt[3]{2}$. $\alpha_2 = w \cdot \sqrt[3]{2}$

$\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1, w)$.

$\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1, w)$



If $[K : F] = 2$, $\text{char } F \neq 0$. then $K = F(\alpha)$ for $\alpha^2 = d \in F$.

(Quadratic extension)

Ruler and compass.

① Two pts on the plane

② Draw a line a circle from two pts.

③ Take intersections.

Prop: ① $P_0(a_0, b_0)$. $P_1(a_1, b_1)$

$a_i, b_i \in F \subset \mathbb{R}$.

Then constructed lines and circles are defined by quadratic equation with coefficients in F.

② Intersection point of A. B.

with coefficients in F.

is in a quadratic extension of F.

Thm: If P is constructible, then

there exist a tower of fields

$K = F_n$

$\vdots$

F_2

$\cup$

F_1

$\cup$

$\mathbb{Q} = F_0$

such that $[F_i, F_{i-1}] = 2$

and all the coordinates of

P is inside K.

Corollary: If $P = (a, b)$ constructible

then $[\mathbb{Q}(a, b) : \mathbb{Q}] = 2^k$.

Trisection is not possible.

$\alpha = \cos 20°$, $\Rightarrow$ $\alpha^3 = \frac{1}{2}\alpha + \frac{1}{2}$.

$x^3 - \frac{3}{2}x - \frac{1}{2}$ is irreducible.

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

Isomorphism between field extensions

Prop: Let $K = F(\alpha)$ and irreducible polynomial of α over F is $f(x)$.

$K' = F(\beta)$ and irreducible polynomial of β over F is $g(x)$

Then $\exists$ field isomorphism

$\varphi : K \to K'$ such that

$\varphi|_F = id_F$ and $\varphi(\alpha) = \beta$

iff $g(x) = f(x)$

Pf: (idea) Use the isomorphism

$K \cong F(x)/(f(x))$

$\alpha \mapsto x$.

Adjoining roots.

Prop: $f(x) \in F[x]$, $\exists$ K/F such that $f(x)$ has a root in K.

Pf: If $f(x)$ is irreducible. Let

$$K = F[x]/(f(x))$$

then $\bar{x} \in F[x]/(f(x))$ is a root of $f(x)$

(Splitting). $f(x)$ splits completely in K if $f(x) = \prod_{i=1}^{n} (x - a_i)$ with $a_i \in K$.

Prop: $f(x) \in F[x]$, $\exists$ K/F such that $f(x)$ splits completely

Pf: Use the adjoining roots process until $f(x)$ splits completely.

Important proposition. about g.c.d.

Prop: K/F, $f(x), g(x) \in F[x]$.

then g.c.d $(f(x), g(x))$ are the same

in both $F[x]$ and $K[x]$.

Pf: (Even though $K[x]$ is larger, potentially there're more common factors, but the g.c.d are the same)

(idea) g.c.d is calculated by

division with remainder

$f(x) = q(x) \cdot g(x) + r(x)$. $\deg r < \deg g$.

g.c.d $(f(x), g(x))$ = g.c.d $(g(x), r(x))$

= .....

This process does not depend on the choice of the base field.

Corollary: If $\mathrm{char} F = 0$, $f(x)$ irreducible,

then $f(x)$ has no multiple roots in

any field extension.

Pf. $f(x)$ has multiple roots

$\Leftrightarrow$ $g.c.d(f(x), f'(x)) \neq 1$

$\mathrm{char} F = 0$, $\Rightarrow$ $f'(x) \neq 0$.

So $g.c.d(f(x), f'(x)) = 1$

Primitive extension. $F(\alpha)$ extension generated by one element.

Thm: K/F finite extension. $\mathrm{char} F = 0$

then $K = F(\alpha)$ for some $\alpha \in K$.

(α is called primitive element)

pf: $K = F(\alpha_1, \cdots \alpha_n)$.

only need to prove $F(\alpha, \beta) = F[\gamma]$.

(Example : $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.)

Let $f(x)$ be the irreducible polynomial of α.

$g(x)$ ---------- of β.

Let L/K such that $f(x), g(x)$ split completely.

$f(x)$ has roots $\alpha_1 = \alpha, \alpha_2 \cdots \alpha_n$.

$g(x)$ has roots $\beta_1 = \beta, \beta_2 \cdots \beta_m$

Choose $c \in F$ such that

$$c\alpha_i + \beta_j \neq c\alpha_{i'} + \beta_{j'}$$

if $(i, j) \neq (i', j')$

Let $\gamma = c\alpha + \beta$.

We claim $F[\gamma] = F[\alpha, \beta)$.

Let $h(x) = g(\gamma - cx) \in F[\gamma]$

Then $h(\alpha) = 0$.

and $h(\alpha_i) \neq 0$, for $i \geq 2$.

So $g.c.d(f, h) = x - \alpha$ in

both $F[\gamma][x]$ and $L[x]$

So $x - \alpha \in F[\gamma][x] \Rightarrow \alpha \in F[\gamma]$

$\beta = \gamma - c\alpha \in F[\gamma]$.

Important fact from the proof.

almost every c works.

as long as $|\alpha_i + \beta_j| \neq |\alpha_{i'} + \beta_{j'}|$.

Last class: Char $F = 0$.

K/F finite extension.

$K = F(\alpha)$.

$F(\alpha, \beta) = F(\alpha + c\beta)$. $c \in F$.

↑ almost all c works.

Splitting field of $f(x) \in F[x]$ over F

if ① $f(x)$ splits completely with roots $\alpha_1 \cdots \alpha_n$.

② $K = F(\alpha_1 \cdots \alpha_n)$

Prop: ① $\forall f$. splitting field exists

② $F \subset L \subset K$. K is splitting field of $f(x)$ over F. then also splitting field over L.

(3) K/F finite extension.

$\exists$ there exist $\bar{K}/K$

a splitting field.

Pf: (Existence) Keep adding roots to split $f(x)$ completely and define $K = F(\alpha_1 \cdots \alpha_n)$

Example: $w = e^{\frac{2\pi i}{3}}$. $f(x) = x^3 - 2$.

$\mathbb{Q}(w, \sqrt[3]{2})$ → This is the splitting field of $f(x)$ over $\mathbb{Q}$

|

$\mathbb{Q}(w)$ → This is not.

|

$\mathbb{Q}$

Most important Thm of splitting field.

Thm: If K/F is a splitting field of $f(x) \in F(x)$.

and $g(x) \in F(x)$ is irreducible with one root $\alpha \in K$,

then $g(x)$ splits completely in K.

Prop: (Uniqueness of splitting field)

① $K_1 \subset L$, $K_2 \subset L$, $F \subset K_i$.

$f(x) \in F[x]$, Assume K_1 and K_2 are both splitting field of $f(x)$, then $K_1 \cong K_2$

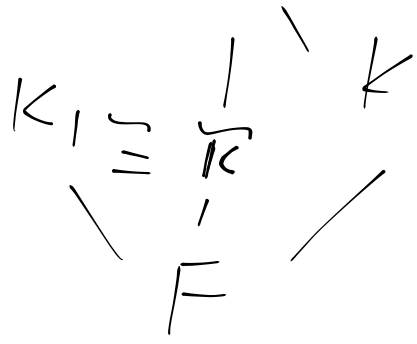
② If K_1, K_2 are both splitting field of $f(x) \in F[x]$, then $K_1 \cong K_2$

Pf: ① $K_1 = K_2 = F(\alpha_1 \cdots \alpha_n)$

② choose $K_1 = F[\alpha_1]$, $K_2 = F[\alpha_2]$.

α_1, α_2. α_1 has irreducible polynomial $g(x)$

choose L/K_2 such that $g(x)$ splits completely with one root $\tilde{\alpha}$.



choose $\tilde{K} = F[\tilde{\alpha}]$. Then $K_1 \cong \tilde{K}$. $\tilde{K}$ is also a splitting field of $f(x)$ so $\tilde{K} = K_2$ from ①.

Galois group $G(K/F)$

$$G(K/F) = \{ g : K \to K \text{ isomorphism} \mid g|_F = id_F \}$$

$$K = \mathbb{Q}[\sqrt{2}, i] \Big/ \mathbb{Q}[\sqrt{2}]$$

$$F$$

$$G(K/F) = \{ id,\ \sigma : a \mapsto \bar{a} \}$$

$$G(K/\mathbb{Q}) = \left\{ \begin{array}{l} id,\ \sigma_1 : \sqrt{2} \mapsto -\sqrt{2} \\ \qquad\quad i \mapsto i \\ \sigma_2 : i \mapsto -i \\ \qquad\quad \sqrt{2} \mapsto \sqrt{2}. \end{array} \quad \sigma_3 : \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{array} \right\}$$

How to specify an element σ in $G(K/F)$?

If $K = F(\lambda)$, we only need to know $\sigma(\lambda)$.

$$\sigma\left(\sum a_i \alpha^i\right) = a_i \sum \sigma(\alpha)^i$$

Prop: $\alpha \in K$, α is a root of $f(x)$
then $\sigma(\alpha)$ is a root of $f(x)$.

① Splitting field $K = F(\alpha)$.

then $\sigma(\alpha) = \alpha_i$.

$(\alpha_1 \dots \alpha_n)$ are the roots of irreducible polynomial of $f(x)$

Two aspects. a) α_i determines σ uniquely.
b) For each α_i, there exists σ_i such that $\sigma_i(\alpha) = \alpha_i$

In other words $|G(K/F)| = n = [K:F]$

Example: $K = \mathbb{Q}(\sqrt{3}+\sqrt{5})$ / $\mathbb{Q}$.

$$G(K/\mathbb{Q}) = \begin{cases} \sigma_1 : \sqrt{3}+\sqrt{5} \longmapsto \sqrt{3}+\sqrt{5} \\ \sigma_2 : \sqrt{3}+\sqrt{5} \longmapsto \sqrt{3}-\sqrt{5} \\ \sigma_3 : \sqrt{3}+\sqrt{5} \longmapsto -\sqrt{3}+\sqrt{5} \\ \sigma_4 : \sqrt{3}+\sqrt{5} \longmapsto -\sqrt{3}-\sqrt{5} \end{cases}$$

(2) In the case that K/F is not a splitting field, then $|G(K/F)| < [K:F]$

In fact $|G(K/F)| \mid [K:F]$

Example: $K = \mathbb{Q}[\sqrt[3]{2}]$.

then $G(K/F) = \{1\}$.

because any root of x^3-2 other than $\sqrt[3]{2}$ is not in K.

Fixed fields. H is a finite subgroup of

$$H \subset Aut(K) \qquad Aut(K)$$

$$K^H = \{ \alpha \in \mathbb{C} \mid \sigma(\alpha) = \alpha \}.$$
$$\forall \sigma \in H$$

① H finite. $\beta \in \mathbb{C}$. $\{\beta_1 \cdots \beta_r\}$ is the H-orbit of β.

then the irreducible polynomial of β over K^H is

$$(x-\beta_1)\cdots(x-\beta_r).$$

② $[\mathbb{C} : K^H]$ is finite.

and $\overline{[\mathbb{C} : K^H]} = |H|$.

Pf: ① $\beta_1 + \cdots \beta_r \in K^H$ because $\sigma \in H$ only change the order of $\beta_1, \cdots \beta_r$

Galois extension. K/F

TFAE: ① K/F is a splitting field.

② $G(K/F) = [K:F]$

③ $F = K^H$ for some H finite in $Aut(K)$

① $\Leftrightarrow$ ② $\Leftrightarrow$ ③. and K/F satisfies this proposition is called Galois extension.

Galois correspondance. K/F Galois

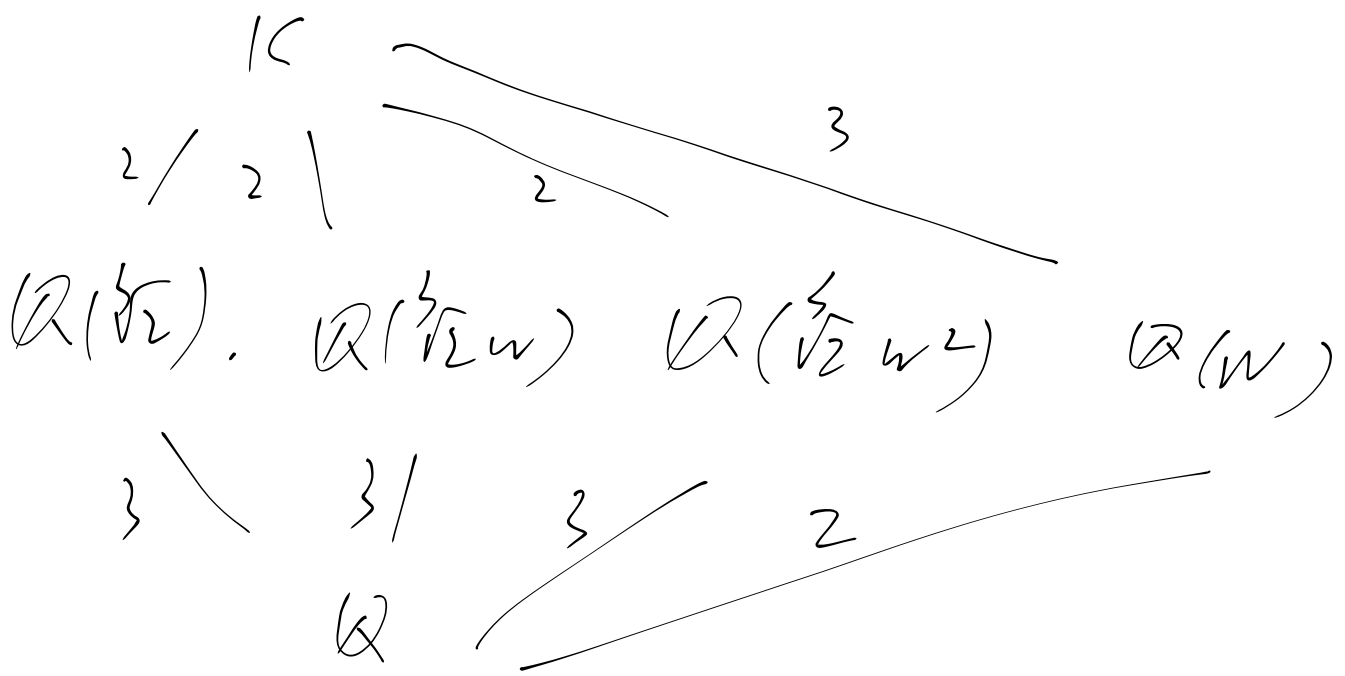
$$\left\{ \begin{array}{l} L \text{ intermediate field} \\ \text{between } K/F. \\ \text{i.e. } F \subset L \subset K \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{l} H. \\ \text{subgroups} \\ \text{of } K/F \end{array} \right\}$$

$$L \longrightarrow Gal(K/L)$$

$$K^H \longleftarrow H$$

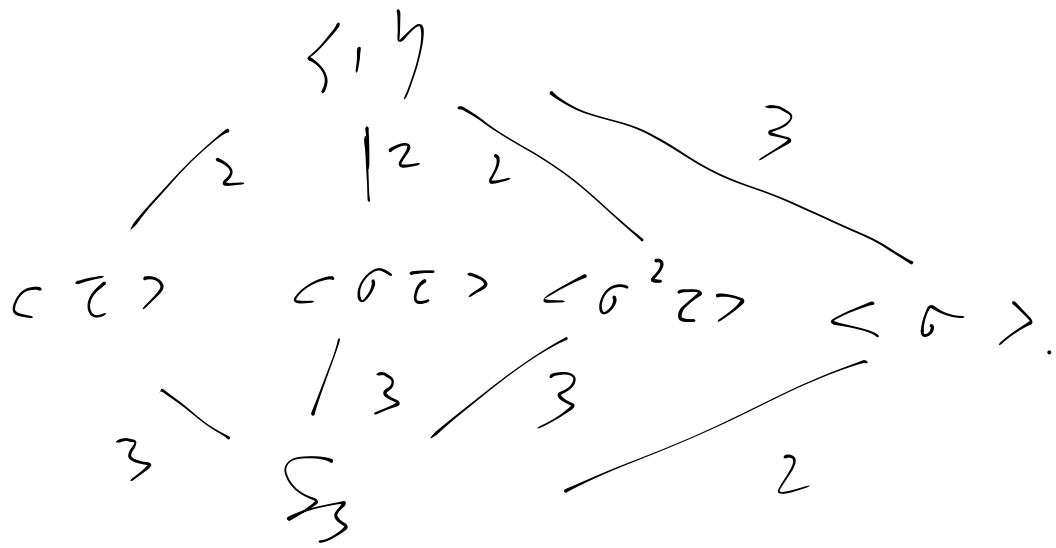
Example (will be explained in the last class)

$K = \mathbb{Q}(w, \sqrt[3]{2})$ (splitting field of $f(x) = x^3 - 2$)



$G(K/\mathbb{Q}) \cong S_3 = \langle \sigma, \tau \rangle$. $\sigma^3 = \tau^2 = 1$

$\tau\sigma\tau = \sigma^2$.



Recall. ① K/F splitting field.

② $|G(K/F)| = [K:F]$.

③ $F = K^H$ for some $H \subset Aut(K)$.

For any field K, $\mathrm{char}\, K = 0$.

$\mathbb{Q} \subset K$, and $\mathbb{Q} \subset K^H$

①, ②, or ③ can be used to define

Galois extension. K/F Galois

Galois correspondence:

$G = G(K/F)$

$H \subset G$ subgroup.

$F \subset L \subset K$ intermediate extension.

$$\left\{\begin{array}{l}\text{subgroups}\\ \text{in } G\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{intermediate}\\ \text{extensions}\end{array}\right\}$$

$H \longmapsto K^H$

$G(K/L) \longleftarrow L$

Splitting field of $f(x)$ over F; $G(K/F)$

Example 1:

$F=\mathbb{Q}$. $x^4-1 = (x^2+1)(x^2-1)$

$=(x+i)(x-i)(x+1)(x-1)$

$\mathbb{Q}(-i, i, 1, -1) = \mathbb{Q}(i)$

$[\mathbb{Q}(i):\mathbb{Q}) = 2$.

$G((\mathbb{Q}(i)/\mathbb{Q})$. $\sigma \in G(\mathbb{Q}(i)/\mathbb{Q})$

$\sigma(a+bi) = \sigma(a) + \sigma(b)\cdot\sigma(i)$ $a, b \in \mathbb{Q}$.

$= a + b\sigma(i)$

$i^2 = 1. \Rightarrow \sigma(i)^2 = 1 \Leftrightarrow \sigma(i) = \pm i$.

σ is determined by $\sigma(i)$

In other words, $G(\mathbb{Q}(i)/\mathbb{Q}) \to \{i, -i\}$ is

$\sigma \longmapsto \sigma(i)$

injective.

On the other hand, we know

$$|G(\mathbb{Q}(i)/\mathbb{Q})| = [\mathbb{Q}(i):\mathbb{Q}) = 2$$

The above map is also surjective

So $G(\mathbb{Q}(i)/\mathbb{Q}) = \{id, \sigma_0\}$

$\sigma_0 : a+bi \mapsto a-bi$.

So $G(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

The Galois correspondence can be shown in the following diagram:

$\{id\}$ $\quad\quad$ $\mathbb{Q}(i)$

$|$ 2 $\quad\quad$ $|$ 2

$G = \mathbb{Z}/2\mathbb{Z}$ $\quad\quad$ $\mathbb{Q}$

Example 2:

$G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

$|G| = 4$. $\quad G \cong C_2 \times C_2$ or C_4.

$\sigma: \sqrt{2} \mapsto \pm\sqrt{2}$ (which one?)

$\sqrt{3} \mapsto \pm\sqrt{3}$.

$$G \to \left\{ \begin{array}{l} (\sqrt{2}, \sqrt{3}) \\ (-\sqrt{2}, \sqrt{3}) \\ (\sqrt{2}, -\sqrt{3}) \\ (-\sqrt{2}, -\sqrt{3}) \end{array} \right\}$$

$$\sigma \longmapsto (\sigma(\sqrt{2}), \sigma(\sqrt{3}))$$

is injective.

since $|G| = 4$. the map is also surjective.

(The map also has the following interpretation.)

Look at the action of

G on the roots $(x^2-2)(x^2-3)$.

then we get a group homomorphism

$$G \longrightarrow S_2 \times S_2$$

S_2: permutation of $\{\sqrt{2}, -\sqrt{2}\}$

S_2: permutation of $\{\sqrt{3}, -\sqrt{3}\}$.

This is injective because $\sqrt{2}$, $\sqrt{3}$ are the generators for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$

since $|G| = 4$, this is an isomorphism.

$$G \cong C_2 \times C_2.$$

$$G = \{1, \sigma, \tau, \sigma\tau\}.$$

σ: $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$.

τ: $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$.

σ : $\sqrt{2} \mapsto -\sqrt{2}$

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

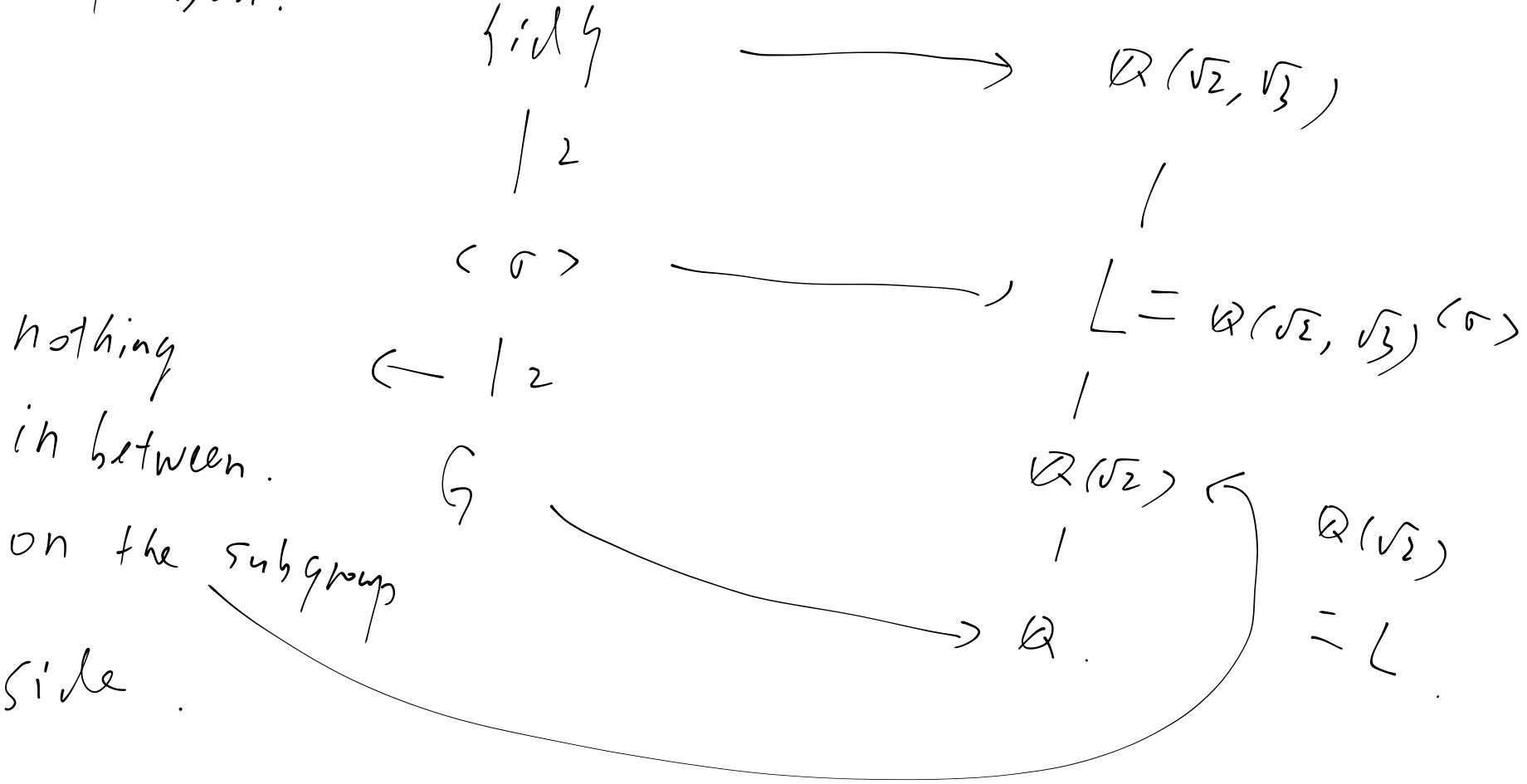
If we look at the fixed field.

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle} \supset \mathbb{Q}(\sqrt{2}).$$

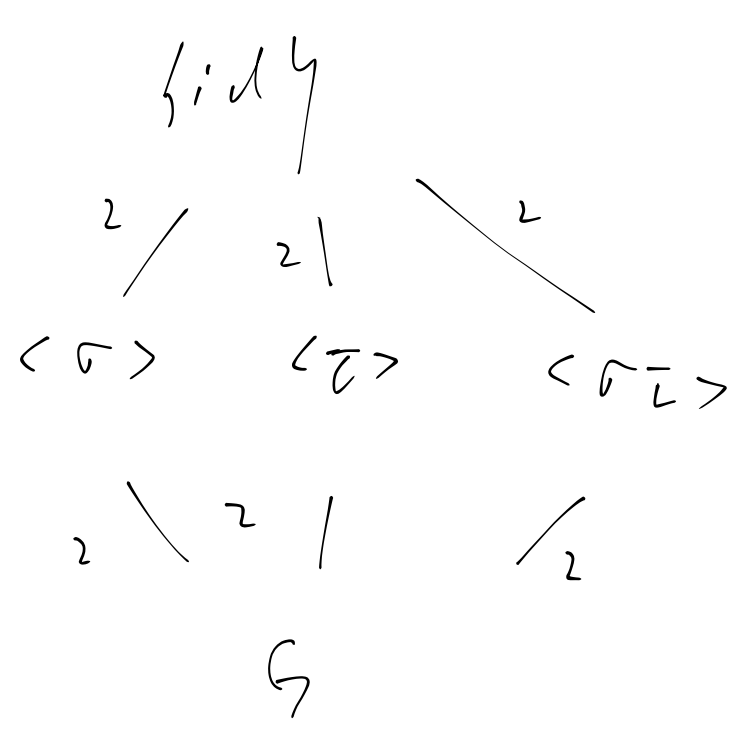
(because $\sigma(\sqrt{2}) = \sqrt{2}$)

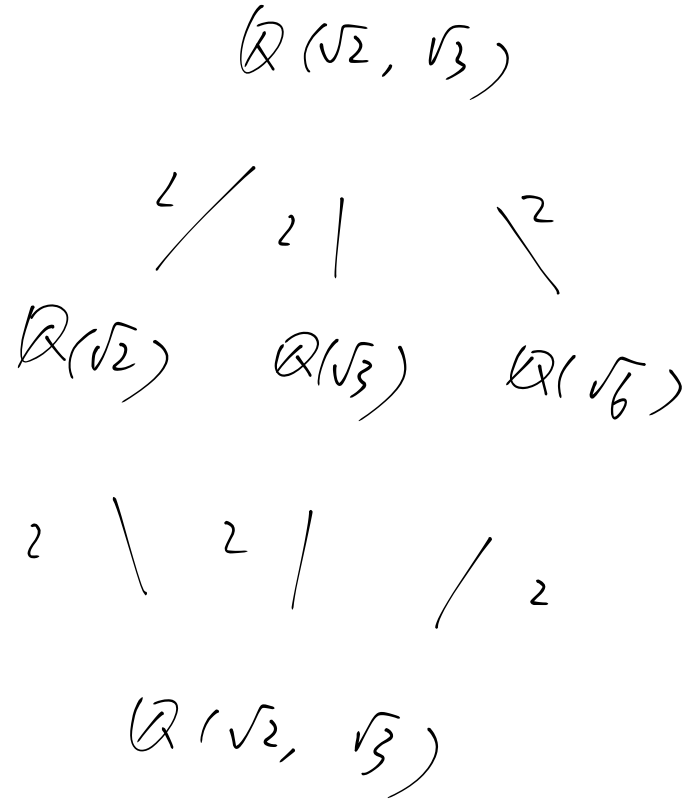
Claim $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle}$

Reason:



In summary:





(This diagram is the same for splitting field of $x^4+1 = (x^2-i)(x^2+i)$

$$= \left(x - \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x - \frac{-\sqrt{2}-\sqrt{2}i}{2}\right)$$

$$\left(x - \frac{\sqrt{2}-\sqrt{2}i}{2}\right)\left(x - \frac{-\sqrt{2}+\sqrt{2}i}{2}\right)$$

$\mathbb{Q}(\sqrt{2}, i)$ is the splitting field

and the same argument shows that

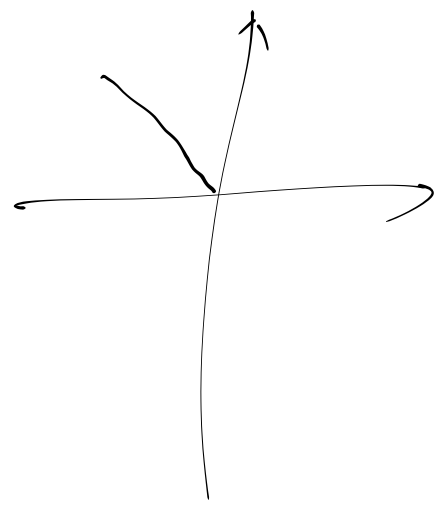
$G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$.

Example 3. Splitting field K of x^3-2

$$(x^3-2) = (x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)$$

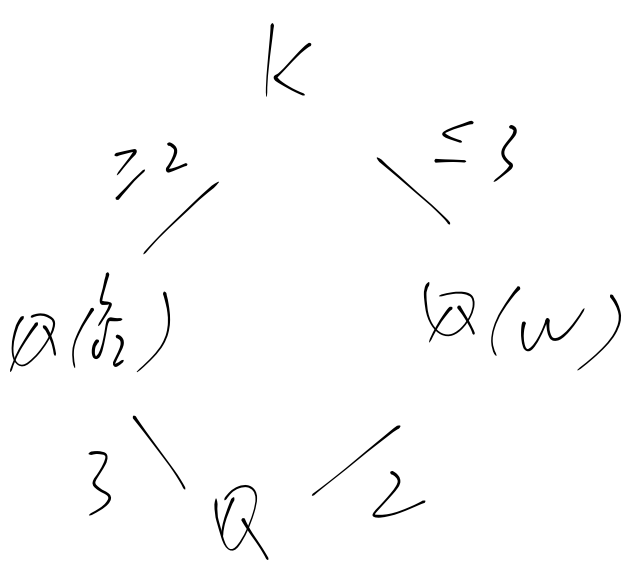
$$\omega = e^{\frac{2\pi i}{3}}$$

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



$$\omega^2+\omega+1=0.$$

So $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$.



$3 \mid [K:\mathbb{Q}]$

$2 \mid [K:\mathbb{Q}]$

and $[K:\mathbb{Q}(\omega)] \leq 2$.

So $[K:\mathbb{Q}] = 6$.

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\,w$, $\alpha_3 = \sqrt[3]{2}\,w^2$.

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

Consider the action of $G(K/\mathbb{Q})$ on the three roots $\{\alpha_1, \alpha_2, \alpha_3\}$, we obtain homomorphism.

$$G \longrightarrow S_3.$$

① It's injective because $\alpha_1, \alpha_2, \alpha_3$ are generators.

② It's surjective because $|G| = 6$, $|S_3| = 6$.

So $G \cong S_3$.

Let $\sigma = (123)$ $\tau = (12)$

$\sigma: \alpha_1 \mapsto \alpha_2$

$\alpha_2 \mapsto \alpha_3$

$\alpha_3 \mapsto \alpha_1$.

So $\sigma(\alpha_1) = \alpha_2$

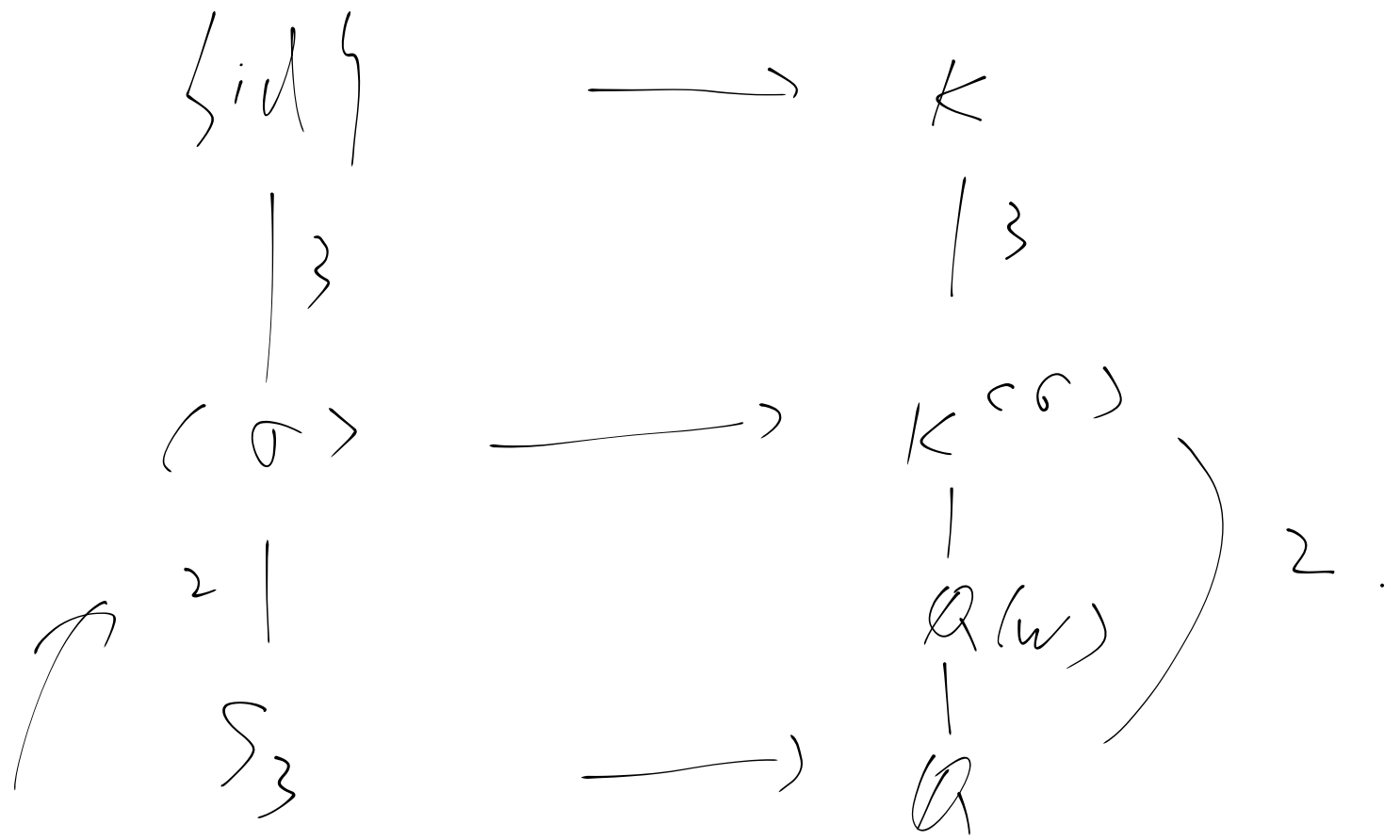
$$\sigma(w) = \sigma\left(\frac{\alpha_2}{\alpha_1}\right)$$

$$= \frac{\sigma(\alpha_2)}{\sigma(\alpha_1)} = \frac{\alpha_3}{\alpha_1} = w.$$

$\sigma : \alpha_1 \longmapsto \alpha_1 \cdot w.$

$w \longmapsto w.$

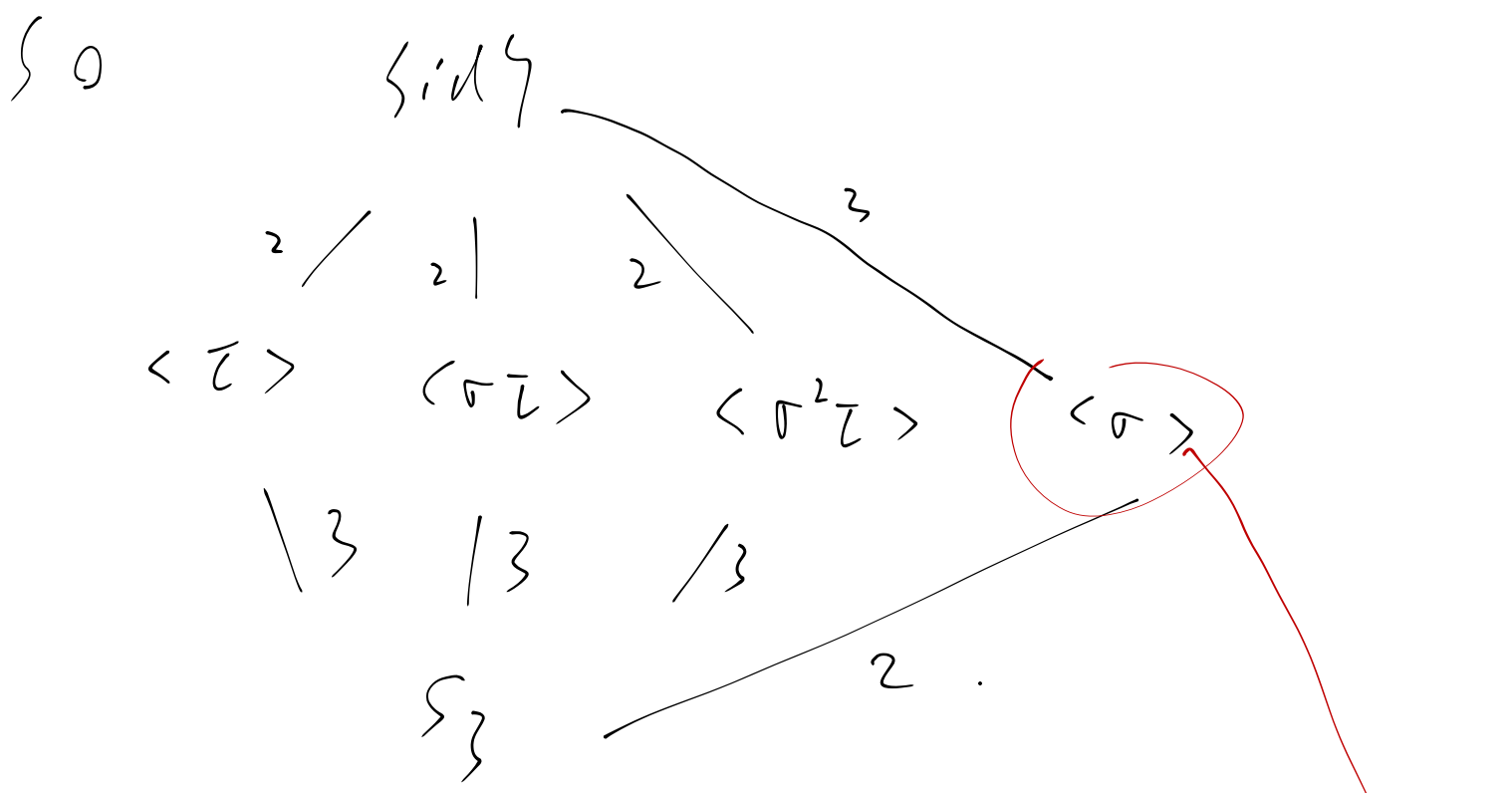
so $\mathbb{Q}(w) \subset K^{\langle \sigma \rangle}$.

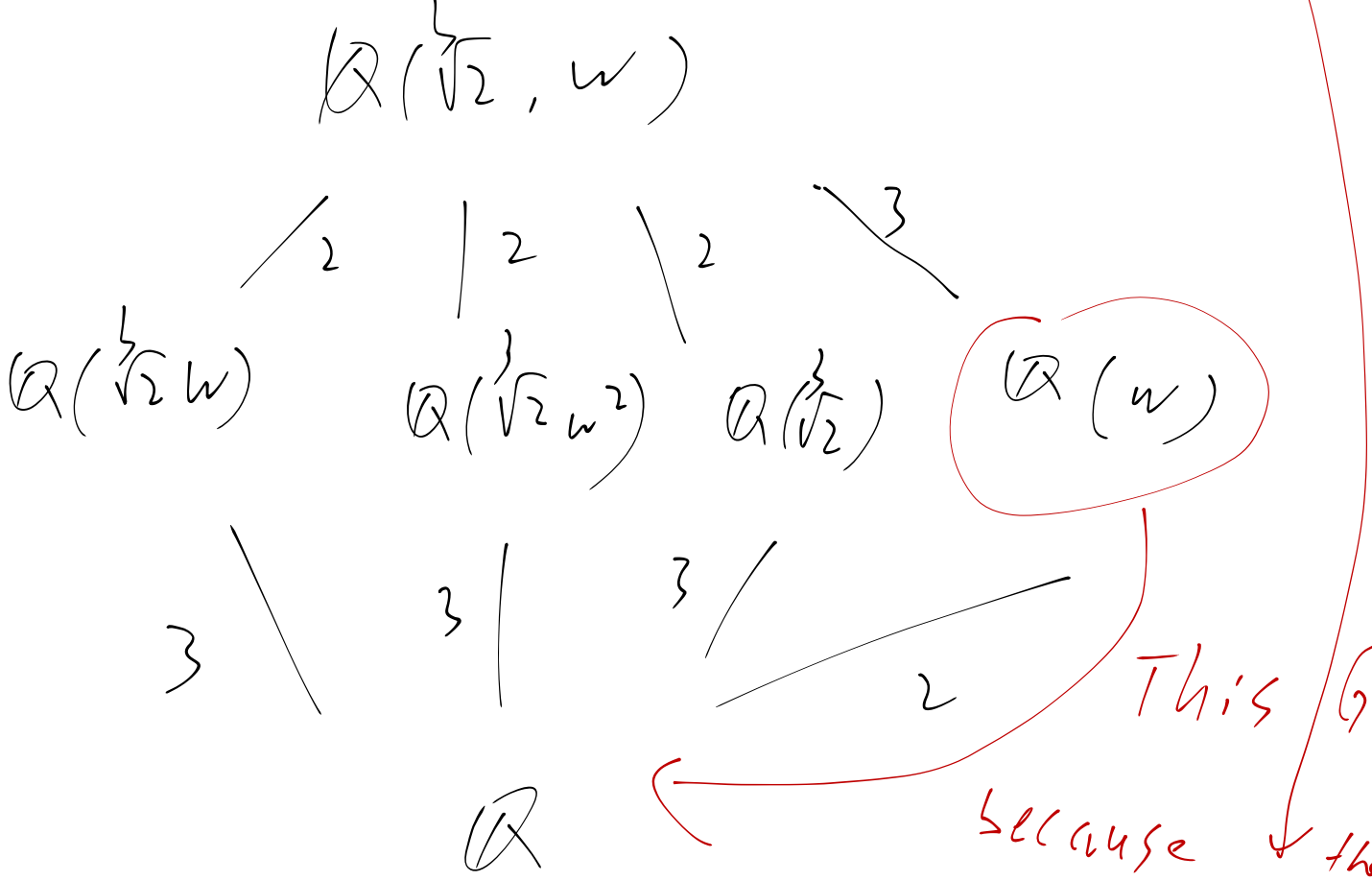


No subgroup

between $\langle \sigma \rangle$ and S_3. so $\mathbb{Q}(w) = K^{\langle \sigma \rangle}$

similarly $K^{\langle \tau \rangle} = \mathbb{Q}(\alpha_3)$





some application to find irreducible polynomial of $p \in K$. K/F is Galois extension.

Just need to find the orbit of

$G(K/\mathbb{Q})$ on β.

For example $\sqrt{2}+\sqrt{3}$ in $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

the orbit is $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$.

$-\sqrt{2}+\sqrt{3}$.

So irreducible polynomial is

$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))$