So $(a_j) = (a_{j+1}) = \cdots$

Non UFD.

$\mathbb{Z}[\sqrt{-5}]$.

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

2. 3. $1+\sqrt{-5}$. $1-\sqrt{-5}$ are all irreducible.

If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 2$.

$$\begin{cases} ac - 5bd = 2 \\ ad + bc = 0 \end{cases}$$ hard to solve.

Instead

$$|a+b\sqrt{-5}|^2 \, |c+d\sqrt{-5}|^2 = 4.$$

$$\underbrace{(a^2+5b^2)(c^2+5d^2) = 4.}$$

$\Rightarrow a^2+5b^2 = 1.2.4.$ has to be 1.

$$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1+\sqrt{-5}.$$

$$(a^2+5b^2)(c^2+5d^2) = 6.$$

$$a^2+5b^2 = 1, \cancel{2}. 3. 6$$

$$a^2+5b^2 = 1. \ 6.$$

The units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

(Similar method by taking 1.1)

Application.

GCD: $d \mid a$. $d \mid b$.

if $e \mid a$. $e \mid b$. then $e \mid d$.

$a = p_1 \cdots p_m$

$b = q_1 \cdots q_n$.

compare $p_1 \cdots p_m$

$q_1 \cdots q_n$.

a, b coprime if $GCD(a,b)=1$.

Fermat Last thm:

$x^n + y^n = z^n \quad xyz \neq 0$

has no integer solutions.

Polynomial version:

$f^n + g^n = h^n$

has no solution in $\mathbb{C}[t]$ such that

$g.c.d(f,g)=1, \quad \deg f \geq 1$.

pf: Assume there is solution (f, g, h).

Choose (f, g, h) such that

$\deg f + \deg g + \deg h$ achieves minimal

$$f^n = \prod_{k=0}^{n-1} (h - \xi_k g)$$

$$\xi_k = e^{\frac{2\pi i}{n} \cdot k}$$

$$\text{g.c.d}(h, g) = 1 \Rightarrow$$

$$\text{g.c.d}(h - \xi_k g,\ h - \xi_l g) = 1$$

for $k \neq l$

(Why ! h, g can be represented by $h - \xi_k g$ and $h - \xi_l g$.

Let $H = h - \xi_k g$

$G = h - \xi_l g$

$$h = \frac{\xi_l H - \xi_k G}{\xi_l - \xi_k}.$$

$$g = \frac{H - G}{\xi_l - \xi_k}.$$)

From UFD.

$$h - \xi_i g = (x_i(t))^n.$$

$\Rightarrow$

$$h - g = x(t)^n$$
$$h - \xi_1 g = y(t)^n$$
$$h - \xi_2 g = z(t)^n.$$

$\Rightarrow$ solve h, g

$\Rightarrow$ after absorbing constants to the n-th power.

$$x(t)^n + y(t)^n = z(t)^n.$$

with lower degrees.

Factorization in $\mathbb{Z}[x]$

$\mathbb{Z}$ PID. but $\mathbb{Z}[x]$ is not.

$\mathbb{Z}[x] \hookrightarrow \underline{\mathbb{Q}[x]}$
$\downarrow$
PID

Goal: $\mathbb{Z}[x]$ is UFD.

Typical problem:

$R \hookrightarrow R'$. R is a subring of R'.

If $r \in R$ is irreducible in R,

r may not be irreducible in R'.

Ex: $R = \mathbb{R}[x]$. $R' = \mathbb{C}[x]$.

$r = x^2+1$, $r = (x+i)(x-i)$ in $\mathbb{C}[x]$.

We use two constructions to analyse $\mathbb{Z}[x]$

$\mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$, $\varphi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ p prime

Defn. (Primitive polynomial).

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

① $a_n > 0$, $n \geq 1$

② $g.c.d(a_n, \ldots a_0) = 1$.

Ex: $f(x) = 2x^2 + 2x + 3$.

Non. Ex: $f(x) = 2x^2 + 4x + 6$.

Lemma: ① $p \mid a_i$

② $p \mid f$

③ $\varphi_p(f) = 0$

① $\Leftrightarrow$ ② $\Leftrightarrow$ ③

Lemma: ① f primitive

equivalent ② $\forall p$ prime number. $p \nmid f$

① $\Leftrightarrow$ ② $\Leftrightarrow$ ③ ③ $\varphi_p(f) \neq 0$ for all p prime number

Lemma: p prime element in $\mathbb{Z}[x]$ iff p prime element in $\mathbb{Z}$.

pf: $\mathbb{Z}[x]/(p) = \mathbb{F}_p[x]$

$\mathbb{F}_p$ is integral domain $\Leftrightarrow$ $\mathbb{F}_p[x]$ is integral domain

(Gauss lemma). $f, g \in \mathbb{Z}[x]$ are both primitive $\Leftrightarrow$ $f \cdot g$ is primitive

pf: $\forall p$, $\varphi_p(f \cdot g) = \varphi_p(f) \cdot \varphi_p(g)$.

and $\mathbb{F}_p[x]$ has no zero divisors

so $\varphi_p(f \cdot g) \neq 0 \Leftrightarrow \varphi_p(f) \neq 0, \varphi_p(g) \neq 0$

(It's quit hard to prove directly!)

$f(x)\cdot g(x)$ the coefficient for

x^3 is $\underline{a_1 b_2 + a_2 b_1 + a_3 b_0 + a_0 b_3}$.

It's hard to figure out the prime factors for the sum of products).

Lemma: $\forall f \in \mathbb{Q}[x] \Rightarrow f = c\cdot f_0(x)$

$c \in \mathbb{Q}$, $f_0(x) \in \mathbb{Z}[x]$ and primitive.

c, f_0 are uniquely determined by f

(If $f(x) \in \mathbb{Z}[x]$, then $c \in \mathbb{Z}$)

Pf: Existence:

$$f(x) = \frac{2}{3}x^2 + \frac{4}{5}x + 6$$

$$\Rightarrow f(x) = \frac{1}{15}(10x^2 + 12x + 90)$$

$$= \frac{\frac{2}{15}}{c}\,\frac{(5x^2+6x+x_5)}{f_0(x)}.$$

Uniqueness: If

$$f(x) = c_0 f_0 = c_0' f_0'.$$

then $mf(x) = (c_0 m) f_0$

$= (c_0' m) f_0'.$

Choose m such that

$c_0 m,\ c_0' m \in \mathbb{Z}$

For $p \mid c_0 m \Rightarrow p \mid mf(x)$

$\Rightarrow p \mid (c_0' m) f_0'$

$\Rightarrow \; p \mid c_0' m$ (since f_0 is primitive)

Cancel p on both sides.

$\Rightarrow \; c_0 m = c_0' m$ use induction

$\Rightarrow \; f_0(x) = f_0'(x)$.

Thm: (I) f_0 primitive in $\mathbb{Z}[x]$

$g \in \mathbb{Z}[x]$

If $f_0 \mid g$ in $\mathbb{Q}[x]$

then $f_0 \mid g$ in $\mathbb{Z}[x]$

Pf. Assume $g = f_0 \cdot h$.

$h(x) \in \mathbb{Q}[x]$.

$h(x) = c\, h_0(x)$. $c \in \mathbb{Q}$, $h_0(x) \in \mathbb{Z}[x]$ primitive

$g = c' g_0(x)$

$g = c' g_0(x) = c\, (\underbrace{f_0 \cdot h_0})$

Gauss Lemma $\Rightarrow f_0 h_0$ primitive.

Uniqueness $\Rightarrow c = c' \in \mathbb{Z}$ (since $g(x) \in \mathbb{Z}[x]$)

so $h(x) \in \mathbb{Z}[x]$.

(2) If f, g has common divisor in $\mathbb{Q}[x]$.

then f, g has common divisor in $\mathbb{Z}[x]$.

Pf: $h \mid f$. then $h_0 \mid f$.

Thm: $f(x)$ irreducible in $\mathbb{Z}[x]$ $a_n > 0$.

then $f(x)$ = prime number in $\mathbb{Z}$

or primitive irreducible in $\mathbb{Q}[x]$.

Pf: $\deg f = 0$. $\Rightarrow$ f is in $\mathbb{Z}$.

f prime in $\mathbb{Z}$ $\Leftrightarrow$ f prime in $\mathbb{Z}[x]$.

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

then
$$\boxed{\begin{aligned} &g(x) \mid f(x) \text{ in } \mathbb{Q}[x] \\ \Leftrightarrow\ &g_0(x) \mid f(x) \text{ in } \mathbb{Z}[x]. \quad (*) \end{aligned}}$$

Thm: Every irreducible element in $\mathbb{Z}[x]$ is a prime element.

Pf: Prove it for primitive polynomials

Use $(*)$ again.

(Division in $\mathbb{Z}[x]$ is the same in $\mathbb{Q}[x]$ when considering primitive polynomials.)

Thm: $\mathbb{Z}[x]$ is UFD.

$$f(x) = c \cdot f_0(x)$$

$$c = p_1 \cdots p_m$$

$$f_0(x) = g_1 \cdots g_k(x)$$

$g_i(x)$ primitive, irreducible in $\mathbb{Q}[x]$

Thm: If R is UFD, then $R[x]$ is UFD.

(same proof)

Ex: $\mathbb{C}[x][y] = \mathbb{C}[x,y]$. (UFD but not PID)

Why care $\mathbb{Z}[x]$.

Consider field extension for $\mathbb{Q}$.

Is $\mathbb{Q}[x]/(f(x))$ a field?

Want to know whether $f(x)$ irreducible in $\mathbb{Q}[x]$.

It's equivalent to $f_0(x)$ irreducible in $\mathbb{Z}[x]$.

In $\mathbb{Z}[x]$, we can consider

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

and use correspondence theorem.

Next class : Eisenstein Criterion.

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

Useful facts :

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

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

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

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

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 $\varphi_p(f(x)) = \bar{f}(x)$ 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

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

$\bar{f} = \bar{g} \cdot \bar{h}$, $\deg \bar{f} = n$ $(p \nmid a_n)$

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

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

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

so $\underbrace{\deg \bar{g} = \deg g}_{\geq 1}$, $\underbrace{\deg \bar{h} = \deg h}_{\geq 1}$.

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

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

Contradiction 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. $\cancel{x^2}$, $\cancel{x^2+1}$, x^2+x+1.

deg 3. $\cancel{x^3}$. $\cancel{x^3+1}$. x^3+x+1,

$\cancel{x^3+x}$, $\cancel{x^3+x^2+x+1}$.

x^3+x^2+1. $\cancel{x^3+x^2}$. $\cancel{x^3+x^2+x}$.

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

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 $g(x) = c x^{m} + \cdots + c_0$

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

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

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

contradiction!

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

choose $p = 5$

Ex: (cyclotomic polynomial)

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

$$= \frac{x^p - 1}{x - 1} \quad \text{is irreducible.}$$

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

change of variable

$$y = x - 1$$

$$\Phi_p(y+1) \cdot y = (y+1)^p - 1$$

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

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

Note

$p \mid \binom{p}{i}$ 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 $\mathbb{Z}[x]$.

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

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.

so $a^2+b^2=p$

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

$\iff$ $p \equiv 3 \mod 4$

Pf: p is not a prime $\iff$

$p \equiv 1 \mod 4$.

p is not a prime $\iff$

$\mathbb{Z}[i]/(p)$ is not a field.

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

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

so $\mathbb{Z}[i]/(p)$ is not a field

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

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

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

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

$\therefore$ $x^2+1 = 0$. $x^2 = -1$

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

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

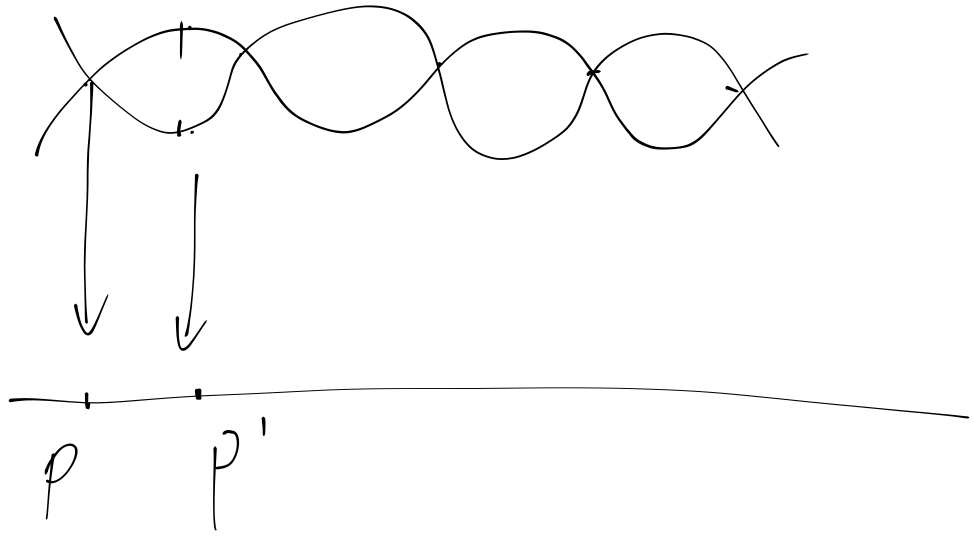
$x^4 = 1$.

$\langle x \rangle$ 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.

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

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

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

Claim:

If $a+bi$ is a prime element.

then a^2+b^2 must be a prime number. or $a+bi = \pm p$, $\pm pi$. $p \equiv 3 \pmod 4$

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

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

$a+bi$ 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 $a+bi = \pm p_1, \pm p_1 i$.

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 case, 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: $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]/(x^2+1)$.

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

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

Ex: $\mathbb{C} \hookrightarrow \mathbb{C}(t) = \left\{ \frac{f(t)}{g(t)} \;\middle|\; f, g \in \mathbb{C}[t], \; g \neq 0 \right\}$,

Two different extensions.

Transcedental.

<u>Algebraic</u> 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: $\varphi: F[x] \to K$.

$x \mapsto \alpha$.

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

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

$F[x]/(f(x)) \hookrightarrow K$ is a subring in K.

So it has no zero divisor

So $F[x]/(f(x))$ 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 $f(x) \mid g(x)$

Corollary:

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

is a <u>subfield</u>

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

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

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: $\forall \alpha \in K$,

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

must be linear dependent for large n.

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

for some $(a_0, \ldots a_n) \in F^n$
$\neq (0, \ldots 0)$

$f(x) = a_0 + a_1 x \cdots a_n x^n$ 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 $f(x) / g(x)$

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. $\alpha_i \beta_j$ $\quad 1 \le i \le m$, $1 \le j \le n$.

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

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

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

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

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

(2) Linear independent.

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

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

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

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

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

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

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

c). $\alpha_1, \alpha_2 \dots \alpha_m$ algebraic

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

simple example. α algebraic

β algebraic

$\alpha+\beta$ algebraic

$\alpha\beta$ algebraic

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

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

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

Corollary: 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.
$[\tilde{K}:F] \le mn$, and $m \mid [\tilde{K}:F]$
$n \mid [\tilde{K}:F]$

$$\begin{tikzcd}
 & \tilde{K} & \\
K_1 \arrow[ur, dash] & & K_2 \arrow[ul, dash, "\le m"'] \\
 & F \arrow[ul, dash, "m"] \arrow[ur, dash, "n"'] &
\end{tikzcd}$$

$$\boxed{\begin{aligned} K_1 &= F[\alpha_1 \dots \alpha_m] \\ \overline{K} &= K_2[\alpha_1 \dots \alpha_m). \end{aligned}}$$

Ex: $x^3 - 2$. has roots $\alpha_1, \alpha_2, \alpha_3$

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

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

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1, w) \arrow[dl, dash, "2"'] \arrow[d, dash, "3"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\alpha_1) \arrow[dr, dash, "3"'] & \mathbb{Q}(w) \arrow[d, dash, "2"] & \mathbb{Q}(\alpha_2) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

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

(Quadratic expansion)

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

$$K = F_n \supset \cdots \supset F_2 \supset F_1 \supset \mathbb{Q} = F_0$$

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

and all the coordinates of P is inside K.

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

Trisection is not possible.

$\alpha = \cos 20^\circ$, $\Rightarrow$ $\alpha^3 = 1 + 3\alpha$.

$x^3 - 3x - 1$ 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

$$\varphi : K \to K' \quad \text{such that}$$

$$\varphi|_F = id_F \quad \text{and} \quad \varphi(\alpha) = \beta$$

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

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 iff

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

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

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

$$\text{g.c.d}(f(x), g(x)) = \text{g.c.d}(g(x), r(x))$$

$$= \cdots\cdots$$

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

Corollary: If 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 $(f(x), f'(x)) \neq 1$

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. char $F = 0$

then $K = F[\alpha]$ for some $\alpha \in K$.

(α is called primitive element)

Pf: $K = F(\alpha_1, \dots \alpha_n)$.

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 $\alpha_1 = \alpha$, $\alpha_2 \dots \alpha_n$.

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

Choose $c \in F$, such that

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

$$\text{if } (i, j) \neq (i', j')$$

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

Last class: $\operatorname{char} F = 0$.

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.

There exist $\widetilde{K}/K$ a splitting field.

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

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

$$\begin{array}{c} \mathbb{Q}(w, \sqrt[3]{2}) \\ | \\ \mathbb{Q}(w) \\ | \\ \mathbb{Q} \end{array}$$

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

$\mathbb{Q}(w) \to$ This is not.

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 $K_1 = K_2$

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

$$\begin{tikzcd} & L \arrow[d, dash] \arrow[dr, dash] & \\ K_1 \cong & \tilde{K} \arrow[d, dash] & K_2 \arrow[dl, dash] \\ & F & \end{tikzcd}$$

choose $\tilde{K} = F[\tilde{\alpha}]$ one root $\tilde{\alpha}$.

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 $G(K/F)$

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

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

$$\mathbb{Q}[\sqrt{2}] = F$$

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

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

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

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

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

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

$(\alpha_1 \ldots \alpha_n)$ 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: $K = \mathbb{Q}(\sqrt{3}+\sqrt{5}) / \mathbb{Q}$.

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

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

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

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 $\mathrm{Aut}(K)$

$$H \subset \mathrm{Aut}(K)$$

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

① H finite. $\beta \in K$. $\{\beta_1, \dots, \beta_r\}$ is the H-orbit of β.

then the irreducible polynomial of β over K^H is

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

② $[K : K^H]$ is finite.

and $[K : K^H] = |H|$.

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

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 $\mathrm{Aut}(K)$

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

Galois correspondance: K/F Galois

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

$$L \longrightarrow \mathrm{Gal}(K/L).$$

$$K^H \longleftarrow H$$

Example (will be explained in the last class)

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

$$\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{2}w) \arrow[d, dash, "3"] & \mathbb{Q}(\sqrt[3]{2}w^2) \arrow[dl, dash, "3"] & \mathbb{Q}(w) \arrow[dll, dash, "2"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

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

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

$$\begin{tikzcd}
 & \{1\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\langle \tau \rangle \arrow[dr, dash, "3"'] & \langle \sigma\tau \rangle \arrow[d, dash, "3"] & \langle \sigma^2\tau \rangle \arrow[dl, dash, "3"] & \langle \sigma \rangle \arrow[dll, dash, "2"] \\
 & S_3 & &
\end{tikzcd}$$

Recall. ① K/F splitting field.

② $|G(K/F)| = [K:F]$.

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

$$\boxed{\begin{array}{l}\text{For any field } K, \ \text{char } K = 0. \\ \mathbb{Q} \subset K, \ \text{and} \ \mathbb{Q} \subset K^H\end{array}}$$

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.

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

$$H \longmapsto K^H.$$

$$G(K/L). \longleftarrow\!\!\!\shortmid \ L$$

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

Example 1:

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

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

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

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

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

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

$$= a + b\,\sigma(i)$$

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

σ is determined by $\sigma(i)$

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

$$\sigma \longmapsto \sigma(i)$$

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 correspondance can be shown in the following diagram:

$$\begin{array}{ccc} \{id\} & & \mathbb{Q}(i) \\ \Big| \, 2 & & \Big| \, 2 \\ G = \mathbb{Z}/2\mathbb{Z} & & \mathbb{Q} \end{array}$$

Example 2:

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

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

which one?

$\sigma: \sqrt{2} \mapsto \pm\sqrt{2}$

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

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

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

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

$$G \longrightarrow \underbrace{S_2}_{\substack{\text{permutation} \\ \text{of } \{\sqrt{2}, -\sqrt{2}\}}} \times \underbrace{S_2}_{\text{permutation of } \{\sqrt{3}, -\sqrt{3}\}}.$$

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.

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

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

$$\sigma: \begin{array}{l} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3}. \end{array} \qquad \tau: \begin{array}{l} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3}. \end{array}$$

$$\sigma_L : \sqrt{2} \mapsto -\sqrt{2}$$
$$\sqrt{3} \mapsto -\sqrt{3}$$

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:

$$\begin{tikzcd}
\{id\} \arrow[r] \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash] \\
\langle \sigma \rangle \arrow[r] \arrow[d, dash, "2"] & L = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle} \arrow[d, dash] \\
G \arrow[rd] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
& \mathbb{Q}.
\end{tikzcd}$$

nothing in between on the subgroup side.

$\mathbb{Q}(\sqrt{2}) = L.$

In summary:

$$
\begin{tikzcd}[column sep=small]
 & \{id\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle \sigma \rangle \arrow[dr, dash, "2"'] & \langle \tau \rangle \arrow[d, dash, "2"] & \langle \sigma\tau \rangle \arrow[dl, dash, "2"] \\
 & G &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) &
\end{tikzcd}
$$

(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

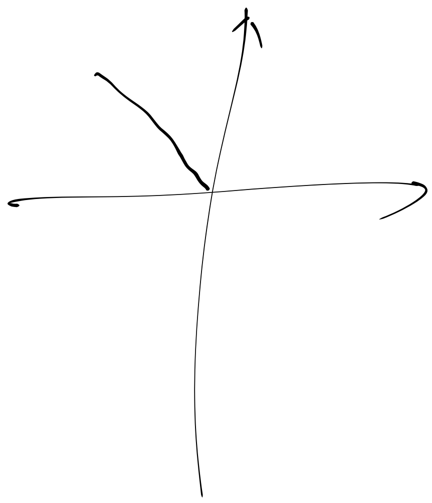
$G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$.

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

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

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

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



$$w^2+w+1=0.$$

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

$$\begin{tikzcd}
 & K & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur, dash, "\geq 2"] & & \mathbb{Q}(w) \arrow[ul, dash, "\leq 3"'] \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

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

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

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

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 $\sigma = (1\,2\,3)$ $\tau = (1\,2)$

$\sigma: \alpha_1 \mapsto \alpha_2$

$\alpha_2 \mapsto \alpha_3$

$\alpha_3 \mapsto \alpha_1$.

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

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

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

$\qquad w \longmapsto w.$

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

$$\begin{tikzcd}
\{id\} \arrow[r] \arrow[d, dash, "3"] & K \arrow[d, dash, "3"] \\
\langle \sigma \rangle \arrow[r] \arrow[dd, dash, "2"'] & K^{\langle \sigma \rangle} \arrow[d, dash] \arrow[dd, bend left, dash, "2"] \\
& \mathbb{Q}(w) \arrow[d, dash] \\
S_3 \arrow[r] & \mathbb{Q}
\end{tikzcd}$$

No subgroup

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

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

So

$$\begin{tikzcd}
 & \{id\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\langle \tau \rangle \arrow[dr, dash, "3"'] & \langle \sigma\tau \rangle \arrow[d, dash, "3"] & \langle \sigma^2\tau \rangle \arrow[dl, dash, "3"] & \langle \sigma \rangle \arrow[dll, dash, "2"] \\
 & S_3 & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, \omega) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\sqrt[3]{2}\omega) \arrow[dr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{2}\omega^2) \arrow[d, dash, "3"] & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] & \mathbb{Q}(\omega) \arrow[dll, dash, "2"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

This Galois extension because the subgroup $\langle \sigma \rangle$ is normal. and $G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong S_3 / \langle \sigma \rangle$

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

Just need to find the orbit of

$G(K/F)$ 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

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