$f(x) \in F[x]$, 要存在下面 extension K s.t. $f(x)$ 的根在里面

不妨设 f irreducible

$\Rightarrow (f)$ is maximal. $\Rightarrow F[x]/(f(x))$ is a field,

call it K.

Define a map $F[x] \to K$, $F[x] \to F[x]/p(x)$ (projection)

$\ker = (f(x))$.

Note that the restriction of constant are injective,

i.e. $\begin{matrix} K \\ | \\ F \end{matrix}$ $\Rightarrow$ K is an extension of F.

if we let $\alpha = \overline{x} = x + (f(x)) \in K$,

Then $f(\alpha) = f(x) + f(f(x)) \in (f(x)) = 0$. ,$\alpha$ 为一根.

So K/F, $\alpha \in K$, $f(\alpha) = 0$

$1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{n-1}$ is a basis of K/F,

have degree n.

In particular, $[K:F] = \deg(f) = n$.

Moreover, $K = \{g(\alpha) \mid g \in F[x], \deg(g) < n\}$ is a linear combination of the basis. $f+g = f+g$. $f \cdot g = [f \cdot g]_p$.

(需要 p irreducible).

e.g. $F = \mathbb{R}$, $p(x) = x^2+1$, $\mathbb{R}[x]/(p(x)) = \mathbb{C}$ (验证)

Same with $F = \mathbb{Q}$, $\mathbb{R}[x]/(p(x)) = \{a+bi \mid a, b \in \mathbb{Q}\}$.

e.g. if $F = \mathbb{Q}$, $p(x) = x^2 - 2$,

$F[x]/(p(x)) = \{a + b\gamma \mid a, b \in \mathbb{Q}\}$.

$\gamma = \overline{x}$, $\gamma^2 = 2$. $\Rightarrow \gamma = \sqrt{2}$.

$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

e.g. $F = F_3 = \{0, 1, 2\}$. $p(x) = x^2 + 1$.

irreducible.

So $k = F[x]/p(x)$ 为什么?

$[k : F] = \deg(p) = 2$,

So $|k| = 9$ (3^2) (a, b) 3.

Note $k \cong F_3(\sqrt{2})$

Turns out: finite fields always have cardinality $q = p^a$, $a \in \mathbb{N}$. p a prime. There is exactly 1 field for each such q.

e.g. F_2 $f(x) = x^2 + 1$ $f(1) = 0$ ✗ reducible.

$f(x) = x^2 + x + 1$ ✓ irre.

$k = F_2[x]/(f(x))$, $[k : F] = 2 \Rightarrow |k| = 4$

Notation: Suppose K/F and $\alpha, \beta, \cdots \in K$,

Then $F(\alpha, \beta, \cdots)$ is the smallest field containing F and $\alpha, \beta, \cdots$

called field generated by $\alpha, \beta, \cdots$ over F.

- If $K = F(\alpha)$, then K : simple extension

  α: primitive element

Thm: if $f \in F[x]$ irr, $\alpha \in K$. a root of f,

then let $F(\alpha) \subseteq K$ be the subfield generated by α over F,

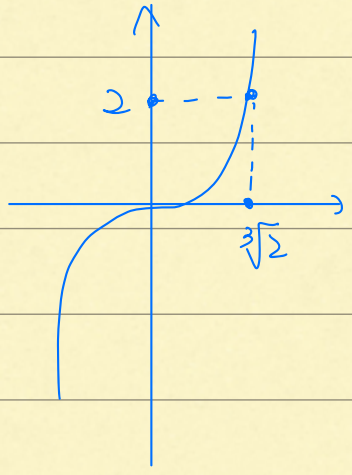
Then $F(\alpha) \cong F[x]/(f(x))$

pf: $F[x] \to F(\alpha) \in K$,

$a(x) \to a(\alpha)$

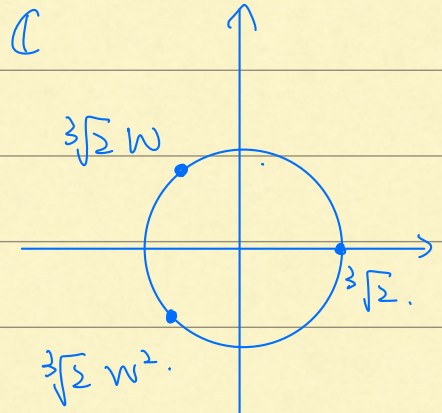
Image contains F (constants) and contains α.

e.g $F = \mathbb{Q}$, $p(x) = x^3 - 2$. (Einstein $\Rightarrow$ irr)



has only one real root

恰好有一个实根.



$\mathbb{Q}(\sqrt[3]{2})$

|

$\mathbb{Q}$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

$\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(w\sqrt[3]{2})$, $\mathbb{Q}(w^2\sqrt[3]{2})$

$\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, other's not.

These 3 fields are isomorphic, but also indistinguishable over $\mathbb{Q}$.

Thm: Suppose $\varphi: F \to F'$ is a field isomorphism,

Suppose $p(x) \in F[x]$, $p'(x) \in F'[x]$ irre,

Suppose $p(\alpha)=0$, $p'(\beta)=0$,

Suppose p' is obtained by applying φ to each each coefficient of p,

Then $F[x]/(p(x)) \cong F'[x]/(p'(x))$

$\exists$ isomorphism $\sigma: F(\alpha) = F'(\beta)$

s.t. $\sigma(\alpha)=\beta$

$\sigma|_F = \varphi$.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\sigma} & F'(\beta) \\ | & & | \\ F & \xrightarrow[\cong]{\varphi} & F' \\ p & & p' \end{array}$$

DEF: K/F, $\alpha \in K$ is "algebraic over F" if

$\exists f(x) \in F[x]$, s.t. $f(\alpha)=0$

otherwise, α is "transcendental"

K/F is algebraic if all elements are.

e.g. $\sqrt{2}$. algebric in $\mathbb{Q}$.

π, transcendental, e.

prop: 设 α is alg over F,

$\Rightarrow \exists!$ monic poly, irreducible, $m_{\alpha,F}$,

s.t. $m_{\alpha,F}(\alpha)=0$

Also $f \in F[x]$, s.t. $f(\alpha)=0 \Leftrightarrow m_{\alpha,F} \mid f$

$m_{\alpha,F}=m_\alpha$ is the minimal polynomial of α/F.

pf: 考虑 set of all f, s.t. $f(\alpha)=0$.

take the minimal degree, 除以首项系数

Euclidean algo.

prop: if α alg/F, $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$

prop: α is alg/F iff $F(\alpha)/F$ is finite.

if k/F, $[k:F]=n$, $\alpha \in k$, then $\deg_F(\alpha) \le n$

col: if k/F algebric, then it algebric.

$F(\alpha)$, basis $\{1, \alpha, \cdots, \alpha^{m-1}\}$. $m=\deg(\alpha)$

$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\} \Rightarrow \{1, i\}$ are basis of $\mathbb{C}/\mathbb{R}$.

$\Rightarrow \mathbb{C} = \mathbb{R}(i) \Rightarrow m_i(x) = x^2+1$

$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. (similarly)

Thm: If $f(x) \in F[x]$, irre, and K/F s.t. $\alpha \in K$, $f(\alpha)=0$,
then $F(\alpha) \cong F[x]/(f(x))$

"pf": $\exists$ homomorphism $F[x] \to F(\alpha)$
$g(x) \mapsto g(\alpha)$
ker contains F since $F(\alpha)=0$ So $F[x]/(f(x)) \to F(\alpha)$

f irreducible $\Rightarrow F[x]/(f(x))$ a field
So $F[x]/(f(x)) \to F(\alpha)$ isomorphism.

Cor: $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in F\}$

e.g. Quadratic extensions deg=2
Assume $\mathrm{char}(F) \neq 2$.
If $f(x) = ax^2+bx+c \in F[x]$ irre,
roots are $\frac{-b \pm \sqrt{\Delta}}{2a}$, $\sqrt{\Delta} \notin F$
(otherwise f would be reducible)

write $\alpha^+ = \frac{-b+\sqrt{\Delta}}{2a}$, $\alpha^- = \frac{-b-\sqrt{\Delta}}{2a}$

for real fields, $\sqrt{}$ means + square root.

In general, "pick one of roots", no canonical way to do it.

$\alpha^+ + \alpha^- = -\frac{b}{a}$, $\alpha^- = \alpha^+ - \frac{a}{b}$

$\Rightarrow F(\alpha^+) = F(\alpha^-) = F(\sqrt{\Delta})$

Thm: if K/F, $[K:F]=2$, $\mathrm{char}(F) \neq 2$,
then $K = F(\sqrt{D})$ with $D = k^2$, $D \in F$

e.g. $\mathbb{F}_2 = \{0,1\}$, all elements are squares.
But X^2+X+1 is irreducible, (无 root)
$\mathbb{F}_2[X]/(X^2+X+1)$ is a quadratic extension of $\mathbb{F}_2$.

Thm: Suppose $L/K/F$, Then $[L:F] = [L:K][K:F]$

pf: $\{e_i\}$, $\{f_i\}$ basis of K/F, L/K.
Then $\{e_i f_j\}$ are basis for L/F

mn (L | m $\{f_i\}$ | K | n $\{e_i\}$ | F)

$L = \{a_0 f_0 + a_1 f_1 + \cdots + a_{m-1} f^{m-1}\}$ $a_i \in K$,
pick $a_i = \{b_0 e_0 + \cdots + b_{n-1} e_{n-1}\}$ 带回

Def: K/F is "finitely generated"

if $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$, the field generated by $\alpha_1, \cdots \alpha_n$.

Lemma: $F(\alpha,\beta) = F(\alpha)(\beta) = F(\beta)(\alpha)$

By induction: $F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$

Thm: K/F is a finite extension $\Leftrightarrow$

$K = F(\alpha_1, \cdots, \alpha_n)$ for algebric elements $\alpha_1, \cdots, \alpha_n$.

pf: easy.

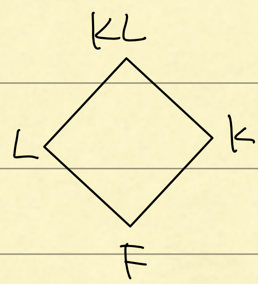
Thm: if α, β are alge $/F$, and so are

$\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$

pf: $\alpha, \beta \in F(a.b) \rightarrow$ algebric.

Suppose K/F, L/F

Def: KL is the smallest field both containing K and L.



Thm: $[KL:F] \leq [K:F][L:F]$

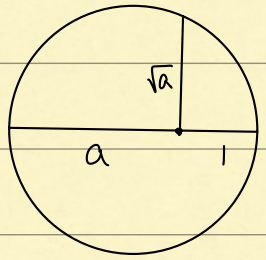
"=" iff a basis for K/F remains linearly independant over L.

↙ 尺规作出的点，(集).

Cor: Constructibles is a field.

prop: a Constructibles $\Rightarrow \sqrt{a}$ constructible.

pf:



So constructible numbers $> \mathbb{Q}$, contains things like.

$\sqrt{2+3\sqrt{5}}$

Start with $\mathbb{Q}$, the only way to generate points are:

① 交两条线

② 交两个圆

③ 交一个线与一个圆

- lines joining constructable points have constructible. coeff in their equations.
- Two circles $(x-a)^2+(x-b)^2=s^2$ ①

$(x-c)^2+(x-d)^2=r^2$ ②

① − ② is linear

$\Rightarrow$ constructible.

Thm: α is constructible $\Rightarrow$ there is a tower of fields that contains α, and each step is a quadratic extension.

If k is the top field

$\mathbb{Q}(\sqrt{a},\sqrt{b},\cdots)$

$\vdots$

$\mathbb{Q}(\sqrt{a},\sqrt{b})$

$\uparrow$

$\mathbb{Q}(\sqrt{a})$

Then $[K:\mathbb{Q}]=2^k$ (每次 ×2)

Then $[\mathbb{Q}(\alpha):\mathbb{Q}]$ divides $[K:\mathbb{Q}]$.

↳ 2^m

但 x^3-2 irre, so $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, 不 constructible.

⇒ 倍立方体 X.

三等分角: 不能三等分 60°: $\sin\theta=\sqrt{1-\cos^2\theta}$

i.e. 只需构造 $\cos\theta$ ($\cos 20°$)

$\cos(3\theta)=4\cos^3\theta-3\cos\theta$

$\Rightarrow 4\cos^2(20°)-3\cos 20°=\frac{1}{2}$

$\Rightarrow (2\cos\theta)^3-3(2\cos\theta)=1$

$\Rightarrow u^3-3u=1$

↳ 无解

只有3的倍数的角度可以尺规作出来.

If $f(x)\in F[x]$, the "splitting field" of $f(x)$ over F is the smallest extension K/F which contains all the roots of $f(x)$

We know that if $f(\alpha)=0$ and $\deg(f)=n$, then $[F(\alpha):F]\le n$.

The natural way to construct a splitting field is to add roots one at a time until you have them all.

Start with $f \in F[x]$, deg n, irre, add root α to get

$[F(\alpha):F] = n$

but $(x-\alpha) \mid f(x)$ over $F(\alpha)[x]$,

$f_1 = \frac{f(x)}{x-\alpha}$ has degree $n-1$.

if $f_2(\alpha_2) = 0$, $[F(\alpha)(\alpha_2):F] \le n(n-1)$ ← if f_2 irreducible.

↳ $[F(\alpha)(\alpha_2)(\alpha_3)\cdots(\alpha_n):F] \le n!$

e.g. Suppose $D \in F$, non-square,

Then $[F(\sqrt{D}):F] = 2$.

And $F(\sqrt{D})$ is the splitting field of $x^2 - D = (x-\sqrt{D})(x+\sqrt{D})$

e.g. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$

there is one real root α.

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

但 1, w, w^2, $\Rightarrow$ $\begin{cases} w^2\alpha, \\ w\alpha \end{cases}$ 也是 roots.

要把 $w = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ 加进 $\mathbb{Q}(\alpha)$ 中

So $K = (\alpha, w) = (\sqrt[3]{2}, \sqrt{-3})$

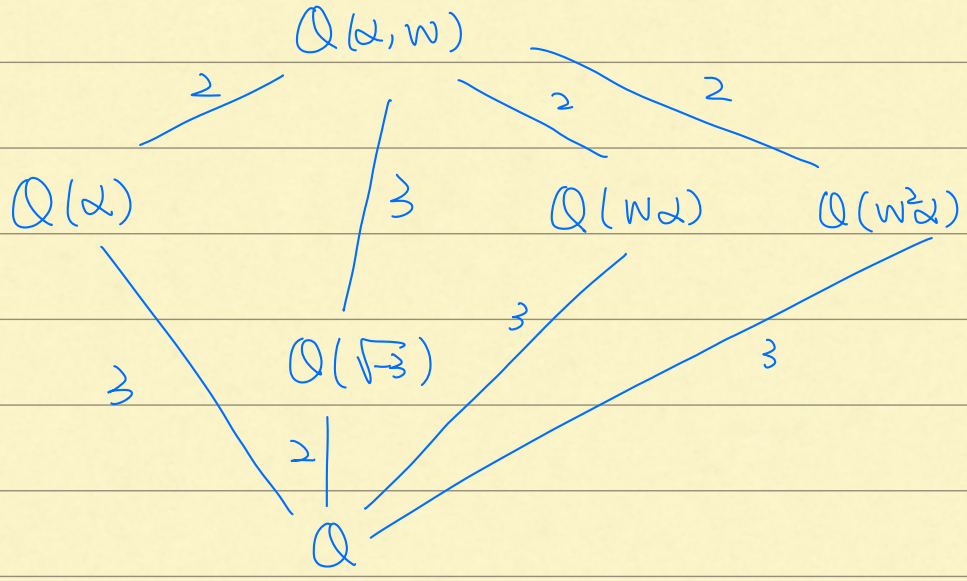
$K = \mathbb{Q}(\alpha, \sqrt{-3})$

$2 \mid$

$\mathbb{Q}(\alpha)$

$3 \mid$

$\mathbb{Q}$



Terminology: Can also talk about the splitting field of a family of polynomials.
The splitting field of f, g, h is the same as the splitting field of fgh.

A splitting field over F is sometimes called normal extension.

Thm: if K, K' are splitting fields of family of polynomials $\{f_i\}, \{f_i'\}$ in $F[x], F'[x]$, respectively, and $\varphi: F \to F'$ is an isomorphism which takes each f_i to corresponding f_i', then φ extends to an isomorphism $K \to K'$

So we can talk about "the" splitting field.

pf: use previous result about a single root.

n-th roots of unity: roots of $f(x)=x^n-1$.

$x-1 \mid f(x)=x^n-1$

$\frac{f(x)}{x-1}=x^{n-1}+x^{n-2}+\cdots+x+1$

若 $n=p$, 则 $\frac{f(x+1)}{x}$ 用 Eisenstein 可得 irre

若 p 为 p 次单位根.

则 $[\mathbb{Q}(p):\mathbb{Q}]=p-1$

因为 p 次单位根为 cyclic group,

The splitting field of x^n-1 over $\mathbb{Q}$ is called the cyclotomic field of n-th roots of unity over $\mathbb{Q}$.

degree: $\varphi(n)$.

Def: $\bar{F}$ is an algebraic closure of F if $\bar{F}/F$ is algebric and $F[x]$ 在 $\bar{F}$ 中有全为一根.

Def: K is algebraic closed $\Leftrightarrow$ $K[x]$ 在 K 中有根.

Prop: if $\bar{F}/F$ is an algebraic closure, then $\bar{F}$ is algebraic closed

pf: 设 $f(x)=\bar{F}[x]$, α 为一根, 在 splitting field 里.

So $\bar{F}(\alpha)/\bar{F}$ is algebric, so $\bar{F}(\alpha)/F$ is algebric.

(因为满了 $\bar{F}/F$ alg)

But that implies $\alpha\in\bar{F}$.

e.g. $\mathbb{C}$ is alg. closed.

Thm: Every field is contained in an algebric closure.

pf: Given a field F. to each $f \in F[x]$, associate another variable x_f.

Consider $F[\cdots x_f \cdots]$ (polynomials in all x_f's).

Let I be the ideal generated by all the $f(x_f)$

If I is not a proper ideal (整个), then $1 \in I$,

so $1 = f_1(x_{f_1}) \cdot g_1(\cdots) + f_2(x_{f_2}) \cdot g_2(\cdots) + \cdots$ (*)

(有限和) $\quad + f_k(x_{f_k}) g_k(\cdots)$

Construct K/F, s.t. K contains a root α_i of f_i $(i = 1, \cdots, k)$

Substitute $x_{f_i} = \alpha_i$ in (*) (因为 $f_i(\alpha_i) = 0$?)

则矛盾, I is a proper ideal, ☆

Axiom of choice: $\exists$ maximal ideal M s.t.

$$I \subseteq M \subsetneq F[\cdots x_f \cdots]$$

$K_1 = F[\cdots]/M$ is a field

in $f(\bar{x}_f) = 0$, $\forall f \in F[\cdots]$.

下证 alg. close.

Construct K_2/K_1, s.t. K_1 中有 poly 就在 K_1 中有解.

继续这个过程, K_2/K_1, K_3/K_2, $\cdots$, K_n/K_{n-1}

令 $K = \bigcup K_n$.

Claim: K is algebric closed.

If $f \in K[x]$, 则存在 k, s.t. $f \in K_k[x]$, then

f has a root in $K_{k+1}[x]$.

The fundamental thm of Algebra:
$\mathbb{C}$ is algebrically closed.

Notice: the algebric closure of $\mathbb{Q}$ 还小于 $\mathbb{C}$ (可数)

Separability:
Def: if $(X-a)^m \| f(x)$, then m is the multiplicity of the root a (in f).

A root is simple if it's multiplicity is 1.
------ multiple root ------ 反面.

A polynomial is separable if all roots are simple.
Inseparable otherwise.
We can define the derivative of f just the usual way. Call it Df. $D(X^n) = nX^{n-1}$ etc.
D satisfies product rule. etc.

Prop: $f \in F[X]$ has a multiple root α iff
$f(\alpha) = Df(\alpha) = 0$.

Prop: f is separable if f, Df 互质. (easy)

In the ring of rational functions,

$\mathbb{F}_2(t)$, let $f(x) = x^2 - t$ (t is a constant)

$Df = 2x = 0$, so $\sqrt{t}$ is a double root.

$f(\sqrt{t}) = 0 = Df(\sqrt{t})$

Prop: if $\mathrm{char}(F) = 0$, then $f \in F[x]$ is separable iff it's a product of distinct irres,

Suppose $\mathrm{char}(F) = p$

for $a, b \in F$, $(a+b)^p = a^p + b^p$ (中间项为 p 的倍数)

$(ab)^p = a^p b^p$

$\Rightarrow x \to x^p$ is a homomorphism $F \to F$.

it's injective, $0 = (a-b)^p \Leftrightarrow a^p = b^p$,

So isomorphism

If F is finite, it's an isomorphism. (Frobenius antomorphism)

Consequence: in a finite field of char p, every field is a p^{th} power.

$\mathrm{char}(F) = p$, $f \in F[x]$, if $Df \equiv 0$, then all powers of f of x must be multiples of p.

$f(x) = a_{pk} x^{pk} + a_{p(k-1)} x^{p(k-1)} + \cdots + a_p x^p + a_0$.

↪ poly of x^p.

(任意系数) $a_{pk} \in F$ 都是什么的 pth power.

所以每一项都是 pth power, 而 pth power 是

在 +, × 下不变的，所以

$f(x) = g(x^p)$, for some $g \in F[x]$.

If F is finite, char $= p$,

p is irre, inseparable.

then $p(x) = g(x^p)$ for some g.

and $p(x) = g(x^p) = (g_1(x))^p$

Prop: 在有限域上, every irre polys are separable.

A general poly over a finite field is separable iff it's product of distinct irres.

Terminology: a field k is perfect if $\text{char}(k) = 0$ or $\text{char}(k) = p$ and $k^p = k$.

(holds for every finite field).

Finite fields: Over F_p, consider the poly

$f(x) = x^{p^n} - x$, $Df = -1$. ← never 0, 无重根.

So f has p^n roots in it's splitting field.

If α, β are roots of f, then $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

$\Rightarrow \alpha\beta$ 也为一根. $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \Rightarrow (\alpha+\beta)$ 也为一根.

$f(0) = f(1) = 0$.

if α is a root, then $\alpha^{p^n-1}=\alpha^{-1} \Rightarrow \alpha^{-1}$ is root.

So the roots forms a field, $\mathbb{F}_{p^n}$.

$|\mathbb{F}_{p^n}| = p^n$.

Another field of the same order also consists of roots of f, so equals a splitting field of f.

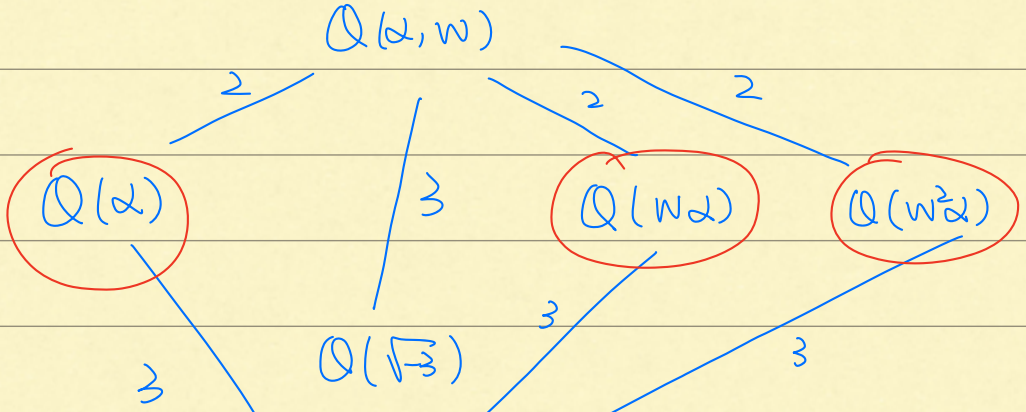
这 splitting fields 不同 $\Rightarrow$ 两 field 不同 (order p^n)

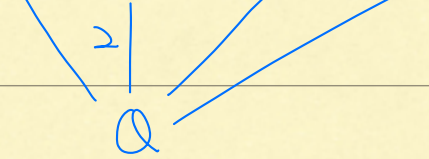
Over a field of char p, if $g(x)=g_{sep}(x^{p^k})$, and k is the possible largest.

Then $\deg(g_{sep})$ is the separable deg of g and p^k is the inseparable degree.

Def: A field K/F is separable (separable alg.) if all $\alpha \in K$ is a root of a separable poly over F; inseparable otherwise.

Cor: Every extension of a perfect field is separable.





这些 field 在 Q 的视角下是完全一样的，所以他们之间会有 isomorphism.

Cyclotomic poly: $\Phi_n(x) = \prod (x-\zeta)$ (ζ primitive nth)

deg $= \varphi(n)$

Facts: $\Phi_n(x)$ is monic, irre in $\mathbb{Z}[x]$.

Galois theory:

we write $Aut(k)$ for the group of automorphism of a field.

e.g. Any field has trivial automorphism.

Complex conjugation. ($a+bi \to a-bi$) in $Aut(\mathbb{C})$

if $char(k)=p$, then $x \to x^p \in Aut(k)$.

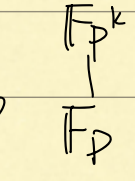
also $x \to x^{(p^k)}$

In $\mathbb{F}_p$, $x^p - x$ has p roots. 所有满都是根.

So $x \to x^p = x$ is the identity.

But it's not the identity on a bigger field

→ 只有 p 个满满足 $x^p = x$



So $x \to x^p$ is an automorphism of $\mathbb{F}_{p^k}$, and the element it fixes are exactly the subfield 子域 $a+bi \to a-bi$, $\mathbb{R}$ ←

Easy to prove: if $S \subseteq Aut(K)$, K field, then $\{x \in K \mid \sigma x = x, \forall \sigma \in S\}$ is a field. (sub)

Prop: if $H \leq Aut(K)$, then the fixed field is a field contains the prime field.

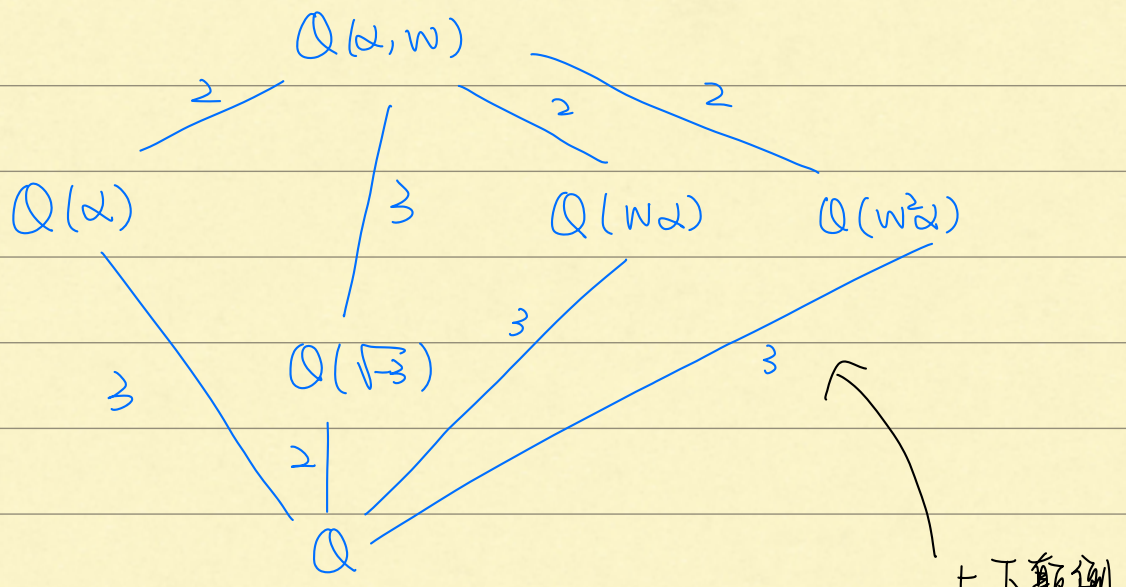
Cor: $Aut($ $\{Id\} = Aut\{\mathbb{F}_p\}$

e.g. $x \to x^{(p^n)}$ on $\mathbb{F}_{p^m}$, the fixed field is $\mathbb{F}_{p^n}$, provided $n \leq m$.

Def: $Aut(K/F)$ = element of $Aut(K)$ that fix F.
$= \{\sigma \in Aut(K) \mid \sigma x = x, \forall x \in F\}$.

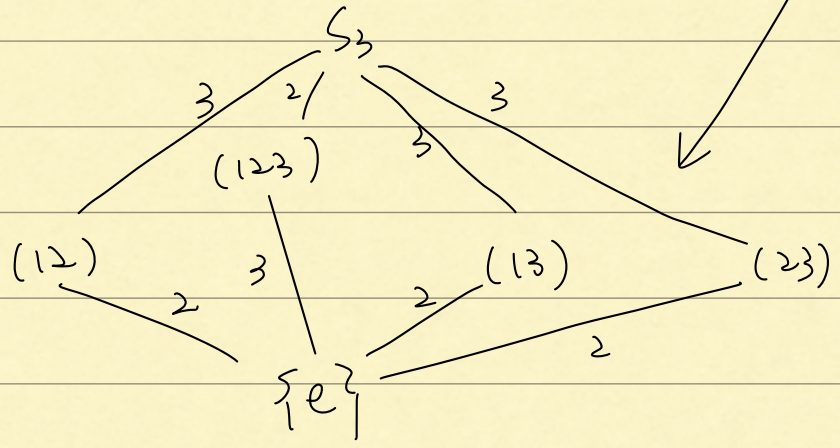
L
|
K if $F \subseteq K \subseteq L$.
|
F $Aut(L/K) \leq Aut(L/F)$
"Inclusion reversing"

Splitting field of $x^3 - 2$ over $\mathbb{Q}$.



上下颠倒

Turns out: $\mathrm{Aut}(\mathbb{Q}(w, \sqrt[3]{2})/\mathbb{Q}) = S_3$



Thm: E/F where E is the splitting field of $f(x) \in F[x]$. Given an isomorphism $\varphi: F \to F'$ then construct $f' \in F'[x]$ by applying φ to coeff, Then construct splitting field E'/F' of f', then φ extends to an isomorphism $E \to E'$.

$$\begin{array}{ccc} E & \dashrightarrow & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

The number of distinct extension is $\leq [E:F]$.

"=" if E/F is separable.

e.g. $E = E' = \mathbb{C}$, $F = F' = \mathbb{R}$.

then $\mathbb{C} \xrightarrow[\text{conjugation.}]{\text{id}} \mathbb{C}$

Sketch of pf: induction. obvious if deg = 1,

$$\begin{array}{ccc} E & & E \\ | & & | \\ F(\alpha) & \to & F'(\alpha') \\ | & & | \\ F & \to & F' \\ f & \to & f' \end{array} \qquad f(\alpha)=f'(\alpha')=0.$$

归纳

Corollary: if E/F is the splitting field of $f(x)$, then $|\mathrm{Aut}(E/F)| \le [E:F]$, "=" if f separable.

Def: A finite extension K/F is a Galois extension (K is Galois over F), if $|\mathrm{Aut}(K/F)| = [K:F]$. In this case, $\mathrm{Aut}(K/F)$ is the "Galois group of K/F" i.e. $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F) = \mathrm{Gal}(f(x))$

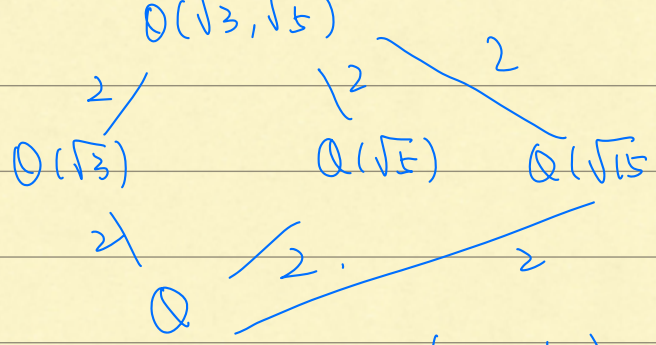
e.g. If char $\neq 2$, $D \in F$ 非平方.

则 $F(\sqrt{D})/F$ is galois of degree 2,

$\mathrm{Gal}(F(\sqrt{D})/F) = \{id, \sigma\}$, $\sigma^2 = id$.

$\sigma(a+b\sqrt{D}) = a-b\sqrt{D}$.

e.g. $k = \mathbb{Q}(\sqrt{3})$, $L = k(\sqrt{5})$.



$L/\mathbb{Q}$, $[L:\mathbb{Q}]=4$.

basis of L:

$1, \sqrt{3}, \sqrt{5}, \sqrt{15}$.

Automorphism: $\sigma: \begin{pmatrix} 1\to 1 \\ \sqrt{3}\to -\sqrt{3} \\ \sqrt{5}\to\sqrt{5} \end{pmatrix}$

$\hookrightarrow \Rightarrow \sqrt{15}\to -\sqrt{15}$

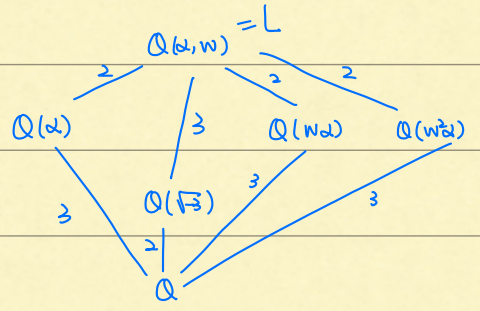
$\tau: \begin{pmatrix} 1\to 1 \\ \sqrt{5}\to -\sqrt{5} \\ \sqrt{3}\to\sqrt{3} \end{pmatrix}$ $\quad \hookrightarrow \Rightarrow \sqrt{15}=-\sqrt{15}$

$\sigma\tau: \begin{pmatrix} 1\to 1 \\ \sqrt{3}\to -\sqrt{3} \\ \sqrt{5}\to -\sqrt{5} \end{pmatrix}$

So $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_2\times\mathbb{Z}_2 =$ Klein-4

σ fixes $\mathbb{Q}(\sqrt{3})$, τ fix $\mathbb{Q}(\sqrt{5})$, $\sigma\tau$ fix $\mathbb{Q}(\sqrt{15})$

e.g. Splitting field of x^3-2.



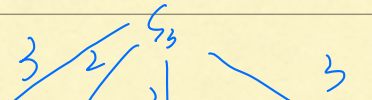
$\mathrm{Gal}(L/\mathbb{Q}) \cong S_3 = \langle\sigma,\tau\rangle$.

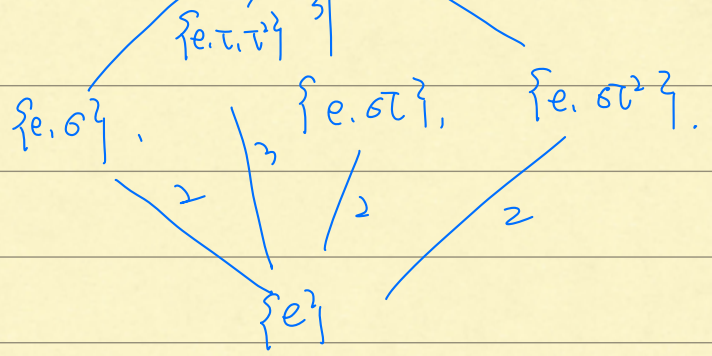
$\sigma^2=\mathrm{id}$, $\tau^3=\mathrm{id}$

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

Guess: $\sigma: \sqrt{-3}\to -\sqrt{-3}$.

τ: "rotates" the cubic subfield, fix $\sqrt{-3}$.





So $\langle e, \tau, \tau^2 \rangle$ fixes $\mathbb{Q}(\sqrt{-3})$.

$\langle e, \sigma \rangle$ fixes $\mathbb{Q}(\sqrt[3]{2})$

$\langle e, \sigma\tau \rangle$ fixes $\mathbb{Q}(\omega^2\sqrt[3]{2})$

$\langle e, \sigma\tau^2 \rangle$ fixes $\mathbb{Q}(\omega\sqrt[3]{2})$

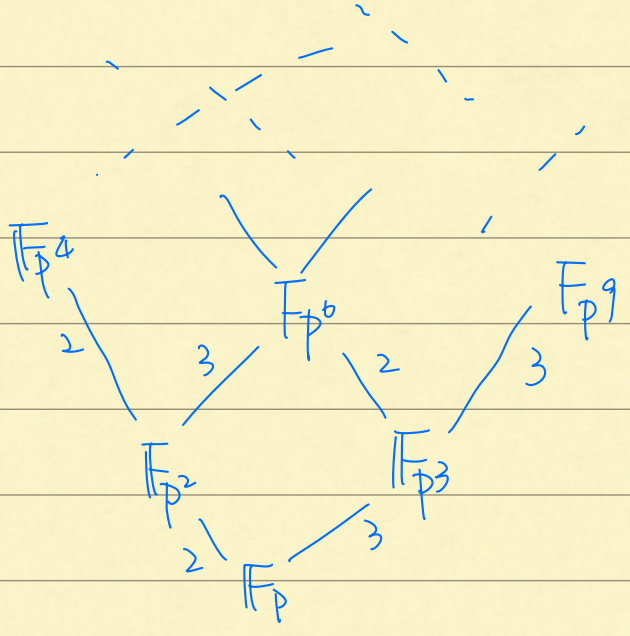
e.g. Finite field $\mathbb{F}_{p^m}/\mathbb{F}_p$ $x \mapsto x^p$ (Frob.) fixes $\mathbb{F}_p$.

i.e. $\mathbb{F}_p$ elements are $x^p - x = 0$.

Frob fixes $\mathbb{F}_p$ and nothing else.

Also, $x \longmapsto x^{p^m} = \text{Frob}^m$ fixes $\mathbb{F}_{p^m}$

So $\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ is cyclic, generated by Frob, order m.



Def: If G is a group and L is a field, then a homomorphism $G \to L^\times$ is a character of G (into L)

Thinking of characters as functions on G with values in L. we can ask if a set of characters is linearly independent.

prop: if G is finite, any set of distinct characters $\chi_1, \chi_2, \cdots \chi_n : G \to L^\times$ is linear. independant.

pf: Suppose not, WLOG, pick a linear combination with the smallest num of non-0 coeff,

$a_1\chi_1 + \cdots + a_m\chi_m = 0$ ($a_i \neq 0$ for all i)

As a function of G,

$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0, \ \forall g \in G.$ *

χ_1, χ_m are dfrt, $\exists g_0 \in G$, s.t. $\chi_1(g_0) \neq \chi_m(g_0)$

So $a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$. * 同为是 character. ($\chi_m(g_0)\chi_m(g)$)

Multiply * by $\chi_m(g_0)$ and subtracts *

$\chi_m(g_0)a_1\chi_1(g) + \cdots + \chi_m(g_0)a_i\chi_i(g) + \cdots + \chi_m(g_0)a_m\chi_m(g)$

$- a_1\chi_1(g_0)\chi_1(g) - \cdots - a_i\chi_i(g_0)\chi_i(g) - \cdots - a_m\chi_m(g_0)\chi_m(g)$

$= a_1(\chi_m(g_0) - \chi_1(g_0))\chi_1(g) + \cdots + a_{m-1}(\chi_m(g_0) - \chi_{m-1}(g_0))\chi_{m-1}(g)$

$a_1(\chi_m(g_0) - \chi_1(g_0)) \neq 0$

等降 ("最少项")

Cor: Distinct embeddings of K into L are linearly indp over K.

Cor: Distinct Auto of K are linearly independant over K.

Thm: If G is a finite subgroup of $Aut(K)$, and
F = Fixed field of G,
then $[K:F] = |G|$
↖ linear independent.

Cor: K/F Then $Aut(K/F) \leq [K:F]$, with equity iff F is fixed field of $Aut(K/F)$
ie. K/F is galois.

Cor: G, G' distinct subgroups of $Aut(K)$,
then their fixed field are distinct.

Thm: K/F is Galois iff K is the splitting field of a separable polynomial $f(x) \in F[x]$
(in which case, every irred poly $g \in F[x]$, 有 K 中有一根 ⇒ 在 K 中有所有根).

Def: if K/F is Galois, $\alpha \in K$, then elements
$\sigma_1\alpha, \sigma_2\alpha, \cdots$ ($\sigma_i \in Gal(K/F)$) are called the conjugate of α.

Fundamental Thm of Galois Thm:
Suppose K/F is Galois, $G = Gal(K/F)$, Then there is a bijection between the subgroups of G and the intermediate field between F and K.

given by

$G \geq H \to$ fixed field of H.

$\{\sigma \in G \mid \sigma|_E = id_E\} \longleftarrow$ K / E / F — — — G / H / {e}

There are inverses.

Moreover,

1. Inclusion reversing $E_1 \subseteq E_2 \Leftrightarrow H_2 \subseteq H_1$

   (E_i = fixed field of H_i)

2. $[K:E] = H$,

   $[G:H] = [E:F]$

3. K/E is Galois, and $Gal(K/E) = H$

4. E/F is Galois $\Leftrightarrow H \lhd G$. In this case, $Gal(E/F) = G/H$

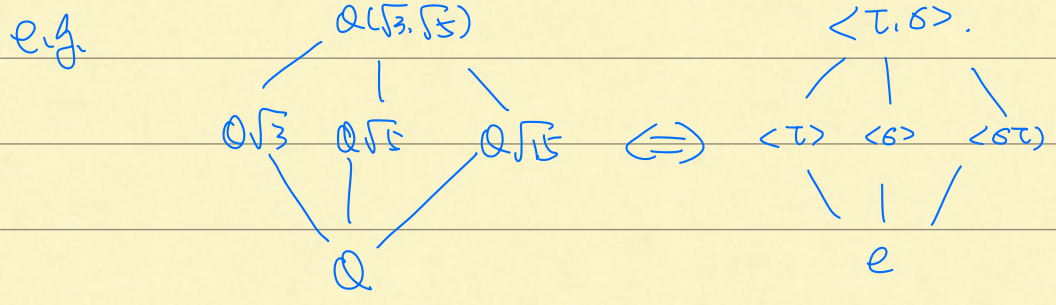
5. If $E_i \Leftrightarrow H_i$, then $E_i \cap E_j \Leftrightarrow \langle H_i, H_j \rangle$

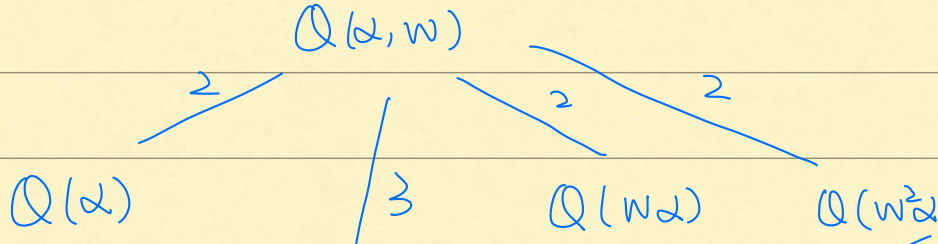
   $E_1 E_2 \Leftrightarrow H_1 \cap H_2$

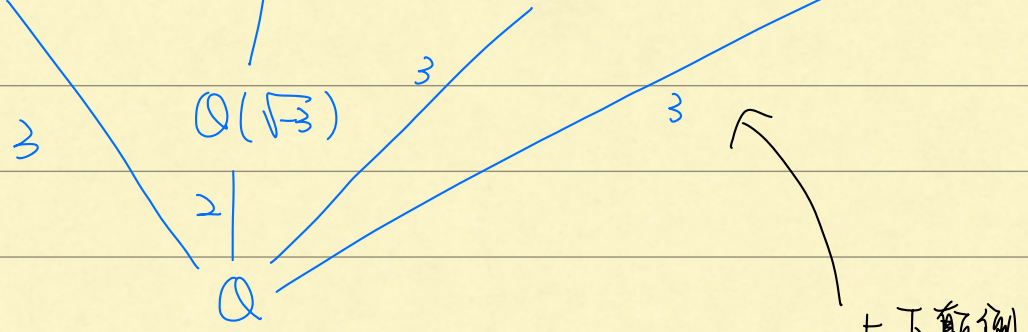
The lattice are "dual"

$E_1 E_2$: composite.

e.g.

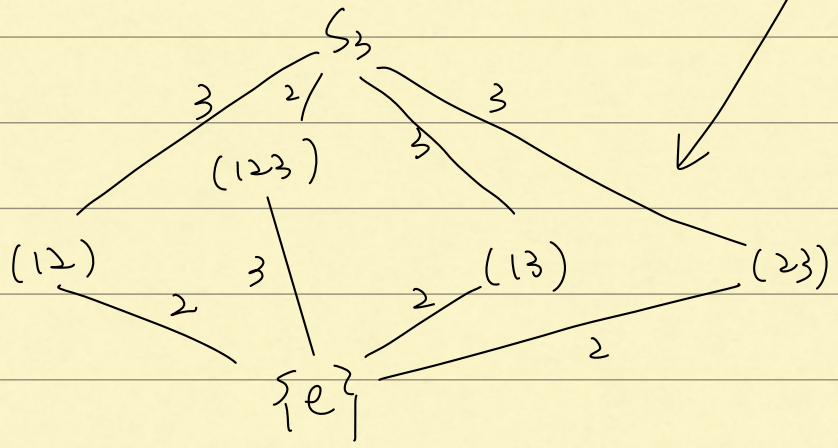






上下颠倒

Turns out: $\mathrm{Aut}(\mathbb{Q}(w, \sqrt[3]{2})/\mathbb{Q}) = S_3$



Def: An extension E/F is abelian if it's Galoi and $\mathrm{Gal}(E/F)$ is abelian.

e.g. cyclotomic extensions.

Kronecker-Weber Thm: Any abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension

Suppose F is a field and consider $F(x_1, \cdots, x_n)$, the field of rational functions in n variables.
S_n acts on $F(x_1, \cdots, x_n)$ by permuting the variables.

Def: The symmetric functions (对称函数): 在 S_n 变换下保持不变.

Def: The "elementary symmetric functions" are:

$S_1 = X_1 + \cdots + X_n$.

$S_2 = \sum_{1 \le i < j \le n} X_i X_j$

$\vdots$

S_k = k 个不同变量的所有乘积和.

$\vdots$

$S_n = S_1 S_2 \cdots S_n$

e.g. $X_1^2 + X_2^2 + \cdots + X_n^2 = S_1^2 - 2S_2$.

Consider $F(X_1, \cdots, X_n)$

Let $f(x) \in F(X_1, \cdots, X_n)[X]$ be

$f(x) = (x - X_1)(x - X_2) \cdots (x - X_n)$ X_i's are roots.

f is the "general polynomial"

$F(X_1, \cdots, X_n)$ has an action of S_n.

$\le n!$ $\quad | n!$ = index of S_n.

Symmetric functions = fixed field of S_n.

$F(S_1, \cdots, S_n)$

Observe: coefficients of f are $S_1, \cdots, S_n$.

So $f(x) \in F(S_1, \cdots, S_n)[X]$.

It's root are $X_1, \cdots, X_n$, so $F(X_1, \cdots, X_n)$ is its splitting field.

But $[F(X_1, \cdots, X_n) : F(S_1, \cdots, S_n)] \le n!$

So $[F(x_1,\cdots,x_n) : F(s_1,\cdots,s_n)] = n!$

$F(s_1,\cdots,s_n)$ = symmetric functions.

e.g. given a polynomial $f(x) \in F(x)$,
with roots $\alpha_1,\cdots,\alpha_n$.
the discriminant is $D = \prod_{i\neq j}(\alpha_i - \alpha_j)$
D can always be expressed in terms
of the coefficient of f.

Thm: Suppose F contains nth root of unity,
$(n, \mathrm{char}(p)) = 1$
Then $F(\sqrt[n]{a})/F$ is cyclic (Gal is cyclic).
Solving a polynomial:
$\alpha \in E$, E/F is expressible as terms of
radicals (surds) if there is a tower
where each E_{i+1}/E_i is obtained by adding
a kth root for some k.

$E = E_m$
$|$
E_{m-1}
$\vdots$
$|$
E_1
$|$
F

poly 有解 $\Leftrightarrow$ 有形如 $\sqrt[3]{\frac{1+\sqrt[10]{2}}{(\sqrt{5}+\sqrt{7})\sqrt[6]{6}}}$ 的根.
Note that each E_{i+1}/E_i is cyclic,
So every Galois groups, $\mathrm{Gal}(E/E_i)/\mathrm{Gal}(E/E_{i+1})$
So f is solvable by radicals iff it's
Galois group is solvable.
But S_5 is not solvable, therefore A_5.