Thm: If P is constructible then there exist a tower of fields

$$\begin{array}{l} K = F_n \\ \vdots \\ F_2 \\ \cup \\ F_1 \\ \cup \\ \mathbb{Q} = F_0 \end{array}$$

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 $g(x) = f(x)$

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

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

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