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 $m \mid [\tilde{K}:F]$
$n \mid [\tilde{K}:F]$

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

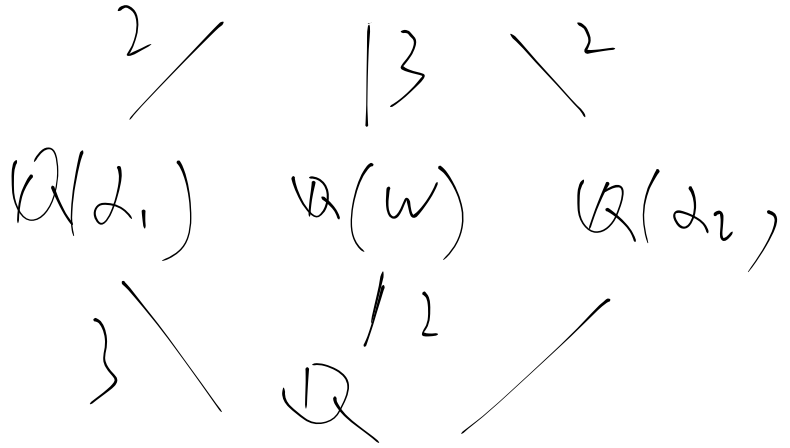
$K_2 = K_2[\alpha_1 \cdots \alpha_m)$.

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

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

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

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



If $[K : F] = 2$, $\mathrm{char} F \neq 0$. 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 $K = F_n$:

$$\begin{array}{c} \vdots \\ \cup \\ F_2 \\ \cup \\ F_1 \\ \cup \\ \mathbb{Q} = F_0 \end{array}$$

such that $[F_i, F_{i-1}] = 2$ and all the coordinates of P is inside K.

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

Trisection is not possible.

$\alpha = 60°$, $\Rightarrow$ $\alpha^3 = 1/2$.

$x^3 - 3x - 1$ is irreducible.

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