Let K/F be Galois. let $\alpha \in K$.

Let $G = Gal(K/F)$, consider $G \cdot \alpha = \{\text{Conjugates of } \alpha\}$,

$\# G \cdot \alpha = \deg_F \alpha$.

Also, $\#(G \cdot \alpha) = |G|/|H|$ where $H = Gal(K/F(\alpha))$

$= |G : H|$

$\deg_F \alpha = [F(\alpha) : F] = |G : H|$.

In particular, α generates K, $K = F(\alpha)$ iff $H = 1$,

iff $\#\{\text{conjugates of } \alpha\} = [K : F] = |G|$,

iff $\varphi(\alpha) \neq \psi(\alpha)$ for all $\varphi \neq \psi \in G$.

<u>Norm</u> Let L/F be separable. Let K/L s.t. K/F is Galois. let $\alpha \in L$.

The norm $N_{L/F}(\alpha) = \prod\limits_{\underbrace{\varphi \in G/H}_{\text{set of left cosets}}} \varphi(\alpha)$ where $H = Gal(K/L)$, $G = Gal(K/F)$

$$\left(\text{If } L = K, \quad N_{L/F}(\alpha) = \prod_{\varphi \in G} \varphi(\alpha) \right).$$

Conjugates of α are in 1-1 correspondence with

$$\left\{ \varphi(\alpha), \ \varphi \in G / \mathrm{Gal}(K/F(\alpha)) \right\}.$$

So each conjugate appears in the product

$$|G/H| \Big/ |G/\mathrm{Gal}(K/F(\alpha))| \quad \text{times}$$

$$= |\mathrm{Gal}(K/F(\alpha))| / |H|$$

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

$\prod$ conjugates of $\alpha = \pm a_0$ where $m_{F,\alpha} = x^n + \cdots + a_1 x + a_0$.

$$= \prod_{i=1}^{n} (x - \alpha_i)$$

conjugates of α.

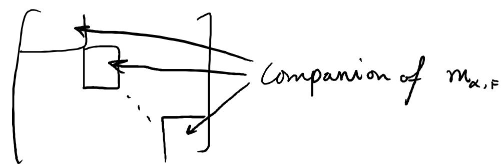
So the norm $N_{L/F}(\alpha) = \left((-1)^n a_0 \right)^{[L:F(\alpha)]}$.

If $L = F(\alpha)$, then $N_{L/F}(\alpha) = \prod \text{conj. of } \alpha = (-1)^n \alpha_0$

<u>Properties</u>: ① $N_{L/F}(\alpha)$ doesn't depend on K.

② $N = N_{L/F}$ is multiplicative: $N(\alpha\beta) = N(\alpha)\,N(\beta) \quad \forall \alpha, \beta \in L$

③ $N_{L/F}(\alpha) = \det T$ where $T(\beta) = \alpha\beta$, $T : L \to L$.

$T =$ 

$[L : F(\alpha)]$ blocks

<u>Recall</u>: $R = \mathbb{Q}(\sqrt{D})$, $\quad N(a+b\sqrt{D}) = a^2 - b^2 D$

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

$R = \mathbb{Q}(i)$, $\quad N(a+bi) = a^2 + b^2$

$$\mathrm{Tr}_{L/F}(\alpha) = \sum_{\varphi \in G/H} \varphi(\alpha) = -[L : F(\alpha)] \cdot a_{n-1} .$$

$\mathbb{Q}(\sqrt[8]{3}) \not\ni \sqrt{2}$?

Theorem Let F be a real field (i.e. $F \subseteq \mathbb{R}$).
Let $n \in \mathbb{N}$, $a \in F$ s.t. $x^n - a$ is irreducible.
Then the only subfields of $F(\sqrt[n]{a}) = L$ are
$F(\sqrt[d]{a})$ where $d \mid n$.

So the only subfields of $\mathbb{Q}(\sqrt[8]{3})$ are $\mathbb{Q}(\sqrt[4]{3})$, $\mathbb{Q}(\sqrt[2]{3})$, and $\mathbb{Q}$.

If $\sqrt{2} \in \mathbb{Q}(\sqrt[8]{3})$, then $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$, which is not true.

Lemma: Any separable finite extension is simple, $K = F(\alpha)$
(unnecessary, as it turns out)

Proof of Theorem: Let $F \subseteq K \subseteq L$. Let $\alpha = \sqrt[n]{a}$, $L = F(\alpha)$

Let $[K:F] = d$
so $[L:K] = n/d$

Let $\beta = N_{K/L}(\alpha) = \prod$ conjugates of α over K

Let $\omega = e^{2\pi i/n}$. all conjugates of α over $\mathbb{Q}$ are of the form $\omega^m \alpha$ for some m.

So $\beta = \omega^\ell \alpha^{n/d}$, but $\beta \in \mathbb{R}$, so $\omega^\ell = \pm 1$.

$\beta \in K$. So $\alpha^{n/d} \in K$. So $\deg_K \alpha \le \frac{n}{d}$.

$\deg_F \alpha^{n/d} = d$, it is a root of $x^d - a$.

So $K = F(\alpha^{n/d})$, and $\alpha^{n/d} = \sqrt[d]{a}$. $\square$

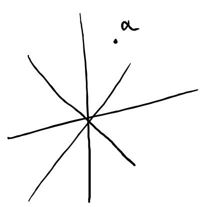
Theorem on the primitive element (The lemma from above)

Any finite separable extension is simple:

L/F fin. sep. $\Longrightarrow$ $L = F(\alpha)$ for some $\alpha \in L$.

Proof If F is finite, L is a finite field, so $L = \mathbb{F}_p(\alpha)$ for some α.

So suppose F is infinite. Let K = Galois Closure of L/F.



L : F-vector space

Then $Gal(K/F)$ is finite, So it has only finitely many subgroups. So K/F has finitely many subextensions. So L/F does too, call them $L_1, \dots, L_m$.

L has infinitely many subspaces, and any $\alpha \notin \bigcup_{i=1}^{m} L_i$ generates L. $\square$

Non-separable extension:

$$L = \mathbb{F}_p(x,y), \quad F = \mathbb{F}_p(x^p, y^p).$$

Then Claim: L/F isn't generated by 1 element.

pf $[L:F] = p^2$, but $\forall \alpha \in L$, $[F(\alpha):F] \leq p$,

since $\alpha^p \in F$ since $\left(\sum a_{ij} x^i y^j\right)^p = \sum a_{ij} x^{ip} y^{jp}$.

So $\quad Gal \leq S_n$ $\quad$ where $n = |Gal|$

permutations of
conjugates
of α