If L/K is a field extension
$\alpha_1, \dots, \alpha_n \in L$
$K(\alpha_1, \dots, \alpha_n) \leftarrow$ smallest subfield of L containing $K, \alpha_1, \dots, \alpha_n$.

Note: $K(\alpha_1, \alpha_2, \dots, \alpha_n) = K(\alpha_1)(\alpha_2, \dots, \alpha_n)$
$= \big((K(\alpha_1))(\alpha_2)\big)(\alpha_3 \dots \alpha_n)$.

$\vdots$

I a set $\alpha_i \in L$ $i \in I$.
Then $K(\alpha_i \mid i \in I)$.

If $L = K(\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n \in L$.
then L is <u>finitely generated</u> over K.

If $[L:K] < \infty$ L is a <u>finite extension</u> of K.

<u>Example</u> $K(x)/K$ is not finite
but it is finitely generated
field of rational functions in the variable x over K.

L/K is <u>algebraic</u> if every $\alpha \in L$ is algebraic over K.
(transcendental otherwise).

Theorem L/K is finite ($[L:K] < \infty$)

if and only if L/K is finitely generated and algebraic.

Main lemma: If L/K is finite, then L/K is algebraic.

Other main lemma: If $M/L/K$ then $[M:K] = [M:L][L:K]$.

Proof Let $\alpha \in L$ $\quad d = [L:K]$.

$$\underbrace{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^d}_{d+1 \text{ vectors in } d\text{-dim'l space.}}$$

There is a non trivial linear dependence.

$$a_0 \cdot 1 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_d \alpha^d = 0$$

$a_i \in K$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

This a non-zero polynomial w/ coeff in K

$f(\alpha) = 0$ So α is algebraic.

Theorem: If K is a field and f is a non-constant polynomial over K

Then $\exists$ an extension L/K s.t.
f has a root in L.

<u>Proof</u>: $K[x]$ is a PID
Take an irreducible factor
$g(x)$ of $f(x)$.

$$L = K[y]/g(y) \quad \text{is a field}$$

<u>Claim</u> $\bar{y}$ for the image of y
in L, then
$\bar{y}$ is a root of $f(x) \in L[x]$

Need to check

$$f(\bar{y}) = 0 \quad \text{in } L$$

$$f(x) = g(x)\,h(x).$$

$$f(\bar{y}) = g(\bar{y})\,h(\bar{y}).$$

suffice to show this is zero.

$$g(\bar{y}) \in L = K[y]/g(y).$$

$$\overline{g(y)} \overset{\text{dfn}}{=} g(y) \text{ mod } g(y)$$

$$= 0.$$

<u>Uniqueness statement</u>: If L_1/K, L_2/K, $\alpha \in L_1$, $\beta \in L_2$ are both roots of an irreducible $f(x) \in K[x]$,

then there is an isomorphism of extensions of K

$$\begin{tikzcd}
L_1 \supseteq & \boxed{K(\alpha) \arrow[r, "\sim"] & K(\beta)} & \subseteq L_2 \\
& K[x]/f(x) \arrow[u, "\wr"] \arrow[ur, "\wr"'] &
\end{tikzcd}$$

$\alpha \leftarrow x$, $x \mapsto \beta$

This isomorphism is not typically unique. But here it is explicit in terms of the extra data.

The unique isomorphism sending α to β.

<u>Example</u> $\mathbb{Q}(e^{2\pi i/3}) \ni e^{2\pi i/3} =$ ζ_3

$\mathbb{Q}[x]/(x^2+x+1)$ $\quad x \mapsto e^{2\pi i/3}$ $\quad x \mapsto e^{-2\pi i/3}$ $\quad$ roots of x^2+x+1

Remark: If $f \in K[x]$, L_1/K, L_2/K are extensions. Then any $\psi: L_1 \to L_2$ s.t. $\psi|_K = \mathrm{Id}$. sends roots of f in L_1 to roots of f in L_2.

If $\alpha \in L_1$ is a root of f

$$f = a_0 + a_1 x + \cdots + a_d x^d \quad a_i \in K.$$

$$\begin{aligned}
\psi(f(\alpha)) &= \psi(a_0 + a_1\alpha + \cdots + a_d\alpha^d) \\
&= \psi(a_0) + \psi(a_1)\psi(\alpha) + \cdots + \psi(a_d)\psi(\alpha)^d \\
&= a_0 + a_1\psi(\alpha) + \cdots + a_d\psi(\alpha)^d \\
&= f(\psi(\alpha))
\end{aligned}$$

If $f(\alpha) = 0$ $\quad f(\psi(\alpha)) = \psi(f(\alpha)) = \psi(0) = 0.$

Bootstrap: Splitting field.

If $f \in K[x]$
then an extension L/K is
a **splitting field** for f
if
(1) f factors into degree 1 polynomials in $L[x]$.
(2) If $\alpha_1, \dots, \alpha_s$ are the roots of f. $(s \le \deg f)$
Then $L = K(\alpha_1, \dots, \alpha_s)$.

Theorem: Splitting fields exist and any 2 are isomorphic as extensions of K.

Proof: For existence – suffices to construct an extension satisfying (1) then take sub ext. generated by roots.
Do by induction on degree.

Note: If L/K is a splitting field for f then $[L:K] \le (\deg f)!$

Given a field K, is there an extension L/K s.t. any $f \in K[x]$ splits into linear factors in $L[x]$?

<u>Theorem/def'n</u>: There exist such an extension which furthermore algebraic over K and such an ext'n is unique up to isomorphism.

(Such an L is called an algebraic closure of K).

<u>Proof</u>

1) Construct an extension where all polynomials split.

2) Show that the subset of elements algebraic over K is a field.

3) Build up uniqueness from splitting field uniqueness.

Part 2: Claim if L/K then

$$L^{alg} \subseteq L$$

$= \{ \alpha \in L \mid \alpha$ is algebraic over $K \}$

is a subfield.

Need to check, e.g., if α, β are algebraic then so is $\alpha + \beta$, $\alpha\beta$, $-\alpha$.

<u>Note</u> If $f(\alpha) = 0$ $\quad g(\beta) = 0$

It's not clear $\exists\, h$ $\quad h(\alpha+\beta) = 0$.

$\alpha\beta$, α^{-1}, ...

$$\alpha + \beta \in K(\alpha, \beta)$$

$$K \underset{\text{finite extension}}{\subseteq} K(\alpha) \underset{\text{Finite extension.}}{\subseteq} K(\alpha, \beta)$$

so $K(\alpha,\beta)/K$ is <u>finite</u>

$$([K(\alpha,\beta) : K] \leq [K(\alpha):K][K(\beta):K]).$$

finite $\Rightarrow$ algebraic.

Example: Every polynomial in $\mathbb{C}[x]$ splits by Liouville's theorem.

- $\mathbb{C}/\mathbb{Q}$ is a field extension

$\overline{\mathbb{Q}} := \mathbb{C}^{alg}$ is an algebraic closure of $\mathbb{Q}$.