Defn. A field F is called *perfect* if every finite extension of F is separable.

Thm Every field of characteristic 0 is perfect.

Pf. Let $f(x) = \operatorname{irr}(\alpha, F)$

suppose $f(x) = \prod (x-\alpha_i)^{\mu_i}$ in $\overline{F}[x]$.

$$= \left(\prod (x-\alpha_i)\right)^{\mu} \text{ in } \overline{F}[x]$$

(since all $\mu_i = \mu = \text{const. in } i$).

Lemma If $m \cdot 1 \neq 0$ in F, then for any monic non-constant polynomial $p(x)$ in $\overline{F}[x]$, if $(p(x))^m \in F[x]$, then $p(x) \in F[x]$.

(Proof: use induction, use binomial expansion ...).

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

$$(f(x))^m = x^{n \cdot m} + \underbrace{(m \cdot 1)a_{n-1}}_{\in F \Rightarrow a_{n-1} \in F} x^{m(n-1)} + \cdots$$

By the Lemma, $\prod(x-\alpha_i) \in F[x]$.

Then $\mu = 1$ (otherwise, the polynomial is not irreducible. $\boxed{}$

Thm Every finite field is perfect.

FYI: An extension field E of F is called *Galois* if it is normal (a splitting field) & separable (& a finite extension)

<u>Thm</u> (Primitive Element Theorem) Let E be a finite separable extension of a field F. Then
$$E = F(\alpha) \text{ for some } \alpha \in E.$$

i.e. every such extension is a simple extension!

[α is called a <u>primitive element</u>.]

<u>Pf.</u> If F is finite, E is finite, and let α be a generator of E^*. ✓ (which is cyclic as a multiplicative group).

If F is infinite, do an induction that starts like this:

Sp. $E = F(\alpha, \beta)$

Show that $\exists\, a \in F$ s.t. $F(\alpha + a\beta) = F(\alpha, \beta)$.

... use this to show the E is a simple extension.

<u>Summary</u>. If E is a Galois extension of F, (finite)

then it's separable & normal

- simple $F(\alpha)$
- splitting field of $\mathrm{irr}(\alpha, F)$.
- $\underbrace{|G(E/F)|}_{\text{Galois group of } E \text{ over } F} = \{E:F\} = [E:F]$.

Fundamental Theorem of Galois Theory.

Given a Galois Extension K/F, there is a 1-1 correspondence between subgroups of $G(K/F)$ and intermediate fields E s.t. $F \leq E \leq K$.

$$\begin{pmatrix} \text{subgroup} \\ H < G(K/F) \end{pmatrix} \longleftrightarrow \begin{pmatrix} \text{subfield} \\ K_H \leq K \\ \text{set of elements of } K \\ \text{fixed by } H. \end{pmatrix}$$

In a lot of books, K^H is the notation for this.

same correspondence

$$\begin{pmatrix} G(K/E) \\ \text{a subgroup of } G(K/F) \end{pmatrix} \longleftrightarrow \begin{pmatrix} \text{subfields } E \\ F \leq E \leq K \end{pmatrix}$$

Furthermore, the subgroup $H \trianglelefteq G(K/F)$ (is a normal subgroup of)

$\Longleftrightarrow$ K_H is a normal extension of F.

FYI for computations

- The Galois group always contains $\Psi_{\alpha,\beta}$ for all α, β roots of $irr(\alpha, F)$ with $\alpha \in K$.

• Thus, the Galois group is transitive on the set of roots of every $\mathrm{irr}(\alpha, F)$.

Ex Let ξ be an n^{th} root of unity in $\mathbb{C}$, i.e. $\xi^n = 1$. Then $G(\mathbb{Q}(\xi)/\mathbb{Q})$ is abelian, in fact a subgroup of $\mathbb{Z}_n^*$.

Pf. $\mathbb{Q}(\xi)$ is the splitting field of an irreducible factor of $x^n - 1$. If $\xi = \alpha^r$, where $\alpha = e^{2\pi i/n}$.

What are the other roots of this factor of $x^n - 1$?