

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 $f(x) = \text{irr}(\alpha, F)$

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 $\mathbb{Q}$).

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 -).

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \dots + a_0 \\ (f(x))^m &= x^{n \cdot m} + \underbrace{(m \cdot 1)a_{n-1}}_{\in F} x^{m(n-1)} + \dots \end{aligned}$$

$$\in F \Rightarrow a_{n-1} \in F.$$

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

Then $\mu = 1$ (otherwise, the polynomial is not irreducible. $\square$)

Thm Every finite field is perfect.

FYI: An extension field E of F is called

Galois if it is normal & separable (a splitting field) (of a finite extension)

Thm (Primitive Element Theorem) Let E be a finite separable extension of a field F . Then
 $E = F(\alpha)$ for some $\alpha \in E$.

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

[α is called a primitive element.]

Pf. 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:

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

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.

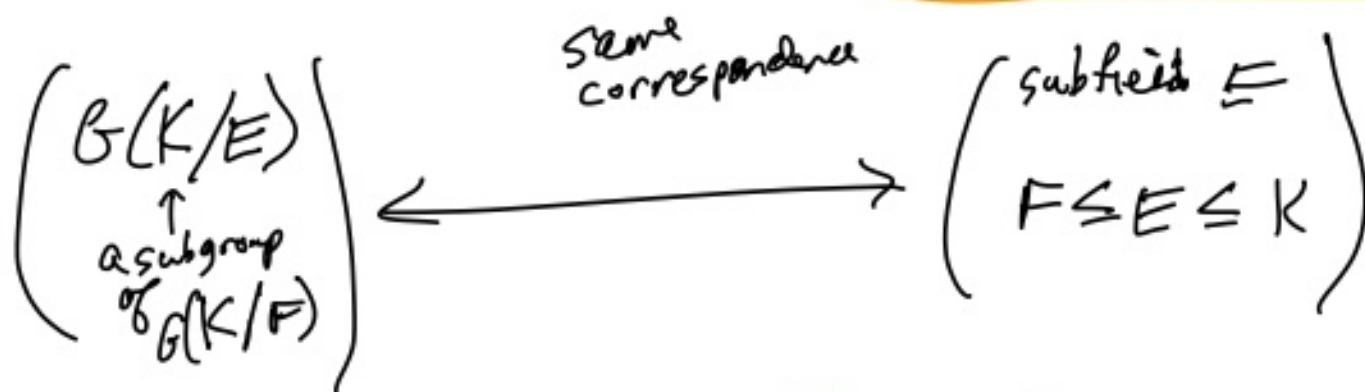
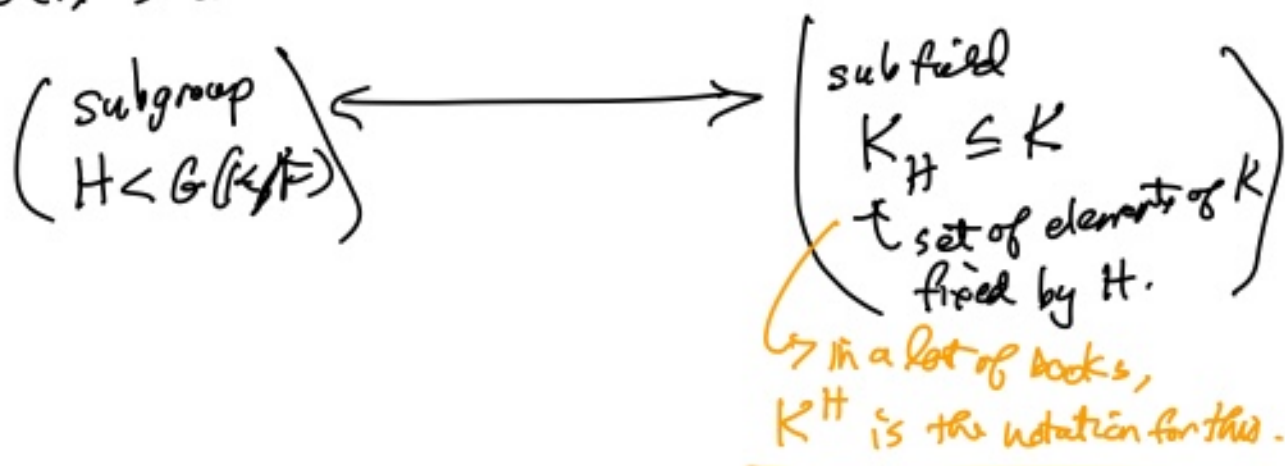
Summary. If E is a Galois extension of F ,
(finite)

then it's separable & normal

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



Furthermore, the subgroup $H < G(K/F)$

$\iff K_H$ is a normal extension of F ,
(is a normal subgroup of)

FYI for computations

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

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

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

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