# Galois extensions

A field ext $F \subset K$ is Galois if for every $\alpha \in K$ the min. poly of $\alpha$ over $F$ splits into distinct linear factors over $K$.

Ex. 1. $F \subset K$ an finite ext of finite fields.

Ex 2. Let $F$ have char $0$. Then $F \subset K$ is Galois if $K$ is a splitting field of some poly. over $F$.

Non ex: $F = \mathbb{F}_p(t)$ Consider $x^p - t \in F[x]$

irred by switching $t, x$ or using Eisenstein.

$K = F[\alpha] / (\alpha^p - t)$ "$\alpha = t^{1/p}$" $K$ is a splitting field of $x^p - t$

$K = F[\alpha] / (\alpha^p - t)$ $\qquad F = \mathbb{F}_p(t)$

In $K[x]$, have

$$x^p - t = (x-\alpha)^p$$

So $F \subset K$ is a splitting field but not Galois.

# Galois Correspondence

Let $F \subset K$ be a finite Galois ext$^n$.
$G = \mathrm{Aut}(K/F)$, "Galois group", finite of order $\deg(K/F)$.

$$\begin{aligned} \text{Intermediate } L &\longrightarrow \text{Subgroups of } G \\ L &\longmapsto \mathrm{Aut}(K/L) \end{aligned}$$

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\} \longleftarrow\!\shortmid \ H \subset G$$

Need to check : Two composites are the identity,
$\longrightarrow$ & then $\longleftarrow$

$F \subset K$ Galois $\qquad\qquad\qquad G = \mathrm{Aut}(K/F).$

Take $L$, $F \subset L \subset K$

$$\begin{array}{ccc} L & \longmapsto & H = \mathrm{Aut}(K/L) \\ \cap & & = \{\sigma : K \to K \text{ s.t. } \sigma(\alpha) = \alpha \ \forall \alpha \in L\} \\ K^H & \longleftarrow & \\ \| & & \\ \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\} & & \end{array}$$

$|H| = \deg(K/L).$

$\nearrow$

$F \subset K$ Galois $\Rightarrow$ $L \subset K$ also Galois. (splitting field of the same poly).

$\text{min poly } (\alpha \text{ over } L)$ divides $\underbrace{\text{minpoly } (\alpha \text{ over } F)}_{\text{splits into distinct factors over } K}$.

Every $\sigma \in H$ defines an aut of $K$ fixing $K^H$.

$$\deg(K/K^H) \geq |H| = \deg(K/L)$$

But $\quad L \subset K^H \subset K$

$\Rightarrow \quad \deg(K/L) \geq \deg(K/K^H)$.

So $K^H = L$.

$\square$

$$\begin{tikzcd} \text{field} \arrow[r, bend left, "\text{first}"] & \text{group} \arrow[l, bend left, "\text{second.}"] \end{tikzcd}$$

$\Rightarrow$ come back to the same field.

$\Rightarrow$ $\{\text{Intermediate fields}\} \longrightarrow \{\text{subgps}\}$ is injective.

$\Rightarrow$ $F \subset K$ any ~~ext~~ finite ext$^n$. (char 0).

Then there are finitely many intermediate fields.

Pf: ~~K~~ $F \underbrace{\subset K \subset}_{\text{finite Galois.}} K'$     $F \subset K'$ has finitely many int. fields.

$\Rightarrow$ $F \subset K$ also has fin. many.

---

$F \subset K$ fin. ext. char 0.

$\alpha \in K$ $\rightsquigarrow$ int. field $F(\alpha)$

---

Let $F$ be an inf. field. Let $K$ be a fin dim $F$ v.space.

Then $K$ cannot be the union of finitely many strict subspaces.

$\therefore$ $K$ cannot be the union of (strict) subfields of $K$.

Applied here: $K$ cannot be the union of (strict) subfields of $K$.

so if $\alpha \in K$ does not lie in this union, then $K = F(\alpha)$.