

Previously on Math 418:

Thm: K the splitting field of $f(x) \in F[x]$.

Then $|\text{Aut}(K/F)| \leq [K:F]$ with equality if f is separable.

Thm: K/F a finite extension where $\text{char}(F) = 0$.

Then $K = F(\gamma)$ for some $\gamma \in K$ and so

$$|\text{Aut}(K/F)| \leq [K:F]$$

Const: G a finite subgroup of $\text{Aut}(K)$, $F = K_G$ the fixed field. Then given $\alpha \in K$, the min poly

$$m_{\alpha, F}(x) = \prod (x - \alpha_i) \text{ where } G \cdot \alpha = \{\alpha_1, \dots, \alpha_n\}$$

in particular α is alg over F of $\text{deg} \leq |G|$.

Today:

Thm: $G \leq \text{Aut}(K)$ finite. Then $[K:K_G] = |G|$.

Hence K/K_G is Galois with $\text{Aut}(K/K_G) = G$.

Focus: K has $\text{char} 0$ or K is finite

Finite Fields:

$K = \mathbb{F}_{p^n}$ = splitting field of $X^{p^n} - X$ over \mathbb{F}_p . ↙ separable

Key: $K^\times = (K \setminus \{0\}, \cdot)$ cyclic.

Pf: By the fund. thm. of finite abelian gps

$$K^\times = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \text{ with } n_1 | n_2 | \cdots | n_k$$

[Q: How many have seen this?]

clt $k > 1$, then have at least $n_1 + \frac{n_2}{n_1}$ elts with $\alpha^{n_1} = 1$. But then $X^{n_1} - 1$ has more than n_1 roots, a contradiction. ▣

Cor: Any extension of finite fields K/F is simple, i.e. $K = F(\alpha)$.

Pf: Let \mathbb{F}_p be the char field of K . clt α gen K^\times , then $K = \mathbb{F}_p(\alpha)$.

Cor: $K = \mathbb{F}_{p^n}$. Then $\text{Aut}(K) = \text{Aut}(K/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ is generated by Frobenius $\sigma: K \rightarrow K$
 $\alpha \rightarrow \alpha^p$.

Pf: Since K is the splitting field of the separable poly $X^{p^n} - X$, have

$$|\text{Aut}(K/\mathbb{F}_p)| = |K:\mathbb{F}_p| = n. \quad \text{Let } \alpha \text{ gen } K^{\times}$$

$$\text{If } \sigma^k = 1, \text{ then } \sigma^k(\alpha) = \alpha^{p^k} = \alpha$$

$$\text{Frob.} \Rightarrow \alpha^{p^k-1} = 1 \Rightarrow k \geq n. \text{ So } |\sigma| = n$$

$$\Rightarrow \text{Aut}(K/\mathbb{F}_p) = \langle \sigma \rangle. \quad \square$$

Thm: $G \leq \text{Aut}(K)$ finite. Then $[K:K_G] = |G|$.

Pf: Assume $\text{char}(K) = 0$ or K is finite. Let $F = K_G$

Know every $\alpha \in K$ is alg/F of $\text{deg} \leq |G|$. Let $\alpha \in K$ have $\text{max. deg}/F = n$.

Claim: $K = F(\alpha)$.

Suppose $\beta \in K$. Then $[F(\alpha, \beta):F] \leq n^2$.

and so $\exists \gamma$ with $F(\gamma) = F(\alpha, \beta)$. Thus

$$[F(\gamma):F] \leq n \Rightarrow F(\gamma) = F(\alpha).$$

Now, $K = F(\alpha)$ is the splitting field/ F of the separable poly $m_{\alpha, F}(x)$. So

$$|G| \leq |\text{Aut}(K/F)| = [K:F] = n \leq |G|.$$

Thus $[K:F] = |G|$ and $G = \text{Aut}(K/F)$. ▣

Thm: A finite extension K/F is Galois iff it is the splitting field of a separable poly $f(x) \in F[x]$.

Pf: (\Leftarrow) Have $|\text{Aut}(K/F)| = [K:F]$, as needed.

(\Rightarrow) By assumption $|\text{Aut}(K/F)| = [K:F]$.

By last Thm, $K_{\text{Aut}(K/F)} = F$. By the

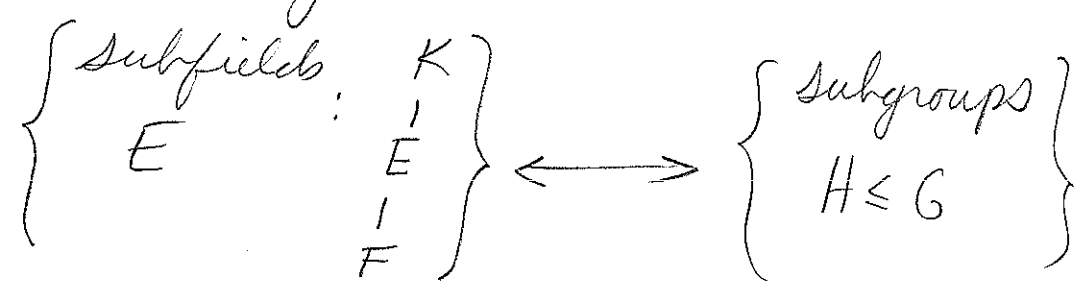
proof of said Thm, $K = F(\alpha)$ and is the splitting field of $m_{\alpha, F}(x)$, for any $\alpha \in K$ with $[F(\alpha):F]$ maximal. ▣

Cor: If $G_1 \neq G_2$ are finite subgroups of $\text{Aut}(K)$, then $K_{G_1} \neq K_{G_2}$.

Pf: Suppose $K_{G_1} = K_{G_2}$. As noted, have $\text{Aut}(K/K_{G_i}) = G_i \Rightarrow G_1 = G_2$.

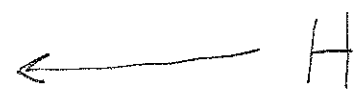
Next time: Let K/F be Galois, set $G = \text{Gal}(K/F)$

There is a bijection



Given by

K_H



E

