Today: min'l polys, finite fields

Thm: Let $G \leq \mathrm{Aut}(K)$, $F = \mathrm{Fix}\, H$

finite gp.

any field

Then K/F is Galois!

More precisely,

$$[K : \mathrm{Fix}\, G] = |G| \quad \text{and} \quad \mathrm{Aut}(K/\mathrm{Fix}\, G) = G$$

We are working towards this by constructing $m_{\alpha,F} \in F[x]$.

Let

$$G\alpha := \{\sigma(\alpha) \mid \sigma \in G\} =: \{\alpha = \alpha_1, \ldots, \alpha_n\}$$

distinct

We know that $\alpha_1, \ldots, \alpha_n$ are roots of $m_{\alpha,F}$,

so set

not nec. $F[x]$

$$f(x) = \prod_{1 \leq i \leq n} (x - \alpha_i) \in K[x]$$

If $f(x) \in F[x]$, then $f = m_{\alpha,F}$.

Claim: This is indeed the case.

Pf: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

If $\tau \in G$, then $\tau(\alpha_i) = \tau(\sigma(\alpha)) = (\tau\sigma)(\alpha) = \alpha_j$,

so τ permutes the α_j.

Then,

$$\tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0)$$

$$= \tau(f(x)) = \tau\left(\prod(x - \alpha_i)\right) = \prod(x - \tau(a_i))$$

$$= \prod(x - a_i) = f(x) = a_n x^n + \cdots + a_0,$$

so $a_i \in \text{Fix}\, G = F$, so $f = m_{\alpha,F}$. $\square$

Def: In the case where $G = \text{Gal}(K/F)$ (by the thm. this will always hold), the elts. of $G\alpha$ are called the <u>Galois conjugates</u> of α.

Focus: char 0 and finite fields

Let $K = \mathbb{F}_{p^n}$ = splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$

Prop: Let $f(x) \in F[x]$ be irred of deg. n. Then

$$L := F[x]/(f) \cong K.$$

Pf: Since $\deg f = n$, $[L:F] = n$, so $|L| = p^n$

$$\left(L = \{c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n\} \right)$$

basis

By uniqueness of $\mathbb{F}_{p^n}$, $L \cong K$.

Thm: $K^\times = K \setminus \{0\}$ is a cyclic gp.

mult gp.

Pf: By the Fundamental thm. of abelian gps.,

$$K^\times = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \quad \text{where } d := \gcd(n_1, \dots, n_k) > 1$$

Suppose $k > 1$, and consider the roots in $K^\times$ of $x^{n_1} - 1$. Everything in $\mathbb{Z}/n_1\mathbb{Z}$ is such a root, and so is $\frac{n_2}{d} \in \mathbb{Z}/n_2\mathbb{Z}$. But this is more than n_1 root of a deg n_1 poly. $\square$

Cor (Primitive elt. thm for finite fields): Any ext'n K/F w/ K finite is simple.

Pf: $K = F(\gamma)$ where γ is any generator of the cyclic gp. $K^\times$. $\square$

Cor: $\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$

w/ generator $\mathrm{Frob}_p : \alpha \mapsto \alpha^p$.

Pf: From D&F Problem 13.6.10, $\langle \mathrm{Frob} \rangle \cong \mathbb{Z}/n\mathbb{Z} \leq \mathrm{Aut}(\mathbb{F}_{p^n})$.

Conversely, since $\mathbb{F}_{p^n}$ is the splitting field of the sep. poly. $x^{p^n} - x$, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and

$$|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n. \quad \square$$

Pf of thm when char $K = 0$ or K: finite.

If $\alpha \in K$, then $m_{\alpha,F}(x) = \prod_{\beta \in G\alpha} (x - \beta)$, so

$$[K:F] = [F(\alpha):F] = \deg m_{\alpha,F} = |G\alpha| \leq |G|.$$

Now, if α is a prim. elt. for K/F i.e. $K = F(\alpha)$, then we have

$$|G| \underset{(c)}{\leq} |\mathrm{Aut}(K/F)| \underset{(a)}{\leq} [K:F] \underset{(b)}{\leq} |G|.$$

Therefore, these are all equalities and so

(a) K/F is Galois

(b) $[K:F] = G$

(c) $\mathrm{Gal}(K/F) = G$

$\square$