Final: Friday 4-6pm EH 1084

OH: Wed 12:30 – 2:00, Fri 10–11:30. Course Eval → do it

Finite Fields

- If F is a finite field $\Rightarrow$ F contains $\mathbb{F}_p$ for some prime p
  - $\hookrightarrow$ F has char p
  - $\Rightarrow \#F = p^n$ as F is a finite dim'l $\mathbb{F}_p$ v.s. w/ dim n
  - $[F:\mathbb{F}_p] = n$
- Given $q = p^n$ $\exists$ finite field $\mathbb{F}_q$ w/ q elts unique up to iso.
  - $\mathbb{F}_q$ = splitting field of $x^q - x$
- $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff $n \mid m$
- $\mathbb{F}_q^\times$ is cyclic of ord $q-1$
- Concretely construct $\mathbb{F}_{p^2}$ if $p \neq 2$ pick $a \in \mathbb{F}_p$ a not $\square$
  - $\mathbb{F}_p(\sqrt{a}) = \mathbb{F}_p[x]/(x^2 - a)$ is field w/ p^2 elts.
  - $p=2$ $\mathbb{F}_q = \mathbb{F}_2[x]/(x^2+x+1)$
- have $\mathbb{F}_q \to \mathbb{F}_q$, $x \to x^p$ is a field aut. $q = p^n$.
  - $\hookrightarrow$ called Frob_p
  - $\hookrightarrow$ gens $\mathrm{Aut}(\mathbb{F}_q) \cong \mathbb{Z}/n$

Galois Thy (Char inf equlty + Char 0)

- E/F - finite extn $\Rightarrow$ $Gal(E/F) = \{$ field auts σ of E st $\sigma|_F = id \}$
- E/F is gal if $[E:F] = \#Gal(E/F)$ (no in $F[x]$)
  - it is a splitting field of some poly.
  - if anything factors it splits
- Important obs. if $\sigma \in gal(E/F)$ wl $a \in E$ root of poly wl coeff in F $\Rightarrow \sigma(a)$ root of
- If E splitting field of $f \in F[x]$
  $\Rightarrow$ $gal(E/F) \leq S_n$ where $n = \deg f$.
  (this new perm n roots of)

  if $f(x)$ is irred $/F$ $\Rightarrow$ this action is transitive.

Pf) if $a \in E$ $a_1, \dots, a_r$ is gal orbit of a

$h(x) = \prod (x - a_i)$ $\Rightarrow$ coeff in F as we just perm a_i's

important: So in case abv if $f(x)$ irred & a is a root
$\Rightarrow h | f$ as abv $\Rightarrow$ $h = f$ as f irred
$\Rightarrow a_1, \dots, a_n$ are all roots of f

- Artin thm if E is any field G is a finite grp of Auts and Then $F = E^G$ $\Rightarrow$ E/F gal w/ grp G.

eg) $E = \mathbb{C}(x_1, \dots, x_n)$ $G = S_n$ permuting vars
$F = \Sigma^{Sn}$ E/F gal grp of S_n $\prod_{i=1}^{n}(t - x_i) = \sum a_i t^i$ $F = \mathbb{C}(a_1, \dots, a_n)$

- Main Thm of Galois Thy

Say E/F is gal w/ gp G

$\Rightarrow \exists$ bijection

$$\{\text{intermediate fields } E/F\} \longleftrightarrow \{\text{subgps of } G\}$$

$$E^H \longleftarrow H$$

$$K \longmapsto \mathrm{Gal}(E/K)$$

Aux

1) if $K = E^H \Rightarrow K/F$ is gal $\Leftrightarrow H \subseteq G$ (normal).

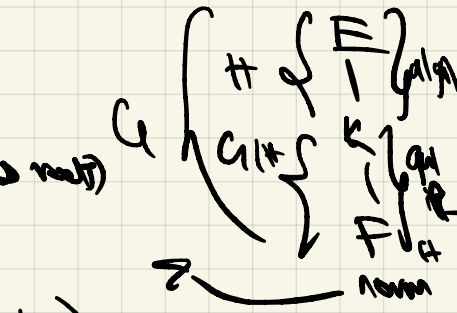
Assume K/F is gal

$\Rightarrow$ every elt of G maps $K \to K$ (prev result)

$\Rightarrow$ restriction map surj

$$\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$$

$$\sigma \longmapsto \sigma|_K$$



surj w/ $\ker = H \Rightarrow \mathrm{Gal}(K/F) \cong G/H$

$\ker H$ is easy & surjectivity by counting.

(or some alg closed counting)

- The gal corr is order reversing,

if $H_1 \longleftrightarrow K_1$, $H_2 \longleftrightarrow K_2$

$\Rightarrow H_1 \subseteq H_2 \Leftrightarrow K_1 \supseteq K_2$

intersection of subgp $\longleftrightarrow$ compositum of fields

prod of subgp $\longleftrightarrow$ intersection of fields.

- If E = splitting field of f of deg n
  $G = Gal(E/F) \subset S_n$
  $G \subset A_n$ iff $disc(f)$ is a sq in F.

e.g. if $f(x) = x^3 + px + q$ is irred $\Rightarrow$ gal grp trans
& $G = \begin{cases} S_3 & disc(f) \neq \square \\ A_3 & disc(f) = \square \end{cases}$ Cb so A_3 or S_3

$disc(f) = -4p^3 - 27q^2$

(quintic Hw 11)

- Important e.g.
  a) if ζ_n = prim n^{th} root
  $F(\zeta_n)$ is gal / F w grp $\leq (\mathbb{Z}/n\mathbb{Z})^\times$ ← group
  Cb equality when $F = \mathbb{Q}$

  b) if $\zeta_n \in F$ & $a \in F$
  $F(a^{1/n})$ is gal w' $Gal(F(a^{1/n})/F) \subset \mathbb{Z}/n$
  Cb equality when non degen i.e. diff n^{th} root of Δ
  Cb as good as sq root

  (cont'd) If $\zeta_n \in F$ & E/F is gal extn w $\mathbb{Z}/n\mathbb{Z}$
  $\Rightarrow E = F(a^{1/n})$ some $a \in F$.

---

1 final trick: if $f(x) \in \mathbb{Q}[x]$ and E - spl field
complex conj defines elt in $Gal(E/\mathbb{Q})$
(non triv if ≥ 1 non-real root)

Solvable not a final.