Last time:

- Showed that given E/F Galois = (normal, separable finite ext)

  the map $\mathrm{Fix}: \{\text{Subgroups of } \mathrm{Gal}(E/F)\} \to \{\text{intermediate fields } K,\ F \subset K \subset E\}$

  is surjective.

- Showed if E/F is Galois then $E = F(\alpha)$

  (used that if E/F has finitely many intermediate subfields

  Artin Thm. & F infinite then E has a prim. element)

  still need the finite case

- Showed that $|G| = [E:F]$

Digression to finite fields

Lemma: Any finite subgroup $A \subset E^*$, E - field, is cyclic.

Pf: enough to show for every prime ℓ, $\exists$ at most ℓ elements of order ℓ. But elements of order ℓ are roots of $x^\ell - 1$ which has at most ℓ roots $\square$.

Cor: if E/F finite w/ F finite, then $E^* = \langle \alpha \rangle$

$\Rightarrow E = F(\alpha)$.

Note also: if E has order $q=p^n$ then every $\alpha\in E$ is a root of $X^q - X = f$

$$X(X^{q-1}-1) = \prod_{\alpha\in E}(X-\alpha)$$

$$|E^*| = q-1$$

$\Rightarrow$ E is the splitting field of f which has distinct roots

$\Rightarrow$ E/F Galois.

Note also: the map $\alpha \mapsto \alpha^p$ from E to E is ~~surjective~~ bijective.

if $\alpha^p = \beta^p \Rightarrow (\alpha^p)^{p^{n-1}} = (\beta^p)^{p^{n-1}}$

$\Rightarrow \alpha^{p^n} = \beta^{p^n}$ $\quad \alpha^q = \beta^q$, $\alpha^q = \alpha$, $\beta^q = \beta$

$\Rightarrow$ injective $\Rightarrow$ bijective.

Def A field F of char p is perfect if $F^p = F$.

$F^p = \{\alpha^p \mid \alpha\in F\}$

(Thm 18.20)

Given E, $G \subset \mathrm{Aut}(E)$ finite let $F = E^G$

then:
- $[E:F] = |G|$ $\leftarrow$
- $G = \mathrm{Gal}(E/F)$
- E/F Galois

Pf of $\leftarrow$

Note: if $\alpha \in E$ then $\min_F \alpha = \prod_{\lambda\in\Lambda}(x-\lambda)$ $\Lambda = \{\sigma\alpha \mid \sigma\in G\}$

$\Rightarrow \forall \alpha\in E$, $[F(\alpha):F] \le |G|$

since each degree $[F(\alpha):F]$ bounded can choose α w/ degree max.

Subclaim: $[E:F] \le |G|$

if $E = F(\alpha)$ done. ~~else: $\forall\alpha$, $\exists\beta$ s.t. $F(\alpha,\beta) \supsetneq F(\alpha)$.~~

if $E \ne F(\alpha)$ choose $\beta \in E\setminus F(\alpha)$

$F(\alpha,\beta)$ separable (it's splitting field of 2 polys of form ^)

Side Lemma: If E/F is finite separable $\Rightarrow E = F(\alpha)$.

by side lemma, $F(\alpha,\beta) = F(\gamma)$

$F(\alpha)/F$ max'l degree, $F(\alpha)\subset F(\gamma)$

$\Rightarrow F(\alpha)=F(\gamma) \Rightarrow \beta\in F(\alpha)$ ↯.

$\Rightarrow E = F(\alpha)$

$|\Lambda| = |G\alpha| = \dfrac{|G|}{|\mathrm{Stab}_G\,\alpha| = 1} = |G| \Rightarrow E = F(\alpha)$, $[F(\alpha):F] = |G|$.

Pf: If $E = F(\alpha_1,\dots,\alpha_n)$ $f_i = \min_F \alpha_i$

then let L = splitting field of $f = \prod f_i$

then $E\subset L$ and L/F is Galois

since each f_i hence f is separable.

$\exists$ finite # of int. fields $F\subset M\subset L$

so also between F & E, Artin D.

Now get: for E/F G-Galois

$$\left\{ \begin{array}{c} \text{intermediate fields } K \\ F \subset K \subset E \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{subgps} \\ H < G \end{array} \right\}$$

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

is surjective!

if $H < G$, consider $K = E^H$

prior result $\Rightarrow$ E/K is Galois w/ gp H. $\Rightarrow K = E^H$.

also: $[E:K] = |H|$

this means: if E/F is G-Galois then

all intermediate fields K & all subgps H are "closed"

w/ rel to Galois correspondence.

So get Fix, Gal are inclusion reversing bijections

between subgps & subfields.

Exercise: If E/F is G Galois, $H < G$, $K = E^H$

what is the subgp of G which stabilizes K?

$\{ \sigma \in G \mid \sigma K = K \}$

$$\sigma K = K \iff \underset{\displaystyle \sigma H \sigma^{-1}}{\underset{\shortparallel}{\mathrm{Gal}(E/\sigma K)}} = \mathrm{Gal}(E/K) = H$$

$\sigma K = K$ means $\sigma H \sigma^{-1} = H$ i.e. $\sigma \in N_G H$

$\leadsto$ if K normal then $\sigma K = K$ all $\sigma \in G$

$\Rightarrow$ if K normal$/_F$ then $H \triangleleft G$

$\Updownarrow$ $\quad N_G H = G$

K/F Galois

<u>Recall:</u> $(fg)' = f'g + g'f$ $\quad (fg)' - f'g - g'f = 0$

works for diff fcns (polys) over $\mathbb{R}$

$\Rightarrow$ works for polys in $\mathbb{Z}[\alpha,\beta] \cong \mathbb{Z}[x,y]$

$\alpha, \beta \in \mathbb{R}$.

<u>check:</u> if works for $R[x]$ & $R \to S$ hom

then also for f in image in $S[x]$

in arbitrary ring R, $f, g \in R[x]$

$\mathbb{Z}[y_1, \dots, y_r] \xrightarrow{y_i \mapsto a_i}$ $\quad f = \sum a_i x^i$

$\sum y_i x^i$

<u>Inseparability</u> F char p.

<u>Note:</u> if f is irred & not separable $\Rightarrow f(x) = g(x^p)$

some g.

irred.

$g(x)$ .... repeat

get <u>$f(x) = h(x^{p^n})$ some n w/ h irred, separable</u>

Def E/F is purely inseparable if $\min_F \alpha$ is insep all $\alpha \in E$.

Claim $\Rightarrow \min_F \alpha = x^{p^n} - a$ some a.

Pf: $\overset{\shortparallel}{f} = h(x^{p^n})$ h sep & irred. $\Rightarrow a = \alpha^{p^n}$

$\min_F a = h(x)$ separable. $\Rightarrow a \in F$, $h = x - a$

$\square$.

Note: $F(\alpha) = \dfrac{F[x]}{x^{p^n} - a} = E$ $a \in F$

then for $\beta \in E$, $\beta^{p^n} \in F$.

Pf: $\beta = \sum c_i \alpha^i$ $\quad \beta^{p^n} = \left(\sum c_i \alpha^i\right)^{p^n} = \sum c_i^{p^n} (\alpha^{p^n})^i$

$= \sum c_i^{p^n} a^i \in F$.

Finally:

Thm: E/F algebraic is p. insep iff $\forall \alpha \in E$ $\alpha^{p^n} \in F$ some n.
(char p.)

Pf: suppose $\alpha^{p^n} \in F$ all α.

$\min_F \alpha \mid x^{p^n} - a \qquad a = \alpha^{p^n}$

h $\shortparallel$

over E, $x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$

$h = (x-\alpha)^s$

$(x-\alpha)^{p^n} = h \cdot g \qquad g(\alpha) = 0$

$\shortparallel \qquad\qquad \Rightarrow h \mid g$

h^t some t

$ts = p^n \Rightarrow s = p^m$

$\Rightarrow h = (x-\alpha)^{p^m} = x^{p^m} - \alpha^{p^m} \Rightarrow b = \alpha^{p^m} \in F$

$x^{p^m} - b$ insep. $\square$.