Midterm 1 Wed. 7-9 pm in 200-205

§9.4, 13.1-6, 14.1

See email for policies

Wed. class: review

Last time: Galois ext'n $|\underbrace{\mathrm{Aut}(K/F)}_{=: \mathrm{Gal}(K/F)}| = [K:F]$

Cor 6: If K is the splitting field $/F$ of a sep. poly., then K/F is Galois.

We will prove the converse (Thm. 13)

---

§14.2: The Fundamental Theorem of Galois Theory

Def: A (linear) (quasi-) character of a gp. G w/ values in a field L is a gp. homom.

$$\chi : G \to L^\times$$

E.g.: $G = \mathbb{Z}/n\mathbb{Z}$, $L = \mathbb{C}^\times$

Fix ζ any nth root of 1.

Then $\chi(a) = \zeta^a$ is a character of $\mathbb{Z}/n\mathbb{Z}$ w/ values in $\mathbb{C}$

$$\chi(a)\chi(b) = \zeta^a \zeta^b = \zeta^{ab} = \chi(ab)$$

Varying ζ gives n distinct chars. of $\mathbb{Z}/n\mathbb{Z}$ w/ values in $\mathbb{C}$

Def: Chars. $\chi_1, \dots, \chi_n$ of G are linearly independent over L if there is no nontrivial rel'n

$$a_1\chi_1 + a_2\chi_2 + \dots + a_n\chi_n = 0 \qquad (a_i \in L \text{ not all } 0)$$

(This rel'n means $a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0 \ \forall g$)

Thm 7: If $\chi_1, \dots, \chi_n$ are distinct chars. of G w/ values in L, they are linearly indep. over L.

Pf: Suppose otherwise, and choose a linear dependence:

$$a_1\chi_1 + \dots + a_m\chi_m = 0 \quad \text{with } m \text{ minimal}$$

So $\forall g \in G$, $a_1\chi_1(g) + \dots + a_m\chi_m(g) = 0 \quad (*)$

Choose $g_0 \in G$ s.t. $\chi_1(g_0) \neq \chi_m(g_0)$ (possible since $\chi_1 \neq \chi_m$)

Then $\forall g \in G$,

$$0 = a_1\chi_1(g_0 g) + \dots + a_m\chi_m(g_0 g)$$

$$= a_1\chi_1(g_0)\chi_1(g) + \dots + a_m\chi_m(g_0)\chi_m(g). \quad (**)$$

Multiply $(*)$ by $\chi_m(g_0)$:

$$0 = a_1\chi_m(g_0)\chi_1(g) + \dots + a_m\chi_m(g_0)\chi_m(g)$$

Subtract $(**)$:

$$0 = (\chi_m(g_0) - \chi_1(g_0))a_1\chi_1(g) + \dots + (\chi_m(g_0) - \chi_{m-1}(g_0))a_{m-1}\chi_{m-1}(g)$$

So

$$0 = (\chi_m(g_0) - \chi_1(g_0))a_1\chi_1 + \cdots + (\chi_m(g_0) - \chi_{m-1}(g_0))a_{m-1}\chi_{m-1}$$

is a shorter dependence. Contradiction! $\square$

Def: An embedding of a field K into a field L is an injective homom. $\sigma : K \to L$.

E.g. $\sigma \in \mathrm{Aut}(K)$ is an embedding $K \to K$

Cor 8: If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings $K \to L$, then they are linearly indep. as functions on K.

Pf: $\sigma_i|_{K^\times}$ is a char. of $K^\times$ w/ values in $L^\times$, so apply Thm. 7

Thm 9: Let $G \leq \mathrm{Aut}(K)$, and let $F = \mathrm{Fix}(G)$. Then $\underbrace{[K:F]}_{m} = \underbrace{|G|}_{n}$. (G is always finite)

Pf:
$G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$

$\omega_1, \ldots, \omega_m$: basis for K/F

If $n > m$, The system

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n &= 0 \end{aligned}$$

m eqns.
n unknowns

has a nontriv. sol'n $x_1 = \beta_1, \ldots, x_m = \beta_m$ in K

We'll show that $\beta_1\sigma_1 + \cdots + \beta_n\sigma_n = 0$, so $\sigma_1, \ldots, \sigma_n$ linearly dep.

Let $\alpha \in K$. Then $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$, $a_1, \ldots, a_m \in F$,

If $a \in F$, a is fixed by G, so $\sigma_i(a_j) = a_j \ \forall i,j$

Multiply the ith eqn above by a_i:

$$\sigma_1(a_1\omega_1)\beta_1 + \cdots + \sigma_n(a_1\omega_1)\beta_n = 0$$

$$\vdots$$

$$\sigma_1(a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_m\omega_m)\beta_n = 0,$$

and add:

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0$$ linearly dep. Contradiction.

If $n < m$, the system

$$\sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_m)x_m = 0$$

$$\vdots$$

$$\sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_m)x_m = 0$$

n eqns.
m unknowns

has a nontriv. sol'n $x_1 = \gamma_1, \ldots, x_m = \gamma_m$ in K

(but <u>not</u> in F, since $\omega_1, \ldots, \omega_m$ linearly indep. $/F$)

Reordering/scaling if necessary, assume $\gamma_1 \notin F$,
$\gamma_r = 1$, $\gamma_{r+1} = \cdots = \gamma_m = 0$

Then,

$$\begin{aligned} \sigma_1(\omega_1)\gamma_1 + \cdots + \sigma_1(\omega_{r-1})\gamma_{r-1} + \sigma_1(\omega_r) &= 0 \\ &\vdots \qquad\qquad (*) \\ \sigma_n(\omega_1)\gamma_1 + \cdots + \sigma_n(\omega_{r-1})\gamma_{r-1} + \sigma_n(\omega_r) &= 0 \end{aligned}$$

Since $\gamma_1 \notin F = \text{Fix}\, G$, choose $k \in \{1, .., n\}$ s.t. $\sigma_k(\gamma_1) \neq \gamma_1$.

Since G is a gp., $\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots, \sigma_k\sigma_n$ is a permutation of $\sigma_1, \ldots, \sigma_n$, so applying σ_k to $(*)$ gives

$$\begin{aligned} \sigma_1(\omega_1)\sigma_k(\gamma_1) + \cdots + \sigma_1(\omega_1)\sigma_k(\gamma_{r-1}) + \sigma_1(\omega_r) &= 0 \\ &\vdots \qquad\qquad (**) \\ \sigma_n(\omega_1)\sigma_k(\gamma_1) + \cdots + \sigma_n(\omega_1)\sigma_k(\gamma_{r-1}) + \sigma_n(\omega_r) &= 0 \end{aligned}$$

Subtracting $(**)$ from $(*)$ gives a smaller nontriv. set of eqns. Contradiction! $\square$

Cor 10: K/F finite extn:

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

w/ equality iff $F = \text{Fix}(\text{Aut}(K/F))$

i.e. K/F Galois $\iff$ $F = \text{Fix}(\text{Aut}(K/F))$

Pf: Let $E = \text{Fix}(\text{Aut}(K/F))$. Then $F \subseteq E \subseteq K$,

and by Thm 9, $|\text{Aut}(K/F)| = [K:E]$.

By the Tower Law $[K:F] = |\text{Aut}(K/F)|\,[E:F]$ $\square$

Sort of converse to the last result:

Cor 11: $G \leq \text{Aut}(K)$, $F = \text{fix}(G)$. Then, $\text{Aut}(K/F) = G$

Pf: By def'n, $G \leq \text{Aut}(K/F)$. By Thm 9, $[K:F] = |G|$,

and by Cor. 10, $|\text{Aut}(K/F)| \leq [K:F]$, so

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

must be equal

Cor 12: If $G, H \leq \text{Aut}(K)$, $G \neq H$, then $\text{Fix}\, G \neq \text{Fix}\, H$.

Pf: If $\text{Fix}\, G = \text{Fix}\, H$, then by Cor. 11,

$$G = \text{Aut}(K/\text{Fix}\, G) = \text{Aut}(K/\text{Fix}\, H) = H$$