Lecture 29

(29.0) Recall: last time we proved the following inequality: if K and L are two fields, $S = \{\sigma_1, \ldots, \sigma_n\} \subset \underset{\text{fields}}{\mathrm{Hom}}(K, L)$

$k := \{\alpha \in K \mid \sigma_1(\alpha) = \cdots = \sigma_n(\alpha)\}$. Then $(K : k) \geq n$.

We will revisit the proof below.

(29.1) Artin's Theorem. – Let E be a field, $G \subset \underset{\text{field}}{\mathrm{Aut}}(E)$ a finite subgroup and $F = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G\}$ $(=: E^G)$

Then $(E : F) = |G|$.

Proof. Let $n = |G|$ and $r = (E : F)$ = dimension of E as an F-vector space.

Let $\{\omega_1, \ldots, \omega_r\}$ be a basis of E (as F-v.s.) and let $G = \{\sigma_1, \ldots, \sigma_n\}$. We form a matrix

$$X = \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_r) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_r) \\ & \vdots & & \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_r) \end{bmatrix}$$

: an $n \times r$ matrix with entries from E

Thus $X : E^r \longrightarrow E^n$ can be viewed as an E-linear map from r-dim'l to n-dim'l vector space.

Theorem (28.3) – independence of characters – implies that

$$X^T = \begin{bmatrix} \sigma_1(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_r) & & \sigma_n(\omega_r) \end{bmatrix} : E^n \longrightarrow E^r$$

is injective (columns are linearly independent over E). Hence $n \leq r$ (see Thm (28.4) of page 6 – we don't need G to be a group for this).

Now we will show that $X : E^r \longrightarrow E^n$ is injective. Assume that it is not, and let $\underline{0} \neq \begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} \in \mathrm{Ker}(X)$. That is,

$$\forall\, 1 \leq j \leq n : \quad \sigma_j(\omega_1)\, a_1 + \dots + \sigma_j(\omega_r)\, a_r = 0.$$

To arrive at a contradiction, we set $p =$ smallest number such that $\exists\ \underline{a} \in \mathrm{Ker}(X)$ with p non-zero entries.

By reordering $\{\omega_1, \dots, \omega_r\}$, if necessary, we may assume

$$\underline{a} = \begin{bmatrix} a_1 \\ \vdots \\ a_p \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} p \text{ non-zero} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} r-p \text{ zeroes} \end{matrix} .$$

$p = 1 \Rightarrow a_1 \sigma_j(\omega_1) = 0 \ \forall j$
$\Rightarrow a_1 = 0$
contradiction!

Let us rescale $a_p = 1$.

Note. if all $a_1, \dots, a_{p-1} \in F$, we take $\sigma_j = id$ of G to get an F-linear dependence rel^n among $\omega_1, \dots, \omega_p$ contradicting the fact that $\{\omega_1, \dots, \omega_r\}$ was an F-basis of E.

So, let $\ell \in \{1, \dots, p-1\}$ be such that $a_\ell \notin F$. Thus there is $k \in \{1, \dots, n\}$ s.t. $\sigma_k(a_\ell) \neq a_\ell$ (remember: $F = E^G$)

$$(1): \sigma_j(\omega_1) a_1 + \dots + \sigma_j(\omega_{p-1}) a_{p-1} + \sigma_j(\omega_p) = 0 \quad (\forall j \; 1 \leq j \leq n)$$

$$\Longrightarrow \quad \sigma_k(\sigma_j(\omega_1)) \sigma_k(a_1) + \dots + \sigma_k(\sigma_j(\omega_{p-1})) \sigma_k(a_{p-1}) + \sigma_k(\sigma_j(\omega_p)) = 0$$

Apply σ_k

As $\{\sigma_k \sigma_1, \dots, \sigma_k \sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$, we get

$$(2): \sigma_j(\omega_1) \sigma_k(a_1) + \dots + \sigma_j(\omega_{p-1}) \sigma_k(a_{p-1}) + \sigma_j(\omega_p) = 0 \quad (\forall j)$$

$$(2) - (1): \quad \sigma_j(\omega_1)(\sigma_k(a_1) - a_1) + \dots + \sigma_j(\omega_{p-1})(\sigma_k(a_{p-1}) - a_{p-1}) = 0 \quad \forall \, 1 \leq j \leq n.$$

This is a non-trivial element of $Ker(X)$, because $\sigma_k(a_\ell) \neq a_\ell$, contradicting our choice of p. $\square$

(29.2) Definition. Let E/F be a field extension.

$$\mathrm{Gal}(E/F) := \{\sigma : E \xrightarrow{\sim} E \text{ iso. of fields} \mid \sigma(a) = a \ \forall a \in F\}$$

(Galois group - in honor of E. Galois 1811 - 1832)

Remark. $G = \mathrm{Gal}(E/F)$. Then $E^G \supset F$ but need not be equal. e.g.

$$\begin{array}{c} E = \mathbb{Q}(\sqrt[3]{2}) \\ | \\ F = \mathbb{Q} \end{array}$$

- $\mathrm{Gal}(E/F) = \{\mathrm{Id}\} \ (= G)$
- $E^G = E$

A good example.

$$\begin{array}{c} E = \mathbb{Q}(\zeta) \\ | \\ F = \mathbb{Q} \end{array} \qquad \zeta = e^{2\pi\sqrt{-1}/7} \in \mathbb{C}.$$

$(E:F) = 6$ because $E \cong \dfrac{\mathbb{Q}[T]}{T^6 + T^5 + \dots + T + 1}$

$\forall\ 1 \le j \le 6$, $\sigma_j : E \xrightarrow{\sim} E$, $\zeta \longmapsto \zeta^j$ $\in \mathrm{Gal}(E/F)$.

By Artin's Theorem $\{\sigma_1, \dots, \sigma_6\} = \mathrm{Gal}(E/F)$

and $F = E^G$ (dimension count!)

(29.3) Definition. Let E/F be an algebraic extension.

We say E/F is a <u>Galois extension</u> if

$$E^{\mathrm{Gal}(E/F)} = F$$

Cor. of Artin's Thm. (1) If E is a field and $G \subset \mathrm{Aut}_{\text{fields}}(E)$ is a finite subgroup, then

$$\begin{array}{c} E \\ | \\ F = E^G \end{array}$$

is a Galois extn.

(2) $G_1 \neq G_2$ finite subgps. of $\mathrm{Aut}_{\text{fields}}(E) \Rightarrow E^{G_1} \neq E^{G_2}$.

(29.4) Let E/F be an algebraic extension. We say that E is <u>normal</u> (extension over F) if $\forall\, \alpha \in E$, the min'l polynomial $f_\alpha(x) \in F[x]$ splits into a product of linear factors in $E[x]$.

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n) \qquad \alpha_1, \ldots, \alpha_n \in E \quad (\text{say } \alpha_1 = \alpha)$$

In other words, E contains the splitting extn. of all its minimal polynomials. Yet another way to say this is:

$\forall\, f(x) \in F[x]$ irreducible s.t. $f(\alpha) = 0$ for some $\alpha \in E$

we have $$f(x) = \prod_{i=1}^{\deg f} (x - \alpha_i) \quad \text{in } E[x].$$

(or Splitting field of $f(x)$ over $F \hookrightarrow E$).

(29.5) Separability. A polynomial $p(x) \in F[x]$ is said to be separable if its roots in the splitting field (of $p(x)$ over F) are distinct.

Warning: there exist irreducible polynomials which are not separable. The fields for which such phenomenon happens are called imperfect fields. We will prove later in the course that fields of char 0 (such as $\mathbb{Q}$ or any of its extns.) are perfect.

An extension (algebraic) E/F is called separable if $\forall \alpha \in E$, the minimal polynomial $f_\alpha(x) \in F[x]$ is separable.

(29.6) Theorem. Let E/F be an algebraic extension. Then E/F is Galois $\Longrightarrow$ E/F is normal and separable.

The converse is also true, but the method of the proof differs in finite and infinite dim'l extns.

Proof. Let us assume E/F is a Galois extn. Let $G = Gal(E/F)$.

So that $F = E^G$. We have to prove that $\forall \alpha \in E$,

$f_\alpha(x)$ (min'l poly. of α) $\in F[x]$ splits <u>completely</u> into <u>distinct</u>

linear factors, in E.

We begin by observing that $\forall \sigma \in G$, $\sigma(\alpha)$ is again a root of $f_\alpha(x)$.

Since there are $\leq \deg(f_\alpha)$ roots of f_α (in any extn of F), G-orbit of

α is finite. Let $\{\alpha_1, \dots, \alpha_n\} = G\cdot\alpha$ (say $\alpha_1 = \alpha$)

Set $p(x) = (x-\alpha_1) \cdots (x-\alpha_n) \in E[x]$

$\forall \sigma \in G$, $\sigma(p(x)) = p(x) \Rightarrow p(x) \in F[x]$ $(E^G = F)$

Claim. $p(x) =$ min'l polynomial of α.

Proof. It is enough to prove that if $f(x) \in F[x]$ is such

that $f(\alpha) = 0$, then degree of $f \geq n =$ degree of p.

But if $f(\alpha) = 0$ then using G-action, $f(\alpha_i) = 0$ $\forall i \in \{1, \dots, n\}$.

i.e. f has at least n distinct roots in $E \Rightarrow \deg(f) \geq n$.

$\square$

(29.7) Converse of Theorem 29.7. Finite case. — Let us assume that E/F is a finite extension. We will need the following

Lemma. If E/F is normal (resp. normal & separable) then E = splitting field of some (resp. separable) polynomial $p(x) \in F[x]$.

Proof. Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of E as an F-v.s. Let $f_1(x), \ldots, f_n(x) \in F[x]$ be the min'l polys. of $\omega_1, \ldots, \omega_n$. Take $p(x)$ = product of f_i's $(1 \leq i \leq n)$ without repitition. $\square$

Thm (29.8). Let E/F be a finite, normal, separable extn. Then E/F is Galois.

Proof The hypothesis implies, by the lemma above, that E = splitting extn. of a separable polynomial $p(x)$.

We want to prove that $E^G = F$ where $G = Gal(E/F)$.

~~So, let $\alpha \in E^G$~~. Again we induct on no. of roots of $p(x)$ outside of F, say k.

$k = 0$ means $E = F$ and hence $G = \{Id\}$ and

$$F = E^G \text{ is true.}$$

Now assume $k \geq 1$, and $p(x) = p_1(x) \cdots p_r(x)$ irreducible separable factors in $F[x]$.

$$\deg(p_1) = s \geq 2.$$

As E is splitting field of $p(x)$, it contains s <u>distinct</u> roots of $p_1(x)$, say $\alpha_1, \ldots, \alpha_s$. Let σ_i denote the iso. of subfields

$$\begin{tikzcd} F(\alpha_1) \arrow[r, phantom, "\simeq"] \arrow[rr, bend right, "\sigma_i"', "\cong"] & F[T]/p_1(T) \arrow[r, phantom, "\simeq"] & F(\alpha_i) \end{tikzcd} \quad (1 \leq i \leq s)$$

And by induction $E/F(\alpha_i)$ is Galois. (= splitting extn. of same $p(x)$; except now there are fewer roots outside of $F(\alpha_i)$)

By our uniqueness theorem of splitting extn. (Thm 28.1 page 2) each σ_i extends

$$\begin{tikzcd} E \arrow[r, "\sim", "\sigma_i"'] \arrow[d, dash] & E \arrow[d, dash] \\ F(\alpha_1) \arrow[r, "\sigma_i"] \arrow[dr, dash] & F(\alpha_i) \arrow[d, dash] \\ & F \end{tikzcd}$$

Now, assume $\theta \in E^G$. Let $G_1 = Gal(E/F(\alpha_1)) \subset G$

Then $\theta \in E^{G_1}$ (because $E^G \subset E^{G_1}$)

As $E/F(\alpha_1)$ is a Galois extn., $\theta \in F(\alpha_1)$, i.e.

$$\theta = c_0 + c_1\alpha_1 + \dots + c_{s-1}\alpha_1^{s-1} \in F(\alpha_1) \simeq F[T]/p_1(T)$$

Apply σ_i to get $\theta = c_0 + c_1\alpha_i + \dots + c_{s-1}\alpha_i^{s-1}$

i.e. $\{\alpha_1, \dots, \alpha_s\}$ are distinct roots of a degree $s-1$ polynomial

$$c_{s-1}X^{s-1} + \dots + c_1 X + c_0 - \theta = 0 \quad (\text{in } F[x])$$

$\Rightarrow$ this polynomial is zero $\therefore$ hence $\theta = c_0 \in F$ as we wanted.

$\square$