Lecture 30

(30.0) Recall: a few definitions and results proved so far. Let E/F be an algebraic extension and $G = \mathrm{Gal}(E/F)$

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

- E/F is a Galois extn. if $E^G = F$ (i.e. $\sigma(a) = a \ \forall \sigma \in G \Rightarrow a \in F$)
- E/F is normal if $\forall\, \alpha \in E$, the min'l poly $f_\alpha(x) \in F[x]$ splits into a product of linear factors in $E[x]$.
- E/F is separable if $\forall\, \alpha \in E$, the min'l poly. $f_\alpha(x) \in F[x]$ is separable, i.e. has $\deg f_\alpha$ <u>distinct</u> roots in the splitting extn. of $f_\alpha(x)$ over F.

Last time we proved (Thm. 29.6, page 6) that:

E/F Galois extn. $\Rightarrow$ E/F is normal and separable.

Now we will prove its converse. For this, it is important to understand normal extensions better.

(30.1) Let E/F be a normal extension (hence algebraic, by our definition). If E/F is finite, we will have

E = splitting extension of some $p(x) \in F[x]$

(see Lemma 29.7, page 8. The idea was to take min'l polynomials of a basis $\{\omega_1, \dots, \omega_n\}$ of E/F.)

The same idea proves that E/F is always (finite or not) a splitting extension of a set of polynomials $\mathcal{P} \subset F[x]$.

Definition. – Let $\mathcal{P} \subset F[x]$ be a set of (monic) polynomials and $\tilde{F}/F$ an extension. We say $\tilde{F}$ is a splitting extn. of $\mathcal{P}$ over F if

(1) $\forall\, f(x) \in \mathcal{P}$, $f(x) = (x-\alpha_1)\dots(x-\alpha_n)$ in $\tilde{F}[x]$

(2) Let $S = \{\alpha \in \tilde{F} \mid f(\alpha) = 0 \text{ for some } f \in \mathcal{P}\} \subset \tilde{F}$

Then $\tilde{F} = F(S)$

Note. When $|\mathcal{P}| < \infty$, may replace it by a single polynomial

$p(x)$ = product of all $f(x) \in \mathcal{P}$.

Thus we have the following

Lemma. E/F normal $\Rightarrow$ E = splitting extension of some subset $\mathcal{P} \subset F[x]$.

(30.2) Theorem. (1) Given any subset $\mathcal{P} \subset F[x]$, there exists a splitting extension of $\mathcal{P}$ over F.

(2) Let F_1, F_2 be two fields, $\sigma : F_1 \xrightarrow{\sim} F_2$ a field iso., $\mathcal{P}_\ell \subset F_\ell[x]$, $\ell = 1,2$, such that $\mathcal{P}_2 = \{\sigma(f(x)) \mid f(x) \in \mathcal{P}_1\}$.

Let E_ℓ = splitting extn. of $\mathcal{P}_\ell$ over F_ℓ $(\ell = 1,2)$.

Then σ extends to an iso. $\sigma : E_1 \xrightarrow{\sim} E_2$.

Remark. When $\mathcal{P}$ is finite, we may assume it is singleton, and this theorem is already proved. (Thms. 27.4, p.4; 28.1 p.2).

We give an alternate proof below, which depends only on Theorems 26.6, 26.7 page 7 – (existence of a single root, and uniqueness of adjoining such a root).

(30.3) Proof of (2) (of Thm (30.2)). Let $\mathcal{S}$ = set of all subextns. $\begin{matrix} E_1 \\ | \\ K_1 \\ | \\ F_1 \end{matrix}$ s.t. $\sigma : F_1 \xrightarrow{\sim} F_2$ extends to $\sigma : K_1 \xrightarrow{\sim} K_2 = (\sigma K_1) \subset E_2$.

Let K_1 be a max'l element of $\mathcal{S}$. The existence of (bad notation: say $\tilde{K}_1$)

such a maximal element is ensured by Zorn's lemma. Namely, we have to check that every totally ordered subset

$$K_1^{(1)} \hookrightarrow K_1^{(2)} \hookrightarrow \cdots \hookrightarrow K_1^{(n)} \hookrightarrow \cdots \quad \text{in } \mathcal{S}$$

(i.e. $K_1^{(1)} \subset K_1^{(2)} \subset \cdots \subset E_1$ are subextns. of E_1/F_1 and $\sigma : F_1 \xrightarrow{\sim} F_2$ extends to $\tau_j : K_1^{(j)} \hookrightarrow E_2$)

then is $\tilde{K}_1 \in \mathcal{S}$, larger than all $K_1^{(j)}$ $(j \geq 1)$. So, take $\tilde{K}_1 = \bigcup_{j \geq 1} K_1^{(j)}$ and set $\tau : \tilde{K}_1 \to E_2$ as τ_j on $K_1^{(j)}$.

Check: (easy!) $\tilde{K}_1 \hookrightarrow E_1$ is a subextn of E_1/F_1 and $\tau : \tilde{K}_1 \to E_2$ extends $\sigma : F_1 \xrightarrow{\sim} F_2$.

Now, let $\tilde{K}_1$ be a max'l element of $\mathcal{S}$. We claim that $\tilde{K}_1 = E_1$. If not, then exists some $\alpha \in E_1$, $f(\alpha) = 0$ for some $f \in \mathcal{P}_1$, such that $\alpha \notin \tilde{K}_1$. Viewing $f(x) \in F_1[x]$ as a polynomial in $\tilde{K}_1[x]$, it has an irreducible factor of deg ≥ 2 whose root is α (namely min'l poly of $\alpha \in E_1$ over $\tilde{K}_1$), say $\tilde{f}_\alpha(x) \in \tilde{K}_1[x]$.

Let $\tilde{K}_2 \subset E_2$ be the image of $\tau : \tilde{K}_1 \longrightarrow E_2$.
Then $\tau(\tilde{f}_\alpha(x)) \in \tilde{K}_2[x]$ is irreducible and has a root, say β, in E_2. By Theorem 26.7, page 7, we have an iso. extending τ, $\tilde{K}_1(\alpha) \xrightarrow{\sim} \tilde{K}_2(\beta)$. This contradicts maximality of $\tilde{K}_1$. □

(30.4) The existence part (1) of Thm (30.2) is exactly as hard as proving the algebraic closure of a field. We begin by

Prop. Let $\mathcal{P} \subset F[x]$ be a set of polynomials. Then there exists an extn. F_1/F s.t. $\forall f(x) \in \mathcal{P}$, $\exists\, \alpha \in F_1$ s.t. $f(\alpha) = 0$.

Proof. - (Artin.) - Let $R = F[T_f : f \in \mathcal{P}]$
polynomial ring in as many variables as the set $\mathcal{P}$.

$\mathfrak{a}$ = ideal generated by $f(T_f) : f \in \mathcal{P}$

Claim. $\mathfrak{a} \subset R$ is proper. (i.e., $1 \notin \mathfrak{a}$)

If the claim is true, let $\mathfrak{m} \subset R$ be a max'l ideal containing

$\mathfrak{o}$, and let $F_1 = R/\mathfrak{m}$. For every $f \in \mathfrak{p}$, the image

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/\mathfrak{m} \quad \text{(natural projection)} \\ \rotatebox{90}{$\in$} & & \\ T_f & \longmapsto & \pi(T_f) =: \alpha_f \end{array}$$

α_f of T_f satisfies $f(\alpha_f) = 0$. (since $f(T_f) \in \mathfrak{o} \subset \mathfrak{m}$)

Proof of the claim. — If $1 \in \mathfrak{o}$, we must have

$$g_1 f_1(T_{f_1}) + \dots + g_N f_N(T_{f_N}) = 1 \quad \text{for some } g_1, \dots, g_N \in R$$

Let us list the variables appearing in the relation above, as $Y_1, \dots, Y_M$; when $Y_i = T_{f_i}$ $(i = 1, \dots, N)$ $(N \le M)$. Then $(\mathcal{Y} = \{Y_1, \dots, Y_M\})$

$$g_1(\mathcal{Y}) f_1(Y_1) + \dots + g_N(\mathcal{Y}) f_N(Y_N) = 1. \text{ in } F[Y_1, \dots, Y_M].$$

As finite splitting extns. exist, take $\tilde{F}$ = splitting extn. of $\{f_1, \dots, f_N\}$ over F, let $\alpha_1, \dots, \alpha_N$ be roots of $f_1, \dots, f_N$ resp.

Specializing $Y_j = \alpha_j$ $(1 \le j \le N)$, yields $0 = 1$ - contradiction.

□

(30.5) Definition. A field K is said to be algebraically closed if $\forall$ $\begin{matrix} L \\ | \\ K \end{matrix}$ algebraic extn, $L = K$.

(In other words, every irreducible $f(x) \in K[x]$ is of degree 1.)

Corollary of Prop. (30.4). For every field F, there exists an algebraic extn. $\overline{F}/F$ s.t. $\overline{F}$ is algebraically closed.

Proof Inductively define: $F_0 = F$

F_{j+1} = a field where every $f(x) \in F_j[x]$ has a root.

(take $\mathcal{P} = F_j[x]$ in Prop. 30.4)

$\overline{F} = \bigcup_{j \geq 0} F_j$ is a field. It is algebraically closed, since

$\forall$ irred $f(x) \in \overline{F}[x]$, then exists $l \geq 1$ s.t. $f(x) \in F_l[x]$

(finitely many coeff.)

but then $\exists\ \alpha \in F_{l+1} \subset \overline{F}$ s.t. $f(\alpha) = 0$; i.e. $x - \alpha$ divides $f(x)$. Irreducibility of $f(x) \Rightarrow f(x) = c \cdot (x - \alpha)$. □

(30.6) Proof of Theorem (30.2) part (1). Take $E =$ smallest subfield of $\overline{F}$, containing F and $\{\alpha \in \overline{F} \mid f(\alpha) = 0$ for some $f \in \mathcal{P}\}$.