Lecture 31

(31.0) Recall – last time we proved the existence and uniqueness of the splitting field of a set $\mathcal{P}$ of monic polynomials. Today we will state and prove several consequences of the results proved so far.

(31.1) Algebraic closure. – see (30.5) page 7.

Let F be a field and $\overline{F}/F$ – an algebraic extn. such that $\overline{F}$ is algebraically closed.

Lemma (1) Let F_1 be the splitting extn. of $\mathcal{P} = F[x]$. Then $F_1 = \overline{F}$. (uniqueness of $\overline{F}$ follows.)

(2) Let k_1 and k_2 be two fields, K_1/k_1 an algebraic extn, $\sigma : k_1 \xrightarrow{\sim} k_2$ an iso. of fields. Then σ extends to a morphism of fields $K_1 \longrightarrow \overline{k_2}$.

Proof. (1) Clearly $F_1 \subset \overline{F}$. Conversely for any $\alpha \in \overline{F}$, let $f_\alpha(x) \in F[x] (\in \mathcal{P})$ be the min'l polynomial of α. Then $f_\alpha(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ in $F_1[x]$

(i.e. $\alpha_1, \ldots, \alpha_n \in F_1$)

$f_\alpha(\alpha) = 0 \Rightarrow \alpha = \alpha_j$ for some j, hence $\alpha \in F_1$ $\square$

A few words of clarification. $\overline{F}/F$ is an algebraic extension s.t. $\overline{F}$ is algebraically closed, i.e. irreducible polynomials of $\overline{F}[x]$ all have degree 1.

Thus $\forall\, f(x) \in F[x]$, the factorization of $f(x)$ into irreducible factors (in $\overline{F}[x]$) implies that $f(x)$ = a product of linear factors in $\overline{F}[x]$. Thus the splitting extension of any set $\mathcal{P} \subset F[x]$ can be viewed as a sub-extension of $\overline{F}/F$.

(2). The argument is exactly the same as that from (30.3) page 4. (extend σ as much as possible, using Zorn's lemma, maximal such prolongation of σ exists. Get a contradiction if max'l $\neq K_1$. One can argue by induction as well if K_1/k_1 is finite.)

$\square$

(31.2) Why the word "normal"?

Proposition.– Let E/F be an algebraic extension. Then the following are equivalent:

(1) E/F is normal

(2) E = splitting extn. of a set of polynomials $P \subset F[x]$.

(3) $\forall\ K/E$ and $\sigma \in Gal(K/F)$, $\sigma(E) = E$

(i.e. $\sigma(\alpha) \in E\ \forall \alpha \in E$, NOT that $\sigma = Id_E$)

(4) $\forall\ \sigma \in Gal(\bar{F}/F)$, $\sigma(E) = E$.

Remark. (3) means we have a group homomorphism

$$Gal(K/F) \longrightarrow Gal(E/F)$$

Its kernel is clearly $Gal(K/E)$, hence a normal subgp. of $Gal(K/F)$.

Proof. We already know (1) $\Rightarrow$ (2) Lemma 30.1 page ~~4~~. 3.

(3) $\Rightarrow$ (4) follows from viewing E as a subfield of $\bar{F}$ and setting $K = \bar{F}$.

(2) $\Rightarrow$ (3). For any K/E, and $\sigma \in Gal(K/F)$; σ must act as an automorphism of

$$S = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some } f \in F[x]\}$$

Since S generates E over F, the assertion follows.

(4) $\Rightarrow$ (1). Now assume we have $F \subset E \subset \overline{F}$

s.t. $\forall \sigma \in Gal(\overline{F}/F) \left(= \{\overline{F} \xrightarrow[\psi]{\sim} \overline{F} \mid \psi(a) = a \ \forall a \in F\}\right)$

$\sigma(E) = E$. We want to prove that E is normal.

So let $\alpha \in E$ and let $f(x) = f_\alpha(x) \in F[x]$ be its

min'l polynomial. Assume that $f_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_r)$ in $\overline{F}[x]$.

($f_\alpha(\alpha) = 0 \Rightarrow \alpha = \alpha_j$ for some j
say $\alpha = \alpha_1$)

To prove : $\alpha_i \in E \ \forall\, 1 \le i \le r$

If not, say $\beta = \alpha_i \notin E$. We get an iso.
(some $1 < i \le r$)

$\sigma : F(\alpha) \longrightarrow F(\beta)$ (since α & β have the same min'l poly.)

Now $F(\alpha) \subset E \subset \overline{F}$ and $F(\beta) \subset \overline{F}$. Using lemma (31.1)(2) page 1 above; σ extends to a field $\overset{\text{iso}}{\text{morphism}}$ $\overline{F} \xrightarrow{\sim} \overline{F}$

[Homework: $\tilde{F}/F$ algebraic $\sigma : \tilde{F} \longrightarrow \tilde{F}$ field morphism s.t.
$\sigma(x) = x \ \forall x \in F$. Then σ is an iso.]

But $\sigma(\alpha) = \beta \notin E$. Contradiction. $\square$

(31.3) Thm E/F normal and separable, implies (iff)

E/F is Galois

Pf. Assume E/F is a normal and separable extn. Let $\alpha \in E$, $\alpha \notin F$, and let $f_\alpha(x) \in F[x]$ be its min'l polynomial. In $E[x]$, $f_\alpha(x)$ has at least 2 distinct roots, $\alpha \neq \beta$.
(so $\deg \geq 2$)

So we get $F(\alpha) \xrightarrow{\sim} F(\beta)$. Extend to $\overline{F} \xrightarrow[\sigma]{\sim} \overline{F}$. Since E/F is normal, $\sigma(E) = E$ $\Rightarrow$ $\exists\, \sigma \in \mathcal{G}al(E/F)$ s.t. $\sigma(\alpha) = \beta \neq \alpha$
$\Rightarrow \alpha \notin E^G$. $\square$

(31.4) Example. E any field. $G \underset{\text{fields}}{\overset{\text{finite subgp.}}{\subset}} \mathrm{Aut}(E)$. $F = E^G$ is Galois, by definition. $(E:F) = |G|$ by Artin's Thm.

e.g. $E = \mathbb{Q}(X_1, \ldots, X_N)$

$G = S_N \hookrightarrow \underset{\text{fields}}{\mathrm{Aut}}(E)$, $F = E^G$

$\mathcal{G}al(E/F) = S_N$ (permutations on N letters).