Lecture 28

(28.0) Recall: for a field F and a polynomial $p(x)$, an extension

E / F is said to be a splitting field of $p(x)$ over F if

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

(2) $E = F(\alpha_1, \ldots, \alpha_n)$

We assumed that $p(x)$ is monic of degree $n \geq 1$. Last time we proved the existence of a splitting field of a polynomial exists.

Heuristically, the argument goes as follows:

- Write $p(x) = p_1(x)\cdots p_r(x)$ as a product of monic irreducible polynomials. We may assume that $\deg(p_i) > 1$ for every $1 \leq i \leq r$. This is because of the following observation.

Observation. – If $p(x) = (x-a_1)\cdots(x-a_j)\underbrace{p_{j+1}(x)\cdots p_r(x)}_{q(x)}$ ($\deg(p_i) \geq 2$ $\forall\, j+1 \leq i \leq r$)

Then a splitting field E / F of $q(x)$ is also a splitting field of $p(x)$.

- Set $E_1 = F[x]/_{p_1(x)}$. There is $\alpha \in E_1$ s.t. $p_1(\alpha) = 0$ (and $E_1 = F(\alpha)$)

i.e. $p_1(x) = (x-\alpha)\cdot q_1(x)$

Use the observation to replace $p(x)$ by $q(x)$ of strictly smaller

degree (over E_1). Use induction to find a splitting field of $q(x)$ over E_1, say $\begin{matrix} E \\ | \\ E_1 \end{matrix}$. Then E is a splitting field of $p(x)$ over F.

(28.1) Uniqueness of splitting field.

Theorem. Let F_1, F_2 be two fields, and $\sigma: F_1 \xrightarrow{\sim} F_2$ an iso. of fields. Let $p(x) \in F_1[x]$ and $q(x) = \sigma(p(x)) \in F_2[x]$. Let $\begin{matrix} E_1 \\ | \\ F_1 \end{matrix}$ be a splitting field of $p(x)$ over F_1 and $\begin{matrix} E_2 \\ | \\ F_2 \end{matrix}$ be a splitting field of $q(x)$ over F_2.

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

Proof. We proceed by induction on k = number of roots of $p(x)$ (in $E_1[x]$) which are not in F_1.

$k = 0$. $p(x) = (x - a_1) \cdots (x - a_n)$ in $F_1[x]$

$q(x) = (x - \sigma(a_1)) \cdots (x - \sigma(a_n))$ in $F_2[x]$

$\Rightarrow$ $E_1 = F_1 \xrightarrow[\sigma]{\sim} F_2 = E_2$.

Now write $p(x) = p_1(x) \cdots p_r(x)$ in $F_1[x]$

(monic irreducible poly. $p_1, \cdots, p_r$)

Assume $\deg(p_1) \geq 2$.

(one of the factors must have degree ≥ 2 otherwise we are back to $k=0$ case which has already been proved.)

Apply σ : $q(x) = q_1(x) \cdots q_r(x)$ where $q_i(x) = \sigma(p_i(x))$.

By Thm (26.7) page 7, if $\alpha \in E_1$ is a root of $p_1(x)$ and $\beta \in E_2$ is a root of $q_1(x)$, then σ extends to an iso of fields

$$\sigma_1 : F_1(\alpha) \xrightarrow{\sim} F_2(\beta)$$

Now we have $< k$ roots of $p(x)$ which are not in $F_1(\alpha)$.

By induction. σ_1 extends to a field iso.

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim} & E_2 \\ | & & | \\ F_1(\alpha) & \xrightarrow{\sim} & F_2(\beta) \\ | & & | \\ F_1 & \xrightarrow{\sim} & F_2 \end{array}$$

□

(28.2) A few words on homomorphisms of fields.

Let k and K be two fields. $\mathrm{Hom}_{\text{fields}}(k, K) \ni \varphi$

if $\varphi : k \to K$ satisfies $\varphi(0) = 0$, $\varphi(1) = 1$ and φ is a ring hom

($\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$)

Since $\ker(\varphi) \subset k$ is an ideal (proper; $1 \notin \ker(\varphi)$)

and k is a field, $\ker(\varphi) = 0$, i.e. $\varphi : k \hookrightarrow K$.

Hence, either $\operatorname{Hom}_{\text{fields}}(k, K) = \phi$ (e.g. $k = \mathbb{Z}/p\mathbb{Z}$, $K = \mathbb{Q}$)

or every element of $\operatorname{Hom}_{\text{fields}}(k, K)$ realizes k as a subfield of K.

e.g. $k = \mathbb{Q}[T]/(T^3 - 2)$ $\qquad K = \mathbb{C}$

$\operatorname{Hom}_{\text{fields}}(k, K)$ has 3 elements.

$T \longmapsto 2^{\frac{1}{3}}$ or $2^{\frac{1}{3}}\omega$ or $2^{\frac{1}{3}}\omega^2$

$\left(\omega = e^{2\pi\sqrt{-1}/3} \in \mathbb{C}\right)$

(28.3) Theorem (Dedekind) Let G be a group and K be a field. Let $S = \{\sigma_1, \ldots, \sigma_n\}$ be a finite set of distinct group homomorphisms

$\sigma_j : G \longrightarrow K^\times$ (= mult. gp. of non-zero elements of K)

Then S is linearly independent over K

That is, for $a_1, \dots, a_n \in K$ s.t.

$$a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0 \quad \forall\, x \in G$$

we have $a_1 = \dots = a_n = 0$. In other words, $S \subset \underset{\text{gps}}{\mathrm{Hom}}(G, K^\times)$

$$\cap$$

has a structure of K-vector space $\longrightarrow \underset{\text{sets}}{\mathrm{Hom}}(G, K)$

$S \subset \underset{\text{sets}}{\mathrm{Hom}}(G, K)$ is linearly independent.

(any finite $S \subset \underset{\text{gps}}{\mathrm{Hom}}(G, K^\times)$)

$\underset{\text{gps}}{\mathrm{Hom}}(G, K^\times)$ * is often called the group of characters of G (valued in K).

(28.4) A non-trivial bound as a consequence of Thm 28.3.

Let K and L be two fields, and assume that $\underset{\text{fields}}{\mathrm{Hom}}(K, L) \neq \phi$. Let $S \subset \underset{\text{fields}}{\mathrm{Hom}}(K, L)$ be a finite set $(S = \{\sigma_1, \dots, \sigma_n\})$. Define

$$k = \{\alpha \in K \mid \sigma_1(\alpha) = \dots = \sigma_n(\alpha) (=: i(\alpha) \in L)\}$$

Theorem. (i) k is a field

(ii) $(K : k) \geq n$

Proof. (i) is obvious since each σ_j is a morphism of fields.

(ii) Take $G = K^\times$ and view S as a finite set of group homomorphisms $G \longrightarrow L^\times$. Theorem (28.3) implies that $S \subset \underset{k\text{-v.s.}}{\mathrm{Hom}}(K, L)$ ← viewed as L-vector space is linearly ~~is~~ independent (over L).

$$\dim_{L\text{-v.s.}} \left(\mathrm{Hom}_k(K, L) \right) = \dim_{k\text{-v.s.}} K = (K : k)$$

↑ fun exercise!

$$|S| = n \leq \dim_{L\text{-v.s.}} \left(\mathrm{Hom}_k(K, L) \right) = (K : k) \qquad \square$$

(28.5) **Example.** (1) $K = \mathbb{Q}[T]/_{T^3 - 2}$ $\qquad L = \mathbb{C}$

$$S = \{\sigma_1, \sigma_2, \sigma_3\} = \underset{\text{fields}}{\mathrm{Hom}}(K, L)$$

ess; not five.

$k = \mathbb{Q}$ and $(K : k) = 3 = |S|$

(28.6) Proof of Dedekind's theorem.

$\sigma_1, \ldots, \sigma_n : G \longrightarrow K^\times$ distinct gp. homs.

We will show, by induction on n, that $\{\sigma_1, \ldots, \sigma_n\}$ is linearly independent (over K).

$n = 1$. $\quad a \cdot \sigma(x) = 0 \ \forall x \in G \implies a \cdot \sigma(e) = 0$ (identity elt. of G)

But $\sigma(e) = 1 \implies a = 0$.

Now assume that every subset of $\mathrm{Hom}_{\text{gps}}(G, K^\times)$, of size $< n$, is linearly independent (as a subset of the K-v.s. $\mathrm{Hom}_{\text{sets}}(G, K)$).

Assume there exist $a_1, \ldots, a_n \in K$; not all zero,

s.t. $\quad a_1\sigma_1(x) + \ldots + a_n\sigma_n(x) = 0 \quad \forall x \in G. \quad - (*)$

Note that we may assume $a_i \neq 0 \ \forall 1 \leq i \leq n$; because otherwise we will have a non-trivial dependence relation among $< n$ elements of $\mathrm{Hom}_{\text{gps}}(G, K^\times)$.

~~Divide by a_n~~

Let $\alpha \in G$ be such that $\sigma_1(\alpha) \neq \sigma_n(\alpha)$.

$(*)$ for $x = y \Rightarrow a_1\sigma_1(y) + \dots + a_n\sigma_n(y) = 0$

$(*)$ for $x = \alpha \cdot y \Rightarrow a_1\sigma_1(\alpha)\sigma_1(y) + \dots + a_n\sigma_n(\alpha)\sigma_n(y) = 0$

Multiply the first eq^n by $\sigma_n(\alpha)$ and subtract from the second to get

$$a_1\left(\sigma_1(\alpha) - \sigma_n(\alpha)\right)\sigma_1(y) + \dots + a_{n-1}\left(\sigma_{n-1}(\alpha) - \sigma_n(\alpha)\right)\sigma_{n-1}(y) = 0 \quad \forall\, y \in G$$

This is a <u>non-trivial</u> dependence rel^n among $\{\sigma_1, \dots, \sigma_{n-1}\}$

↑ because $a_1 \neq 0$, $\sigma_1(\alpha) \neq \sigma_n(\alpha)$

Contradiction!

□