# Lecture 27

(27.0) A little review of $R = K[x]$ where $K$ is a field.

(i) $\forall\ f, g \in K[x]$, $\deg(f) \geq 1$ ; the division algorithm of polynomials gives $g = q \cdot f + r$ with $\deg(r) < \deg(f)$. (unique such expression)

(ii) Given an ideal $\mathfrak{a} \subset K[x]$, if $\mathfrak{a} \neq (0)$, choose $f \in \mathfrak{a}$ of smallest degree. Then (i) implies that $\mathfrak{a} = (f)$.

(iii) A polynomial $f(x) \in K[x]$ is said to be <u>irreducible</u> if

$$f = f_1 \cdot f_2 \Rightarrow f_1 \in K^\times \ (= K \setminus \{0\}) \text{ or } f_2 \in K^\times$$

(iv) Every polynomial can be written as a product of irreducible ones. Such expression is unique up to reordering the factors, or scaling by elements of $K^\times$.

(v) If $\mathfrak{p} \subset K[x]$ is a prime ideal then either $\mathfrak{p} = (0)$ or $\mathfrak{p} = (f)$ for an irreducible polynomial $f$.

[ if $f = f_1 \cdot f_2$ where $\deg(f_2) \geq 1$ and hence $\deg(f_2) < \deg(f)$ then either $f_1$ or $f_2$ is in $\mathfrak{p}$, because $\mathfrak{p}$ is prime. This contradicts the choice of $f$ so that $\mathfrak{p} = (f)$ ]

(vi) $\mathfrak{p} \subset K[x]$ prime, $\mathfrak{p} \neq (0)$ implies $\mathfrak{p}$ is maximal.

[ As $\mathfrak{p} = (f)$ for an irred. $f$, assuming $\mathfrak{p} \subset \mathfrak{a} = (g)$ we have $f \in (g) \Rightarrow \exists\ h \in K[x]$ s.t. $f = g \cdot h$

As $f$ is irreducible, either $g \in K^\times$ ($\Rightarrow \mathcal{O}_L = K[x]$)
or $h \in K^\times$ ($\Rightarrow \mathcal{O}_L = \mathfrak{p}$). Hence $\mathfrak{p}$ is max'l. ]

(27.1) Last time we introduced the following notions.

- Field extension: $F \subset E$; or $E/F$; $\begin{matrix} E \\ | \\ F \end{matrix}$ means $E$ is a field and $F$ is a subfield.
- $(E : F)$ = dimension of $E$ as an $F$ vector space.
- Let $\alpha \in E$. Consider $ev_\alpha : F[x] \longrightarrow E$. $\ker(ev_\alpha) = I_\alpha$ is a <u>prime ideal</u> of $F[x]$ since $F[x]/I_\alpha \xhookrightarrow{ev_\alpha} E$ and hence $F[x]/I_\alpha$ is an integral domain (subring of a field).

Case 1. $I_\alpha = (0)$. In this case $\alpha$ is <u>transcendental</u> over $F$ and we get $ev_\alpha : F[x] \xhookrightarrow{\text{(U.P. of localization)}} F(x) \hookrightarrow E$ whose image is the smallest subfield of $E$ containing $F$ and $\alpha$.

Case 2. $I_\alpha = (f_\alpha)$. $f_\alpha$ is then (assumed to be monic) irreducible and $I_\alpha$ is a max'l ideal.

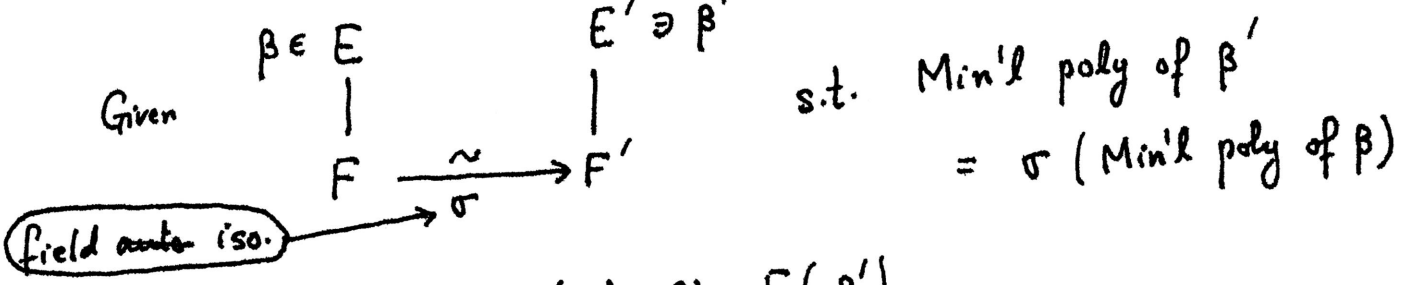
- $\alpha$ is said to be algebraic over $F$
- $f_\alpha$ is called the minimal polynomial of $\alpha$.
- $F[x]/(f_\alpha)$ is a field contained in $E$

- $F[\alpha] = F(\alpha) \cong F[x]/(f_\alpha)$ is of dimension equal to degree of $f_\alpha$ ; as an $F$-vector space.

(27.2) Recall that we proved (Lecture 26 page 7)

1. Kronecker's Thm. Given $f(x) \in F[x]$, $\deg(f) \geq 1$, we can find a field $E/F$ and $\alpha \in E$ such that $f(\alpha) = 0$.

2. Minimal polynomial determines extension !




$\sigma$ extends to $F(\beta) \xrightarrow{\sim} F(\beta')$.

(27.3) Example. $F = \mathbb{Q}$, $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible (Check this).

$$F[x]/(x^3-2) \simeq \mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\sqrt[3]{2} \cdot \omega) \quad \text{where } \omega = e^{\frac{2\pi i}{3}}.$$

Degree 3 extension of $\mathbb{Q}$.

Let $E \subset \mathbb{C}$ be the smallest subfield containing $\mathbb{Q}$ and 3 roots of $x^3 - 2 = 0$, namely $2^{\frac{1}{3}}$. $2^{\frac{1}{3}} \cdot \omega$, $2^{\frac{1}{3}} \omega^2$

Thus $\omega \in E$, $2^{\frac{1}{3}} \in E$ etc.

$(E : \mathbb{Q}) = 6$. This is because $E = \mathbb{Q}(2^{\frac{1}{3}}, \omega)$

Min'l poly of $\omega$ (over $\mathbb{Q}$) is $x^2 + x + 1 = 0$

$$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(2^{\frac{1}{3}}, \omega) = E$$

deg 2 deg 3 (Check: $x^3 - 2$ is still irred. as a polynomial in $\mathbb{Q}(\omega)[x]$)

(27.4) Splitting extension of a polynomial. f is assumed to be monic

Let $F$ be a field, $f(x) \in F[x]$, $\deg(f) \geq 1$. An extension

$E$
$|$
$F$ is said to be a splitting extension (of $f$ over $F$) if

(i) $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $E[x]$

here $n = \deg(f)$.

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

Theorem. Let $p(x) \in F[x]$ be a monic polynomial. Then there exists a splitting field $E$ (of $p(x)$ over $F$).

Proof. Let us write $p(x)$ as a product of irreducible (monic)

polynomials : $p(x) = f_1(x) \cdots f_r(x)$

Let $n$ = degree of $p(x)$. So that $r \leq n$ and we argue by induction on $n-r$.

Base case. $n-r = 0$ means each $f_i(x) = x - a_i$ is of degree 1.

Take $E = F$ in this case.

Now if $n-r \geq 1$, there must be an irreducible factor of degree $> 1$. We may assume, after relabelling, that it is $f_1$, i.e.

$\deg(f_1) \geq 2$. Using Kronecker's theorem, there exists

$$\begin{array}{c} F_1 \\ | \\ F \end{array} \quad , \quad \alpha_1 \in F_1 \quad \text{s.t.} \quad f_1(\alpha_1) = 0.$$

That is, in $F_1[x]$,

$$f_1(x) = (x - \alpha_1) \cdot g_1(x) \; .$$

We will take $F_1 = F(\alpha_1)$.

Hence, $p(x)$, viewed as a polynomial in $F_1[x]$ has strictly larger number of irreducible factors. ~~than~~ By induction, there exist

$$\begin{array}{c} E \\ | \\ F_1 \end{array} \quad \text{s.t.} \quad \begin{array}{l} E = F_1(\beta_1, \cdots, \beta_n) \\ p(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n) \text{ in } E[x]. \end{array}$$

As $p(\alpha_1) = 0$, one of $\beta_n$'s must equal $\alpha_1$, say $\beta_1$.

Then $E = F_1(\beta_2, \cdots, \beta_n) = F(\alpha_1, \beta_2, \cdots, \beta_n)$

i.e. $E$ is a splitting field of $p(x)$ over $F$. $\square$