Lec 15 2/12/2021

Fields.

Examples –

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ p prime.

From rings, we get other examples by –

- if R is an integral domain, taking its field of fractions K.

  e.g. $R = F[x]$, F a field, field of fractions is $F(x)$

- if R is commutative, m max ideal then R/m is a field.

Ex. F a field, $R = F[x]$. R is a PID, so max ideal are (f) where f is irreducible. If $\deg f = n$ Then $F[x]/(f) = K$ is a field and $\theta : F \longrightarrow F[x]/(f)$

$a \longmapsto a + (f)$

is an injective homomorphism.

Identifying F with $\theta(F) \cong F$

and think of $F \subseteq K$.

Also, K is an F-vector space.

and $\bar{1} + (f), \bar{x} + (f), \ldots, \bar{x}^{n-1} + (f)$

form an F-basis of K.

(if $h \in F[x]$, $h = fq + r$

$\deg r < \deg f = n$.

$h + (f) = \underline{r} + (f)$

<u>Ex.</u> $\frac{\mathbb{R}[x]}{(x^2+1)}$ is a field,

and $\frac{\mathbb{R}[x]}{(x^2+1)} \longrightarrow \mathbb{C}$

$f \longmapsto f(i)$ is an $\cong$.

We could define $\mathbb{C}$ as $\dfrac{\mathbb{R}[x]}{(x^2+1)}$.

Ex. $\dfrac{\mathbb{Q}[x]}{(x^2-D)} \cong \mathbb{Q}(\sqrt{D})$ D squarefree

$= \{a+b\sqrt{D} \mid a, b \in \mathbb{Q}\}$

which is a field. $\subseteq \mathbb{C}$.

Def. A field extension is an inclusion of fields $F \subseteq K$. K is a v.s. over F and we define the degree of the extension as $\dim_F K = [K:F]$.

We also write K/F for the extension. "K over F".

Ex. if f irr. in $F[x]$, $K = F[x]/(f)$ is a field and $F \subseteq K$ is a field extension. $[K:F] = \deg f$

Since $\{1+(f), \ldots, x^{n-1}+(f)\}$

is a basis of K over F.

Ex. $[\mathbb{C}:\mathbb{R}]=2$, $[\mathbb{Q}(\sqrt{D}):\mathbb{Q}]=2$ when D is squarefree.

Def. $F \subseteq K$ a field extension.

If $X \subseteq K$ is a subset,

$F(X)$ = subfield generated by X over F

= the intersection of all subfields of K containing X and F.

This is the unique smallest subfield of K containing F and X.

When $X=\{\alpha_1,\dots,\alpha_m\}$ we write $F(\alpha_1,\dots,\alpha_m)$ for $F(X)$.

$F(\alpha)$ is a simple extension of F

Ex. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$.

$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$.

Ex: $\mathbb{Q}(i) \subseteq \mathbb{C}$.

$\{a+bi \mid a, b \in \mathbb{Q}\}$

= field of fractions of $\mathbb{Z}[i]$.

Thm. $F \subseteq K$ a field extension, $\alpha \in K$.

There is a homomorphism

$$\phi : F[x] \longrightarrow F(\alpha) \subseteq K$$
$$f \longmapsto f(\alpha)$$

and either.

(i) $\ker \phi \neq 0$ then $\ker \phi = (f)$ where f is irreducible in $F[x]$ and

$$F(\alpha) \cong F[x]/(f). \quad [F(\alpha):F] = \deg f.$$

There is a unique monic f and we call it the minimal polynomial of α $\text{minpoly}_F(\alpha)$.

(ii) $\ker \phi = 0$. Then ϕ extends to an isomorphism $F(x) \longrightarrow F(\alpha)$

and $[F(\alpha) : F] = \infty$

Ex. With $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{Q}(\sqrt[3]{2})$ is in case 1,

where $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$

where x^3-2 is irreducible by Eisenstein.

Fact: $\mathbb{Q}(\pi)$ is in case 2, i.e.

π does not satisfy any poly in $\mathbb{Q}[x]$.

Pf. Assume case (i), so $\ker\phi \neq 0$

$$\phi : F[x] \longrightarrow F(\alpha) \subseteq K.$$
$$f \longmapsto f(\alpha).$$

1st $\cong$ thm says $F[x]/(\ker\phi) \cong \operatorname{im}\phi$.

$\operatorname{Im}\phi$ is a domain, so $\ker\phi$ is prime, so maximal ($F[x]$ a PID) so

$\ker\phi = (f)$ for an irreducible (f).

There is unique monic f.

So $F[x]/(f) \cong \operatorname{im}\phi$.

Now $\operatorname{im}\phi$ is a field and it contains F and α so $F(\alpha) \subseteq \operatorname{Im}\phi$.

Also $\operatorname{Im}\phi \subseteq F(\alpha)$

Since for $g \in F[x]$ $g = \sum a_i x^i$

$g(\alpha) = \sum a_i \alpha^i \subseteq F(\alpha)$.

So $\operatorname{Im} \phi = F(\alpha)$.

And since $F(\alpha) \cong F[x]/(f)$

$\dim_F F(\alpha) \cong \dim_F F[x]/(f) = \deg f$.

In case (ii),

$$\begin{aligned} \phi : F[x] &\longrightarrow F(\alpha) \\ f &\longmapsto f(\alpha) \end{aligned}$$

is injective ($\ker \phi = 0$)

Universal property of the localization says ϕ extends to

$$\begin{aligned} \tilde{\phi} : F(x) &\longrightarrow F(\alpha) \\ f/g &\longmapsto f(\alpha)/g(\alpha) \end{aligned}$$

(we need for $g \neq 0$ $g \in F[x]$, $\phi(g)$ is a unit in $F(\alpha)$)

$\operatorname{Im} \tilde{\phi}$ is a field ($\tilde{\phi}$ still injective)

So same argument as in (i) shows

$\operatorname{Im} \tilde{\phi} = F(\alpha)$.

Finally, $\dim_F F[x] = \infty$, so $\dim_F F(x) = \infty$. Then

$\dim_F F(\alpha) = \dim_F F(x) = \infty$.

<u>Rmk.</u> If $F \subseteq K$ and $\alpha_1, \dots, \alpha_n \in K$ then

$$F(\alpha_1, \dots, \alpha_n) = \underline{F(\alpha_1})(\alpha_2)(\alpha_3)\dots(\alpha_n)$$

<u>Ex.</u> $\mathbb{Q}(\sqrt{2}, i) = K$

(we always take this inside $\mathbb{C}$ if no larger field is mentioned)

What is degree $[K : \mathbb{Q}]$

(answer: 4 next time).

$K = \mathbb{Q}(\sqrt{2})(i)$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

$\text{minpoly}_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$

$[K : \mathbb{Q}(\sqrt{2})]$ = deg minpoly of i over $\mathbb{Q}(\sqrt{2})$ $\quad \text{minpoly}_{\mathbb{Q}(\sqrt{2})}(i)$

i satisfies $x^2+1 \in \mathbb{Q}(\sqrt{2})[x]$.

if this is not the min poly, then

$[K : \mathbb{Q}(\sqrt{2})] = 1$, so $i \in \mathbb{Q}(\sqrt{2})$.

which is false since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$.

So $[K : \mathbb{Q}(\sqrt{2})] = 2$.

Def. $F \subseteq K$, $\alpha \in K$ is *algebraic over F* if we are in case (i), i.e. $f(\alpha) = 0$ for some $f \in F[x]$.

Then $\text{minpoly}_F(\alpha)$ is the unique irreducible f s.t. $f(\alpha) = 0$.

Also the poly of minimal degree with α as a root.

Otherwise we are in case (ii) and α is transcendental over F.