Field Extensions §29

Recap: Let R be a commutative ring with unity. $N \subseteq R$ an ideal:

Def • N is maximal: if $\nexists\ N' \subsetneq R$ ideal s.t. $N \subsetneq N'$

• N is prime: $\forall\ a, b \in R$ if $ab \in N \Rightarrow a \in N$ or $b \in N$.

Thm
• N is maximal $\iff$ R/N is a field
• N is prime $\iff$ R/N is an integral domain

Cor
N max $\Rightarrow$ N prime

§ 27 Ideals in $F[x]$ F a field

Def 27.21 R commut. ring with unity and $a \in R$. The **principal ideal generated by a** is

$$\langle a \rangle = \{ ra \mid r \in R \}$$

N an ideal of R is **principal** if $N = \langle a \rangle$ for some $a \in R$

Ex 1) $R = \mathbb{Z}$ all ideals are $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ ⇒ principal.

2) $R = \mathbb{Z}[x]$ $N = \{ ax + b2 \mid a, b \in \mathbb{Z}[x] \} = \{ g(x) = a_d x^d + \dots + a_1 x + a_0 \mid a_0 \text{ even} \}$

if $N = \langle f(x) \rangle$, since $2 \in N$ $\deg f(x) = 0$ and $f(x) \mid 2$

$f(x) \neq 1$ if $f(x) = 2 \Rightarrow$ all coeff a_i of $g(x) \in N$ are even

$\Longrightarrow$ N is not principal.

Thm 27.24 Every ideal in $F[x]$ is principal for F a field.

Proof $N \subseteq F[x]$ an ideal. If $N = \{0\}$ then $N = \langle 0 \rangle$.

Otherwise take $0 \neq g(x) \in N$ with min degree.

- If $\deg(g) = 0$, then $g(x) = c \in F$ and is a unit in $F[x]$ so N contains a unit hence $N = F[x] = \langle 1 \rangle$.

- If $\deg(g) \geq 1$, for $f(x) \in N$ apply division alg:

$$f(x) = q(x) \cdot g(x) + r(x)$$

where $\deg(r) < \deg(g)$ but $r(x) \in N$ since $r(x) = \underset{\in N}{f(x)} + \underset{\in N}{q(x)} \cdot g(x) \Rightarrow r(x) = 0$ and $N = \langle g(x) \rangle$. $\square$

Thm 27.25 Max ideals of $F[x]$

An ideal $\langle p(x)\rangle \neq \{0\}$ of $F[x]$ is maximal $\iff$ $p(x)$ is irreducible / F.

Recall Irreducible / F $\Rightarrow$ $p(x) \neq \underset{\overset{\uparrow}{F[x]}}{f(x)}\,\underset{\overset{\uparrow}{F[x]}}{g(x)}$ $\quad 0 < \deg f < \deg p$.

Proof Suppose $\langle p(x)\rangle$ is maximal $\Rightarrow$ $\langle p(x)\rangle$ is prime.

so if $\langle p(x)\rangle = \langle f(x)g(x)\rangle \Rightarrow f(x)$ or $g(x) \in \langle p(x)\rangle$

but this is impossible if $0 < \deg f, \deg g < \deg p$. so

p is irreducible.

$\Leftarrow$ Suppose $p(x)$ is irreducible and consider $\langle p(x) \rangle \subsetneq N \subsetneq F[x]$. some some ideal N. Then $N = \langle g(x) \rangle$ since all ideals are principal.

But $p(x) \in N$ so $p(x) = f(x) \cdot g(x)$,

Since p is irred. $\deg(g) = 0$ or $\deg p(x)$.

- if $\deg g = 0$ $N = \langle g(x) \rangle = F[x]$
- if $\deg g = \deg p$ $f(x) = c \in F$ so $N = \langle p(x) \rangle$.

Hence $\langle p(x) \rangle$ is maximal $\square$

Recall: N is max $\iff$ $F[x]/N$ is a field.

Ex: 1) x^3+3x+2 is irreducible / $\mathbb{Z}_5$ $\Rightarrow$

$$\mathbb{Z}_5[x]/\underbrace{\langle x^3+3x+2\rangle}_{N=} = E \quad \text{is a field.}$$

Claim N has 5^3 cosets. $\{ f(x)+N \mid \deg f(x) \le 2,\ f \in \mathbb{Z}_5[x] \}$.

E is a field with 125 elts.

2) x^2-2 is irreducible $/\mathbb{Q} \Rightarrow E = \mathbb{Q}[x]/\langle x^2-2\rangle$ field.

Claim E contains a zero of x^2-2.

$x+\langle x^2-2\rangle \in E$ $\quad (x+\langle x^2-2\rangle)^2-2 = x^2+\langle x^2-2\rangle - 2$

$$= (x^2-2)+\langle x^2-2\rangle = \langle x^2-2\rangle = 0_{\text{in } E}.$$

Thm (Kronecker) For every non-constant $f(x) \in F[x]$ there is a field $E \supseteq F$ and $\alpha \in E$ s.t. $f(\alpha) = 0$ in E.

Rmk: Notice above $\mathbb{Q}[x]/\langle x^2-2\rangle = E$ contains a subfield $F' = \{a + \langle x^2-2\rangle \mid a \in \mathbb{Q}\} \cong \mathbb{Q}$.

$\psi : \mathbb{Q} \to F' \subseteq E \quad \psi(a) := a + \langle x^2 - 2\rangle$

ψ injective: $a + \langle x^2-2\rangle = a' + \langle x^2-2\rangle$

$\iff a - a' \in \langle x^2 - 2\rangle$

$a - a' = 0$ if its in ideal.

$\psi(a+b) = \psi(a) + \psi(b)$

$\psi(ab) = \psi(a)\psi(b)$

since coset add'n + mult'n are defined via representatives

Def A field E is an *extension* field of F if $F \subseteq E$.

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash] \\ \mathbb{R} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}
\qquad
\begin{tikzcd} & F(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\ F(x) \arrow[dr, dash] & & F(y) \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Proof By Thm 23.20 we can assume $f(x)$ is irred $/F$ (if not factor and find a zero of any irred. factor).

Since $f(x)$ is irred $\langle f(x) \rangle$ is a maximal ideal and hence $E = F[x]/\langle f(x) \rangle$ is a field.

Claim F can be identified with a subfield of E, i.e. $\psi : F \to E$ $\psi(a) := a + \langle f(x) \rangle$ is an injective homomorphism (see textbook for verification and ex above)

$\Rightarrow$ view E as an extension of F.

Claim $\alpha = x + \langle f(x) \rangle \in E$ is a zero of $f(x)$.

Suppose: $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

$f(\alpha) = a_0 + a_1(x + \langle f(x) \rangle) + \cdots + a_n (x + \langle f(x) \rangle)^n$

Compute w/ coset representative x

$$f(\alpha) = a_0 + a_1 x + \dots + a_n x^n + \langle f(x)\rangle$$
$$= f(x) + \langle f(x)\rangle \qquad f(x) \in \langle f(x)\rangle$$
$$= \langle f(x)\rangle = 0 \text{ in } E \Leftarrow \qquad \square$$

Ex x^2+1 is irreducible over $\mathbb{R}$ not over $\mathbb{C}$. $(\mathbb{R} \subseteq \mathbb{C})$

$\alpha = x + \langle x^2+1\rangle \in \dfrac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ is a zero

$\exists$ $\cong$ sending $\mathbb{R} \xrightarrow{id} \mathbb{R}$ and α to i.

also $i \in \mathbb{C}$ is a zero.

Algebraic & Transcendental Extensions

Def 29.6 $\alpha \in E \supseteq F$ is <u>algebraic / F</u> if $f(\alpha) = 0$ for some $f(x) \in F[x]$. Otherwise it is transcendental/F.

Ex $\sqrt{2} \in \mathbb{R}$ is algebraic / $\mathbb{Q}$. $i \in \mathbb{C}$ is algebraic / $\mathbb{R}$
$\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$ (HARD)

When $E = \mathbb{C}$, $F = \mathbb{Q}$ call α a <u>algebraic/transcendental number</u>

Recall evaluation homomorphism: $\varphi_a : F[x] \to F$ $a \in F$
$f(x) \mapsto f(a)$

For $F \subseteq E$
upgrade this to: $\varphi_\alpha : F[x] \to E$
$a \mapsto a$
$x \mapsto \alpha$

ie. $\varphi_\alpha(a_0 + a_1 x + \dots + a_n x^n)$
$= a_0 + a_1\alpha + \dots + a_n\alpha^n$.

Thm 29.12 Let $E \geq F$ then $\alpha \in E$ is transcendental $/F$ if and only if φ_α is injective.

Proof α is transcendental $\iff f(\alpha) \neq 0 \quad \forall f \in F[x]$

$\iff \varphi_\alpha(f(x)) \neq 0 \quad \forall f \in F[x]$

$\iff \varphi_\alpha$ is injective $\boxtimes$.

Thm 29.13 Let $E \geq F$ and suppose $\alpha \in E$ is algebraic over F. Then $\exists$ an irred polynomial $p(x) \in F[x]$ s.t. $p(\alpha) = 0$. Moreover, $p(x)$ is uniquely determined up to constant factor and has min degree among poly's in $F[x]$ with α as a zero.

Proof Idea: consider $\varphi_\alpha : F[x] \to E$ by above

Thm $\ker \varphi_\alpha \neq \{0\}$ moreover it must be a principal ideal $\ker \varphi_\alpha = \langle p(x) \rangle = \{ f(x) \mid f(\alpha) = 0 \}$.

Any generator of $\ker \varphi_\alpha$ can be taken as $p(x)$ $\square$.

convenient to take monic one: $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$.

Def 29.14 Let $F \subseteq E$ and $\alpha \in E$ algebraic / F.

the unique monic polynomial $p(x)$ from above is the irreducible polynomial of α over F.

denote it by $\operatorname{irr}(\alpha, F) \in F[x]$ and its degree by $\deg(\alpha, F)$.