Field Extensions §28

Recap: Let R be a commutative ring with unity.

$N \subseteq R$ an ideal:

Def • N is <u>maximal</u>: if $\nexists$ $N' \subsetneq R$ s.t. $N \subsetneq N$

• N is <u>prime</u>: if $\forall\, a,b \in R$ $ab \in N \Rightarrow$ either a or $b \in N$

Thm

• N is maximal $\Longleftrightarrow$ R/N is a field

• N is prime $\Longleftrightarrow$ R/N is an integral domain (no zero divisors)

Cor

N max $\Longrightarrow$ N prime.

§ 27 Ideals in $\underset{\parallel\, R}{F[x]}$ F a field

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

$$\underbrace{\langle a \rangle}_{\text{notation}} = \{ ra \mid r \in R \}$$

An ideal N is called principle if $N = \langle a \rangle$ for some $a \in R$.

Ex 1) $R = \mathbb{Z}$ every ideal is of the form $n\mathbb{Z} = \{ kn \mid k \in \mathbb{Z} \} = \langle n \rangle = \langle -n \rangle$

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

Does $N = \langle f(x) \rangle$? since $2 \in N$ if $\deg f(x) = 0 \Rightarrow f(x) = 2$

$\Rightarrow 2 \mid a_i \; \forall a_i \; \forall g(x) \in N$. [$x+2 \in N$ but $x+2 \notin \langle 2 \rangle$.

If $\deg(f(x)) > 0$ then $2 \notin \langle f(x) \rangle$ but $2 \in N \Rightarrow$ N is not principal.

Thm 27.24 Every ideal in $F[x]$ is principal for F 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 $c \in N$, $\frac{1}{c} \in R \Rightarrow \frac{1}{c} \cdot c \in N \Rightarrow 1 \in N \Rightarrow N = R$
  $N = \langle 1 \rangle$

- If $\deg(g) \geq 1$, for $f(x) \in N$ apply division alg:
  $f(x) = q(x) g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$
  or $r(x) = 0$
  but $r(x) \in N$ since $r(x) = \underset{\in N}{f(x)} - \underset{\in N}{q(x) g(x)}$.
  $\Rightarrow r(x) = 0 \Rightarrow f(x) \in \langle g(x) \rangle \Rightarrow N = \langle g(x) \rangle$. $\square$

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 $\underset{\in F[x]}{p(x)}$ irreducible / F := $p(x) \neq \underset{\underset{F[x]}{\uparrow}}{f(x)}\,\underset{\underset{F[x]}{\uparrow}}{g(x)}$ $\quad 0 < \deg f < \deg p$, $\deg g$

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

if $p(x)$ red then $\langle p(x) \rangle = \langle f(x) g(x) \rangle$ $\quad \deg f$, $\deg g$ $< \deg p$

$\Rightarrow f(x) g(x) \in \langle p(x) \rangle \xRightarrow{\text{prime ideal}}$ one of $f(x)$ or $g(x)$ must be in $\langle p(x) \rangle$ but min deg of all polynomials $\neq 0$ in $\langle p(x) \rangle$ is $\deg(p(x))$. contradiction

$\Leftarrow$ 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 of $F[x]$ are principal

But $p(x) \in N$ so $p(x) = f(x) \cdot g(x)$ for some $f(x) \in F[x]$

since p is irred this factorisation is boring i.e.

either $\deg g(x) = 0$ $g(x) = c \leftarrow$ unit. $\Rightarrow N = \langle 1 \rangle = F[x]$

hence N is not a proper ideal.

$\deg g(x) = \deg p(x)$ then $p(x) = c\,g(x)$ and

$\{f(x) p(x)\} = \langle p(x) \rangle = \langle g(x) \rangle = \{\tilde{f}(x) \cdot g(x)\}$ $\square$

Hence $\langle p(x) \rangle$ maximal.

Question Who are prime ideals in $F[x]$?

Answer: N prime $\Longleftrightarrow$ N maximal in $F[x]$

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

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

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

x^3+3x+2 irreducible / $\mathbb{Z}_5$ since if not

$$x^3+3x+2 = f(x)g(x) \quad \deg f = 1 \quad \deg g = 2.$$
$$= (x-a)g(x).$$

and x^3+3x+2 has a root in $\mathbb{Z}_5$.

$a=0 \Rightarrow 0^3+3\cdot 0+2 \neq 0$ $\qquad$ $a=2 \ldots \neq 0$

$a=1 \Rightarrow 1^3+\underline{3\cdot 1}+\underline{2} = 1 \neq 0$ $\qquad$ $\vdots$

$a=4 \ldots \neq 0$

<u>claim</u> N has $5^3 = 125$ cosets in $\mathbb{Z}_5[x]$.

cosets look like $p(x) + N \subseteq \mathbb{Z}_5[x]$

for $\deg p(x) \leq 2$. $p(x) = a_2 x^2 + a_1 x + a_0$

$p(x) = 0$

$5 \cdot 5 \cdot 5$

such polynomials

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

$\mathbb{Q} \subseteq E$

<u>Claim</u> E contains a zero of $x^2 - 2$

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

$= x^2 + \langle x^2 - 2 \rangle - 2$

$= x^2 - 2 + \langle x^2 - 2 \rangle = \langle x^2 - 2 \rangle = 0_E$

if $a \in N$

then $a + N = N$

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

E extension of F.

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

$$F' = \{ a + \langle x^2-2\rangle \mid a \in \mathbb{Q} \} \subseteq E$$

$$\begin{array}{ccc} F' & & a + \langle x^2 - 2\rangle \\ \uparrow \psi & & \uparrow \\ \mathbb{Q} & & a \end{array}$$

ψ is an isomorphism of fields.

must show bijection + respects addition + multiplication.

(see textbook)

tower of fields

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$

$$\begin{tikzcd}[column sep=small] & F(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\ F(x) \arrow[dr, dash] & & F(y) \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Def A field E is an <u>extension</u> field of F if $F \subseteq E$.

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 $f(x)$ irred, $E = F[x]/\langle f(x) \rangle$ is a field.

Claim 1 F can be identified with a subfield of E.

$$\begin{aligned} \varphi : F &\longrightarrow E \\ a &\longmapsto a + \langle f(x) \rangle \end{aligned}$$

this is an injective field homomorphism (see text book)

Claim 2 $\alpha = x + \langle f(x) \rangle \in E$ 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

$$f(\alpha) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \langle f(x) \rangle \text{ in } E$$

$$= \langle f(x) \rangle = 0 \text{ in } E.$$

$\square$

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

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

$\downarrow \exists\, \varphi$ field isomorphism

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

such that

$$\varphi(\underbrace{x + \langle x^2+1 \rangle}_{\alpha}) = i$$

Algebraic & Transcendental Extensions

Def 29.6 $\alpha \in E \supseteq F$ is algebraic $/F$ 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 $/\mathbb{R}$ $/\mathbb{Q}$

$f(x) = x^2 - 2$ $\qquad$ $f(x) = x^2 + 1$

$\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$. (HARD).

When $E = \mathbb{C}$, $F = \mathbb{Q}$ call α a algebraic/transcendental #.

Recall evaluation homomorphism: $\varphi_a : F[x] \to F$ $\quad a \in F$

$f(x) \mapsto f(a)$

For $F \subseteq E$ upgrade $\quad \varphi_\alpha : F[x] \to E$ $\quad \alpha \in E$

$a \mapsto a \quad a \in F$

$x \mapsto \alpha$

i.e. $\varphi_\alpha(a_0 + a_1 x + \cdots a_n x^n) = a_0 + a_1\alpha + \cdots a_n\alpha^n$

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

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

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

$\iff \varphi_\alpha$ is injective. $\boxed{\checkmark}$.

Thm 29.13 Let $E \supseteq F$ 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

$p(x)$ irred over $F[x] :=$ $p(x) \neq f(x)g(x)$ where $f(x), g(x) \in F[x]$
and $0 < \deg f, \deg g < \deg p$
$\Leftrightarrow \langle p(x) \rangle$ is maximal in $F[x]$.

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

Then $\ker \varphi_\alpha \neq \{0\}$ and $\ker \varphi_\alpha = \underset{\text{ideal}}{N} = \langle p(x) \rangle$

any generator of $\ker \varphi_\alpha$ gives the polynomial $p(x)$ $\square$

Convenient to take the generator with leading coeff $= 1$ "monic"

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 $\deg(\alpha, F)$.

$\cancel{2x^2-4}$ not monic

Ex. $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$ $\quad \operatorname{irr}(i, \mathbb{Q}) = 1 + x^2$ $\quad$ i "$\sqrt{-1}$" $\quad (\sqrt{-1})^2 + 1 = 0$

$\operatorname{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2} \in \mathbb{R}[x]$ $\quad \operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$

$\deg(\sqrt{2}, \mathbb{Q}) = \deg(i, \mathbb{Q}) = 2$ $\quad \deg(\sqrt[3]{2}, \mathbb{Q}) = 3$

$\deg(\sqrt{2}, \mathbb{R}) = 1$

$$\operatorname{irr}\left(\sqrt[3]{\frac{1+\sqrt{2}}{5}}, \mathbb{Q}\right) \overset{?}{=}$$

Simple Extensions

if $E \geq F$ and $\alpha \in E$ there is a field $F(\alpha)$ s.t. $F \subseteq F(\alpha) \subseteq E$ defined by

- If α algebraic $/F$ $\quad F(\alpha) := \dfrac{F[x]}{\langle irr(\alpha, F)\rangle}$ $\Leftarrow$ maximal ideal

$\ker \phi_\alpha$

$\Downarrow$

$f(x) + \langle irr(\alpha, F)\rangle$

$a \mapsto a + \langle irr(\alpha, F)\rangle$

$F \subseteq F(\alpha)$

Recall $\phi_\alpha : F[x] \to E$ then $F(\alpha) = \phi_\alpha[F[x]] \subseteq E$

$F \subseteq F(\alpha) \subseteq E$

- if α transcendental $/F \iff \phi_\alpha$ is injective.

$\Rightarrow F[x] \cong \phi_\alpha(F[x]) \subseteq E$ $\qquad F(\alpha)$ is field of fractions of $\phi_\alpha[F[x]]$.

not a field but int domain

Def An extension field E of F is a simple extension if $E = F(\alpha)$ for some $\alpha \in E$.

Ex. $\mathbb{C}$ is a simple extension of $\mathbb{R}$ $\mathbb{C} = \mathbb{R}(i) \cong \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$.

- Non-example: $\mathbb{R}$ is not a simple ext. over $\mathbb{Q}$.

Thm 29.18 If $E = F(\alpha)$ be a simple extension with α alg over F. Every $\beta \in E$ can be written uniquely in the form

$$\beta = b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}$$

where b_i are in F and $n = \deg(\alpha, F)$.

Ex $\mathbb{Z}_5/\langle \underline{x^3+3x}+2\rangle = E$ is a simple extension

since $\alpha = x + \langle x^3+3x+2\rangle$. then $\mathrm{irr}(\alpha, \mathbb{Z}_5) = x^3+3x+2$
$\deg(\alpha, \mathbb{Z}_5) = 3$.

Thm 29.13 says $\forall$ $\beta \in E = \mathbb{Z}_5(\alpha)$ can be written *uniquely* as $b_0 + b_1\alpha + b_2\alpha^2$ $b_0, b_1, b_2 \in \mathbb{Z}_5$

$\beta \in E$ $\beta = f(x) + \langle x^3+3x+2\rangle$ $f(x)$ is not unique.

$$= f(x) + \underbrace{(x^5+1)\cdot(x^3+3x+2)}_{} + \langle x^3+3x+2\rangle.$$

Notice: $\alpha^3+3\alpha+2 = 0$ in E since $(x+\langle x^3+3x+2\rangle)^3 + 3(x+\langle x^3+3x+2\rangle) + 2$

$$= x^3 + \langle x^3+3x+2\rangle + 3x + \langle x^3+3x+2\rangle + 2 = \langle x^3+3x+2\rangle = 0 \text{ in } E.$$

$\Rightarrow \alpha^3 = -3\alpha - 2$

$\alpha^3 = -3\alpha - 2$ $\qquad$ $\alpha^4 = \alpha \cdot \alpha^3 = -3\alpha^2 - 2\alpha$

$$\alpha^5 = \alpha^4 \cdot \alpha = -3\alpha^3 - 2\alpha^2 = -3(-3\alpha - 2) - 2\alpha^2$$

$$= 4\alpha + 1 + 3\alpha^2$$

<u>Why unique?</u>

If $b_0 + b_1\alpha + b_2\alpha^2 = c_0 + c_1\alpha + c_2\alpha^2$ holds in E $\quad b_i, c_i \in \mathbb{Z}_5$

$$(b_0 - c_0) + (b_1 - c_1)\alpha + (b_2 - c_2)\alpha^2 = 0$$

1) α is a zero of some poly of degree ≤ 2.
but $irr(\alpha, \mathbb{Z}_5)$
was $x^3 + 3x + 2$ deg 3.

or 2) $b_i = c_i \quad \forall i$

Field Operations in E $\qquad |E| = 5^3 = 125$

$$(3+2\alpha)(1+4\alpha^2) = 3 + 2\alpha + 12\alpha^2 + 6\alpha^3$$
$$= 3 + 2\alpha + 2\alpha^2 + \alpha^3$$
$$= 3 + 2\alpha + 2\alpha^2 - 3\alpha - 2$$
$$= 1 + 4\alpha + 2\alpha^2 \in E.$$

see Ex 29.19 for a similar example with 4 elements. $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$.

Thm 29.18 If $E = F(\alpha)$ be a simple extension with α alg over F. Every $\beta \in E$ can be written uniquely in the form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

where b_i are in F and $n = \deg(\alpha, F)$.

$F[x]/\langle \operatorname{irr}(\alpha, F)\rangle$

$c_0 + c_1\alpha + \cdots + c_d\alpha^d \quad c_i \in F$

Proof $F(\alpha) = \phi_\alpha[F[x]] = \{ f(\alpha) \mid f \in F[x]\} \subseteq E$

Suppose $\operatorname{irr}(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$

$p(\alpha) = 0 \Rightarrow \alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0)$.

Any monomial α^m can be written in terms of α^k $k<n$

$\alpha^m = \alpha^{m-n}(-a_{n-1}\alpha^{n-1} + \dots + a_0) = \dots\dots$ (see example for concrete calculations)

$\Rightarrow$ for any $f(x) \in F[x]$ $f(\alpha) = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}$ for some $b_0, \dots b_{n-1} \in F$. Existence of expression is proven.

Now for uniqueness: Suppose in $F(\alpha)$ we have:

$$b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \quad b_i, c_i \in F$$

then $(b_0 - c_0) + (b_1 - c_1)\alpha + \dots + (b_{n-1} - c_{n-1})\alpha^{n-1} = 0$

$\Rightarrow$ α is a zero of a polynomial of degree $\leq n-1$ in $F[x]$ <u>or</u> $b_i = c_i$ $\forall i$

1st case we arrive at a contradiction since

$\text{irr}(\alpha, F) = p(x)$ $\deg p(x) = n$. $\square$.