PAGE NO.:
DATE: / /

$SL_4(\mathbb{R})$ $\qquad PSL_n = \frac{SL_n}{Z(SL_n)}$

Gaussian Integers →

$$\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$$

{
is UFD ✓

We prove it is ED.

$$\phi : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$
$$a+ib \longmapsto a^2+b^2$$

$\alpha, \beta \in \mathbb{Z}[i]$

$$\phi(\alpha\beta) = \phi(\alpha)\,\phi(\beta)$$

$\alpha, \beta \qquad \frac{\alpha}{\beta} = r + si$ (Note that $r, s \in \mathbb{Q}$)

Choose a and $b \in \mathbb{Z}$ s.t.

$|r-a| \leq \frac{1}{2}$ and $|s-b| \leq \frac{1}{2}$

$$\alpha = \beta(r+is)$$
$$= \beta\underbrace{(a+ib)}_{\gamma} + \beta\underbrace{((r-a)+i(s-b))}_{\delta}$$

$$\phi(\delta) < \phi(\beta)$$

$$= \phi(\beta)\left|(r-a)^2+(s-b)^2\right| \leq \frac{1}{2}\phi(\beta) < \phi(\beta)$$

ED

$\{1, -1, i, -i\}$

PAGE NO.:
DATE: / /

ED ⊂ PID ⊂ UFD.

GCD → a, b d is gcd of a, b if

$d \mid a$ & $d \mid b$

and if $c \mid a$, $c \mid b \Rightarrow c \mid d$.

In a UFD $a = u p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

$b = w q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$

gcd exists.

Irreducible polynomials.

$f(x) \in \mathbb{Z}[x]$ irred. over $\mathbb{Q}[x]$.

Ex $\rightarrow 2x$.

But not irreducible in $\mathbb{Z}[x]$.

UFD

$f(x)$ $\quad c(f(x))$

content

gcd of all the coefficients

$f(x) = c(f)\, f^*(x)$.

Defn We call a polynomial $g(x)$ primitive if $c(g(x))$ is a unit.

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\} \qquad \frac{a}{b} = \frac{c}{d}$$

R as an ID then R can be a embedded in a field.

$$R \times (R \setminus \{0\}) = \{(a, b) : a, b \in R\}$$

Equivalence Relation: $(a, b)\ R\ (c, d)$ if $ad = bc$

smallest field containing R.

$$F = \left\{ \frac{a}{b} \right\}$$

Quotient field OR field of fraction

$\frac{a}{b}$ Defined to be equivalence class.

Define operations –

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \& \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Ring ✓ also field ✓.

$\frac{0}{1}$ → Additive identity $\qquad \frac{1}{1}$ → Multiplicative Identity

$$\mathbb{Q}[x] \subset \mathbb{Q}(x) \quad (F)$$

$$= \left\{ \frac{f(x)}{g(x)} : g(x) \neq 0 \right\}$$

\# $F' \subseteq F$ any field

"Prime subfield"

↳ smallest subfield contained in F.

⟶

Proposition: Let F be a field. Then the prime subfield of F is either $\mathbb{Z}_p$ or $\mathbb{Q}$.

Pf →

$$\varphi : \mathbb{Z} \longrightarrow F$$
$$n \longmapsto n.1 = \underbrace{1+1+\cdots+1}_{n \text{ times}}$$

ring homomorphism

$$\frac{\mathbb{Z}}{\ker\varphi} \cong \varphi(\mathbb{Z}) \subset F$$

F is ID, Image is ID.

$\ker\varphi = 0 \rightarrow$ characteristic is prime

$\ker\varphi = 0$ or (p)

$$\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \varphi(\mathbb{Z}) \checkmark$$

$$\mathbb{Z} \cong \varphi(\mathbb{Z})$$

Extend the map → $\varphi : \mathbb{Q} \to F$

$$\frac{m}{n} \longmapsto \varphi(m)(\varphi(n))^{-1} \checkmark.$$

1.6 $\varphi : \mathbb{R} \to \mathbb{R}$

$\varphi(1) = 1 \rightarrow \varphi(m) = m$

$$\varphi\left(\frac{m}{n}\right) = \varphi(m)\,\varphi(n^{-1}) = \frac{m}{n}.$$

$r > 0 \Rightarrow \varphi(r) > 0$

$r \in \mathbb{R}$, $r > 0$: $r = y^2$, $\varphi(r) = (\varphi(y))^2$, $\varphi(r) > 0$ ⇒ $x > y \Rightarrow \boxed{\varphi(x) > \varphi(y)}$ ⇒

Let $\phi(r) \neq r$

Assume $r < \phi(r)$

$r < q < \phi(r)$

$\Rightarrow \phi(r) < \phi(q) = q < \phi(r) \Rightarrow \Leftarrow$

PS-8 Q.2 $I \subset I_1 \cup I_2$

Let $I \not\subseteq I_1$ and $I \not\subseteq I_2$

$a \qquad b$

$a + b \notin I_1 \cup I_2$

19/04/23

UFD ✓ **Primitive Polynomial** – A polynomial $f(x) \in R[x]$ is called primitive if content of $f(x)$ is a unit.

gcd of all the coefficients. ←

$$f(x) = \underbrace{c(f)}_{\text{content}} \underbrace{f^*(x)}_{\text{primitive}}$$

$f(x) = 2 + 2x$

$= 2(1+x) \in \mathbb{Z}[x]$

↳ Reducible over $\mathbb{Z}$ (2 is not a unit)

Irreducible over $\mathbb{Q}$ (2 is a unit)

Irreducible Polynomial:- $R[x]$ is an irreducible element in $R[x]$.

$f(x) \neq g(x)\, h(x)$.

↔

- Units on $R[x]$ = Units in R.
- $f.g$ **Proposition** → $c(fg) = c(f) \cdot c(g)$

(f, g → are non-zero non constants polynomials)

$f = c(f) f^*$ $\quad f^*, g^*$ → primitive.

$g = c(g) g^*$

$$fg = c(f)c(g) f^* g^*$$

$\Rightarrow c(fg)(fg)^* = c(f)c(g) f^* g^* \Rightarrow c(f)c(g) \mid c(fg)$ ✓

$\Longrightarrow$

PAGE NO.:
DATE: / /

Lemma → $0 \neq f, g, h \in R[x]$. Let p be a prime in R.
Suppose $pf(x) = g(x)\,h(x)$
then either $p \mid g(x)$ or $p \mid h(x)$

Pf $pf(x) = c(g)\,c(h)\,g^*(x)\,h^*(x)$.

$\Rightarrow p \mid c(g)c(h) = p \mid c(g)$ or $p \mid c(h)$

To show $c(fg) \mid c(f)c(g)$

Let p be a prime s.t. $p \mid c(fg)$

T.S. $p \mid c(f)\,c(g)$.

$fg = c(fg)(fg)^*$

$p \mid c(fg) \Rightarrow p \mid fg \overset{\text{Lemma}}{\Rightarrow} p \mid f$ or $p \mid g$

$\Rightarrow p \mid c(f).c(g)$ ✓

$\therefore\ c(fg) = c(f).c(g)$.

$\Rightarrow$ Product of 2 primitive polynomials is primitive.

Gauss Lemma –
Suppose R is a UFD and F be its quotient field.
Let $f(x) \in R[x]$ be a non constant primitive polynomial in $R[x]$.
Then $f(x)$ is irreducible over R iff it is irreducible over F.
(over F : in $F[x]$; over R : in $R[x]$)

irreducible

Pf → ($\Rightarrow$) $f(x) \in R[x]$

Suppose $f(x)$ is ~~reducible~~ reducible over F.

$f(x) = g(x)\,h(x)$ $\quad \deg g(x) \geq 1$ & $\deg h(x) \geq 1$

as working over field.

$f(x) = \frac{a}{b}\, g^*(x)\, \frac{c}{d}\, h^*(x)$

$= \frac{ac}{bd}\, g^*(x)\, h^*(x)$

$\frac{ac}{bd}$ → Unit in R

$g^*(x)\,h^*(x)$ → primitive

$\Rightarrow\Leftarrow$

($\Leftarrow$) Trivial

$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in \mathbb{Z}[x]$.

→ can have rational root say $\frac{a}{b} \in \mathbb{Q}$ s.t. $(a,b)=1$.

$\Rightarrow f\left(\frac{a}{b}\right) = 0$

$\Rightarrow a_0 + a_1 \frac{a}{b} + \ldots + a_n \frac{a^n}{b^n} = 0$

$\Rightarrow \underbrace{a_0 b^n + a_1 a b^{n-1} + \ldots}_{\text{divisible by } b} + \underbrace{a_n a^n}_{\text{divisible by } b} = 0$

$(a,b) = 1$

$\Rightarrow \boxed{b \mid a_n}$

Similarly $\Rightarrow \boxed{a \mid a_0}$

$\Longrightarrow$

If $a_n = 1$ then f has an integer root iff f has a rational root.

$f(x) \in \mathbb{Z}[x]$

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

Suppose $\exists p$ be a prime s.t.

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

(Assuming degree $a_0 + a_1 x + \dots + a_n x^n \longmapsto \bar{a_0} + \bar{a_1} x + \dots + \bar{a_n} x^n$ remains same)

$$f(x) \longmapsto \overline{f(x)}$$

(If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p[x]$

$\Downarrow$

$f(x)$ is irreducible over $\mathbb{Z}$

$x^4 + 1$

$x^4 - 10x^2 + 1$

Eisenstein criterion UFD R

$f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$

non-constant

Suppose p is a prime s.t.

$$p \mid a_i \quad \forall\ i \leq n-1$$

$$p \nmid a_n \text{ and } p^2 \nmid a_0$$

Then $f(x)$ is irreducible.

PAGE NO. :
DATE : / /

20/4/23

$c(f)$: gcd of all coefficients

$f \to$ primitive iff $c(f)$ - is unit.

f, g primitive

$a_0 + a_1 x + \dots + a_n x^n$

$b_0 + b_1 x + \dots b_n x^n$

Alt. Proof: Let p be a prime s.t $p \mid c(fg)$

i be smallest s.t. $p \nmid a_i$

j ——— n ——— $p \nmid b_j$

p is not divisible by p

coefficient of $x^{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \dots + a_i b_j + \dots + a_{i+j} b_0$

$\therefore$ ✓

Thm → $R \to$ UFD, $f \in R[x]$ is primitive.

Then f is irreducible over R iff f is irreducible over F.

(F is the Q.F. of R)

Pf ($\Rightarrow$) Suppose f is not irred. over F.

$f(x) = g(x) \cdot h(x)$ ~~g, h~~ $g, h \in F[x]$

$= \frac{a}{b} g^*(x) \frac{c}{d} h^*(x)$

$f(x) = \frac{ac}{bd} g^*(x) h^*(x)$

$\frac{ac}{bd} \to$ unit on R $\Rightarrow f$ is not irreducible over R.

$bd f(x) = ac\, g^*(x) h^*(x)$

$u(bd) = w(ac)$

$\Rightarrow$

PAGE NO.:
DATE: / /

($\Leftarrow$) $f(x) = g(x)\,h(x) \in R[X]$

$\deg g(x) \geq 1$
$\deg h(x) \geq 1$

↓ avoided non zero non unit.

Thm → R is a UFD. Then $R[X_1, X_2, \ldots X_n]$ is a UFD.

Pf → Sufficient to prove for 1 variable. Then use induction as $R[X_1][X_2] = R[X_1, X_2]$ ↳ coefficients.

$f(x) \in R[X]$

$f(x) = c(f)\, f^*(x)$ ↳ irred → done ✓.

If not irred → $f^*(x) = g(x)\,h(x)$ $\deg g(x) \geq 1$, $\deg h(x) \geq 1$ } as if $\deg = 1$ ↓ constant. ⇒ ∈ to 'primitive'

Now to prove uniqueness –

$$f(x) = a_1 a_2 \ldots a_k \underbrace{P_1(x) P_2(x) \ldots P_r(x)}_{\text{primitives}}$$

$$= b_1 b_2 \ldots b_s \underbrace{q_1(x) q_2(x) \ldots q_s(x)}$$

$c(f(x)) = u a_1 a_2 \ldots a_k$
$= w b_1 b_2 \ldots b_s$ } R is a UFD ✓ (given)

⇓

$$P_1 P_2 \ldots P_r = u q_1 q_2 \ldots q_s \in F[x]$$

$$P_i = u q_j \in F[x]$$

complete the proof.

PAGE NO. :
DATE : / /

Eisenstein Criterion → Let R be a UFD and F be its quotient field. Let $f(x)$ be a non-constant polynomial in $R[x]$. Let

P be a prime s.t. $P \mid a_i$ $i \le n-1$, $P \nmid a_n$ and $P^2 \nmid a_0$

$a_0 + a_1 x + \dots + a_n x^n$

Then f is irreducible over F.

Pf → $f(x) = c(f) \cdot f^*(x)$

Taking $f(x)$ primitive.

$f(x) = g(x)\, h(x)$

$g(x) = g_0 + g_1 x + \dots + g_r x^r$

$h(x) = h_0 + h_1 x + \dots + h_s x^s$

$P \mid g_0 h_0$, $P \nmid g_r h_s$

$P^2 \mid g_0 h_0$

$\Rightarrow P \mid g_0$ & $P \nmid h_0$ (WLOG)

Choose i smallest s.t. $P \nmid g_i$

$x^i : g_0 h_i + g_1 h_{i-1} + \dots + g_i h_0$

divisible by P — not divisible

$\Rightarrow\Leftarrow$

PAGE NO.:
DATE: / /

Corollary → $f(x) = 1 + x + x^2 + \dots + x^{p-1}$ is irreducible

Pf → $f(x) = \dfrac{x^p - 1}{x - 1}$

If $f(x)$ is reducible so is $f(x+1)$

$$f(x+1) = \frac{(x+1)^p - 1}{x}$$

$$= x^p + (\ )x^{p-1} + \dots + p$$

Eisenstein criterion ✓

$f(x) \longrightarrow$ irreducible.

21/4/23 What do you know about the fields?

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \boxed{\mathbb{Z}_p}, K(x)$

$\mathbb{Z}_p$ → prime; $K(x)$ → any field.

F → finite field

↳ contains $\mathbb{Q}$ or $\mathbb{Z}_p$

↳ as finite.

$\mathbb{Z}_p \subseteq F$ (finite; n)

a b

$a \cdot b = ab$

$\{a_1, a_2, \dots a_n\}$ - basis

$a = k_1 a_1 + k_2 a_2 + \dots + k_n a_n$ $\quad p^n$

$$\boxed{|F| = p^n}$$

Field of order 6, 10, 15, 14 not possible

Ex →

Ex →

Ex →

$k[x]$ $\quad f \to$ poly. $k[x]$ - irred.

$\frac{k[x]}{(f)} \to$ field.

maximal ideal.

PS-9 Q.6 Let f be an irred. poly. $f(x) \in \mathbb{Z}_p[x]$ → prime
f degree n.

$$\frac{\mathbb{Z}_p[x]}{(f(x))}$$

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

$\deg r(x) < \deg f(x)$.

$$g(x) + (f) = \underbrace{f(x)q(x)}_{\in (f)} + r(x) + (f)$$

$$g(x) + (f) = r(x) + (f)$$

$$a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + (f)$$

Ex → Order 25 field $\mathbb{Z}_5[x]$ find $f(x) \in \mathbb{Z}_5[x]$ irreducible of degree 2.

Take $f(x) = x^2 + x + 1$.

Ex → $\mathbb{C}[X]$ irreducible poly. →

Ex → $\mathbb{R}[X]$ irreducible possible → quadratic.

PAGE NO.:
DATE: / /

Hilbert Nullstellensatz Thm –

$\mathbb{C}[x_1, x_2, \ldots, x_n]$

All the maximal ideals of $\mathbb{C}[x_1, x_2, \ldots, x_n]$ are of the form $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ $a_i \in \mathbb{C}$.

PS-9 Q.1 $R = \{f : [0,1] \to \mathbb{R} : f \text{ is cts.}\}$

$\mathbb{C}[0,1]$ $\quad \varphi_a : C[0,1] \to \mathbb{R}$

$f(x) \longmapsto f(a)$ $\quad a \in \mathbb{R}$

Surjective ✓

for every a, take constant fun^n. #

$$\frac{C[0,1]}{\ker \varphi_a} \cong \mathbb{R}$$

$M_a \longrightarrow$ maximal ideal as $\mathbb{R}$ is field.

Claim – Any max. ideal of $C[0,1]$ is of the form M_a for some a

$$\| \quad \{f \in C[0,1] : f(a) = 0\}$$

Pf → Suppose not ⇒ for every $a \in [0,1]$ $\exists f$ s.t. $f_a(a) \neq 0$

As f is cts. $\exists V_a$ – nbd. of a.

s.t. $f_a(V_a) \neq 0$

$\Longrightarrow$

$[0,1] \subset \bigcup_{a\in[0,1]} V_a \Rightarrow \exists\ a_1, a_2, \ldots a_n$ s.t.

$[0,1]$ — compact; $a\in[0,1]$ — finitely many.

$[0,1] \subset \bigcup_{i=1}^{n} V_{a_i}$, V_{a_i} ↓ f_{a_i}

Let $g = f_{a_1}^2 + f_{a_2}^2 + \ldots + f_{a_n}^2$

$g(x) > 0 \quad \in M$ (Invertible element in M.)

$\Rightarrow M = R$ ↓ will become whole R.

$\Rightarrow\Leftarrow$

F is a field, infinite

$G \subseteq F\setminus\{0\}$ → grp. wrt $\times$

finite → will be cyclic.

G is abelian by defn of field & it is finite.

$\Rightarrow \quad G = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_s^{r_s}}$

$m = \operatorname{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots p_s^{r_s}) \leq |G|$ (T.P. $|G| = m$)

$\Rightarrow \forall\ a\in G \Rightarrow,\ a^m = 1$

Every element of G is a root of $x^m - 1 = 0$ → atmost m roots. (working over F.)

$\Rightarrow |G| \leq m$

$\Rightarrow |G| = m$.

$\Leftarrow$

PS-9 Q.4 $\frac{\mathbb{R}[X]}{(x^2+1)} \cong \mathbb{C}$

$\mathbb{R}[X] \longrightarrow \mathbb{C}$

$f(x) \longmapsto f(i)$

PS-9 Q.5 $f(x) \in \mathbb{Q}[x]$ $q^2 \mid f$ iff

$\gcd(f(x), f'(x)) = d(x)$ → positive degree.

converse of Q.3 # $R[X]$ is a PID $\Rightarrow$ R is field.

(Ring)

$\frac{R[X]}{(x)} \cong R$ $f(x) \longmapsto f(0)$ → field

maximal ideal ✓ x → irreducible.

PS-8 Q.9

R	$M_n(F)$
I	$M_n(I)$ ✓
ideal	ideal

J

To find : I s.t. $J = M_n(I)$

$\Rightarrow$

$E_{ij} A E_{kl} = a_{jk} E_{il}$

PAGE NO. :
DATE : / /

$I = \{ a_{11} : a_{11} \text{ is the first entry of } A \in J \}$

Claim — $J = M_n(I)$

$\subseteq$

$A \in J \qquad a_{ij} \in I.$

$a_{ij} E_{11} = \qquad \in J \qquad \subseteq \checkmark$