

# §9.1

1. D PID.

$p$  prime  $\Leftrightarrow p$  irreducible

$(\Rightarrow)$   $p$  prime. Say  $p = ab$ . So  $a|p$ ,  $b|p$

Then  $p|ab \therefore p|a$  or  $p|b$

$\therefore$   $p$  and  $a$  are associates, i.e.  $b$  is a unit

OR  $p$  and  $b$  " " " " " " " " " " " "

$\therefore p$  is irreducible

$(\Leftarrow)$  This is a theorem for class //

2.  $b|a$   $a \nmid b$  E.D.

$$\left. \begin{array}{l} b = aq + r \quad r = 0 \\ a = bp \end{array} \right\} \delta(r) < \delta(a)$$

$$b = bpq + r$$

$$b(1-pq) = r$$

$$\delta(b) \leq \delta(b(1-pq)) = \delta(r) < \delta(a)$$

$$\therefore \delta(b) < \delta(a)$$

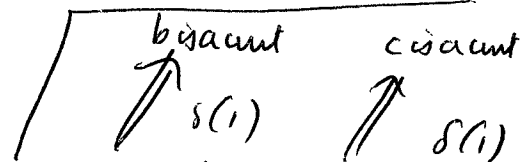
3. This question is wrong. It needs to say "Let  $D$  be a E.D. that is not a field".  
Assuming that's corrected ...

Note there's  $x \in R$  with  $\delta(x) \neq 0$ .

Indeed, let  $x$  be any non-unit.  $1 = xq + r$   $r \neq 0$   $\delta(r) < \delta(x)$   $\therefore \delta(x) > 0$ .

Then  $\delta(x) = \delta(x \cdot 1) = \delta(x) \delta(1)$ ,  $\delta(x) \neq 0$ .

$$\therefore 1 = \delta(1)$$



If  $\delta(a)$  is prime,  $a = bc$  per  $\delta(a) = \delta(b) \delta(c)$   $\therefore$  either  $\delta(b) = 1$  or  $\delta(c) = 1$

4.  $a, b \neq 0$ .

$$\text{Let } a = u p_1^{m_1} \cdots p_k^{m_k}$$

$$b = v p_1^{n_1} \cdots p_k^{n_k}$$

$u, v$  units

$p_1, \dots, p_k$  pairwise non-associate irreducibles

$$m_i, n_i \geq 0.$$

Claim  $\text{GCD}(a, b) = p_1^{\min(m_1, n_1)} \cdots p_k^{\min(m_k, n_k)}$

Proof It divides both  $a$  &  $b$

Say  $c|a, c|b$ . Then  $c = w p_1^{s_1} \cdots p_k^{s_k}$   $w$  a unit

$$\therefore c \mid p_1^{\min(m_1, n_1)} \cdots p_k^{\min(m_k, n_k)} \quad \left( \begin{array}{l} s_i \leq m_i \text{ and } \\ s_i \leq n_i \end{array} \right) \quad \left( \because s_i \leq \min(m_i, n_i) \right)$$

6.  $d|a$  and  $d|b$  in  $R$

$$\therefore a = dr \quad b = dr' \quad \text{for } r, r' \in R \subseteq S$$

$$\therefore d|a \text{ and } d|b \text{ in } S \quad \text{—————} \textcircled{1}$$

Say  $c|a$  and  $c|b$  in  $S$

$$\therefore c|ra + rb = d$$

$$\therefore c|d \quad \text{—————} \textcircled{2}$$

$$\textcircled{1} \& \textcircled{2} \Rightarrow d = \text{GCD}(a, b) \text{ in } S \text{ too}$$

11(a) Define

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}[i] / \langle a+bi \rangle$$

$$k \longmapsto k + \langle a+bi \rangle$$

$$\text{Let } n = a^2 + b^2$$

$$\gcd(a,b) = 1 = sa + tb$$

$$\begin{aligned} \text{Note } i &= sa + tb = t(a+bi) - ta + (a+bi)si + sb \\ &= sb - ta + (a+bi)(t+si) \end{aligned}$$

$$\therefore i \equiv sb - ta \pmod{a+bi}$$

This shows  $\varphi$  is onto, as every elt. of  $\mathbb{Z}[i] / \langle a+bi \rangle$  looks like  $k + \langle a+bi \rangle$  same  $k \in \mathbb{Z}$ .

$$\text{Ker } \varphi? \quad n = (a+bi)(a-bi) \quad \therefore n \in \text{Ker } \varphi.$$

Say  $k \in \text{Ker } \varphi$ .

$$\therefore k = (a+bi)(p+qi)$$

$$\therefore \left. \begin{aligned} k &= ap - bq \\ 0 &= aq + bp \end{aligned} \right\}$$

$$\therefore \left. \begin{aligned} ka &= a^2p - abq \\ 0 &= abq + b^2p \end{aligned} \right\}$$

$$\left. \begin{aligned} kb &= abp - b^2q \\ 0 &= a^2q + abp \end{aligned} \right\}$$

$$\hline ka = (a^2 + b^2)p$$

$$\hline kb = -(a^2 + b^2)q$$

$$\therefore k = k(sa + tb) = s(a^2 + b^2)p - t(a^2 + b^2)q = (sp - tq) \underbrace{(a^2 + b^2)}_n$$

$$\therefore n | k$$

$$\Rightarrow \text{Ker } \varphi = \langle n \rangle$$

$$\text{1st Ism. Theorem } \Rightarrow \mathbb{Z}_n \cong \mathbb{Z}[i] / \langle a+bi \rangle$$

14: See class.

§ 9-2 #4.

Take  $0 \neq a \in D$ .

Consider  $\langle a, x \rangle \trianglelefteq D[x]$

It  $\langle f(x) \rangle$  some  $f(x) \in D[x]$ .

As  $a \in \langle f(x) \rangle$ ,  $f(x)$  is a constant,  $b$ , say,  $b|a$

As  $b \in \langle a, x \rangle$ ,  $b$  is a multiple of  $a$ ,  $a|b$

$\therefore a, b$  are associates.

As  $x \in \langle b \rangle$ ,  $x = b \cdot c \cdot x$  some  $c$

$$\therefore 1 = bc$$

$\therefore b$  is a unit

$\therefore a$  is a unit

$\therefore D$  is a field