

1. (a) What is a Euclidean domain?

An integral domain plus a function  $\delta: D - \{0\} \rightarrow \mathbb{Z}_{\geq 0}$

such that

$$\forall a, b \in D - \{0\} \begin{cases} \textcircled{1} \delta(ab) \geq \delta(a) \\ \textcircled{2} a = bq + r \text{ either } r=0 \\ \text{or } r \neq 0, \delta(r) < \delta(b) \end{cases}$$

(b) Prove that if  $R$  is a Euclidean domain then  $R$  is a principal ideal domain.

Let  $I$  be a non-zero ideal.

Let  $a \in I$  be non-zero element with  $\delta(a)$  minimal.

Claim  $I = \langle a \rangle$

Proof  $a \in I \implies \langle a \rangle \subseteq I$

Conversely, take  $0 \neq b \in I$

Write  $b = aq + r$

If  $r \neq 0$  then  $\delta(r) < \delta(a)$ ,  $r = b - aq \in I$   $\neq$

$\therefore r=0$  so  $b \in \langle a \rangle$

$\therefore I \subseteq \langle a \rangle$

$\therefore I = \langle a \rangle$

2. (a) Let  $R$  be an integral domain and  $a, b \in R$  be non-zero elements. What are the two properties defining a *greatest common divisor*  $d$  of  $a$  and  $b$ ?

①  $d|a, d|b$

② If  $c|a, c|b$  then  $c|d$

(b) Suppose  $R$  is a principal ideal domain and  $a, b \in R$  are non-zero elements. Prove that a greatest common divisor of  $a$  and  $b$  always exists, and moreover it can be expressed as a linear combination of  $a$  and  $b$ .

Consider  $\langle a, b \rangle$ . It's  $\langle d \rangle$  for some  $d \in R$   
is a PID.

Since  $d \in \langle a, b \rangle$ ,  $d$  is a lin. comb. of  $a$  and  $b$

Claim  $d = \text{GCD}(a, b)$

Proof  $a \in \langle d \rangle \therefore d|a$        $b \in \langle d \rangle \therefore d|b$  ✓ ①

Say  $c|a, c|b$ . Then  $c$  divides any linear combination  
of  $a$  and  $b$   $\therefore c|d$  ✓ ②

3. In this question you may appeal to the theorem from question 2(b) that if  $R$  is a principal ideal domain and  $a, b \in R$  are non-zero elements, then  $GCD(a, b)$  exists and can be written as a linear combination of  $a$  and  $b$ .

(a) What is the definition of an *irreducible* element  $p \in R$ ?

non-zero non-unit

If  $p = ab$  then either  $a$  or  $b$  is a unit.

(b) If  $R$  is a principal ideal domain and  $0 \neq a \in R$ , prove that the following properties are equivalent:

(1)  $a$  is irreducible;

(2)  $R/\langle a \rangle$  is a field.

(1)  $\Rightarrow$  (2): As  $a$  is non-zero non-unit,  $R/\langle a \rangle$  is not the zero ring.  
 Take  $b \in R/\langle a \rangle$  non-zero in  $R/\langle a \rangle$ .  
 $\Rightarrow a \nmid b$   
 $a$  irreducible  $\Rightarrow GCD(a, b) = 1$

Write  $1 = as + bt$

Then  $(b + \langle a \rangle)(t + \langle a \rangle) = 1$   $\therefore b + \langle a \rangle$  is a unit  
 $\therefore R/\langle a \rangle$  is a field

(2)  $\Rightarrow$  (1): As  $R/\langle a \rangle$  is not the zero ring,  $a$  is not a unit.

Say  $a = bc$

Then  $(b + \langle a \rangle)(c + \langle a \rangle) = 0$ . Since in a field, hence an integral

domain So either  $b + \langle a \rangle = 0$  or  $c + \langle a \rangle = 0$

$a/b$

$\therefore b = ay$

$\therefore a = ayc$

$\therefore 1 = yc$

$\therefore c$  is a unit

$\Downarrow$

similarly  $b$  is a unit

4. Consider the ring  $\mathbb{Z}[\sqrt{10}]$ .

(a) By considering the multiplicative function

$$\delta: \mathbb{Z}[\sqrt{10}] \rightarrow \mathbb{Z}, x + y\sqrt{10} \mapsto x^2 - 10y^2,$$

prove that 2 is an irreducible element.

Use:  $x + y\sqrt{10}$  is a unit  $\Leftrightarrow x^2 - 10y^2 = \pm 1$ .

$\therefore$  As  $\delta(2) = 4$ , 2 is not a unit.

Say  $2 = a \cdot b$   $a, b$  not units  $\therefore \delta(a), \delta(b) \neq \pm 1$

$$4 = \delta(a)\delta(b)$$

$$\therefore \delta(a) = \delta(b) = \pm 2$$

But no elt.  $q \in \mathbb{Z}[\sqrt{10}]$  has  $\delta = \pm 2$  as  $\pm 2$  is not a square modulo 10.

(b) Give an example of a ring  $R$ , an irreducible element  $p \in R$ , and elements  $a, b \in R$  such that  $p|ab$  but  $p \nmid a$  and  $p \nmid b$ .

$$\begin{array}{l} \mathbb{Z}[\sqrt{10}] \quad p=2 \quad a = \sqrt{10}+2 \quad b = \sqrt{10}-2 \\ ab = 6 \quad p|6 \quad \checkmark \\ p \nmid a \quad \checkmark \\ p \nmid b \quad \checkmark \end{array}$$

$$\text{set } \delta(z) = |z|^2$$

$$\delta(ab) = \delta(a)$$

!!!EXTRA CREDIT PROBLEM!!!

5. Prove that the ring  $\mathbb{Z}[i]$  of Gaussian integers is a Euclidean domain.

Take  $a = x+iy$   $b = u+iv$  non-zero.

$$\text{Consider } \frac{a}{b} = p+iq \in \mathbb{C}$$

Define  $z$  to be the Gaussian integer closest to this in the complex plane

$$\text{So } |z - \frac{a}{b}| \leq \frac{\sqrt{2}}{2}$$



$$\text{Then Let } r = a - bz$$

$$\text{So } a = bz + r$$

$$\text{Either } r = 0$$

$$\text{Or } r \neq 0, \quad |r|^2 = |a - bz|^2 = |z - \frac{a}{b}|^2 |b|^2 \\ \leq \frac{1}{2} |b|^2 < |b|^2$$

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