

## Last lecture

- The ring of **Gaussian integers** is the subring  $\mathbb{Z}[i]$  of  $\mathbb{C}$  generated by  $i = \sqrt{-1}$ . Then  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ .
- $\mathbb{Z}[i]$  is an integral domain (Corollary 11.4).
- $a$  **divides**  $b$ , or  $b$  is a **multiple** of  $a$ , if  $b = at$  for some  $t \in R$ .  
If  $a$  divides  $b$  we write  $a|b$ .
- A **unit** is any element of  $R$  which has an inverse
- $a$  and  $b$  are **associates** if  $a = bu$  for some unit  $u \in R$

### This lecture

Properties of associates, units and greatest common divisors.

## Associates and units

### Lemma 12.1

If  $a, b \in R$  write  $a \sim b$  if  $a$  and  $b$  are associates.  
Then  $\sim$  is an equivalence relation on  $R$ .

**Proof (Reflexive)**  $a \sim a$  since  $a = a \cdot 1$

**(Symmetric)**  $a \sim b \implies a = bu \implies b = au^{-1} \implies b \sim a$

**(Transitive)** Suppose  $a \sim b$  and  $b \sim c$

$$\implies a = bu \text{ and } b = cv \implies a = cvu$$

$$\implies a \sim c \text{ since } vu \text{ is a unit with inverse } u^{-1}v^{-1}. \quad \square$$

### Lemma 12.2

Let  $R^* = \{u \in R : u \text{ is a unit}\}$ .

Then  $R^*$  is a commutative group under multiplication.

**Proof** By definition,  $1 \in R$ , multiplication in  $R$  is associative and every element of  $R^*$  has an inverse. Finally,  $R^*$  is commutative since  $R$  is.  $\square$

## Associates in integral domains

### Lemma 12.3

Suppose  $u \in R$ . Then  $u$  is a unit if and only if  $uR = R$ .

**Proof** Obvious!!  $\square$

### Lemma 12.4

Suppose that  $R$  is an integral domain and that  $a, b \in R$ .  
Then  $a$  and  $b$  are associates if and only if  $a|b$  and  $b|a$ .

**Proof** Suppose that  $a$  and  $b$  are associates

$$\implies a = bu \text{ for some unit } u \implies b|a$$

Similarly,  $b = au^{-1}$  so that  $a|b$ .  $\checkmark$

Conversely, suppose that  $a|b$  and  $b|a$ .

$$\implies a = bs \text{ and } b = at \text{ for some } s, t \in R$$

By Lemma 3.6,  $a = 0$  if and only if  $b = 0$

If  $a$  and  $b$  are both non-zero then  $a = ast \implies a(1 - st) = 0$

$$\implies 1 - st = 0 \implies s \text{ and } t \text{ are both units}$$

$$\implies a \text{ and } b \text{ are associates in } R. \quad \checkmark \quad \square$$

## Greatest common divisors

### Lemma 12.5

Suppose that  $R$  is an integral domain and that  $a, b \in R$ .

①  $aR \subseteq bR$  if and only if  $b|a$ .

②  $aR = bR$  if and only if  $a$  and  $b$  are associates.

**Proof** (1) is obvious and (2) follows from (1) and Lemma 12.4.  $\square$

### Definition 12.6

Suppose that  $R$  is an integral domain and that  $a, b \in R$ . Then  $d \in R$  is a **greatest common divisor** of  $a$  and  $b$  if

①  $d|a$  and  $d|b$

②  $e|d$  whenever  $e|a$  and  $e|b$ , for  $e \in R$

We write  $d = \gcd(a, b)$

**Warning** The notation  $\gcd(a, b)$  is not well-defined because  $a$  and  $b$  may have more than one greatest common divisor. For example,  $\pm 2$  are both GCDs for 4 and 6.

## GCDs in PIDs

Recall from Tutorial 4.4a that if  $I$  and  $J$  are ideals then  $I + J = \{x + y : x \in I \text{ and } y \in J\}$  is an ideal.

### Lemma 12.7

Suppose that  $R$  is a principal ideal domain and that  $a, b, d \in R$ .

- 1  $d|a$  and  $d|b \iff aR + bR \subseteq dR$
- 2  $(\forall e \in R, e|a \text{ and } e|b \implies e|d) \iff dR \subseteq aR + bR$ .

Consequently,  $d = \gcd(a, b)$  if and only if  $dR = aR + bR$ .

**Proof** (1) Suppose that  $d|a$  and  $d|b \iff aR, bR \subseteq dR$  by Lemma 12.5  
 $\iff aR + bR \subseteq dR$  ✓

(2) Suppose that  $e|d$  whenever  $e|a$  and  $e|b$   
 $\iff dR \subseteq eR$  whenever  $aR + bR \subseteq eR$  by Lemma 12.5 and (1)  
If  $dR \subseteq aR + bR$  then the last statement certainly holds.

Conversely,  $aR + bR = fR$  for some  $f \in R$  since  $R$  is a PID  
 $\implies aR + bR \subseteq fR \implies dR \subseteq fR = aR + bR$  ✓ □

## GCDs in PIDs.../2

### Proposition 12.8

Suppose that  $R$  is a principal ideal domain and  $a, b \in R$ . Then

- 1  $d = \gcd(a, b)$  if and only if  $aR + bR = dR$
- 2 The greatest common divisor of  $a$  and  $b$  always exists
- 3 Any two GCDs of  $a$  and  $b$  are associates
- 4 An associate of a GCD of  $a$  and  $b$  is a GCD of  $a$  and  $b$

**Proof** (1) is a restatement of the conclusion of Lemma 12.7.

(2) Follows from Lemma 12.7 since  $aR + bR = dR$ , for some  $d \in R$ .

(3) and (4):

$$d = \gcd(a, b) \iff aR + bR = dR \text{ by Lemma 12.7}$$
$$d \text{ and } d' \text{ are associates} \iff dR = d'R \text{ by Lemma 12.5}$$

Hence, (3) and (4) both follow. □

Hence, the notation  $\gcd(a, b)$  is well-defined only up to associates.

That is,  $\gcd(a, b)$  is well-defined only up to multiplication by a unit.