

## Announcements:

Midterm exams etc. now scheduled (see website or email)

Office hours: Mon/Fri after class

Problem sessions: Tues. 3:00-4:20pm

Join Gradescope course if you haven't already!

(entry code: VB7EY2)

---

## Euclidean Domains

Unless otherwise stated, all rings are commutative and have 1.

Def: An (integral) domain is a (commutative, nonzero) ring w/out zero divisors: if  $a \neq 0$ ,  $b \neq 0$ , then  $ab \neq 0$ .

Def:

a) A norm is a function  $N: R \rightarrow \mathbb{Z}_{\geq 0}$  with  $N(0) = 0$

b)  $N$  is Euclidean if  $\forall a, b \in R$ ,  $b \neq 0$ ,  $\exists q, r \in R$  s.t.

•  $a = qb + r$

↑ quotient      ↑ remainder

•  $r = 0$  or  $N(r) < N(b)$

c) A Euclidean domain is an int. domain w/ a Euclidean norm

Idea: we can use the Euclidean algorithm to find gcds

Ex: a)  $\mathbb{Z}$  w/  $N(a) = |a|$

b)  $F$ : field w/  $N(a) = 0$

c)  $F[x]$  ( $F$ : field) w/  $N(p(x)) = \deg p$

d)  $\mathbb{Z}[i]$  w/  $N(a+bi) = |a+bi|^2 = a^2 + b^2$  ←

Non-ex:  $\mathbb{Z}[\sqrt{-5}]$  (next week)

later  
today

Def:

a) Write  $a|b$  (in  $R$ ) if  $\exists x \in R$  s.t.  $ax = b$   
"a divides b"

b)  $d \in R$  is a gcd of  $a$  and  $b$  if

- $d|a$  and  $d|b$

- If  $d'|a$  and  $d'|b$ , then  $d'|d$

(gcd is always unique up to units)

Thm: Let  $R$ : Euclidean domain,  $a, b \in R$ ,  $b \neq 0$ .

Then  $a$  and  $b$  have a gcd.

Pf: Apply Euclidean algorithm:

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$\begin{pmatrix} a = r_{-2} \\ b = r_{-1} \end{pmatrix}$$

$$r_0 = q_2 r_1 + r_2$$

$$\vdots$$

$$r_{n-1} = q_{n+1} r_n + 0 = r_{n+1}$$

where

$$N(b) > N(r_0) > \dots > N(r_n)$$

At each step, notice that

$d$  is a common divisor  
of  $r_i$  and  $r_{i+1}$

$$\iff$$

$d$  is a common divisor  
of  $r_{i+1}$  and  $r_{i+2}$

So gcds are unchanged at each step. Therefore, the  
gcd of  $a$  and  $b$  equals  $\gcd(r_n, 0) = r_n$ .  $\square$

Recall (from D&F (1.7)):

a) An ideal  $I \subseteq R$  is an additive subgp. s.t.

if  $a \in I$ ,  $r \in R$ , then  $ra \in I$ .

b)  $I$  is principal if  $I$  has the form

$$(a) := \{ra \mid r \in R\}$$

Thm: If  $R$ : Euclidean domain, then every ideal  
is principal.

Pf: Choose  $d \neq 0$  in  $I$  w/ minimum norm. If  $a \in I$ ,

then by the Euclidean property

$$a = qd + r$$

w/  $r = 0$  OR  $r \neq 0$  and  $N(r) = N(d)$   
impossible by assumption

Thus,  $d|a$ , so  $\pm = (d)$ .

□

Pf that  $\mathbb{Z}[i]$  is a Euclidean domain:

Let  $a, b \in \mathbb{Z}[i]$ .

Let  $q$  be an element of  $\mathbb{Z}[i]$  closest to  $a/b$  (in  $\mathbb{C}$ ). (i.e.  $|q - a/b|$  is minimal)

Let  $r = a - qb \in R$  (so that  $a = qb + r$ )

We have

$$N(r) = |r|^2 = |a - qb|^2 = \underbrace{\left| \frac{a}{b} - q \right|^2}_{\leq \frac{1}{2}} |b|^2 \leq \frac{1}{2} |b|^2 < N(b)$$

□

