

12/5/06  $R$  an integral domain.

$r$  nonunit is  
 Recall irreducible means any factorization  $r=ab$ ,  $a$  or  $b$  must be a unit.

$p \neq 0$  is prime is  $plab \Rightarrow pla$  or  $p|b$

Thm

1. In I.D. prime  $\Rightarrow$  irred. ( $2 \in \mathbb{Z}/6\mathbb{Z}$  is prime, not irred!)

2. In a PID prime  $\Leftrightarrow$  irred. ( $3$  is irred, not prime in  $\mathbb{Z}[\sqrt{-5}]$ )

Def An integral domain  $R$  is a U.F.D. if every nonunit  $r \neq 0$  factors

(i)  $r = p_1 p_2 \dots p_n$  into irreducibles,

(ii) factorization unique up to order & associates!

Examples

1. Any field trivially

2. PIDs

3.  $R$  a UFD  $\Rightarrow R[x]$  is (False! PID, E.D.)

4.  $\mathbb{Z}[2i]$  not a UFD

$$4 = 2 \cdot 2$$

$$4 = (2i)(-2i)$$

$2i$  &  $2$  not associates!

Remark  $\mathbb{Z}[i]$  is a UFD.

Prop In a UFD, prime  $\leftrightarrow$  irred

Proof ETS irred  $\Rightarrow$  prime. Let  $p$  be irreducible and  $plab$ , so  $ab=pc$ . Now factor  $a$  &  $b$ .

Prop In a UFD, gcd's exist.

Proof Write  $a = u p_1^{e_1} \dots p_n^{e_n}$   $b = v p_1^{f_1} \dots p_n^{f_n}$   
 Choose  $d = p_1^{\min\{e_1, f_1\}} \dots p_n^{\min\{e_n, f_n\}}$   
 Claim  $d$  is a gcd.

Theorem PID  $\Rightarrow$  UFD

Proof Let  $R$  be a PID,  $0 \neq r \in R$  a nonzero.

Step 1 Show  $r$  factors into irreducibles  
 If  $r$  irred, done. Else  $r = r_1 r_2$ , keep factoring!  
 $(r) \subset (r_1) \subset (r_{11}) \dots$

Process terminates else  $(r) \subset (r_1) \subset (r_{11}) \subset \dots \subset R$

Lemma In a PID any ascending chain terminates (Rank only used ideals)  
 t.e.

Cor Factorization terminates

Steps Suppose  $f = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$   $m \geq 4$ .

$p_i \nmid \prod_{j \neq i} p_j$  so  $R$  divides some  $q_i$ ,  $p_i | q_i u$  cancel  
Thus  $p_i = q_i u$  cancel and  $m \geq 4$ .

Corollary (FTO arithmetic)  $\mathbb{Z}$  is a UFD

Corollary Let  $R$  be a PID then  $R$  has a multiplicative Dedekind-Hasse norm. (Greene 1997)

Proof  $R$  is a PID & a UFD. Define  $N(0) = 0$ ,  $N(u) = 1$  if  $u$  a unit,  $N(a) = 2^n$   $n = \#$  irreducible factors.

Suppose  $a, b \in R$ . Let  $(a, b) = (r)$ . We must show  $(a, b)$  has an element of norm smaller than norm of  $b$  or that  $b \in (a)$ .

If  $b \notin (a)$  then  $\exists a \in (b)$  then  $r \in (b)$  so  $b = xr$   $x$  not a unit.  
Thus  $N(b) > N(r)$  //

## Summary

### Euclidean Domains

- \* gcd's exist,  $\text{gcd}(a,b) = ax + by$
- \* algorithm to find gcd's
- \* gcd's unique up to units

E.D.  $\Rightarrow$  PID

### Principal Ideal Domains

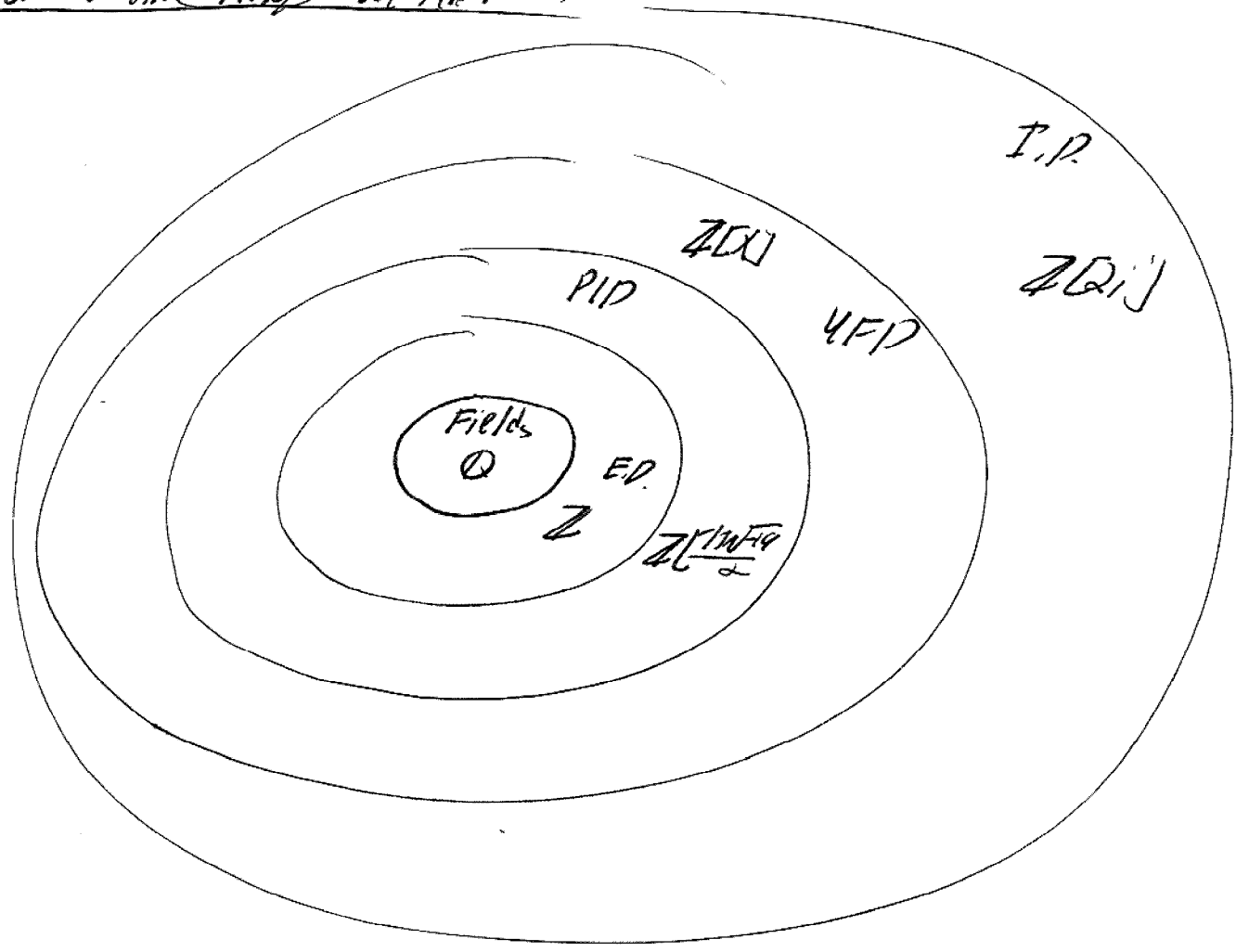
- \* gcd's exist
- \*  $d = ax + by$ , unique up to unit
- \* no algorithm
- \* prime ideal  $\iff$  maximal
- \* I.D. is a PID  $\iff \exists$  Dedekind-Hasse Num.
- \* prime  $\iff$  irreducible

PID  $\Rightarrow$  UFD

### Unique Factorization Domains

- \* prime  $\iff$  irreducible
- \* gcd's exist, must factor to find them

Commutative rings w/ identity



Some assorted examples. - -

Def. Let  $D$  be a squarefree integer.  $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$   
is a field.

$$(a + b\sqrt{D})^{-1} = \frac{a - b\sqrt{D}}{a^2 - Db^2} \quad \text{quadratic extension of } \mathbb{Q}$$

Rmk. Assuming  $D$  is squarefree is no loss of generality.

Def.  $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$  is a subring.

Lemma.  $D \equiv 1 \pmod{4}$  then  $\mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right] = \left\{a + b \frac{1 + \sqrt{D}}{2} \mid a, b \in \mathbb{Z}\right\}$  is a subring.

$$\left(a + b \frac{1 + \sqrt{D}}{2}\right) \left(c + d \frac{1 + \sqrt{D}}{2}\right) = ac + bd \frac{D+1}{4} + (ad + bc) \frac{1 + \sqrt{D}}{2}$$

Def.  $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega]$  where  $\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{D}}{2} & D \equiv 1 \pmod{4} \end{cases}$

This is the ring of integers in the field  $\mathbb{Q}(\sqrt{D})$

Example  $D = -1$ ,  $\mathbb{Z}[i]$

Def.  $N: \mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{Q}$   $N(a + b\sqrt{D}) = a^2 - Db^2$   
Field norm