

## 8. PID's, UFD's and Euclidean domains (Chapters 11.1-11.3)

$R$ -a domain, i.e. a commutative unital integral domain  
 $R^* = R \setminus \{0\}$

Definition 8.1 Let  $r, s \in R$ . We say that  $r$  divides  $s$  if  $\exists t \in R$  such that  $s = rt$ . In this case we write  $r|s$ .

Definition 8.2 (1) An element  $p \in R^*$  is prime if:  
(i)  $p$  is not a unit, and  
(ii)  $p|rs \Rightarrow p|r$  or  $p|s$  for  $r, s \in R$ .  
(2) An element  $q \in R^*$  is irreducible if  
(i)  $q$  is not a unit, and  
(ii)  $q = rs$  for some  $r, s \in R \Rightarrow r$  or  $s$  is a unit.

Example 8.3 (1)  $R = \mathbb{Z}$ , units are  $\pm 1$ ,  
 $\left\{ \begin{array}{l} \text{prime} \\ \text{elements} \end{array} \right\} = \left\{ \begin{array}{l} \pm \\ \text{numbers} \end{array} \right\} = \left\{ \begin{array}{l} \text{irreducible} \\ \text{elements} \end{array} \right\}$ .  
(2)  $R = F[X]$  where  $F$  is a field, units are nonzero constant polynomials,  
 $\left\{ \begin{array}{l} X+a \\ a \in F \end{array} \right\} \subsetneq \left\{ \begin{array}{l} \text{prime} \\ \text{elements} \end{array} \right\} = \left\{ \begin{array}{l} \text{irreducible} \\ \text{elements} \end{array} \right\}$

Lemma 8.4. Let  $R$  be an integral domain.

(1) Let  $r, s \in R$ . Then  $r|s$  and  $s|r \Rightarrow \exists$  unit  $u \in R$  such that  $s = ur$ .

(2) Let  $r, p \in R$ ,  $r$  not a unit,  $p$  prime. Then  $r|p \Rightarrow \exists$  unit  $u \in R$  such that  $r = up$ .

(3) Let  $p, u \in R$ ,  $u$  a unit. Then

$$p \text{ is } \begin{cases} \text{irreducible} \\ \text{prime} \end{cases} \iff pu \text{ is } \begin{cases} \text{irreducible} \\ \text{prime} \end{cases}$$

(4) Let  $p \in R$ . Then  $p$  is prime  $\implies p$  is irreducible.

(5) Let  $r, s \in R$ . Then  $r|s \iff (s) \subseteq (r)$ .

Proof. Exercise.

□

Definition 8.5.  $R$  is a unique factorization domain (UFD)

iff:

(i)  $\forall r \in R^*$ ,  $r$  not a unit,  $\exists$  irreducible elements  $p_1, \dots, p_n \in R$  with  $r = p_1 \cdots p_n$ , and

(ii) if  $\exists$  irreducible elements  $q_1, \dots, q_m$  such that

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

then  $n=m$  and, up to reordering, we have  $p_i = u_i q_i$  for all  $1 \leq i \leq n$ , where  $u_i \in R$  are units.

Theorem 8.6. Let  $R$  be a PID and  $p \in R$  be irreducible. Then  $p$  is prime.

Proof. Assume  $p|rs$  and  $p \nmid r$  and we show  $p|s$ . Since  $R$  is a PID,  $\exists x \in R$  such that

$$(p) + (r) = (x).$$

Since  $p \in (p) \subseteq (x)$ ,  $\exists y \in R$  such that  $p = xy \xrightarrow{p \text{ irreducible}} x$  or  $y$  is a unit. If  $y$  is a unit, then

$$(p) = (xy) = (x)$$

and so

$$(p) + (r) = (p).$$

In particular  $r \in (p)$ , which contradicts  $p \nmid r$ . Hence

$x$  is a unit and so

$$(p) + (r) = (x) = R.$$

Therefore  $\exists c, d \in R$  such that

$$pc + rd = 1 \Rightarrow spc + srd = S.$$

Then  $p \mid rs \Rightarrow \left. \begin{array}{l} p \mid srd \\ p \mid spc \end{array} \right\} \Rightarrow p \mid S.$

□