

## 5. PRINCIPAL RINGS

(Lecture by Alex Charis, notes by Andrew Gainer)

**Definition 5.1.** Given a ring  $R$ , a *norm* is a function  $N : R \rightarrow \mathbb{N} \cup \{0\}$  with  $N(0) = 0$ .

**Definition 5.2.** A domain  $R$  is a *Euclidean domain* if there is a norm on  $R$  such that, for all  $a, b \in R$  with  $b \neq 0$ , there exists  $q \in R$  so that  $a = bq + r$  with  $r = 0$  or  $N(r) < N(b)$ .

**Example 5.3.** (1)  $R = \mathbb{Z}$  with  $N = |\cdot|$ .  
 (2)  $R = \mathbb{Z}[i]$  with  $N = |\cdot|$ .  
 (3)  $R = F[x]$  with  $F$  a field and  $N = \deg$ .

**Definition 5.4.** Let  $A$  be a domain. An element  $a \in A$  with  $a \neq 0$  is *irreducible* if  $a = bc$  only if  $b$  or  $c$  is a unit in  $A$ .

**Proposition 5.5.** Let  $a \in A$  be such that  $a \neq 0$  and  $(a)$  is prime. Then  $a$  is irreducible.

*Proof.* Suppose  $a = bc$ . Then  $bc \in (a)$ . So, one is in the ideal. Suppose that  $b \in (a)$ . Then  $b$  is not a unit because  $(a) \neq A$ . But  $b = ar$ . So,  $b = bcr$ . Since  $A$  is a domain,  $cr = 1$  and  $c$  is a unit as required.  $\square$

**Definition 5.6.** Let  $A$  be a domain and  $a \in A$ ,  $a \neq 0$ . Then  $a$  is said to have a *unique factorization into irreducibles* if there exist a unit  $u$  and irreducibles  $p_i$  so that  $a = up_1p_2 \cdots p_r$  and, if  $a = vq_1 \cdots q_s$  for  $v$  a unit and  $q_i$  irreducible, then  $s = r$  and  $q_i = u_i p_i$  up to reordering.

*Remark 5.7.* • If  $p$  is irreducible and  $u \in U(A)$ , then  $up$  is irreducible.  
 • By convention, for  $u \in U(A)$ ,  $u = u$  is a factorization into irreducibles (with  $r = 0$ ).

**Definition 5.8.** A domain  $A$  is a *unique factorization domain* (UFD) if every  $a \in A$  with  $a \neq 0$  has a unique factorization into irreducibles. Lang calls this a “factorial entire ring.”

**Definition 5.9.**  $a$  *divides*  $b$  (denoted  $a|b$ ) if there exists  $c \in A$  so that  $ac = b$ .

**Definition 5.10.** If  $d \in A$  such that  $d \neq 0$  then  $d$  is a *greatest common divisor* (gcd) of  $a$  and  $b$  if  $d|a$ ,  $d|b$  and, if, for  $e \neq 0$ ,  $e|a$ ,  $e|b$ , then  $e|d$ .

**Proposition 5.11.** If  $A$  is a PID and  $a, b \in A$  with  $a, b \neq 0$  then  $c$  is the gcd of  $a$  and  $b$  if  $(a, b) = (a) + (b) = (c)$ .

*Proof.* Since  $a, b \in (c)$  it is clear that  $c|a$  and  $c|b$ . Since  $c \in (a, b)$ , we can write  $c = va + sb$ . So, if  $d|a$  and  $d|b$  then  $c = vdx + sdy$  for some  $x, y \in R$ . So,  $d|c$  as required.  $\square$

[I reversed the order in the notes and put uniqueness first:]

**Lemma 5.12.** *If  $A$  is a PID,  $p$  is irreducible in  $A$  and  $a, b \in A$  with  $p|ab$  then  $p|a$  or  $p|b$ .*

*Proof.* Suppose  $p \nmid b$ . Then  $1 = \gcd(p, b)$ . So,  $1 = px + qb$ . So,  $a = pax + qab$ . So,  $p|a$ .  $\square$

This lemma implies the uniqueness of factorization in a PID. If  $a = p_1 \cdots p_r = q_1 \cdots q_s$  then  $p_1|a$  implies  $p_1|q_i$  for some  $i$ . So,  $q_i = up_1$ . Then  $up_2 \cdots p_r = q_1 \cdots \widehat{q}_i \cdots q_s$ . By induction on  $r$  it follows that  $r = s$  and the factorization is unique.

**Theorem 5.13.** *Let  $A$  be a PID. Then  $A$  is a UFD.*

*Proof.* Let  $S$  be the set of nonzero principal ideals whose generators do not have unique factorizations into irreducibles. Suppose  $S \neq \emptyset$ . Consider a chain  $(a_1) \subsetneq (a_2) \subsetneq \cdots$  which is as long as possible (or infinite) and take its union. This union must be an ideal and is therefore principal. So, we call its generator  $a$ . Then  $a \in (a_n)$ . So,  $(a) = (a_n)$  and the chain is finite. So, the generator of any ideal strictly containing  $(a)$  has a factorization.

Note that  $a$  cannot be irreducible (because then  $a = a$  is a factorization). So, we can write  $a = bc$  where  $b, c$  are not units. Then  $(b) \supsetneq (a)$  and  $(c) \supsetneq (a)$ . So,  $b, c$  have factorizations. Then the product of these factorizes  $a$  and the factorization is unique by the lemma. So,  $(a) \notin S$ , a contradiction. So,  $S = \emptyset$  which means that every nonzero element of  $A$  has a unique factorization.  $\square$