

## *PIDs and primes*

Okay, so now we've managed to generalize both the Division Algorithm and greatest common divisors to polynomial rings over fields. Before we ask the question "what else can be generalized?" let's pause for a moment to see what it is about polynomial rings  $k[x]$  that allowed us to perform our generalization.

**Definition.** Suppose the ring  $R$  has the property that every ideal  $I$  in  $R$  is principal. That is, given  $I$  there exists some  $d \in R$  such that  $I = (d)$ . We call  $R$  a \_\_\_\_\_ domain, or PID, for short.

### **Examples.**

1. From our last homework set, we know that  $\mathbb{Z}$  is a PID.
2. Since a field  $k$  has only two ideals (what are they?),  $k$  is easily seen to be a PID.
3. The next result will show that if  $k$  is a field then  $k[x]$  is a PID:

**Theorem (3.59).** If  $k$  is a field and  $I$  is an ideal in  $k[x]$ , then there exists a unique monic polynomial  $d(x) \in k[x]$  such that  $I = (d)$ .

*Proof.* We may as well assume that  $I \neq \{0_k\}$ . Why is this?

Thus there are nonzero polynomials in  $I$ , and we can choose one, say  $d(x)$ , of least degree. Why can we assume that  $d$  is monic?

You should be able to show that every  $g \in I$  is a multiple of  $d$ :

See how easy?

Not every polynomial ring is a PID. Your text (on page 261) shows that  $\mathbb{Z}[x]$  is not a PID, since the ideal

$$I = \{a_0 + a_1x + \cdots + a_nx^n \mid a_0 \text{ is even}\}$$

is not principal. Why does this not violate our theorem above?

If we compare our definition of a PID with our proof that showed the existence of GCDs, we can see that PIDs are exactly the places where we expect GCDs to exist!

Incidentally, since greatest common divisors in  $\mathbb{Z}$  go hand-in-hand with *least* \_\_\_\_\_, it should come as no surprise that in PIDs we can define the analogues of these latter creatures as well (see your text for more information).

What else? Well, I'll be darned if we can't generalize one of the most interesting ideas involving integers, *prime* numbers:

**Definition.** If  $R$  is a commutative ring and  $p \in R$  then  $p$  is called \_\_\_\_\_ if  $p \notin U(R) \cup \{0_R\}$  and if  $p = ab$  then either  $a \in U(R)$  or  $b \in U(R)$ .

**Examples.**

1. For  $R = \mathbb{Z}$ ,  $p$  is irreducible if and only if  $p$  is prime. Why is this?

2. If  $R = k[x]$  it's not too hard to describe the irreducible elements in  $R$ :

**Proposition (3.64).**  $p(x) \in k[x]$  is irreducible if and only if  $p$  cannot be written as a product  $fg$  in which both  $f$  and  $g$  are nonconstant polynomials satisfying  $\deg(f), \deg(g) < \deg(p)$ .

*Proof.*

**Homework.** Here are a few problems for you to think about for *Friday, February 13th*. (None are committee problems.)

1. Find all irreducible polynomials in  $\mathbb{Z}_2[x]$  of degree at most 3.
2. Find all irreducible polynomials in  $\mathbb{Z}_3[x]$  of degree at most 2.
3. Find all irreducible polynomials in  $\mathbb{Z}_4[x]$  of degree at most 1.

**Note:** Your first exam will be handed out on Monday, February 16th!