

## Ideals and Another Look

at Theorem 1.1.4

**Definition:** A non-empty subset  $I$  of the integers is called an *ideal* if it has the following three properties:

1. if  $a \in I$ , then  $-a \in I$ ;
2. if  $a, b \in I$ , then  $a + b \in I$ ; and
3. if  $a \in I$ , then  $az \in I$  for all integers  $z$ .

**Lemma:** If  $I$  is an ideal, then  $0 \in I$ .

**Theorem 1.1.4 redux:** If  $I$  is an ideal, then  $I$  consists of all integer multiples of some number.

In other words,  $I = a\mathbb{Z} = \{a \cdot z : z \in \mathbb{Z}\}$ .

**IMPORTANT:** You can prove this using the “Division Algorithm” (Theorem 1.1.3) and the fact that an ideal with more than one element has a non-zero element of least absolute value.

## Axioms for Polynomials

The set of polynomials with rational coefficients,  $\mathbb{Q}[X]$ , is a non-empty set with two binary operations  $+$  and  $\times$ . It has a shockingly familiar set of axioms.

The addition  $+$  satisfies the following:

1.  $(a + b) + c = a + (b + c)$  for any  $a, b, c \in \mathbb{Q}[X]$  ( $+$  is associative);
2. there is a polynomial  $0$  where  $0 + a = a + 0 = a$  for all  $a \in \mathbb{Q}[X]$  (there is an additive identity);
3. for every  $a \in \mathbb{Q}[X]$  there is a  $b \in \mathbb{Q}[X]$  where  $a + b = b + a = 0$  (every element has an additive inverse); and
4.  $a + b = b + a$  for all  $a, b \in \mathbb{Q}[X]$  (addition is commutative).

In other words,  $\mathbb{Q}[X]$  with  $+$  is an abelian group.

The multiplication  $\times$  satisfies the following:

1. it is associative;
2. it has an identity not equal to the additive identity;
3. it distributes through addition on both the left and right, i.e.,  $a \times (b + c) = a \times b + a \times c$  and  $(a + b) \times c = a \times c + b \times c$  for all  $a, b, c \in \mathbb{Q}[X]$ ; and
4. it is commutative.

So  $\mathbb{Q}[X]$  with  $+$  and  $\times$  satisfies the same axioms as  $\mathbb{Z}$  with  $+$  and  $\times$ .

Is there an order relation on  $\mathbb{Q}[X]$  which totally orders  $\mathbb{Q}[X]$  in the same way  $\leq$  totally orders  $\mathbb{Z}$ ?

## The Degree Function for Polynomials

Suppose  $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Q}[X]$  and  $a_n \neq 0$ . Then the *degree* of  $P(X)$  is  $n$ . The degree of 0 is defined to be  $-\infty$ . We write  $\deg(P(X))$  (or just  $\deg(P)$ ) for the degree of the polynomial  $P(X)$ .

Aside: for our purposes, we'll say  $-\infty < n$  and  $-\infty + n = -\infty$  for all integers  $n$ .

**Lemma:** For any two polynomials  $P(X)$  and  $Q(X)$ ,

$$\deg(P \times Q) = \deg(P) + \deg(Q)$$

and

$$\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}.$$

**Lemma:** If  $P(X) \times Q(X) = 0$ , then either  $P(X) = 0$  or  $Q(X) = 0$ .

**Division Algorithm:** For any polynomials  $A(X)$  and  $B(X)$  with  $B(X) \neq 0$ , there are polynomials  $Q(X)$  and  $R(X)$  with

$$A(X) = Q(X) \times B(X) + R(X)$$

and  $\deg(R) < \deg(B)$ .

We can prove this in a manner similar to the proof in the text for the division algorithm (Theorem 1.1.3).

**Proof:** If  $A(X) = 0$ , then we simply let  $Q(X) = R(X) = 0$ , too, and we're done.

Suppose  $A(X) \neq 0$ . Consider the set of all polynomials of the form  $A(X) - Q(X)B(X)$ . If 0 is in this set, then we're done. If not, then this set has an element of least degree (since the set of degrees of such polynomials is a non-empty subset of the natural numbers). Let  $R(X)$  be such a polynomial. Suppose  $\deg(R) \geq \deg(B)$ . We can write

$$R(X) = r_m X^m + \cdots + r_0,$$

where  $r_m \neq 0$ . Write

$$B(X) = b_n X^n + \cdots + b_0,$$

where  $b_n \neq 0$  and  $n \leq m$ . Then

$$R(X) - \frac{r_m}{b_n} X^{m-n} B(X) = 0X^m + \cdots$$

is also in the set of polynomials above, and moreover its degree is less than  $m$ . This contradicts the way  $R(X)$  was chosen, so  $\deg(R) < \deg(B)$ .

Little Results from the  
Axioms for Polynomials  
(with the same old proof hints)

**Lemma:** The additive identity is unique.

Of course, the identity element in any group is unique, right? To see this, try adding two putative additive identities together. What do you get?

**Lemma:** For any  $P(X)$ , the additive inverse of  $P(X)$  is unique.

And inverses in any group are unique, too. To see this, add  $P(X)$  to two putative inverses, getting 0. Now add the first inverse to each sum. What do you get?

**Lemma:** For any polynomial  $P(X)$ ,  $P(X) \times 0 = 0$ .

To see this, look at  $(0 + 0) \times P(X)$ . Note how we are using *more* than just the group structure here.

**Lemma:** For any polynomial  $P(X)$ ,  $-1 \times P(X) = -P(X)$ .

To see this, see what happens when you multiply  $(1 + -1)$  by  $P(X)$  using what we already know.

**Lemma:** If  $P(X) \times Q(X) = 0$ , then either  $P(X) = 0$  or  $Q(X) = 0$ .

(Recall we had the following little result for integers: If  $a > 0$ , then  $-a < 0$ . If  $a < 0$ , then  $-a > 0$ .)

Does the old “hint” still work?

“To see this, show that  $a \times b = 0$  implies that  $a \times b = a \times (-b) = -(a \times b)$ .”

**Lemma:** If  $P(X) \times Q(X) = P(X) \times R(X)$  and  $P(X) \neq 0$ , then  $Q(X) = R(X)$ .

**Lemma:** The multiplicative identity is unique.

## Ideals and Polynomials:

### Yet Another Look at Theorem 1.1.4

**Definition:** A non-empty subset  $I$  of the polynomials is called an *ideal* if it has the following three properties:

1. if  $a \in I$ , then  $-a \in I$ ;
2. if  $a, b \in I$ , then  $a + b \in I$ ; and
3. if  $a \in I$ , then  $az \in I$  for all polynomials  $z$ .

**Lemma:** If  $I$  is an ideal, then  $0 \in I$ .

**Theorem 1.1.4 for polynomials:** If  $I$  is an ideal, then  $I$  consists of all multiples of some polynomial. In other words,  $I = P(X)\mathbb{Q}[X] = \{P(X) \cdot Q(X) : Q(X) \in \mathbb{Q}[X]\}$ .

(Recall the former note: “You can prove this using the “Division Algorithm” (Theorem 1.1.3) and the fact that a non-zero ideal has a non-zero element of least absolute value.”)

**Proof:** If  $I$  consists of just 0, we’re done (use 0 for  $P(X)$ ). If not, the set of *degrees* of non-zero elements of  $I$  is a non-empty set of natural numbers. Therefore, it has a least element. This means there is a non-zero element  $P(X) \in I$  of least degree.

Now suppose  $A(X) \in I$ . By the division algorithm, we can divide  $A$  by  $P$  and get a remainder of degree smaller than the degree of  $P$ :

$$A(X) = Q(X) \times P(X) + R(X), \quad \deg(R) < \deg(P).$$

But  $R(X) = A(X) - Q(X) \times P(X)$  is in  $I$  since  $I$  is an ideal. So the only way  $R$  can have smaller degree than  $P$  is when  $R = 0$ .