

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 $R = 0$.

Definition: Given two polynomials $P(X)$ and $Q(X)$, not both 0, the greatest common divisor of P and Q is the monic common divisor of largest degree.

Why does such a beast exist? Just like with integers, we use Theorem 1.1.4 for polynomials to show that the set of linear combinations

$$I = \{P \cdot R + Q \cdot S : R(X), S(X) \in \mathbb{Q}[X]\} = D(X)\mathbb{Q}[X]$$

where D is a common divisor divisible by all other common divisors. Moreover, we can take D to be monic (which makes the choice unique).

We can find the greatest common divisor of two polynomials using the Euclidean algorithm for polynomials, just like we can for integers. It's a lot faster than factoring (especially considering that factoring polynomials can be extremely hard)!