

Homework for Math 420, Section 1

Week #2

In class we've discussed the set of polynomials with rational coefficients, $\mathbb{Q}[X]$. We saw how these polynomials satisfy a set of axioms very similar to the integers, how the degree of a polynomial could take the place of the absolute value, how the division algorithm held for polynomials, and how we could define ideals and prove a version of Theorem 1.1.4 for polynomials. This leads to a definition for greatest common divisor of two polynomials which is very similar to Definition 1.1.5 in the textbook. In fact, replace every instance of the word "integer" in Definition 1.1.5 with "polynomial" and the word "positive" with "monic," and you have a definition of greatest common divisor of two non-zero polynomials. One could prove the polynomial version of Theorem 1.1.6, and even compute the greatest common divisor via the Euclidean algorithm (for polynomials).

Exercise: Find the greatest common divisor of $4x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ in $\mathbb{Q}[X]$.

We could also look at the set of polynomials with *integer* coefficients, $\mathbb{Z}[X]$. It isn't difficult to see that $\mathbb{Z}[X]$ satisfies the same eight axioms for addition and multiplication that the integers and $\mathbb{Q}[X]$ satisfy. Also, just as with $\mathbb{Q}[X]$, we have the degree of polynomials with integer coefficients as a substitute for "size," with the same two basic results:

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

and

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

for any two polynomials $P(X), Q(X) \in \mathbb{Z}[X]$. However, unlike $\mathbb{Q}[X]$, the division algorithm doesn't hold for $\mathbb{Z}[X]$. For example, if we divide X by 2 (in $\mathbb{Z}[X]$) we can't get a remainder of degree less than 1.

Just as with $\mathbb{Q}[X]$, there is a definition for ideal.

Definition: A non-empty subset I of $\mathbb{Z}[X]$ 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 $a + b \in I$;
3. if $a \in I$, then $az \in I$ for all $z \in \mathbb{Z}[X]$.

Now we used the division algorithm (for integers and polynomials with rational coefficients) to prove Theorem 1.1.4, which says that all ideals consist of the multiples of an element (of \mathbb{Z} or $\mathbb{Q}[X]$). Since we don't have a division algorithm for $\mathbb{Z}[X]$, you might wonder if Theorem 1.1.4 is true or not for $\mathbb{Z}[X]$. In fact, it is false.

Exercise: Give an example of a subset $I \subseteq \mathbb{Z}[X]$ which is an ideal, but I is *not* of the form $\{P(X) \times Q(X) : Q(X) \in \mathbb{Z}[X]\}$.