Math 547/702I – Notes on Polynomial Rings

Frank Thorne

February 1, 2015

These notes will develop the theory of *polynomial rings* and their ideals.

Throughout, except where explicitly noted to the contrary, we write R for an arbitrary commutative ring with unity. This theory is still interesting if you relax these applications! – but we will concentrate on the most common case.

0.1 Polynomial rings

Definition 1 *We write $R[x]$ for the set of polynomials*

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where each of the a_i is in R.

If $a_n \neq 0$ then we refer to n as the *degree* of the polynomial. (And if $a_n = 0$ then we rewrite our polynomial so as to omit the zero coefficients, and the degree will be less than n.) The degree of a polynomial can be any nonnegative integer, but not that we do not allow infinite power series.

Theorem 2 *If R is a commutative ring with unity, then so is $R[x]$.*

The proof of this is rather boring and so we omit it. I presume that you are familiar with addition and multiplication of polynomials, and could verify the associative and distributive laws step by step if forced to.

We also consider polynomial rings in multiple variables. We write $R[x_1, \cdots x_r]$ for the ring of polynomials in the variables x_1 through x_r; the elements of $R[x_1, \cdots x_r]$ are precisely finite sums of terms of the form $a x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r}$, where $a \in R$ and the e_i are all nonnegative numbers.

We can also use other variables (i.e., write $R[x, y]$ for the ring of polynomials with two variables).

Exercise 1 *Explain informally why $R[x, y] = (R[x])[y]$. Generalize!*

0.2 Ideals in polynomial rings

Recall that if R is any commutative ring with unity (where we most definitely include the case that $R = S[x]$, where S is some other commutative ring with unity), the *principal ideal* generated by an element $r \in R$ is the set

$$(r) := \{ra \ : \ a \in R\}.$$

Exercise 2 *Prove (in this generality) that any principal ideal is, in fact, an ideal.*

In polynomial rings we encounter ideals which are not principal.

Exercise 3 *In the ring $R[x, y]$, let I be the ideal of polynomials of degree at least one. Prove that I is a nonprincipal ideal.*

Exercise 4 *If I and J are ideals of R, let*

$$I + J := \{a + b \ : \ a \in I, b \in J\}.$$

1. *Prove that $I + J$ is an ideal.*
2. *Prove that $I + J$ is the minimal ideal which contains both I and J. (In other words, prove that $I + J$ contains I and J, and that if K is any other ideal containing I and J we have $I + J \subseteq K$.)*
3. *Prove that in general $I + J \neq I \cup J$. (It is enough to find a counterexample with $R = \mathbb{Z}$.)*

If $r_1, \ldots r_k \in R$, then we write $(r_1, \cdots r_k)$ to mean $(r_1) + \cdots + (r_k)$.

Exercise 5 *In $\mathbb{Z}$, prove that the ideal $(6, 11)$ is principal. (In other words, prove that it equals (a) for some $a \in \mathbb{Z}$.)*

0.3 Polynomial rings as abelian groups

Recall that if R is any ring whatsoever, then $(R, +)$ is an abelian group, and any subgroup is normal. In particular, if I is any ideal of R, then $(I, +)$ is a normal subgroup of R.

Exercise 6 *Review the theory of quotient groups, normal subgroups, and homomorphisms – including Theorem 13.2 of Saracino, or its equivalent in other books or your notes.*

Exercise 7 *Prove, as abelian groups, that*

$$\mathbb{Z}[x]/(x) \simeq \mathbb{Z}.$$

The best way to do this is to construct a homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ and prove that its kernel is (x).

Exercise 8 *Prove, as abelian groups, that*

$$\mathbb{Z}[x]/(x^2) \simeq \mathbb{Z} \times \mathbb{Z},$$

that

$$\mathbb{Z}[x, y]/(x^2, xy, y^2) \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z},$$

and that for any polynomial f of degree 3 we have

$$\mathbb{Z}[x]/(f) \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}.$$

Later, we will discuss a quotient *ring* structure: 'ideal' will turn out be the correct analogy of 'abelian group'.

Exercise 9 *Prove, as abelian groups, that*

$$\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}.$$

Formally we have not yet learned what an isomorphism of rings is, but $\mathbb{C}$ is an integral domain and $\mathbb{R} \times \mathbb{R}$ is not, so you can damn well guess that your isomorphism is *not* an isomorphism of rings.

0.4 Division algorithm for $F[x]$.

Please read Theorem 19.2, including its proof, in Saracino.

Exercise 10 *Prove that the theorem still holds if the field F is replaced with any commutative ring with unity R, provided that the leading coefficient of $g(X)$ is a unit in R.*

Moreover, find a counterexample that shows that the condition that the leading coefficient be a unit cannot be removed. (I recommend looking for a counterexample in $\mathbb{Z}[x]$.)

0.5 Proving that $F[x]$ is a principal ideal domain

Theorem 3 *Let F be a field, and let I be any nonzero ideal of $F[x]$. Then I is a principal ideal.*

(We call $F[x]$ a *principal ideal domain* or *PID.*)
Proof: Let n be the minimal degree of any polynomial in I. Then, if $I \neq F[x]$, we have $n \geq 1$. (Why?) Choose any polynomial $f \in I$ which is of degree n. We claim that $I = (f)$. To prove this, suppose $g \in I - f$. Then, by the division algorithm, we may write uniquely

$$g = f \cdot q + r,$$

where r has degree less than n. Now, we have $f \in I$ and $g \in I$, so $r = g - f \cdot q \in I$. Moreover, $r \neq 0$ because $g \notin (f)$.

But we have just found an element of I of degree less than n, which is a contradiction. □

Exercise 11 *That proof was really important and beautiful. Please read it again.*

Exercise 12 *In $\mathbb{R}[x]$, write the ideals (x^3, x^4), $(x^3, x^4 + x^2)$, and $(x^3, x^5 - 2x + 1)$ as principal ideals.*

(Discuss the primality and maximality of various ideals of $\mathbb{R}[x]$ and $\mathbb{R}[x, y]$.)