POLYNOMIALS

LECTURE NOTES: MATH 422, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

1. Polynomial Rings

Let R be a commutative ring. Then $R[x]$ signifies the set of polynomials $a_n x^n + \ldots + a_1 x + a_0$ with coefficients $a_i \in R$. For example, $7x^3 - 3x^2 + 11$ is in $\mathbb{Z}[x]$, which is also in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and in $\mathbb{C}[x]$ since $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Observe that $\frac{7}{11}x^3 - 3x^2 + 11$ is in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$. Observe that $7x^3 - \sqrt{2}x^2 + x - 11$ is in $\mathbb{R}[x]$ but not in $\mathbb{Q}[x]$.

If $a_n x^n + \ldots + a_1 x + a_0$ is a polynomial with coefficients a_i, we adopt the convention that $a_i = 0$ for all values of i not occurring in the expression $a_n x^n + \ldots + a_1 x + a_0$. For example, when writing $7x^3 + x - 11$ as $a_n x^n + \ldots + a_1 x + a_0$, then we consider $a_2 = 0$ and $a_4 = 0$, but $a_3 = 7$ and $a_0 = 11$, etc. Two polynomials $a_n x^n + \ldots + a_1 x + a_0$ and $b_k x^k + \ldots + b_1 x + b_0$ are defined to be equal if $a_i = b_i$ for all $i \geq 0$.

For example, $\overline{6}x^3 + \overline{2}x^2 - x + \overline{1} = -x^2 + \overline{2}x + \overline{1}$ in $\mathbb{F}_3[x]$.

Among the polynomials in $R[x]$ are the *constant* polynomials a_0. In other words, $a_0 \in R$ it can be thought of as both an element of R and as a constant polynomial in $R[x]$. Thus $R \subset R[x]$.

We define multiplication and addition of polynomials in the usual way. (I will skip the details of the definition since these procedures are so familiar). Both operations are closed on $R[x]$. For example, in $\mathbb{Z}_6[x]$ the product of $\overline{2}x^2 + \overline{3}x + \overline{1}$ with $\overline{3}x^2 + \overline{2}$ can be computed as follows

$$(\overline{2}x^2 + \overline{3}x + \overline{1})(\overline{3}x^2 + \overline{2}) = \overline{6}x^4 + \overline{4}x^2 + \overline{9}x^3 + \overline{6}x + \overline{3}x^2 + \overline{2} = \overline{3}x^3 + x^2 + \overline{2}.$$

Exercise 1. Multiply $\overline{2}x^2 + \overline{3}x + \overline{1}$ by $\overline{3}x^2 + \overline{x} - \overline{2}$ in $\mathbb{F}_5[x]$.

Multiplication and addition are defined on $R[x]$ and are closed in the sense that the result is in $R[x]$. So $+$ and $\times$ give two binary operations $R[x] \times R[x] \to R[x]$. These operations are associative and commutative (we skip the proofs). The distributive law holds between them. The constant polynomials 0 and 1, given by $0, 1 \in R$, are respectively the additive and multiplicative identities. Given a polynomial f, when we multiply each coefficient by -1 we get another polynomial $-f$ such that $f + (-f) = 0$. These properties taken together give us the following:

Theorem 1. *Let R be a commutative ring. Then the set $R[x]$ is a commutative ring under the usual addition and multiplication.*

2. Substitutions

If $f \in R[x]$ then $f(a)$ denotes what we get when we substitute a for x in f. It is defined whenever the substitution makes sense (typically when a is in R, or when a is in a ring containing R). For example, $f(x)$ is just f itself since when we replace x with x we get

Date: Spring 2008. Version of April 5, 2009.

what we started with. So $f(x)$ is another way of writing f. I will typically write f, but will write $f(x)$ whenever I want to remind you that f is a polynomial in x. Another example: if $f = x^2 + \overline{1}$ in $\mathbb{Z}_8[x]$ then $f(\overline{3}) = \overline{2}$. Yet another example: if $f = x^3$ in $\mathbb{Z}_{12}[x]$ then $f(x + \overline{2}) = (x + \overline{2})^3 = x^3 + \overline{6}x^2 + \overline{8}$. (Did you see what happened to the linear term?). If $f \in R[x]$, and y is another variable, then $f(y)$ is in $R[y]$ and has the same coefficients. However, if x and y are different variables, then $f(x)$ is not considered to be equal to $f(y)$ (although if f is a constant polynomial, you can consider them to be equal in the common subring R). If $f = c$ is a constant polynomial, then $f(a) = c$ for all $a \in R$. Observe that if $a \in R$ and $f \in R[x]$ then $f(a) \in R$. Addition and multiplication were defined in such a way to make the following true: $(f + g)(a) = f(a) + g(a)$ and $(f \cdot g)(a) = f(a) \cdot g(a)$ for all $a \in R$. A fancy way of saying this is that substitution is a "homomorphism".

Here is an amusing example. Let $f = x^3 - x \in \mathbb{Z}_3[x]$. Then $f(\overline{0}) = \overline{0}$, $f(\overline{1}) = \overline{0}$, and $f(\overline{2}) = \overline{0}$. So $f(a) = \overline{0}$ for all $a \in \mathbb{Z}_3$ but $f \neq \overline{0}$. So polynomials cannot be treated as functions when R is finite: two distinct polynomials, for example, f and $\overline{0}$ above, can have identical values. This cannot happen for functions.

Definition 1. An element $a \in R$ is called a *root* of $f \in R[x]$ if $f(a) = 0$. The above example is amusing: every element of $\mathbb{Z}_3$ is a root of $x^3 - x \in \mathbb{Z}_3[x]$.

Exercise 2. Find the roots of $x^3 - \overline{1}$ in $\mathbb{F}_7$. Find the roots of $x^3 - \overline{1}$ in $\mathbb{F}_5$.

Remark. For $R = \mathbb{Z}_m$, I will dispense with the practice of writing bars over integers to denote elements. Instead of writing $\overline{3}$, say, I will write 3 to denote the equivalence class of the integer 3 in $\mathbb{Z}_m$. As long as I am clear about the ring of coefficients R, this practice should not result in any confusion.

3. The Quotient-Remainder Theorem for Polynomials

Let F be a field. The ring of polynomials $F[x]$ has a quotient-remainder theorem, a Bezout's identity, a Euclidean algorithm, and a unique factorization theorem. In fact, $F[x]$ and $\mathbb{Z}$ have a surprising number of similarities.

Let's begin with the quotient-remainder theorem. To state this theorem we need to discuss a notion of size for $F[x]$ traditionally called the *degree*:

Definition 2. Let $f \in R[x]$ where R is a commutative ring. If $f = a_n x^n + \ldots + a_1 x + a_0$ with $a_n \neq 0$ then the *degree* of f is defined to be n and the *leading coefficient* is defined to be a_k. If $f = 0$ then the degree of f is not defined as an integer (some authors define it to be $-\infty$).

Be careful when using this definition modulo m. For example, $6x^3 + 2x^2 - x + 1$ in $\mathbb{F}_3[x]$ has only degree 2, and $6x^3 + 2x^2 - x + 1$ in $\mathbb{F}_2[x]$ has degree 1. However, $6x^3 + 2x^2 - x + 1$ in $\mathbb{F}_5[x]$ has degree 3

You would hope that the degree of fg would be the sum of the degrees of f and g individually. However, examples such as $(2x^2 + 3x + 1)(3x^2 + 2) = 3x^3 + x^2 + 2$. in $\mathbb{Z}_6[x]$ spoil our optimism. However, if the coefficients are in a field F then it works.

Proposition 1. *If $f, g \in F[x]$ are non-zero polynomials where F is a field, then*

$$\deg(fg) = \deg f + \deg g.$$

Exercise 3. Give a proof of the above theorem. Explain why the proof does not work if the coefficients are in $\mathbb{Z}_m$ where m is composite.

As mentioned above, the degree of a polynomial is a measure of size. When we divide we want the size of the remainder to be smaller than the size of the quotient. This leads to the following:

Theorem 2 (Quotient-Remainder Theorem for Polynomials)**.** *Let $f, g \in F[x]$ be polynomials where F is a field. Assume g is not zero. Then there are unique polynomials $q(x)$ and $r(x)$ such that (i) $f(x) = q(x)g(x) + r(x)$, and (ii) the polynomial $r(x)$ either the zero polynomial or has degree strictly smaller than $g(x)$.*

Remark. The polynomial $q(x)$ in the above is called the *quotient* and the polynomial $r(x)$ is called the *remainder*.

Remark. This theorem actually holds for polynomials in $R[x]$ where R is a commutative ring that is not a field, as long as we add the extra assumption that the leading coefficient of g is a unit in R.

Remark. We can use this theorem as a basis to prove theorems about GCD's and unique factorization in $F[x]$ just as we did for $\mathbb{Z}$.

As an important special case, consider $g(x) = x - a$ where $a \in R$. Then $r(x)$ must be zero, or have degree zero. So $r = r(x)$ is a constant: $r \in R$. What is this constant? Well $f(x) = q(x)(x - a) + r$ so when we substitute $x = a$ we get

$$f(a) = q(a)(a - a) + r = 0 + r = r.$$

In other words, $r = f(a)$. This gives the following:

Corollary 1. *Let $a \in F$ where F is a field, and let $f \in F[x]$. Then there is a $q \in F[x]$ such that*

$$f(x) = (x - a)q(x) + f(a).$$

Remark. This actually works for commutative rings as well as for fields F since the leading coefficient of $g(x) = x - a$ is 1 which is always a unit.

The following is a special case of the above corollary (where $f(a) = 0$).

Corollary 2. *Let $a \in F$ where F is a field, and let $f \in F[x]$. Then a is a root of f if and only if $(x - a)$ divides f.*

4. A Theorem of Lagrange

As you learned long ago, a polynomial f with coefficients in $\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) has at most $n = \deg f$ roots. This generalizes to all fields.

Theorem 3. *Let $f \in F[x]$ be a non-zero polynomial with coefficients in a field F. Then f has at most $n = \deg f$ roots in F.*

Proof. This is proved by induction. The induction statement is as follows: *if f has degree n then f has at most n roots in F.* The case $n = 0$ is easy. In this case f is a non-zero constant polynomial which obviously has no roots.

Suppose that the statement is proved for $n = k$. We want to prove it for $n = k+1$. To do so, let f be a polynomial of degree $k+1$. If f has no roots, then the statement is trivially true. Suppose that f does have a root $a \in F$. Then, by Corollary 2,

$$f(x) = q(x)(x - a).$$

By Proposition 1, $\deg f = 1 + \deg q$. In other words, $\deg q = k$. By the inductive hypothesis, q has at most k roots.

We will now show that the only possible root of f that is not a root of q is a (but a could also be a root of q). Suppose that f has a root $b \neq a$. Then $0 = f(b) = q(b)(b - a)$. Since $b - a \neq 0$, we can multiply both sides by the inverse: $0(b-a)^{-1} = q(b)(b-a)(b-a)^{-1}$. Thus $0 = q(b)$. So every root of f not equal to a must be a root of $q(x)$. Since $q(x)$ has at most k roots, it follows that $f(x)$ must have at most $k+1$ roots. □

The following is usually attributed to Lagrange.

Corollary 3 (Lagrange)**.** *Let $f \in \mathbb{F}_p[x]$ be a non-zero polynomial with coefficients considered modulo p where p is a prime. Then f has at most $\deg f$ roots in $\mathbb{F}_p$.*

Proof. It follows from the previous theorem since $\mathbb{F}_p$ is a field. □

Remark. Observe how this can fail if m is not a prime. The polynomial $x^2 - 1 \in \mathbb{Z}_8$ has degree 2, yet it has four roots! (Can you find them?)

Of course, Lagrange and Gauss would have stated (and proved) Corollary 3 differently since the concept of a field is essentially a twentieth century idea. They might have said something closer to

If p is a prime and $f(x)$ is a polynomial with integer coefficients not all divisible by p, then the congruence $f(x) \equiv 0$ has at most $\deg f$ solutions modulo p.

or

If p is a prime and $f(x)$ is a polynomial with integer coefficients not all divisible by p, then $p | f(a)$ for at most $\deg f$ integers a in the range $0 \le a < p$.

Exercise 4. Show that if $f, g \in F[x]$ are non-zero polynomials where F is a field, then the set of roots of fg is the union of the set of roots of f with the set of roots of g.

Exercise 5. Show that the result of the above exercise does not hold $\mathbb{Z}_8[x]$ by looking at $x^2 - 1$.

Exercise 6. Although the result of Exercise 4 does not hold if F is replaced by a general ring (such as $\mathbb{Z}_m$ where m is composite), one of the two inclusions does hold. Which one and why?

5. Irreducible Polynomials

One can prove unique factorization into irreducible polynomials for $F[x]$. A polynomial $f \in F[x]$ is said to be *irreducible* if it is not a constant and if it has no divisors g with $0 < \deg g < \deg f$. These polynomials play the role of prime numbers in polynomial rings. One can prove, in a manner similar to that used for primes in $\mathbb{Z}$, that there is an infinite number of irreducible polynomials in $F[x]$ (even when F is finite).