CHAPTER 10: POLYNOMIALS (DRAFT)

LECTURE NOTES FOR MATH 378 (CSUSM, SPRING 2009). WAYNE AITKEN

The material in this chapter is fairly informal. Unlike earlier chapters, no attempt is made to rigorously prove the results contained here.[1]

1. Polynomial Rings

Definition 1. Let R be a commutative ring, and x a variable. Then $R[x]$ is the set of polynomial $a_n x^n + \ldots + a_1 x + a_0$ with coefficients $a_i \in R$.

Example. Observe that $7x^3 - 3x^2 + 11$ is in $\mathbb{Z}[x]$. It is also in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and in $\mathbb{C}[x]$ since $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Observe that $\frac{7}{11}x^3 - 3x^2 + 11$ is in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$. Observe that $7T^3 - \sqrt{2}T^2 + T - 11$ is in $\mathbb{R}[T]$ but not in $\mathbb{Q}[T]$. Observe that $Z - i$ is in $\mathbb{C}[Z]$ but not in $\mathbb{C}[S]$.

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 $7x^3 + x - 11$ in the form $a_n x^n + \ldots + a_1 x + a_0$, we consider $a_2 = 0$ and $a_4 = 0$, but $a_3 = 7$ and $a_0 = 11$. 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 and only if $a_i = b_i$ for all $i \geq 0$.

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

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

We define multiplication and addition of polynomials in the usual way. 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 $\mathbb{F}_5[x]$.

The set $R[x]$ is closed under addition and multiplication. So $+$ and $\times$ give two binary operations $R[x] \times R[x] \to R[x]$.

Lemma 1. *If R is a commutative ring, then addition and multiplication are associative and commutative on $R[x]$. In addition, the associative law holds.*

Date: version of May 4, 2009.

[1] This may change in the 2010 edition

Lemma 2. *If R is a commutative ring, then the constant polynomial* 0 *is an additive identity for $R[x]$, and the constant polynomial* 1 *is a multiplicative identity for $R[x]$.*

Theorem 3. *If R is a commutative ring, then $R[x]$ is also a commutative ring.*

2. Substitutions

Definition 2. 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).

Example. If $f = x^2 + \overline{1}$ in $\mathbb{Z}_8[x]$ then $f(\overline{3}) = \overline{2}$.

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?).

Example. 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 $f(y)$ unless f is a constant polynomial.

Example. Let $f \in R[x]$. Observe that $f(x)$ is just f itself since when we replace x with x we get what we started with. So $f(x)$ is another way of writing f. So we can write f as $f(x)$ when we want to emphasize that f is a polynomial in x.

Example. 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 $\overline{0}$ as above, can have identical values. This cannot happen for functions.

Definition 3 (Root of a polynomial)**.** Let $f \in R[x]$ and $a \in R$. If $f(a) = 0$ then a is called a *root* of $f \in R[x]$.

The above example (preceding the definition) shows that every element of $\mathbb{F}_3$ is a root of $x^3 - x \in \mathbb{F}_3[x]$.

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

3. The Quotient-Remainder Theorem for Polynomials

Let F be a field. The ring of polynomials $F[x]$ has a quotient-remainder theorem. To state this theorem we need to discuss a notion of size for $F[x]$ traditionally called the *degree*:

Definition 4. Let $f \in R[x]$ where R is a commutative ring. If f has form $a_n x^n + \ldots + a_1 x + a_0$ with $a_n \neq 0$ then the *degree* of f is defined to be n and the *leading coefficient* is defined to be a_n.

If $f = 0$ then the degree of f is said to be *undefined* (some authors give it degree $-\infty$).

Be careful when using this definition in modular arithmetic. 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.

Theorem 4. *If $f, g \in F[x]$ are non-zero polynomials where F is a field, then*

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

Informal Exercise 3. Justify the above theorem. Explain why the proof does not work if the coefficients are in $\mathbb{Z}_m$ where m is composite. Hint: focus on the leading coefficients.

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 5 (Quotient-Remainder Theorem)**.** *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 $r(x)$ is either the zero polynomial or has degree strictly smaller than $g(x)$.*

Remark 1. The polynomial $q(x)$ in the above is called the *quotient* and the polynomial $r(x)$ is called the *remainder*.

Remark 2. This theorem extends to 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 3. We could use this theorem as a basis to prove theorems about GCD's and unique factorization in $F[x]$.

As an important special case of the above theorem, consider $g(x) = x - a$ where $a \in R$. Then the remainder $r(x)$ must be zero, or have degree zero. So $r = r(x)$ is a constant polynomial. What is this constant? To find out, write $f(x) = q(x)(x - a) + r$. 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 6. *Let $a \in F$ where F is a field, and let $f \in F[x]$. Then there is a unique polynomial $q \in F[x]$ such that*

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

Remark 4. 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 7. *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. The number of roots

Theorem 8. *Let $f \in F[x]$ be a nonzero polynomial with coefficients in a field F. Then f has at most $n = \deg f$ roots in F.*

Proof. This is proved by induction. Let S be the set of natural numbers n such that every polynomial f that has degree n has at most n roots in F. Our goal is to show that $S = \mathbb{N}$.

Showing $0 \in S$ is easy. If f is a non-zero constant polynomial of degree 0, then it has 0 roots since it is a nonzero constant polynomial.

Suppose that $k \in S$. We want to show $k + 1 \in S$. 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 7,

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

By Proposition 4, $\deg f = 1 + \deg q$. In other words, $\deg q = k$. By the inductive hypothesis $k \in S$, the polynomial 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. So $k + 1 \in S$.

By the principle of mathematical induction, $\mathbb{N} = S$. The result follows. □

Remark 5. 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?)

Informal 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 $x^2 - \overline{1}$.

Informal Exercise 6. Although the result of Exercise 4 does not hold if F is replaced by a general commutative 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 use the methods of

Chapter 4 to prove that every polynomial is the product of a constant times irreducible polynomials.

Finally, even if F is finite, one can prove that there are an infinite number of irreducible polynomials in $F[x]$ using a similar argument to that used in showing that there are an infinite number of primes.

6. Fundamental Theorems

Theorem 9 (Fundamental Theorem of Algebra, Part 1)**.** *Every nonconstant polynomial in* $\mathbb{C}[X]$ *has a root in* $\mathbb{C}$*.*

Corollary 10. *Every non-constant polynomial with real or complex coefficients has a root in* $\mathbb{C}$*.*

Corollary 11 (Fundamental Theorem of Algebra, Part 2)**.** *Every non-constant polynomial in* $\mathbb{C}[x]$ *is the product of linear polynomials in* $\mathbb{C}[x]$*.*

For real roots we get the following weaker results:

Theorem 12. *Every polynomial of odd degree in* $\mathbb{R}[x]$ *has a root in* $\mathbb{R}$*.*

Real polynomials do not always factor into linear real polynomials. The following weaker result is true:

Theorem 13. *Every non-constant polynomial in* $\mathbb{R}[x]$ *factors into a product of linear and quadratic real polynomials in* $\mathbb{R}[x]$

In other words, we have to allow for the possibility of quadratic factors that have no real roots. The irreducible polynomials of $\mathbb{R}[x]$ are the linear polynomials and the quadratic polynomials with negative discriminate. Contrast this with $\mathbb{C}[x]$ where the irreducible polynomials are just the linear polynomials.

In $\mathbb{Q}[x]$ the situation is even worse. We can find polynomials of any degree that have no roots in $\mathbb{Q}$, and we can find polynomials of any degree that are irreducible, and do not factor into smaller degree factors.

Exercise 7. Factor $x^4 - 1$ into irreducible polynomials in $\mathbb{C}[x]$. Factor $x^4 - 1$ into irreducible polynomials in $\mathbb{R}[x]$.