APPENDIX C: POLYNOMIALS

WAYNE AITKEN AND LINDA HOLT

Summer 2019 Edition

This appendix contains an informal survey of some key results concerning polynomials. These results illustrate some very important properties of various number systems. For example, one reason the complex numbers are so important in mathematics is that every polynomial with coefficients in $\mathbb{C}$ has a full set of roots.

Only some of the results in this appendix are proved. With or without proof they are included due to their importance in mathematics.

1. Polynomial rings

Polynomials can be constructed in a rigorous manner in the style of our other constructions of the number systems, and the operations of addition and multiplication can be defined rigorously. However, to do so here would take us to far afield. So we will appeal to common (precalculus level) experience in our approach to polynomials.

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

Remark 1. We adopt the usual conventions for identity, negation and subtraction used in algebra. So $x^2 - 2x - 1$ is short for $1x^2 + (-2)x + (-1)$, and $-x^3 + x$ is short for $(-1)x^3 + 0x^2 + 1x + 0$.

In the above x can be replaced by any given variable. The variable must be a "symbolic" variable. That is, it must be a variable not currently being used to represent a fixed value. So if y is not being used to represent a fixed value, we can define $\mathbb{Z}[y]$, say, to be the set of polynomials with variable y and coefficient in $\mathbb{Z}$. This set would contain $3y^2 - 2$, but would not contain $3x^2 - 2$ or $(1/2)y^2$.

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 $a_3 = 7$, $a_1 = 1$ 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 that $\overline{6}x^3 + \overline{2}x^2 - x + \overline{1} = -x^2 + \overline{2}x + \overline{1}$ 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 $R \subseteq R[x]$. (More formally, we define an injective canonical embedding $R \to R[x]$ which maps c to the constant polynomial c.)

Polynomials are added and multiplied 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 $\overline{3}x^2 + x - \overline{2}$ in $\mathbb{F}_5[x]$.

The set $R[x]$ is closed under addition and multiplication. So $+$ and $\times$ give two binary operations $R[x] \times R[x] \to R[x]$. It turns out (but we skip the proofs), that these operations satisfy the expected associative, commutative, distributive, identity and inverse laws. More precisely, the following holds.

Theorem 1. *If R is a commutative ring, then $R[x]$ is also a commutative ring. The additive identity is the constant 0 polynomial, and the multiplicative identity is the constant 1 polynomial.*

2. Substitutions

Definition 2 (Substitution)**.** 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. Suppose $f = x^3 - x \in \mathbb{Z}_3[x]$. 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 shows that for finite fields, polynomials are not exactly the same thing as functions. The only function $\mathbb{Z}_3 \to \mathbb{Z}_3$ whose values are all zero is the zero function. In fact two functions are said to be equal if and only if they have the same values. In contrast, we have found two distinct polynomials whose values are zero.)

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 $F[x]$, called the *degree*:

Definition 4 (Degree)**.** Let $f \in R[x]$ where R is a commutative ring. If f has the 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, the polynomial $6x^3+2x^2-x+1$ 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 2 (Additivity of degree)**.** *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 3 (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 2. The polynomial $q(x)$ in the above is called the *quotient* and the polynomial $r(x)$ is called the *remainder*.

Remark 3. 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 4. This theorem can be used a basis to prove theorems about GCDs 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 4. *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 5. 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 5. *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 6. *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 5,

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

By Theorem 2, $\deg f = 1 + \deg q$. 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 6. Observe how this can fail if F is replaced by the ring $\mathbb{Z}_m$ where m is not a prime. The polynomial $x^2 - 1 \in \mathbb{Z}_8[x]$ has degree 2, yet it has four roots! (Can you find them?)

Exercise 4. Find all four roots of $x^2 - 1 \in \mathbb{Z}_8[x]$ in $\mathbb{Z}_8$.

Exercise 5. 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 6. Show that the result of the above exercise does not hold in $\mathbb{Z}_8[x]$ by looking at a factorization of $x^2 - \overline{1}$.

Exercise 7. Although the result of Exercise 5 does not hold if F is replaced by a commutative ring with zero divisors (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 5 to prove that every nonconstant polynomial is the product of a constant times one or more 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.

Exercise 8. Show that every linear polynomial is irreducible. (We will see that in $\mathbb{C}$, these are the only irreducible polynomials).

Exercise 9. Show that a quadratic polynomial $f \in F[x]$ with no roots in F must be irreducible. Show that, because of this, $x^2 + \overline{1}$ is irreducible in $\mathbb{F}_3[x]$.

6. Fundamental theorem of algebra

One of the great advantages of using the field $\mathbb{C}$ is that every nonconstant polynomial has a root. This is called the *fundamental theorem of algebra*.

Theorem 7 (Fundamental theorem of algebra, part 1)**.** *Every nonconstant polynomial in* $\mathbb{C}[X]$ *has a root in* $\mathbb{C}$*.*

Corollary 8. *Every non-constant polynomial with real or complex coefficients has a root in* $\mathbb{C}$*.*

Corollary 9 (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 (which can be proved using the intermediate value theorem):

Theorem 10. *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 11. *Every non-constant polynomial in* $\mathbb{R}[x]$ *factors into a product of linear and irreducible quadratic 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 no real roots.[1] 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 10. Show that the only irreducible polynomials in $\mathbb{C}[x]$ are the linear polynomials.

Exercise 11. Factor x^4-1 into irreducible polynomials in $\mathbb{C}[x]$. Factor x^4-1 into irreducible polynomials in $\mathbb{R}[x]$.

Exercise 12. Assume the fundamental theorem of algebra, Part 1. Prove from this the fundamental theorem of algebra, part 2. (Use induction based on degree. Start with degree 1).

[1] Irreducible quadratic polynomials in $\mathbb{R}[x]$ are those for which the quadratic formula requires square roots of negative numbers. In this case the polynomial has two complex roots, and the roots are complex conjugates of each other.