MAT 3530: Assignment 6
Polynomial Rings, Euclidean Rings, and Factorization

Charles Delman

March 6, 2012

Due at the beginning of class on Wednesday, March 21.

Much of mathematics, especially European mathematics from the fifteenth through the nineteenth centuries, was concerned with understanding polynomials with integer, rational, real, or complex coefficients and their solutions. The importance of this topic for both theoretical mathematical development and practical applications is reflected in the contemporary secondary school algebra curriculum. The following exercises begin to explore it, establishing some fundamental results.

An important characteristic of polynomial is its *degree*, which we now define with some care. This definition and its consequences apply to polynomials with coefficients in any integral domain.

Definition. If $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, and $a_n \neq 0$, the *degree* of $P(x)$, denoted by deg $P(x)$, is the natural number n.

Note that this definition applies to a constant polynomial $P(x) = a_0$ as long as $a_0 \neq 0$; that is, the degree of a non-zero constant is 0. The degree of 0 is not defined; this omission is purposeful, as it not only allows for the consistent definition given above, but also avoids an exception to the following useful property of degree:

Lemma. *If $P(x) \neq 0$ and $Q(x) \neq 0$, then deg $P(x)Q(x) =$ deg $P(x)$ + deg $Q(x)$.*

This lemma is an immediate consequence of the definition of the product of two polynomials, along with the fact that the ring of coefficients is a domain.

1. Give a rigorous proof of the lemma stated above.
2. Let R be any commutative ring, and consider R as a subring of the polynomial ring $R[x]$ by identifying its elements with constant polynomials.
   (a) Prove that the group of units of $R[x]$ is the same as the group of units of R. (Hint: Use an argument about the degree of a product to reduce to the constant case.)
   (b) In particular, what are the units of:
      i. $\mathbb{Z}[x]$?
      ii. $\mathbb{Q}[x]$?
      iii. $\mathbb{R}[x]$?
      iv. $\mathbb{C}[x]$?

In what follows it will be helpful to recall that, thanks to unique factorization, any two integers have a *least common multiple*, defined (up to units) in a manner analogous to the greatest common divisor as follows:

Definition. The least common multiple of integers k and l, denoted by $LCM(k,l)$ is the integer m such that:

- m is a common multiple of k and l: $k \mid m$ and $l \mid m$
- m is least in the sense that if $k \mid n$ and $l \mid n$, then $m \mid n$.

It is clear that $LCM(k,l)$ (if it exists) is unique (justifying the anticipatory use of the word "the" above): if m' is another such, then $m \mid m'$ and $m' \mid m$; hence, $m = \pm m'$.

That $LCM(k,l)$ does exist is proven as follows: Using zero exponents as needed, we may write $k = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$ and $l = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}$, where $p_1, p_2, p_3, \ldots, p_n$ are distinct primes. Let $g_i = MAX(e_i, f_i)$ for $i = 1, 2, 3, \ldots, n$. Then one readily shows that $m = p_1^{g_1} p_2^{g_2} p_3^{g_3} \cdots p_n^{g_n}$ is the least common multiple of k and l.

3. Prove that $m = p_1^{g_1} p_2^{g_2} p_3^{g_3} \cdots p_n^{g_n}$, as defined above, is the least common multiple of k and l.

4. Define the *content* of a polynomial with integer coefficients, $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$, by $c(P) = GCD(a_0, a_1, a_2, \ldots, a_n)$. The content is only defined up to units, of course; it is convenient to choose the positive value. A polynomial whose content is 1 is called *primitive*.

   (a) Compute the content of each of the following polynomials. Circle the item numbers of those that are primitive. (Note: You can do this in Tex: ①!)

      i. $2 + 4x + 6x^2$
      ii. $1 + 4x + 6x^2$
      iii. $2 + 4x + 9x^2$
      iv. $12 + 18x + 24x^2 - 30x^5$

   (b) What is the smallest positive integer n such that $n(\frac{2}{3} + \frac{5}{7}x + \frac{1}{6}x^3)$ has integer coefficients?

   (c) For what fraction $\frac{m}{n}$ in lowest terms and what primitive polynomial $P(x)$ with integer coefficients does $\frac{m}{n}P(x) = \frac{2}{3} + \frac{6}{7}x + \frac{4}{5}x^3$?

Lemma. *The product of primitive polynomials is primitive.*

Proof. Let $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$ and $Q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$ be primitive polynomials; thus, by definition, $a_0, a_1, a_2, \ldots, a_m$ have no common factor and $b_0, b_1, b_2, \ldots, b_n$ have no common factor. If $P(x)Q(x)$ were not primitive, then by definition the coefficients of $P(x)Q(x)$ would have some common factor; in particular, they would have some common prime factor p. We will prove the result by showing that for any prime number p, p cannot divide all of the coefficients of $P(x)Q(x)$.

We know by hypothesis that p does not divide all of the coefficients of $P(x)$ or $Q(x)$. Let i be the smallest value such that $p \nmid a_i$; similarly, let j be the smallest value such that $p \nmid b_j$.

We claim that p does not divide the coefficient of x^{i+j} in $P(x)Q(x)$. The coefficient of x^{i+j} in $P(x)Q(x)$ is

$$(a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \cdots + a_{i+j}b_0).$$

Suppose by way of contradiction that p does divide this coefficient. Since i is the smallest value such that $p \nmid a_i$, p does divide every term of $(a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_{i-1}b_{j+1})$; similarly, since j is the smallest value such that $p \nmid b_j$, p divides every term of $(a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+\cdots+a_{i+j}b_0)$. Subtracting these terms off, we are left with $p \mid a_ib_j$, but this is impossible, since p is prime and does not divide either factor a_i or b_j. □

5. Prove as a consequence of the preceding lemma that content is multiplicative: $c(PQ) = c(P)c(Q)$. (Hint: factor out the content to write each polynomial as the product of a constant and a primitive polynomial.)

Divisibility plays a major role in understanding the roots of polynomials. Let F be a field. (Recall this means that all non-zero elements of F have multiplicative inverses. The group of units of F, which of course consists of all non-zero elements of F, is often denoted by F^*.) The process of "synthetic division" shows that for any non-zero polynomial $D(x)$ and any polynomial $E(x)$, there exists polynomials $Q(x)$ and $R(x)$ (the *quotient* and *remainder*, respectively) such that $E(x) = Q(x)D(x)+R(x)$, and either $R(x) = 0$ or $\deg R(x) < \deg D(x)$. A rigorous proof that this works relies on induction on the degree of $E(x)$, as outlined in the following exercises. Note that the argument works for any field of coefficients.

6. The following steps prove that given any non-zero polynomial $D(x) \in F[x]$ and any polynomial $E(x) \in F[x]$, there exists polynomials $Q(x) \in F[x]$ and $R(x) \in F[x]$ such that $E(x) = Q(x)D(x) + R(x)$, and either $R(x) = 0$ or $\deg R(x) < \deg D(x)$.

   (a) Special cases: $E(x) = 0$ or $\deg E(x) < \deg D(x)$. In these cases the values of $Q(x)$ and $R(x)$ should be obvious!

   (b) General case: $\deg E(x) \geq \deg D(x)$; hence, $E(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ and $D(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, with $m \leq n$.

      i. Initial case: $\deg E(x) = 0$; hence, $E(x) = b_0$ and $D(x) = b_0 \neq 0$. (Hint: Remember that the coefficients are in a field, so you can divide by any non-zero element! Note the necessity of being able to do this.)

      ii. Inductive claim: Assume the result holds if $\deg E(x) < n$. Then it holds if $\deg E(x) = n$. (Hint: $E(x) - \frac{b_n}{a_m}x^{n-m}D(x)$ has degree less than n.)

7. A real or, more generally, complex number ρ is called *algebraic* if there is a polynomial with integer coefficients, $S(x) \in \mathbb{Z}[x]$, such that $S(\rho) = 0$. (Terminology: ρ is a *root* of S, ρ *satisfies* S.) For example, $\sqrt{2}$ and $i\sqrt{7}$ are algebraic numbers. A number that is not algebraic is called *transcendental*; it can be proven, for example, that e and π are transcendental. (In a sense that can be precisely defined, almost all real or complex numbers are transcendental; however, we only have names for a couple of them!)

   (a) Verify that $\sqrt{2} + i\sqrt{2}$ is algebraic by finding a polynomial in $\mathbb{Z}[x]$ that it satisfies. (Hint: Write it in exponential form or graph it.)

(b) Prove that ρ is algebraic if and only if there is a polynomial with rational coefficients, $T(x) \in \mathbb{Q}[x]$, such that $T(\rho) = 0$. (The *only if* direction is obvious, since integers are rational.)

(c) If $r \in \mathbb{C}$ is a root of $P(x)$, prove that $P(x) = (x - r)Q(x)$ for some $Q(x) \in \mathbb{C}[x]$.

(d) Let $P(x) \in \mathbb{Z}[x]$ be the primitive polynomial *of lowest degree* such that $P(r) = 0$. Let $S(x)$ be any primitive polynomial such that $S(r) = 0$. Prove that there is a primitive polynomial $Q(x) \in \mathbb{Z}[x]$ such that $S(x) = P(x)Q(x)$; in particular, $P(x) \mid Q(x)$ in the ring $\mathbb{Z}[x]$. (Hints: Use division with remainder in the ring of polynomials with rational coefficients to find a polynomial $Q'(x)$. For some suitable integer n, $Q''(x) = nQ'(x)$ has integer coefficients, and for $m = c(Q'')$, $Q''(x) = mQ(x)$ and $Q(x)$ is primitive. Use multiplicativity of the content to show that $m = n$, concluding that $S(x) = P(x)Q(x)$.)

We have seen that the existence of division with remainder makes $F[x]$ into a *Euclidean* ring. Recall that a ring R is *Euclidean* if there is a function $d : R - \{0\} \to \mathbb{N}_0$ such that:

- If $a, b \neq 0$, then $d(a) \leq d(ab)$
- If $a \in R$ and $b \neq 0$, then there are elements $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $d(r) < d(b)$.

For polynomials, degree gives the function d. As we showed in class using a geometric argument, another example of a Euclidean ring is $\mathbb{Z}[i]$, where $d(z) = N(z) = z\bar{z}$. serves the purpose.

The reason for the name *Euclidean* is that for any such ring the greatest common divisor of any two elements exists and may be found by the Euclidean algorithm using repeated division with remainder. As a consequence, irreducible elements of Euclidean rings must be prime, and any element of a Euclidean ring factors uniquely (up to order of multiplication and multiplication by units) into prime elements.

8. Compute the unique primitive polynomial with integer coefficients and positive leading coefficient (that is, coefficient of the highest degree term) that is the greatest common divisor of $x^6+6x^5+x^4-6x^3+4x^2-3x+1$ and $x^5+2x^4+5x^3+7x^2-2x-3$. (Stipulating that the polynomial is primitive and has positive leading coefficient specifies a unique representative of the equivalence class under the relation of multiplication by units.)

9. Compute the unique element $a + bi \in \mathbb{Z}[i]$ with $a > 0$ and $b \geq 0$ that is the greatest common divisor of $19+9i$ and $15-23i$. (Hint: Use graph paper or, even better, Geogebra or Geometer's Sketchpad!)

10. Up to multiplication by the units ± 1 and $\pm i$, why is any element of $\mathbb{Z}[i]$ equivalent to a unique element of the form described in the previous exercise? Give a proof!