Math 250A Lecture 15 Notes

Daniel Raban

October 17, 2017

1 Polynomials and Divisibility

1.1 Polynomial division with remainder

We start with some results you should already know.

Theorem 1.1. *Suppose f, g are polynomials in $R[x]$, where R is a commutative ring. Also suppose that f has leading coefficient 1, so $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $g(x) = f(x)q(x) + r(x)$, where $\deg(r) < \deg(f)$.*

Corollary 1.1. *If K is a field, $K[x]$ is a Euclidean domain.*

Proof. We can make the leading coefficient of any polynomial 1 by multiplying by a unit. Then apply the theorem. $\square$

Corollary 1.2. *If K is a field, $K[x]$ is a principal ideal domain.*

Proof. All Euclidean domains are PIDs. $\square$

Corollary 1.3. *If K is a field, $K[x]$ is a unique factorization domain.*

Proof. All PIDs are UFDs. $\square$

Example 1.1. How can we find the prime elements of $F_2[x]$, where $F_2 = \mathbb{Z}/2\mathbb{Z}$, the field with 2 elements? Recall the sieve of Eratosthenes[1]. List all numbers > 1, identify the smallest number as prime, and cross out all multiples of it.

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, \ldots$$

Then, identify the first non-crossed out number as prime, and cross out all multiples of it.

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, \ldots$$

[1]Erathosthenes was the first person to accurately calculate the circumference of the Earth.

If we repeat this process, we can find all the prime numbers.

For $F_2[x]$, we list all elements (other than 0 or units) in order of degree.

$$x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, \ldots$$

Cross out all multiples of x.

$$x, x+1, \cancel{x^2}, x^2+1, \cancel{x^2+x}, x^2+x+1, \ldots$$

The next element, $x+1$, is prime, so we cross out multiples of it. Note that $x^2+1 = (x+1)^2$ in $F_2[x]$.

$$x, x+1, \cancel{x^2}, \cancel{x^2+1}, \cancel{x^2+x}, x^2+x+1, \ldots$$

The polynomials not divisible by x and $x+1$ are

$$x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, \cancel{x^4+x^2+1}, x^4+x^3+1, x^4+x^3+x^2+x+1,$$

and we can continue the process.

Proposition 1.1. *Suppose a polynomial $f \in R[x]$ has a root a ($f(a) = 0$). Then $f(x) = g(x)(x-a)$ for some g.*

Proof. Apply division to get that $f(x) = g(x)(x-a) + r$. We have $\deg(r) < 1$, so r is constant. Put $x = a$ to get $f(a) = g(a)(a-a) + r =$ r, so $r = 0$. $\square$

Corollary 1.4. *A polynomial $f \in R[x]$ of degree n over an integral domain R has $\leq n$ roots.*

Proof. If $a_1, \ldots, a_k$ are roots, then $f(x) = (x-a_1)\cdots(x-a_k)g(x)$, so $k \leq n$. If the product is 0, then so is some factor $(x-a_i)$ because R is an integral domain. $\square$

Example 1.2. Let $R = \mathbb{Z}/8\mathbb{Z}$, which is not an integral domain. Let $f(x) = x^2 - 1$, which has degree 2. Then $f(x)$ has 4 roots: 1, 3, 5, and 7.

Example 1.3. Let R be the quaternions (this is noncommutative), and look at $f(x) = x^2 + 1$. Then f has roots $\pm i, \pm j, \pm k$, and roots $ai + bj + ck$ for real a, b, c that satisfy $a^2 + b^2 + c^2 = 1$. This is an uncountable number of roots!

1.2 An application to field theory

We first prove a lemma.

Lemma 1.1. *Any abelian group G with $\leq n$ elements of order n ($\forall n \geq 1$) is cyclic.*

Proof. Recall that $G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots$. Suppose that $p_1 = p_2$; then G has p^2 elements x with $x^p = 1$ (since G contains $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$). This is impossible, so all p_i are distinct. Then G is cyclic by the Chinese remainder theorem ($\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if m, n are coprime). $\square$

Proposition 1.2. *The group $(\mathbb{Z}/p\mathbb{Z})^*$ of units mod p is cyclic if p is prime.*

Proof. Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. So any polynomial in $R[x]$ of degree n has $\leq n$ roots. So $x^n - 1$ has $\leq n$ roots for any $n \geq 1$. Then G has $\leq n$ elements x with $x^n = 1$ (for $n \geq 1$). Using the lemma finishes off the proof. $\square$

Example 1.4. This need not hold if p is not prime. $(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$, and these are both cyclic of order 2.

Definition 1.1. A generator of $(\mathbb{Z}/p\mathbb{Z})^*$ is called a *primitive root.*

We have shown that primitive roots always exist when p is prime.

Example 1.5. Let's find a primitive root of $p = 23$. The element should have order 22. Check the elements $-1, 1, 2, 3, 4, 5$. We find that 5 is the primitive root because $5^2, 5^{11} \not\equiv 1 \pmod{23}$.

The same argument shows that the following is true.

Theorem 1.2. *If F is a field, any finite subgroup of F^* is cyclic.*

Example 1.6. Let $F = \mathbb{C}$, and take the subgroup of 8th roots of unity. This has primitive root $e^{2i\pi/8}$.

This also gives us the following corollary.

Corollary 1.5. *If F is any finite field, then F^* is cyclic.*

1.3 Unique factorization in polynomial rings

We want to show that $\mathbb{Z}[x]$ is a UFD, and we know that $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, which is a UFD because $\mathbb{Q}$ is a field. We cannot do this as we usually do, because $\mathbb{Z}[x]$ is not a Euclidean domain or a PID. For example, $(2, x)$ is a non-principal ideal. So we use the fact that $\mathbb{Q}[x]$ is a UFD.

Definition 1.2. Let $f \in \mathbb{Q}[x]$. The *content* $c(f)$ is defined as follows: Suppose $f(x) = a_n x^n + \cdots + a_0$. For each prime p, $a_n = p^{m_n} b_n, a_{n-1} = p^{m_{n-1}} b_{n-1}, \ldots$ with $m_i \in \mathbb{Z}$ and b_i not having any factors of p in the numerator or denominator. Let $c(f) = p^{\min(m_i)} \times b$, where b is some number with no factors of p.

Example 1.7. Let $f(x) = (2/3)x^2 + 4$. Then $c(f) = 2/3$.

Proposition 1.3. *$\mathbb{Z}[x]$ is a unique factorization domain.*

Proof. The key point of the proof is that $c(fg) = c(f)c(g)$. We may assume that $c(f) = c(g) = 1$; otherwise, we multiply f and g by constants to make this so. We want to show that $c(fg) = 1$. We know that f has integer coefficients, so $c(f) \in \mathbb{Z}$. Suppose p is any prime in $\mathbb{Z}$; we show that p does not divide $c(fg)$.

Since $c(f) = c(g) = 1$, p does not divide all coefficients of f or all the coefficients of g. So $f = a_n x^n + \cdots + a_i x^i + \cdots + a_0$ and $g = b_m x^m + \cdots + b_j x^j + \cdots + b_0$ where i and j are the lease indices such that a_i and b_j are not divisible by p. So the coefficient of x^{i+j} in fg is

$$a_0 b_{i+j} + a_1 b_{i+j-1} + a_2 b_{i+j-2} + \cdots + a_i b_j + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0,$$

which has all terms except $a_i b_j$ divisible by p. This means that the coefficient of x^{i+j} in fg is not divisible by p. This is true for any prime p, so $c(fg) = 1$.

We sketch the rest of the proof. The main point is that we need to show that irreducible elements are prime. Recall that irreducible elements are such that $f \neq gh$ with $\deg(g), \deg(h) < \deg(f)$; prime elements are such that if f divides g, h, then f divides g or h.

The irreducibles of $\mathbb{Z}[x]$ are the primes $2, 3, 5, 7, \ldots \in \mathbb{Z}$ and the polynomials $f(x)$ of degree > 1 with $c(f) = 1$.

We leave the following two statements as exercises:

1. These are all the irreducibles of $\mathbb{Z}[x]$.

2. Any element of $\mathbb{Z}[x]$ is a product of irreducibles.

If $\deg(f) = 0$, then $f = p$ is prime in $\mathbb{Z}$. If f divides gh, this means that $c(gh)$ is divisible by p. So $c(g)$ or $c(h)$ is fivisible by p (since $c(gh) = c(g)c(h)$. So p divides gh. The case of $\deg(f) > 0$ is similar and left as an exercise. $\square$

We have really proved the following them.

Theorem 1.3. *If R is a UFD, then so is $R[x]$.*

Proof. Perform the same proofbut with a few modificaitons. First, $c(f)$ is now only defined up to multiplication by a unit. Also, irreducibles of $R[x]$ are either irreducibles of R ($\deg = 0$) or irreducibles of $K[x]$ with content 1, where K is the quotient field of R. $\square$

Corollary 1.6. *$\mathbb{Z}[x_1, \ldots, x_n]$ is a unique factorization domain.*[2]

Corollary 1.7. *If K is a field, $K[x_1, \ldots, x_n]$ is a unique factorization domain.*

Proof. These two have the same proof: induction on the number of variables. $\square$

[2] In fact, $\mathbb{Z}[x_1, x_2, \ldots]$ in infinitely many variables is a field, but we will not prove that here.

1.4 Irreducibility tests in $\mathbb{Z}[x]$ (or $\mathbb{Q}[x]$)

Given $f \in Z[x]$, how do we factor f into irreducibles?

Example 1.8. Here is an algorithm, due to Kronecker:

Suppose that $f - gh$. We can assume $g, h \in Z[x]$. Then $f(n) = g(n)h(n)$ for any $n \in \mathbb{Z}$. So we factor $f(0), f(1), \ldots, f(m)$, where $m = \deg(f)$. Then $g(0)$ divides $f(0)$ or $g(1)$ divides $f(1)$, (and so on), so there are only a finite number of possibilities for $g(0), \ldots, g(m)$. But $\deg(g) \leq m$, so g is determined by $g(0), \ldots, g(m)$.

Kronecker's algorithm is pretty slow. There are faster algorithms.

Example 1.9. The LLL algorithm[3] is fast but not necessarily precise. We can write $f = af_1 f_2 \cdots f_n$, where f_i is irreducible with degree > 0 and $a \in \mathbb{Z}$. We can do this in polynomial time, but to find a, we must factor an integer, which may not be possible in polynomial time.

To test for reducibility, we can use reduction mod p: If $f(x) = g(x)h(x)$, then $f(x) = g(x)h(x) \pmod{p}$ for any prime p.

Example 1.10. Is $9x^4 + 6x^3 + 26x^2 + 13x + 3$ irreducible? Yes. It is $x^4 + x + 1 \pmod{2}$, and we saw that this was irreducible $\pmod{2}$.

Example 1.11. Let's test if $x^4 - x^2 + 3x + 1$ is irreducible.

$$(\text{mod } 2) : x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1),$$

which are both irreducible $\pmod{2}$.

$$(\text{mod } 3) : x^4 - x^2 + 1 = (x^2 + 1)^2.$$

which is also irreducible $\pmod{3}$.

Combine these results. The first one says that the only possible factorization is a degree 1 polynomial times a degree 3 polynomial. The second says that the only possible factorization is into 2 degree 2 polynomials. So the polynomial must be irreducible.

Theorem 1.4 (Eisenstein)**.** *Suppose $f(x)$ has the following properties:*

1. *The leading coefficient is 1.*
2. *All other coefficients are divisible by p.*
3. *The constant term is not divisible by p^2.*

Then f is irreducible.

[3] This stands for Lenstra, Lenstra, and Lovasz.

We will not prove this right now. First, let's see some examples.

Example 1.12. The polynomial $x^5 - 4x + 2$ is irreducible by Eisenstein's criterion.

Example 1.13. Look at the p-th roots of 1. These are the roots of the polynomial $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$. We want to show that the latter term is irreducible by Eisenstein's criterion. We need a trick to make this work. Put $z = x - 1$. Then

$$\begin{aligned} x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} &= \frac{(z+1)^p - 1}{z} \\ &= \frac{(z^p + pz^{p-1} + \frac{p(p-1)}{2} z^{p-2} + \cdots + pz + 1) - 1}{z} \\ &= z^{p-1} + pz^{p-2} + \cdots + p, \end{aligned}$$

so Eisenstein applies, and $z^{p-1} + pz^{p-2} + \cdots + p$ is irreducible. So $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible, as desired.

Why does this work? The prime p is *totally ramified* in $\mathbb{Z}[\zeta]$, where $\mathbb{Z}^p = 1$. We have that p factorizes in $\mathbb{Z}[\zeta]$ as $(1 - \zeta)^{p-1} u$, where u is a unit.