Math 313/623 Notes 4

David L. Meretzky

Tuesday February 5th, 2019

> The central notion in commutative algebra is that of a prime ideal. This provides a common generalization of the primes of arithmetic and the points of geometry.
>
> M.F. Atiyah

Recall from last class that we discussed some consequences of unique factorization and some basic properties of commutative rings. Today we will show that that certain polynomial rings behave like the integers in that they have primes, congruences, and unique factorization. We will also discuss more general constructions and perhaps an algorithm or two.

The fields we know about so far are $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Let k be a field. What follows will be perhaps easiest if you set $k = \mathbb{Q}$ or $\mathbb{R}$ in your mind. Then $k[x]$ denotes the ring of polynomials with coefficients coming from k. We can add and multiply polynomials as usual. It is left to you to check that the distributive law holds. The constant polynomials $z(x) = 0$ and $i(x) = 1$ are the additive identity and multiplicative identity of $k[x]$ respectively. Does $k[x]$ have units? Does it have zero divisors?

Definition 1. The degree of a polynomial $f \in k[x]$ is the positive integer which is the largest power of x appearing in f. We denote the degree of f by $\deg f$.

Proposition 1. $\deg fg = \deg f + \deg g$.

Proof. Let ax^n be the leading term of f and bx^m be the leading term of g. Thus $\deg f + \deg g = m + n$. The leading term of $fg = abx^{m+n}$ thus $\deg fg = m + n$. □

We say that the degree of a constant polynomial is 0.

Proposition 2. The units of $k[x]$ are precisely the constant polynomials.

Proof. Let $p(x) = c = c1 + 0x + 0x^2 + 0x^3$ be a constant polynomial. Then since $c \in k$ which is a field, c has a multiplicative inverse d. Let $q(x) = d$ then $p(x)q(x) = cd = 1 = i(x)$. So $p(x)$ has a multiplicative inverse.

Suppose that $p(x)$ is a unit of $k[x]$. Then $p(x)$ has a multiplicative inverse $q(x)$ such that $p(x)q(x) = i(x) = 1$ for all x. Computing $\deg(p(x)q(x)) =$

deg $p(x)$+deg $q(x)$ = deg $i(x) = 0$. We must have that deg $p(x)$ = deg $q(x) = 0$ since the degree is always positive. Thus $p(x)$ and $q(x)$ are both constant. □

Proposition 3. The polynomial ring $k[x]$ is an integral domain, that is, it has no zero divisors.

Proof. The nonzero constant polynomials all have multiplicative inverses and therefore are units and cannot be zero divisors. Let $f(x)$ be a polynomial of degree greater than 0. Suppose there is a nonzero polynomial $g(x)$ such that $f(x)g(x) = 0$. Then deg $(f(x)g(x)) = 0$ but $0 <$ deg $f(x) \leq$ deg $(f(x)g(x))$ since deg $(f(x)g(x))$ = deg $f(x)$ + deg $g(x)$. □

We turn now to section 2 of the modern text *A Classical Introduction to Modern Number Theory*.

Unique Factorization in $k[x]$

If $f, g \in k[x]$, we say that f divides g if there is an $h \in k[x]$ such that $fh = g$. A nonconstant polynomial p is said to be irreducible if $q|p$ implies that q is either a constant polynomial or a constant polynomial times p. Irreducible polynomials are the analog of prime numbers.

Lemma 1. Every nonconstant polynomial is the product of irreducible polynomials.

First look at the proof of Lemma 1 from lecture 2. We proved that by contradiction. Now we will use induction to give a direct proof of this lemma.

Proof. Polynomials of degree 1 are irreducible. Assume the result is true for polynomials of degree less than n and deg $f = n$. If f is irreducible then we are done. Otherwise $f = gh$ where $1 \leq$ deg g, deg $h < n$ by the induction assumption both g and h are products of irreducible polynomials. Thus, so is $f = gh$. □

A monic polynomial is one whose leading term is 1. The polynomial $x^2 + x - 3$ is monic but $2x^5 + 1$ is not.
Let p be a monic irreducible polynomial. We define $ord_p(f)$ to be the integer a with the property that $p^a|f$ but $p^{a+1} \nmid f$. Note $ord_p(f) = 0$ if and only if $p \nmid f$.

Theorem 2. Let $f \in k[x]$. Then we can write

$$f = c \prod_p p^{a(p)},$$

where the product is over all monic irreducible polynomials and c is a constant. The constant c and all the exponents $a(p)$ are uniquely determined by f and $a(p) = ord_p(f)$.

Again, the existance of such a product follows from the previous lemma. The uniqueness of this product will require more work.

Now we will get a result which is analogus to article 3 and lemma 2 guaranteeing the existance of unique least resiude for each modulus. This will allow us to extend the language of congruence to polynomials if we so desire. For the most part, our discussion of polynomials rings will take a modern approach.

Lemma 2. Let $f, g \in k[x]$. If $g \neq 0$, there exist polynomials $h, r \in k[x]$ such that $f = hg + r$ (classically, $f \equiv r \pmod{g}$), where either $r = 0$ or $r \neq 0$ and $\deg r \leq \deg g$.

Review the analogous proof in lecture 2.

Proof. If $g|f$ then set $h = f/g$ and $r = 0$. If $g \not| f$, let $r = f - hg$ be the polynomial of least degree among all polynomials of the form $f - lg$ for $l \in k[x]$. We claim that $\deg r < \deg g$. If, not let the leading term of r be ax^d and the leading term of g be bx^m where $m < d$. Thus, $ax^d/bx^m = \frac{a}{b}x^{d-m}$ is a polynomial in $k[x]$. Call it q. Note that the leading term of gq is $bx^m * \frac{a}{b}x^{d-m} = ax^d$, the leading term of r. We have

$$r = f - hg,$$

subtracting gq from both sides we obtain,

$$r - gq = f - (h + q)g.$$

Since gq and r have the same leading term, their difference is of degree less than r. Hence r cannot be the polynomial of least degree among all polynomials of the form $f - lg$, because we just showed $f - (h+q)g$ has lower degree then $f - hg$. We have reached a contradiction, therefore $\deg r < \deg g$ as desired. □

Definition 1. If $f_1, f_2, ..., f_n \in k[x]$, then $(f_1, f_2, ..., f_n)$ is the set of all polynomials of the form $f_1h_1 + f_2h_2 + \cdots f_nh_n$, where $h_1, h_2, ..., h_n \in k[x]$. Collections of this form are called ideals. We say $(f_1, f_2, ..., f_n)$ is the ideal generated by the polynomials $f_1, f_2, ..., f_n \in k[x]$.

Lemma 3. Given $f, g \in k[x]$ there is a $d \in k[x]$ such that $(f, g) = (d)$.

Proof. Let d be an element of least degree in (f, g) clearly $(d) \subset (f, g)$. We need to show the reverse inclusion. Let $c \in (f, g)$, then if $d \not| c$ we have that there exists $q, r \in k[x]$ such that $c = dq + r$ where r has lower degree than d. Thus r has degree 0. So $d|c$ thus $c \in (d)$ and it follows that $(f, g) \subset (d)$ and thus $(f, g) = (d)$. □

Definition 2. Let $f, g \in k[x]$. Then $d \in k[x]$ is said to be a greatest common divisor of f and g if d divides f and g, and if any other $c \in k[x]$ divides both f and g, then c must divide d.

Notice that if $d(x)$ is the greatest common divisor of two polynomails, then any constant multiple of $d(x)$ is also a greatest common divisor. When we talk about the greatest common divisor we mean the unique monic greatest common divisor. That is, there exists some constant polynomail