LECTURE 12: POLYNOMIALS & THEIR CONSTRUCTION

4.5 Lecture 25: polynomials in an indeterminant

It seems to me something is missing here in Gallian and I need to add a bit of material from Rotman (and many other texts) to build up the foundations of polynomials over a ring.

We use the phrase **indeterminant form** in early calculus to capture the idea of a limit whose form does not indicate its eventual convergence or divergence. The term **indeterminant** here is given mainly to divorce the concept of a **polynomial function** from a **polynomial expression**. This much I should say, when x is an indeterminant this means x is not a variable. We do not have in mind some bucket of things which we can pour into x as our imagination warrants. We wish instead to think of x as a sort of place-holder. Of course, x and x^2 are different. Moreover, $1, x, x^2, x^3, \ldots$ are distinct. I could go on about the idea here, but, the best way to be clear is to give the actual definition. Before we define polynomials we first define **formal power series**[4].

Definition 4.5.1. *Suppose R is a commutative ring, then a* **formal power series over** *R is a function $\sigma : \mathbb{N} \cup \{0\} \to R$. Write $\sigma(j) = s_j$ for $j \in \mathbb{N} \cup \{0\}$ and we use the sequential notation:*

$$\sigma = (s_0, s_1, \ldots, s_j, \ldots)$$

where we call $s_j \in R$ the **coefficients**[5] *of the formal power series.*

So, what is a polynomial?

Definition 4.5.2. *A formal power series $\sigma = (s_o, s_1, \ldots, s_j, \ldots)$ over a commutative ring R is called a* **polynomial over** *R if there is some integer $m \geq 0$ with $s_j = 0$ for all $j > m$; that is $\sigma = (s_0, s_1, \ldots, s_m, 0, 0, \ldots)$. Furthermore, the* **zero polynomial** *is $\sigma = (0, 0, \ldots)$. If $\sigma = (s_0, s_1, \ldots)$ is a nonzero polynomial and $n \in \mathbb{N}$ is the smallest integer for which $s_j = 0$ for all $j > n$ then we say $deg(\sigma) = n$ and s_n is the* **leading coefficient**.

We are using sequences to build polynomial expressions. Our next step is to define addition and multiplication of such sequences:

Definition 4.5.3. *Denote the set of polynomials with coefficients in R by $R[x]$. If $\sigma, \tau \in R[x]$ then*

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \ldots, s_j + t_j, \ldots)$$

where $\sigma = (s_j)$ and $\tau = (t_j)$. Moreover,

$$\sigma\tau = (s_0t_0, s_ot_1 + s_1t_0, s_0t_2 + s_1t_1 + s_2t_0, \ldots),$$

where to be precise $\sigma\tau = (a_0, a_1, \ldots, a_k, \ldots)$ and $a_k = \sum_{i+j=k} s_it_j = \sum_{i=0}^{k} s_it_{k-i}$.

To be careful, we should explain why this definition is reasonable. Let me outline the argument:

(1.) $\deg(\sigma + \tau) \leq \max(\deg(\sigma), \deg(\tau))$. It follows that the number of nonzero entries in $\sigma + \tau$ is finite. Hence $\sigma + \tau$ is a polynomial.

(2.) either $\sigma\tau = 0$ or $\deg(\sigma\tau) \leq \deg(\sigma)\deg(\tau)$. Therefore the product of two polynomials is once more a polynomial.

[4] These are known as **formal** power series because there is no expectation of convergence. For example, $\sum_{j=0}^{\infty} s_jx^j = s_0 + s_1x + s_2x^2 + \cdots$ is a formal power series. But, I'm getting a bit ahead of the story here.

[5] Rotman, page 236 of *First Course in Abstract Algebra* shares that the term **coefficient** means **acting together to some single end**, here the coefficients together form the formal power series.

Next, we should show $R[x]$ forms a commutative ring with respect to the addition and multiplication just defined. Consider,

$$(s_0, s_1, \dots, s_n, 0, \dots) + (0, 0, \dots) = (s_0 + 0, s_1 + 0, \dots, s_n + 0, 0 + 0, \dots) = (s_0, s_1, \dots, s_n, 0, \dots)$$

hence $0 = (0, 0, \dots)$. Moreover, setting $n = max(\deg(\sigma), \deg(\sigma))$,

$$\sigma + \tau = (s_0 + t_0, s_1 + t_1, \dots, s_n + t_n, 0, \dots) = (t_0 + s_0, t_1 + s_1, \dots, t_n + s_n, 0, \dots) = \tau + \sigma$$

hence addition is commutative. Clearly, $\sigma = (s_j)$ has additive inverse $-\sigma = (-s_j)$. Addition of sequences is addition of functions from $\mathbb{N} \cup \{0\}$ and we know that is associative. It remains to prove multiplication is associative and distributive. I leave those to the reader. Let me explain how x comes into the picture. We need to assume R is unital for our convenience at this point.

Definition 4.5.4. *Let R be a commutative ring with unity 1 then in the polynomials $R[x]$ we define $x = (0, 1, 0, \dots)$.*

We finally learn why the notation $R[x]$ is warranted. Also, it should be fairly clear we cannot make x a variable in this context. Is $(0, 1, 0, \dots)$ a variable ?

Theorem 4.5.5. *Let R be a commutative unital ring and $\sigma \in R[x]$ with $\sigma = (s_j)$ then $\sigma = \sum_{j=0}^{\infty} \vec{s}_j x^j$ where we define $\vec{r} = (r, 0, \dots)$ for each $r \in R$.*

Proof: first, we note a property of the multiplication, if $\vec{c} = (c, 0, 0, \dots)$ and $\tau = (t_0, t_1, \dots, t_n, 0 \dots)$ then $\vec{c}\tau = (ct_0, ct_1, \dots, ct_n, 0, \dots)$. Second, notice $x^2 = xx$ is calculated by:

$$x^2 = (0, 1, 0, \dots)(0, 1, 0, \dots) = (0, 0, 1, 0, \dots)$$

since $\alpha = (0, 1, 0, \dots) = x$ and $\beta = (0, 1, 0, \dots) = x$ has $\alpha = (a_i)$ and $\beta = (b_j)$ with $a_i = b_i = 0$ for $i \neq 1$ hence:

$$\alpha\beta = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots) = (0, 0, 1, 0, \dots).$$

Furthermore, if we suppose inductively for some $n \in \mathbb{N}$, $x^n = e_{n+1}$ where $(e_i)_j = \delta_{ij}$ defines the sequence which is everywhere zero except in the i-th entry where we find 1. Then, $xx^n = e_{n+2}$ by the definition of the multiplication, only the $(n+2) - th$ entry is nontrivial since x has $x_1 = 1$ whereas $(x^n)_{n+1} = 1$ and all other entries are zero. Hence inductively $x^n = e_{n+1}$ for all $n \in \mathbb{N}$. We also define $x^0 = \vec{1}$ and $x^1 = x$ where we may note $x^0 x = \vec{1}x = x$ as we should expect. Now that we have the structure of x and powers of x sorted out we can produce the main result. Observe, we can write a polynomial as a sum of mostly zero sequences: σ with $\deg(\sigma) = n$,

$$\begin{aligned}
\sigma &= (s_0, s_1, \dots, s_n, \dots, 0) \\
&= (s_0, 0, \dots) + (0, s_1, 0, \dots) + \cdots + (0, \dots, 0, s_n, 0, \dots) \\
&= \vec{s}_0(1, 0, \dots) + \vec{s}_1(0, 1, 0, \dots) + \cdots + \vec{s}_n e_{n+1} \\
&= \vec{s}_0 x^0 + \vec{s}_1 x + \cdots + \vec{s}_n x^n \\
&= \sum_{j=0}^{\infty} \vec{s}_j x^j
\end{aligned}$$

where we threw in a few zeros in the last step. □

discuss

At this point, we tire of the notation $\vec{s}_j$. It is customary to simply write s_j in place of $\vec{s}_j$. With this notation, a typical polynomial in $R[x]$ can be expressed as:

$$\sigma = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n$$

where $s_0, s_1, \ldots, s_n \in R$ and $\deg(\sigma) = n$. I hope you appreciate how removed this is from our standard viewpoint in previous math courses. Notice this is merely notation to overlay sequences with finitely many nonzero entries. In any event, what we should take with us going forward is that $R[x]$ behaves precisely as we have assumed thus far in this course. The construction I've outlined merely shows you how we can construct indeterminants and expressions without use of functions on R. At this point we return to Gallian and follow his presentation going forward from Theorem 16.1 on page 286. Gallian has a concrete example worth including from page 284:

make explicit difference between variable and indeterminant or polynomial function vs. polynomial

Example 4.5.6. *The polynomials $f(x) = x^3+2x$ and $g(x) = x^5+2x$ are distinct in $\mathbb{Z}_3[x]$. However, if we consider f, g as functions on $\mathbb{Z}_3$ notice*

$$f(1) = 1^3 + 2(1) = 1 + 2 = 0, \quad \& \quad g(1) = 1^5 + 2(1) = 1 + 2 = 0$$
$$f(2) = 2^3 + 2(2) = 8 + 4 = 0, \quad \& \quad g(2) = 2^5 + 2(2) = 32 + 4 = 0$$
$$f(3) = 3^3 + 2(3) = 0, \quad \& \quad g(1) = 3^5 + 2(3) = 0$$

Thus, as polynomial functions on $\mathbb{Z}_3$, $f = g$.

I should also mention, Example 4.4.4 is a bit more interesting with our new view of $R[x]$. In fact, when I write $\phi_a(f(x)) = f(a)$ we mean to define the value $f(a)$ as if f was a function of R. Very sneaky.

Definition 4.5.7. *Let R be a commutative unital ring. Define the* **evaluation map** *for $a \in R$ by:*

$$\phi_a(s_0 + s_1 x + \cdots + s_n x^n) = s_0 + s_1 a + \cdots + s_n a^n.$$

for each $s_0 + s_1 x + \cdots s_n x^n \in R[x]$.

Pragmatically, it doesn't matter for many applications if we think of $R[x]$ as polynomial functions, but, algebraically, we take the viewpoint $R[x]$ is the set of polynomials in **indeterminant** x. If we wish to obtain the corresponding function then we simply make use of the evaluation map (in fact, $\phi_a : R[x] \to R$ is a ring homomorphism).

Theorem 4.5.8. *If D is an integral domain then $D[x]$ is an integral domain.*

maybe a rerun.

Proof: suppose $f(x), g(x) \in D[x]$ are nonzero polynomials $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ where a_n, b_m are the leading coefficients of $f(x), g(x)$ respective. Observe,

$$f(x)g(x) = a_n b_m x^{m+n} + \cdots + a_0 b_0.$$

Note $a_n, b_m \neq 0$ in integral domain D hence $a_n b_m \neq 0$ and we find $f(x)g(x) \neq 0$. Therefore, there are no zero divisors in $D[x]$. Furthermore, $D[x]$ is a commutative ring with unity $f(x) = 1$ hence $D[x]$ is an integral domain. □

The proof of the following is really not much removed from standard highschool algebra.

Theorem 4.5.9. *Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$. We call $q(x)$ the* **quotient** *and $r(x)$ the* **remainder** *in the division of $f(x)$ by $g(x)$.*

Proof: see page 286-287 of Gallian. If you don't understand it when you read it, try getting out a piece of paper and writing it out. It's not too hard to follow. □

Corollary 4.5.10. *Let F be a field and $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.*

Proof: by the division algorithm, there exists $g(x), r(x)$ for which $f(x) = (x-a)g(x)+r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(x-a) = 1$. It follows $r(x) = r \in R$. Moreover, by the evaluation homomorphism at a we find,

$$\phi_a(f(x)) = f(a) = (a-a)g(a) + r = r \quad \Rightarrow \quad r = f(a). \quad \square$$

Definition 4.5.11. *Let F be a field. Let $f(x) \in F[x]$, we say $c \in F$ is a* **zero** *of $f(x)$ if $\phi_c(f(x)) = f(c) = 0$. If $(x-c)^k$ is a factor of $f(x)$ and $(x-c)^{k+1}$ is not a factor of $f(x)$ then we say c* **is a zero with multiplicity** *k.*

There are pretty connections between the algebra of calculus and the existence of repeated zeros. But, we save that for another time.

Corollary 4.5.12. *Let F be a field and $a \in F$ and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.*

Proof: left to reader. □

Example 4.5.13. *An interesting counterpoint to the Corollary below is found in the polynomials with coefficients in $\mathbb{Z}_6$. The polynomial $f(x) = x^2 + 3x + 2$ has four zeros. Gallian mentions Lagrange proved the Corollary below for $\mathbb{Z}_p$ where p is prime. Another interesting point, $\mathbb{Z}_6[x]$ is also not an integral domain; $(2x+2)(3x^2+3) = 0$ yet $2x+2, 3x^2+3 \neq 0$. The study of zero divisors in $D[x]$ for D which is not integral is a nice topic to investigate. Perhaps we'll look at that further in a future lecture.*

interesting but, a bit off topic for today

Corollary 4.5.14. *A polynomial of degree n over a field F has at most n zeros counting multiplicity.*

Proof: the proof is by induction on degree. If $f(x) \in F[x]$ has $\deg(f(x)) = 0$ then $f(x) = c \neq 0$ hence there are zero zeroes for $f(x)$. Suppose inductively that each polynomial up to degree $n-1$ has at most $n-1$ zeros. Consider $f(x)$ with degree n. Suppose a is a zero with multiplicity k then $f(x) = (x-a)^k q(x)$ for some $q(x)$ with degree $n-k$. If $f(x)$ has no additional zeros then the Corollary holds since $f(x)$ has less than n zeros. Otherwise, $f(b) = 0$ for some $a \neq b$ hence $f(b) = (b-a)^k q(b) = 0$ and as $(b-a)^k \neq 0$ and F is an integral domain since it's a field it follows $q(b) = 0$. But, the $\deg(q(x)) = n - k < n$ hence by the inductive hypothesis $q(x)$ has at most $n-k$ zeros counting multiplicity thus $f(x) = (x-a)^k q(x)$ has at most $k + n - k = n$ zeros counting multiplicity. □

The argument above is great for you who are fans of formal induction, but, I am also fond of the simple argument, n is the degree of $f(x)$. Notice each zero a_1 generates a factor $(x - a_1)$ in the factorization of $f(x)$. Suppose there were $n+1$ zeros (possibly duplicate). Then

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_{n+1})g(x)$$

for some polynomial $g(x)$ and degree of $f(x)$ is at least $n+1$. This contradicts $\deg(f(x)) = n$ hence there cannot be more than n-zeros. I'm not usually a fan of contradiction, but, this argument resonates for me.

Example 4.5.15. *Consider $f(x) = x^n - 1 \in \mathbb{C}[x]$. Notice $\omega = exp(2\pi i/n)$ has $\omega^n = 1$ but $\omega^k \neq 1$ for $k = 1, 2, \ldots, n-1$. It follows that $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are all solutions of $\omega^n = 1$. Furthermore,*

$$f(x) = x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1})$$

The number $\omega = exp(2\pi i/n)$ is called the **primitive n-th root of unity** *in $\mathbb{C}$. To be pedantic, we really should say ω_n is the primitive n-th root. Then $\omega_2 = -1$, $\omega_3 = \cos(2\pi/3) + i\sin(2\pi/3)$ and $\omega_4 = i$ etc. For example,*

$$f(x) = x^4 - 1 = (x^2+1)(x^2-1) = (x+i)(x-i)(x-1)(x+1)$$

where $\omega_4 = i$ and $\omega_4^2 = -1$ and $\omega_4^3 = -i$ and $\omega_4^4 = 1$.

nice algebra!

We have studied principal ideals a bit in previous lectures, we now give a name to a ring where every ideal is principal.

Definition 4.5.16. *A* **principal ideal domain** *or* **PID** *is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.* (been here, done this.)

Many of our examples are PIDs, some are not. This much we can say:

Theorem 4.5.17. *If F is a field then $F[x]$ is a principal ideal domain.* (review of part lecture)

Proof: we know $F[x]$ is an integral domain. Suppose I is an ideal in $F[x]$. If $I = 0$ then $I = \langle 0 \rangle$ is principal. If $I \neq 0$ then the degree of polynomials in I is bounded below hence there must be an polynomial of least degree by the well-ordering-principal. Let $g(x)$ be a polynomial of least degree in I. If $f(x) \in I$ then note the division algorithm provides $q(x)$ with $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. But, $g(x)$ is of minimal degree in I and $r(x) = f(x) - g(x)q(x) \in I$ hence $r(x) = 0$. Thus $f(x) = g(x)q(x)$ and $f(x) \in \langle g(x) \rangle$ and hence $I \subseteq \langle g(x) \rangle$. Conversely, it is easy to see $\langle g(x) \rangle \subseteq I$ thus $I = \langle g(x) \rangle$ and as I was arbitrary we've shown $F[x]$ is a PID. □

From the proof above we also obtain the following:

Theorem 4.5.18. *If F is a field and I a nonzero ideal in $F[x]$ and $g(x) \in F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.*

Example 4.5.19. *Consider $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by $\phi(f(x)) = f(i)$. Observe $Ker(\phi)$ is an ideal in $\mathbb{R}[x]$ hence $Ker(\phi)$ is a principal ideal. Notice, no linear polynomial $f(x) = mx + b$ has $f(i) = 0$ since $mi + b = 0$ implies $b = -mi$ which is impossible as $m, b \in \mathbb{R}$. Consequently, $x^2 + 1 \in Ker(\phi)$ is an element of smallest degree in $Ker(\phi)$ which implies $Ker(\phi) = \langle x^2 + 1 \rangle$. If $a + ib \in \mathbb{C}$ then $\phi(a + bx) = a + bi$ hence $\phi(\mathbb{R}[x]) = \mathbb{C}$. Thus, by the first isomorphism theorem for rings, $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.*

important and cool.