# Lecture 7: Polynomial rings

Rajat Mittal ⋆

IIT Kanpur

You have seen polynomials many a times till now. The purpose of this lecture is to give a formal treatment to constructing polynomials and the rules over them. We will re derive many properties of polynomials with the only assumption that the coefficients arise from a ring or a field.

We are used to thinking of a polynomial (like $4x^2 + 2x + 6$) as an expression of coefficients (in $\mathbb{Z}, \mathbb{R}$ etc.) and variables ($x, y$ etc.). Mostly the purpose is to solve equations and find out the value of the variable or indeterminate. But the polynomials are useful not just to figure out the value of the variable but as a structure itself. The values $x, x^2, \cdots$ should be thought of as placeholder to signify the position of the coefficients. Using this view lets define a *formal polynomial*.

## 1 Polynomials over a ring

A polynomial over a ring $R$ is a formal sum $a_n x^n + \cdots + a_1 x + a_0$, where the coefficients come from the ring $R$. The set of all polynomials (in one variable) over a ring $R$ are denoted by $R[x]$. The *degree* of the polynomial is the highest power of $x$ with a non-zero coefficient.

We can define the addition and multiplication over polynomials (in $R[x]$) so as to match the definitions learned till now. Given two polynomials $a(x) = a_n x^n + \cdots + a_1 x + a_0$ and $b(x) = b_n x^n + \cdots + b_1 x + b_0$, their sum is defined as,

$$a(x) + b(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

If the degree of two polynomials is not equal, we can introduce extra zero coefficients in the polynomial with the smaller degree. For multiplication, given two polynomials $a(x) = a_n x^n + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$, their product is defined as,

$$p(x) = a(x)b(x) = (a_n b_m)x^{n+m} + \cdots + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + (a_0 b_1 + a_1 b_0)x + (a_0 b_0).$$

More formally, the product is defined using distribution and the fact that $(ax^i)(bx^j) = (ab)x^{i+j}$.

*Exercise 1.* What is the degree of $a(x)b(x)$ if the degree of $a(x)$ is $n$ and $b(x)$ is $m$?

Hint: It need not be $n + m$. why?

We mentioned while giving examples of rings that if $R$ is a commutative ring then $R[x]$ is a commutative ring too. Using the definition above, the polynomials in multiple variables can be defined using induction. We can consider $R[x_1, x_2, \cdots, x_k]$ to be the ring of polynomials whose coefficients come from $R[x_1, x_2, \cdots, x_{k-1}]$.

Another definition of interest is the *monic* polynomial whose leading coefficient (non-zero coefficient of the highest degree) is 1. A polynomial is *constant* iff the only non-zero coefficient is the degree 0 one ($a_0$).

The most important polynomial rings for us would be $\mathbb{Z}_m[x]$ and $\mathbb{Z}[x], \mathbb{R}[x]$ etc..

*Exercise 2.* Suppose $a(x) = 2x^3 + 2x^2 + 2$ is a polynomial in $\mathbb{Z}_4[x]$, what is $a(x)^2$?

## 2 Polynomials over fields

After defining addition and multiplication we would like to define division and gcd of polynomials. It turns out that these definitions make sense when $R$ is a field. For this section, we will assume that we are given a field $F$ and the polynomials are in $F[x]$. We know that $F[x]$ is an integral domain since $F$ is one.

⋆ Thanks to the book from Dummit and Foote and the book from Norman Biggs.

*Exercise 3.* Show that $F[x]$ is an integral domain if $F$ is an integral domain.

*Exercise 4.* For the remaining section, note where we use that the underlying ring of coefficients $F$ is a field.

**Theorem 1.** *Division: Given two polynomials $f(x)$ and $g(x)$, there exist two* unique *polynomials called quotient $q(x)$ and remainder $r(x)$, s.t.,*

$$f(x) = q(x)g(x) + r(x).$$

*where the degree of $r(x)$ is less than the degree of $g(x)$.*

*Proof.* Existence: Suppose the degree of $f(x)$ is less than degree of $g(x)$ then $q(x) = 0$ and $r(x) = f(x)$. This will be the base case and we will apply induction on the degree of $f(x)$.

Say $f(x) = f_n x^n + \cdots + f_1 x + f_0$ and $g(x) = g_m x^m + \cdots + g_1 x + g_0$ with $m \leq n$. Multiply $g$ by $f_n g_m^{-1} x^{n-m}$ and subtract it from $f$.

$$f(x) - f_n g_m^{-1} x^{n-m} g(x) = (f_{n-1} - g_{m-1} f_n g_m^{-1}) x^{n-m-1} + \cdots = l(x).$$

So $l$ is a polynomial with lower degree and by induction it can be written as $l(x) = q'(x)g(x) + r(x)$. This implies $f(x) = (f_n g_m^{-1} x^{n-m} + q'(x))g(x) + r(x)$. So we can always find $q(x)$ and $r(x)$ with the condition given above. This method is called *long division* and is the usual method of dividing two numbers.

*Exercise 5.* What is the relation between the usual division between two integers you learnt in elementary classes and long division.

Uniqueness: Suppose there are two such decompositions $f = q_1 g + r_1$ and $f = q_2 g + r_2$ (notice that we have suppressed $x$ for the sake of brevity). Then subtracting one from another,

$$0 = (q_1 - q_2)g + (r_1 - r_2).$$

*Exercise 6.* Show that this implies $q$ and $r$ are unique.

□

Using the division algorithm, we can define the Euclidean GCD algorithm.

*Exercise 7.* Read and understand the Euclidean gcd algorithm for two positive numbers.

Lets define *greatest common divisor (gcd)* first. Given two polynomials $f, g$, their greatest common divisor is the highest degree polynomial which divided both $f, g$. The important observation for Euclidean gcd is, if $f = gq_1 + r_1$ then

$$gcd(f, g) = gcd(g, r_1).$$

Without loss of generality we can assume that $f$ has higher degree than $g$ and hence $r$ has lower degree than $g$ and $f$. We can continue this process, say $g = q_2 r_1 + r_2$. Then the task reduces to finding the gcd of $r_1$ and $r_2$. Ultimately we get two polynomials, s.t., $r_n \mid r_{n-1}$. Then $r_n$ is the gcd of $f$ and $g$.

*Exercise 8.* Show that any polynomial which divides both $f$ and $g$ will also divide $r_n$ mentioned above. Show that $r_n$ divides both $f$ and $g$.

From the previous exercise it is clear that $r_n$ is one of the gcd (it divides both and has highest degree).

*Exercise 9.* Why is gcd unique?

*Exercise 10.* Imp: Show that using Euclidean algorithm for gcd, if $gcd(f, g) = d$ then there exist two polynomials $p, q$, s.t., $d = pf + qg$.

Lets define *primes* in the ring of polynomials. They are called *irreducible* polynomials (irreducible elements of integral domain $F[x]$). A polynomial $f$ is *irreducible* iff it is not constant and there does NOT exist two non-constant polynomials $g$ and $h$, s.t., $f = gh$.

*Exercise 11.* Given that a monic polynomial $g$ is irreducible, show, any polynomial $f$ is divisible by $g$ or their gcd is 1. This property can be re-stated, any irreducible polynomial can't have a non-trivial gcd (trivial gcd: 1 or the polynomial itself).

With this definition we can start finding the factors of any polynomial $f$. Either $f$ is irreducible or it can be written as $gh$. If we keep applying this procedure to $g$ and $h$. We get that any polynomial $f$ can be written as,

$$f = cg_1g_2 \cdots g_k.$$

Where $g_i$'s are irreducible monic polynomials and $c$ is a constant in the field $F$.

Can two such factorizations exist? It turns out, like in the case of natural numbers, this factorization is unique up to ordering of polynomials. For the contradiction, suppose there are two such factorizations $cg_1 \cdots g_k$ and $ch_1 \cdots h_l$.

*Exercise 12.* Why can we assume that the constant is the same for both factorizations?

We know that since $g_1$ is irreducible it can't have a non-trivial gcd with either $h = h_1 \cdots h_{l-1}$ or $h_l$. We will also show that it can't have gcd 1 with both. Suppose $gcd(h_l, g_1)$ is 1. Then using Euclidean gcd,

$$1 = ph_l + qg_1 \Rightarrow h = pf + qg_1h.$$

Since $g_1$ divides both terms on the R.H.S, it divides $h$. Hence the gcd of $h$ and $g_1$ is $g_1$. So $g_1$ either divides $h_l$ or $h = h_1 \cdots h_{l-1}$.

If it divides $h_1 \cdots h_{l-1}$, we can further divide it and ultimately get that $g_1$ divides $h_i$ for some $i$. But since $g_1$ and $h_i$ both are irreducible and monic, hence $g_1 = h_i$. This gives the theorem,

**Theorem 2.** *Unique factorization: Given a polynomial $f$ it can be written in a unique way as a product of irreducible monic polynomials up to ordering.*

$$f(x) = cg_1(x)g_2(x) \cdots g_k(x)$$

*Where $c$ is a constant in $F$ (the leading coefficient of $f$) and $g_i$'s are irreducible monic polynomials.*

*Exercise 13.* The order of going from division algorithm to Euclidean GCD to unique factorization is important. Where else have you seen this?

There is an easy way to find out whether a degree 1 polynomial $x - a$ divides a polynomial $f$ or not. Substitute $a$ in the polynomial $f$ (we call the evaluation f(a)), if it evaluates to zero then $x - a$ divides $f$ otherwise not. If $f(a) = 0$, we say that $a$ is a *root* of $f$. The proof of this is given as an exercise.

Using the factorization theorem we can show that any polynomial of degree $d$ can have at most $d$ roots. The proof of this theorem is left as an exercise.

**Theorem 3.** *Given a polynomial $p$ of degree $d$ over a field $F$. There are at most $d$ distinct roots of $p$.*

## 3 Field extension

*Exercise 14.* Why do we need complex numbers?

It might seem a weird question given the context. But lets look at the answer first. Mathematician didn't have the roots of polynomial $x^2 + 1$ in the field $\mathbb{R}$. So they came up with another field $\mathbb{C}$ where the solution existed.

Can we do it for other fields and other polynomials? This can be done and is known as *field extension*. Lets try to construct such a field extension.

Suppose we are given a field $F$ and a polynomial $p$ in it. We can look at the set of all polynomial in $F[x]$ modulo the polynomial $p$. This set is known as $\frac{F[x]}{(p)}$. The reason for this is that $(p)$ is an ideal generated by polynomial $p$ (it contains all multiples of $p$).

*Exercise 15.* Show that $(p)$ is an ideal.

So $\frac{F[x]}{(p)}$ is just the quotient ring generated by the ideal $(p)$.

A more intuitive way to understand this ring is, it is the set of polynomials in $F[x]$ assuming that two polynomials are equal if they only differ by a multiple of $p$. Using the division algorithm we can always reduce any polynomial $f$ to a polynomial $r$, s.t., $f = qp + r$. Then by above discussion $r = f$ in $\frac{F[x]}{(p)}$. In the algebraic language, $r$ is the representative of the additive coset of $F[x]$ containing $f$.

*Exercise 16.* Show that the elements of $\frac{F[x]}{(p)}$ are basically all the polynomials with degree less than $deg(p)$.

The ring $\frac{F[x]}{(p)}$ is a field iff $p$ is irreducible (proof is left as an exercise). This field $\frac{F[x]}{(p)}$ is called the field extension of $F$. It is easy to see that an isomorphic copy of $F$ is a subfield of $\frac{F[x]}{(p)}$.

The great thing is that there is a root of $p$ in this new field. If you think for a minute the root is $x$ !!

The field $\frac{F[x]}{(p)}$ can also be viewed as a vector space over $F$.

*Exercise 17.* What is the dimension of that vector space?

We are interested in these field extensions because they will help us characterize finite fields.

### 3.1 Another way to look at field extension

More general way to define field extensions is through subfields. Suppose $K$ is a subset of a field $L$, s.t., $K$ is field itself. Then we say that $K$ is a sub-field of $L$ or $L$ is an extension of $K$.

Suppose $s$ is an element of $L$ not in $K$. We can extend $K$ to include $s$. The smallest subfield of $L$ which contains $K$ as well as $s$ is called $K(s)$. We can similarly define $K(S)$, where $S$ is a set.

Why are the two interpretations given above similar. If $s$ was a root of an irreducible polynomial $p$ in $K$ then the field $K(s)$ is precisely $\frac{K[x]}{(p)}$. All the elements of $K(s)$ can be viewed as polynomials in $K[x]$ with degree less than $deg(p)$ (substituting $s$ for $x$).

*Exercise 18.* Show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \quad a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

Notice that complex numbers can be viewed as $\mathbb{R}(i)$ or as $\frac{\mathbb{R}[x]}{x^2+1}$.

Suppose $L$ is a field extension of $K$. Then $L$ can be seen as a vector space over $K$. The dimension of the vector space is known as the *degree* of the extension.

*Note 1.* You might have seen vector spaces over reals and complex numbers. They can be defined over arbitrary field $F$ by assuming that the coefficients (scalars) come from $F$ and any addition and multiplication of scalars can be done in accordance with the field.

*Exercise 19.* What is the degree of extension $\frac{K[x]}{p}$.

Note that the subfield perspective of field extension is more general than the field extension using polynomials. Reals are an extension of rationals. It can be shown that such an extension cannot be obtained by any irreducible polynomial over rationals.

## 4 Assignment

*Exercise 20.* Write a program to compute the coefficient of $x^i$ in $a(x)b(x)$ given two polynomials $a(x)$ and $b(x)$.

*Exercise 21.* Compute the product of $7x^3 + 2x^2 + 2x + 4$ and $2x^2 + 5x + 1$ in $\mathbb{Z}_{14}$.

*Exercise 22.* Show that in $\mathbb{Z}_p$ ($p$ is a prime), $(x + y)^p = x^p + y^p$.

*Exercise 23.* Show that if $R$ is an integral domain then so is $R[x]$.

*Exercise 24.* Show that $f(x)$ in $F[x]$ has an inverse iff $f(x)$ is a constant polynomial (zero excluded).

*Exercise 25.* Find out the quotient and remainder when $x^3 + 5x^2 + 2x + 3$ is divided by $x^2 + 1$ in $\mathbb{Z}_7$.

*Exercise 26.* If $F$ is a field, is $F[x]$ also a field?

*Exercise 27.* What is the gcd of $x^n + 1$ and $x^m - 1$ in $\mathbb{Z}_2[x]$.

*Exercise 28.* Show that $x - a$ divides $f$ iff $f(a) = 0$.

*Exercise 29.* Hard: Prove that the ring $\frac{F[x]}{(p)}$ is a field iff $p$ is irreducible.

*Exercise 30.* Prove the theorem 3.