Lecture 4 — Polynomials

Dr. D. Bernhard

In this lecture: definition of polynomials — degree — polynomials over rings — polynomial arithmetic — calculation modulo polynomials

Learning outcomes. After this lecture and revision, you should be able to:

- Convert polynomials between a representation as sequences and a representation using a formal variable X.
- Divide polynomials with remainder, over both $\mathbb{Q}$ and any finite field.
- Add and multiply polynomials over any field and in polynomial rings over fields.

4 Polynomials

If we have any group $\mathbb{G} = (G, +)$ we can make a new group $\mathbb{G}^n$ by taking tuples of length n of G-elements and adding them component-wise. We can do the same for rings but the result is not that interesting: any tuple with a 0 element anywhere is a zero divisor (except the all-zero tuple, which is the zero element). Polynomials are a much "richer" structure to look at tuple of ring elements.

4.1 Definition of polynomials

Let's look at polyomials over $\mathbb{Z}$ in one variable X to start with. A polynomial is a finite sequence of monomials, each of which is a coefficient multiplied with a power of X such as $p = 2X^2 + X - 1$ or $q = 2X$. We can add polynomials, this means we add the coefficients of the same powers so $p + q = 2X^2 + 3X - 1$. We can also multiply polynomials, the rule here is that you multiply every monomial of p with every one of q, multiplying coefficients and adding powers: $p \cdot q = 4X^3 + 2X^2 - 2X$.

Polynomials over $\mathbb{Z}$ are of course functions from $\mathbb{Z}$ to $\mathbb{Z}$, since you can stick an integer in the variable and get an integer out. In Algebra, we are more interested in polynomials as objects in their own right rather than their effects as functions. The variable X is not important: all the information about polynomials is contained in the coefficients. We can write a polynomial over the integers as a sequence of integers, starting with the coefficient for the power 0 and proceeding in order of ascending powers, so $p = (-1, 1, 2, 0, \ldots)$ and $q = (0, 2, 0, \ldots)$. This way, a polynomial is an infinite sequence of which at most finitely many elements are nonzero. To save ourselves from always writing out dots, we can break off as soon as no more nozero elements follow and write for example $q = (0, 2)$.

With this example in mind we give the definition of a polynomial ring over an arbitrary ring $(R, +, \cdot)$:

Definition 4.1 (polynomial ring). Let $\mathcal{R} = (R, +, \cdot)$ be any ring. The polynomial ring in one variable $\mathcal{R}[X]$ over $\mathcal{R}$ is the following ring:

- Elements are (countably) infinite sequences of R-elements, of which at most finitely many in a sequence are nonzero.
- Addition is element-wise, so $(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$.
- Multiplication is defined as follows. For two elements $a = (a_0, a_1, \ldots)$ and $b = (b_0, b_1, \ldots)$ the product is the element $c = (c_0, c_1, \ldots)$ with

$$c_j := \sum_{i=0}^{j} a_i \cdot b_{j-i}$$

The formula for multiplication describes each coefficient of c in terms of addition and multiplication in the ring $\mathcal{R}$ and does exactly what the informal definition over "powers of X" says. Note that the element X in the name $\mathcal{R}[X]$ never appears later in the definition: it is just a label and it is beat not to think of it as a "variable" too much. Of course we can write polynomials using a formal variable X as well, if we want to.

The zero of $\mathcal{R}[X]$ is the sequence that is zero (the zero of $\mathbb{R}$) everywhere and the one is the sequence $(1, 0, 0, \ldots)$; written as a polynomial in a formal variable X this sequence is simply $1 + 0X + 0X^2 \ldots = 1$ (which is the one of the ring $\mathcal{R}$).

Exercise. $(\star)$ *Polynomials modulo* 7. Compute the following in $\mathbb{Z}_7[X]$:

1. $(4X^3 + 5X + 2) + (6X^3 + 2X^2 + 3)$
2. $(X^2 + 6X + 4) \cdot (3X^3 + 2X^2 + 1)$

4.2 Degree

We should check that the product of two polynomials (as sequences) really is another polynomial, that is only finitely many elements end up non-zero. We introduce the degree:

> **Definition 4.2.** The degree of a non-zero polynomial is the index of the highest coefficient that is non-zero, starting the count at 0. The degree of p is denoted by $\mathsf{deg}(p)$.

So the degree of $p = 4X^2+2X+1 = (1, 2, 4)$ is 2 since we start counting at coefficient zero (which has the value 1 in p). The degree of the zero polynomial can either be left undefined or we can define it to be minus infinity.

> **Proposition 4.3.** For polynomials p, q we have $\mathsf{deg}(p + q) \leq \max(\mathsf{deg}(p), \mathsf{deg}(q))$ and $\mathsf{deg}(p \cdot q) \leq \mathsf{deg}(p) + \mathsf{deg}(q)$.

This is almost the rule we are used to from polynomials over $\mathbb{Z}$ and it proves that the sum and product of polynomials is again a polynomial, since the resulting sequence has a finite degree. The reason for $\leq$ instead of $=$ is that zero divisors can cancel the highest coefficients. In $\mathbb{Z}_6[X]$, for polynomials $p = 2X = (0, 2)$ and $q = 3X^2 = (0, 0, 3)$ we have $pq = (0)$ since $2 \cdot 3 = 0 \pmod 6$. An even more “unusual” event happens in $\mathbb{Z}_4[X]$ for the polynomial $2X + 1 = (1, 2)$: we compute $(2X + 1) \cdot (2X + 1) = [4X^2 + 4X + 1] = 1$ (i.e. compute normally and reduce modulo 4) so this polynomial is a unit and also its own inverse.

4.3 Polynomial arithmetic

In Algebra, we often treat polynomials as “another kind of number”. We can perform operations like greatest common divisor or division with remainder on polynomials too, as long as the ring over which we’re building them is “nice” enough. In this course we only consider the case when the base ring is a field.

> **Proposition 4.4 (polynomial division with remainder).** Let $\mathbb{F}$ be a field and consider the polynomial ring $\mathbb{F}[X]$. For any two polynomials a, b with $b \neq 0$, there are unique polynomials q and r such that $a = q \cdot b + r$ and $\mathsf{deg}(r) < \mathsf{deg}(b)$.

Here the condition that the remainder be less than the modulus is replaced by the new condition that it be of lesser degree. The usual “long division” algorithm works fine for polynomials over any finite field (division of coefficients is performed in the field; this is why we need a field not just any ring). We will revisit this when we discuss finite fields in a later lecture.

Time for some actual polynomial arithmetic. Let’s take the field $\mathbb{F}_7 = (\mathbb{Z}_7, +, \cdot)$ with the following addition/multiplication tables:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- Divide $(X^2 + 5X + 1)$ by $(3X + 2)$ with remainder.

$$\begin{array}{rrrrrrrl}
(& X^2 & + & 5X & + & 1) & & : (3X+2) = 5X+3 \\
-(& X^2 & + & 3X) & & & & \\
\cline{1-4}
 & & & 2X & + & 1 & & \\
 & & -(& 2X & + & 6) & & \\
\cline{3-6}
 & & & & & 2 & &
\end{array}$$

To match up the highest coefficients, we need to solve $X^2 = 3X \cdot a$ which gives $a = 5X$ since $3 \cdot 5 = 1 \pmod 7$. We compute $5X(3X+2) = X^2+3X$ and subtract $(X^2+5X+1)-(X^2+3X) = (2X+1)$ giving $(X^2+5X+1) = 5X(3X+2)+(2X+1)$. The remainder $2X + 1$ still has degree 1 so we divide with remainder again: first, solve $2X = 3X \cdot b$ to get $b = 3$, $3 \cdot (3X + 2) = 2X + 6$, $(2X + 1) - (2X + 6) = 2$ so

$$(X^2 + 5X + 1) = (5X + 3) \cdot (3X + 2) + 2$$

- Find the greatest common divisor of $(2X^2 + 4X + 5)$ and $(X^2 + 3X + 3)$.

  Euclid's algorithm for greatest common divisors says to repeatedly divide with remainder until a remainder becomes 0, the last non-zero remainder is then the greatest common divisor. So:

$$\begin{array}{rrrrrrl}
(& 2X^2 & + & 4X & + & 5) & : (X^2+3X+3) = 2 \\
-(& 2X^2 & + & 6X & + & 6) & \\
\cline{1-6}
 & & & 5X & + & 6 &
\end{array}$$

$$\begin{array}{rrrrrrl}
(& X^2 & + & 3X & + & 3) & : (5X+6) = 3X+4 \\
-(& X^2 & + & 4X) & & & \\
\cline{1-4}
 & & & 6X & + & 3 & \\
 & & -(& 6X & + & 3) & \\
\cline{3-6}
 & & & & & 0 &
\end{array}$$

This gives us a greatest common divisor of $(5X + 6)$ and indeed $2X^2 + 4X + 5 = (5X + 6)(6X + 2)$ and $X^2 + 3X + 3 = (5X + 6)(3X + 4)$.

NOTE — factorisations, gcds etc. of polynomials are unique "up to units", just like in $\mathbb{Z}$. For example, what is the gcd of 12 and -9? For sure, 3 is a candidate but also -3 — both are common factors of the same magnitude. It's just that in $\mathbb{Z}$ we have the convention that we take the positive one (since the only units are 1 and -1, so there are only two to choose from). In $\mathbb{F}_7[X]$, there is a whole field to choose from. We could take $2X^2 + 4X + 5 = (5X + 6)(6X + 2)$ and multiply the first bracket with 2 and the second with the inverse of 2, which happens to be 4, to get $2X^2 + 4X + 5 = (3X + 5)(3X + 1)$ which is an equally correct factorisation.

Exercise. ($\star\star$) *Division with remainder.* Over $\mathbb{Z}_7[X]$, divide $p(X)$ by $q(X)$ with remainder:

- $p(X) = 2X^5 + 2X^2 + X + 4, \quad q(X) = 2X^2 + 1$
- $p(X) = 3X^3 + 2X^2 + 5X + 1, \quad q(X) = 3X + 2$
- $p(X) = 3X^3 + 2X^2 + 5X + 1, \quad q(X) = 2X + 6$

Exercise. ($\star\star$) *Division without remainder.* We know that a polynomial of degree $n > 0$ can have at most n distinct roots (values of a such that $p(a) = 0$) and this holds over any finite field. Further, we know that $(X - a)$ divides $p(X)$ (leaves remainder 0 in division with remainder) if and only if a is a root of p — this too holds over any field.

Over $\mathbb{Z}$, any polynomial has a unique factorisation. However, over $\mathbb{F}_7$, the polynomial $X^2 + 5X - 1$ divides all of the following: $(X + 2)$, $(X + 3)$, $(2X + 4)$, $(4X + 5)$, $(3X + 6)$, $(3X - 1)$, $(5X + 1)$.

1. Find the roots of $X^2 + 5X - 1$ in $\mathbb{F}_7$. Explain why these many different linear factors do not give more than 2 roots.
2. Give an example where a degree-2 polynomial can be written in several different ways as products of degree-1 polynomials without using any "modulus" operations, i.e. over a field where $1 + 1 + 1 + \ldots$ can never become 0.

4.4 Fields modulo polynomials

Just like we produced $\mathbb{Z}_n$ from $\mathbb{Z}$ by repeatedly subtracting n from anything that is n or above, we can take a polynomial ring modulo a polynomial p to get a ring of elements "less than" p. This is called taking the polynomial ring modulo p. While this works for any ring $\mathcal{R}$, it only really gives a nice structure to work in if we start with a field.

Formally, we start with any field $\mathbb{F}$ and any polynomial p in $\mathbb{F}[X]$ and define an equivalence relation $\sim_p$ under which two polynomials a, b are equivalent if there is a polynomial q such that $a + p \cdot q = b$, i.e. you can add a multiple of p to a to get b. This is an equivalence relation. We can do division with remainder in $\mathbb{F}[X]$ and the equivalence relation is the same as saying two elements are equivalent if and only if they leave the same remainder when dividing by p. Each equivalence class contains exactly one polynomial of degree less than $\texttt{deg}(p)$ and we choose this as the representative of the class.

> **Definition 4.5 (field modulo polynomial).** For a field $\mathbb{F}$, we mean by $\mathbb{F}[X]/p(X)$ the ring of equivalence classes of polynomials under $\sim_p$ where the representative of each class is the unique polynomial in that class of degree less than $\texttt{deg}(p)$.

As an example, let's compute $(X^2 + X + 4) \cdot (2X + 3)$ in $\mathbb{F}_7[X]/(X^3 + X + 1)$.

$$\begin{aligned} \left[(X^2 + X + 4)(2X + 3)\right] &= \\ \left[2X^3 + 5X^2 + 4X + 5\right] &= \\ \left[2(X^3 + X + 1) + (5X^2 + 2X + 3)\right] &= \\ 5X^2 + 2X + 3 & \end{aligned}$$

We reduce $\pmod 7$ along the way; the last step is division with remainder by the modulus polynomial $X^3 + X + 1$.

From this example we see that since the modulus polynomial has degree 3, every polynomial in $\mathbb{F}_7[X]/(X^3+X+1)$ will have degree at most 2. So the size of the resulting ring will be 7^3 elements as polynomials in this ring can be represented by length-3 vectors of elements of $\mathbb{F}_7$.

We will soon use this idea to construct finite fields. Before we do so however we will use the next lecture to introduce homomorphisms which will help us understand better what is going on in these fields and when two diffferent-looking fields are “essentially” the same.

Exercise. ($\star\star$) *The relation $\sim_p$.* Check that $\sim_p$ used in this section really is an equivalence relation. For an added challenge, check the same when the construction is done over an arbitrary ring instead of a field.

4.5 ◇ Representatives modulo $\sim_p$

◇ Let's check that the representatives modulo $\sim_p$ do what we claim, i.e. that there is a unique element of each class with degree less than that of p. For any class C, pick any element c in the class and divide c by p with remainder; the remainder is a member of the same class but has degree less than $\mathtt{deg}(p)$. If two members a, b of the same class both have degree less than the degree of p then we divide a by p with remainder and must get b, but a already had degree less than that of p so $a = b$.

Note that over an arbitrary ring $\mathcal{R}$, equivalence classes can contain several different elements of low degree so there is no longer such an obvious choice of representatives.

4.6 ◇ Euclidean domains

◇ Just like we can cancel $\cancel{a\cdot}x = \cancel{a\cdot}y$ in integral domains without being able to invert a, we can sometimes perform division with remainder without being able to invert ring elements. In this case we call the ring an Euclidean domain:

> **Definition 4.6 (Euclidean domain).** A ring $(R, +, \cdot)$ with a function $\mathtt{deg} : R\backslash\{0\} \to \mathbb{N}$ is an Euclidean domain if the function $\mathtt{deg}$ has the property that for all nonzero $a, b \in R$ we have $\mathtt{deg}(a \cdot b) \geq \mathtt{deg}(a)$ and for all $a, b \in R$ with $b \neq 0$ there exist q, r with $\mathtt{deg}(r) < \mathtt{deg}(b)$ so that we can write $a = q \cdot b + r$.

The degree function may be any function that satisfies the conditions given, not just the usual one for polynomials. We could define the degree of the ring's zero to be minus infinity if we wanted. The general definition just says that q, r exist but not that they are unique. If we take the ring $(\mathbb{Z}, +, \cdot)$ with the degree function $\mathtt{deg}(x) := |x|$, the absolute value, we still have a Euclidean domain but remainders are no longer unique (exercise: why? What are we doing differently to Lecture 1?)

If we take any field $\mathbb{F}$, the ring of polynomials $\mathbb{F}[X]$ is a Euclidean domain with the usual degree function and quotients and remainders are unique.