Math 332 Winter 2023, Lecture 25: Polynomials

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

3. Monoid algebras and polynomials

Recall: For this entire chapter, we fix a **commutative** ring R.

3.2. Polynomial rings (cont'd)

3.2.3. Evaluation of univariate polynomials

Polynomials can not only be added, scaled and multiplied, but also **evaluated** (i.e., we can substitute elements of an R-algebra for the indeterminates). This is what makes polynomial rings special (as compared to arbitrary monoid algebras).

Let us first define evaluation for univariate polynomials.

Definition 3.2.4. Let $p \in R[x]$ be a univariate polynomial. Let A be any R-algebra. Let $a \in A$.

We define the element $p(a) \in A$ as follows: Write p as

$$p = \sum_{i \in \mathbb{N}} p_i x^i \qquad \text{(where } p_i \in R\text{, and all but finitely many } i \text{ satisfy } p_i = 0\text{)},$$

and set

$$p(a) := \sum_{i \in \mathbb{N}} p_i a^i.$$

This element $p(a)$ is called the **evaluation** of p at a; we also say that it is obtained by **substituting** a for x in p.

Instead of $p(a)$, we also write $p[a]$. (See the warning below for the reason why.)

Here, A can be any R-algebra (not necessarily commutative): for example, it can be R itself, or a matrix ring $R^{n \times n}$, or a polynomial ring like $R[x]$. Thus, polynomials are "like functions but better" (since a function can only be evaluated at the elements of its domain, whereas a polynomial can be evaluated at any element of any R-algebra).

Evaluation is also the reason why polynomials are better-behaved than formal power series. For example, you cannot evaluate the formal power series $1 + x + x^2 + x^3 + \cdots$ at 1 (since $1 + 1 + 1^2 + 1^3 + \cdots$ is ill-defined).

Note that $p(x) = p$ for any $p \in R[x]$. Indeed, $p(x)$ is the result of substituting x for x, and clearly this substitution doesn't actually change anything in the polynomial.

Warning 3.2.5. The notation $p(a)$ can be quite ambiguous. For example, is $p(p+1)$ the evaluation of p at $p+1$ or rather the product of p with $p+1$? Thus, I recommend writing $p \cdot (p+1)$ for the product and $p[p+1]$ for the evaluation. Generally, I will use the $p[a]$ notation as often as possible, but sometimes I will use $p(a)$ for the sake of familiarity.

Here is a slightly surprising example of evaluation:

Example 3.2.6. Let $R = \mathbb{Z}/2$, and let $p \in R[x]$ be the polynomial $x^2 + x = x \cdot \left(x + \overline{1}\right)$. Let us evaluate p at elements of R:

$$p\left[\overline{0}\right] = \overline{0}^2 + \overline{0} = \overline{0};$$
$$p\left[\overline{1}\right] = \overline{1}^2 + \overline{1} = \overline{2} = \overline{0}.$$

Thus, the polynomial p gives $\overline{0}$ whenever it is evaluated at any element of $\mathbb{Z}/2$. This does not mean that p is the zero polynomial! Evaluating p on 2×2-matrices reveals that p can take nonzero values as well:

$$p\left[\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}\right] = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}^2 + \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \neq 0_{2\times 2}.$$

(And of course, evaluating p at x itself gives $p[x] = p$, which is nonzero as well.)

Given an R-algebra A and an element $a \in A$, the operation of evaluating polynomials $p \in R[x]$ at a is rather well-behaved:

Theorem 3.2.7. Let A be an R-algebra. Let $a \in A$. Then, the map

$$R[x] \to A,$$
$$p \mapsto p[a]$$

is an R-algebra morphism. In other words:

- This map respects multiplication and addition. In other words: For any two polynomials $p, q \in R[x]$, we have
$$(pq)[a] = p[a] \cdot q[a] \qquad \text{and}$$
$$(p+q)[a] = p[a] + q[a].$$
- This map respects scaling. In other words: For any $\lambda \in R$ and $p \in R[x]$, we have
$$(\lambda p)[a] = \lambda \cdot p[a].$$
- This map respects zero and one. In other words: We have $0[a] = 0$ and $1[a] = 1$.

The proof of this becomes easy using the following lemma (which shows that "respects multiplication" can be proved by checking it on monomials):

Lemma 3.2.8. Let A and B be two R-algebras. Let $f : A \to B$ be an R-linear map. Let $(m_i)_{i \in I}$ be a family of vectors in A that spans A. If we have

$$f\left(m_i m_j\right) = f\left(m_i\right) f\left(m_j\right) \qquad \text{for all } i, j \in I,$$

then

$$f\left(ab\right) = f\left(a\right) f\left(b\right) \qquad \text{for all } a, b \in A.$$

Proof of Lemma 3.2.8. By linearity. See Lemma 4.2.9 in the text for details. □

Proof of Theorem 3.2.7. The first bullet point is easy using Lemma 3.2.8. The other two bullet points are easy on their own. See Theorem 4.2.8 in the text for details. □

3.2.4. Evaluation for multivariate polynomials

So much for evaluation of univariate polynomials. An analogous concept exists for multivariate polynomials, but it requires that the "inputs" (i.e., the values at which we evaluate our polynomial) mutually commute. Here is the precise definition:

Definition 3.2.9. Let $n \in \mathbb{N}$. Let $p \in R\left[x_1, x_2, \ldots, x_n\right]$ be a multivariate polynomial. Let A be any R-algebra. Let $a_1, a_2, \ldots, a_n \in A$ be n elements of A that mutually commute (i.e., that satisfy $a_i a_j = a_j a_i$ for all $i, j \in \{1, 2, \ldots, n\}$).

We define the element $p\left(a_1, a_2, \ldots, a_n\right) \in A$ as follows: Write the polynomial p as

$$p = \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \qquad \left(\text{for } p_{i_1, i_2, \ldots, i_n} \in R\right),$$

and set

$$p\left(a_1, a_2, \ldots, a_n\right) := \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}.$$

This element $p\left(a_1, a_2, \ldots, a_n\right)$ is called the **evaluation** of p at $a_1, a_2, \ldots, a_n$; we also say that it is obtained by **substituting** $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$ in p. We also denote it by $p\left[a_1, a_2, \ldots, a_n\right]$.

There is an analogue of Theorem 3.2.7:

Theorem 3.2.10. Let $n \in \mathbb{N}$. Let A be any R-algebra. Let $a_1, a_2, \ldots, a_n \in A$ be n elements of A that mutually commute (i.e., that satisfy $a_i a_j = a_j a_i$ for all

$i, j \in \{1, 2, \ldots, n\}$). Then, the map

$$\begin{aligned} R\left[x_1, x_2, \ldots, x_n\right] &\to A, \\ p &\mapsto p\left(a_1, a_2, \ldots, a_n\right) \end{aligned}$$

is an R-algebra morphism.

Proof. See Theorem 4.2.11 in the text. (Here we need the $a_i a_j = a_j a_i$ condition.) □

3.2.5. Constant polynomials

In Convention 3.1.4 (in Lecture 24), we defined the notion of a constant element of a monoid ring $R[M]$: This is just an element of the form $r \cdot 1 = r \cdot e_1$, where $r \in R$ and where 1 is the neutral element of M.

Since polynomial rings are monoid rings, we obtain in particular the notion of a constant polynomial. This is exactly what you think: a polynomial of the form $r \cdot x^0$ (or, in the multivariate case, $r \cdot x_1^0 x_2^0 \cdots x_n^0$) for $r \in R$. We identify such a polynomial with the scalar $r \in R$ itself.

For example, the polynomial $3x^0 = 3 \in \mathbb{Z}[x]$ is constant, but the polynomial $3x$ is not.

3.2.6. Coefficients

By their definition, polynomials are R-linear combinations of monomials. Let us introduce a notation for the coefficients in these R-linear combinations:

Definition 3.2.11. Let $p \in R\left[x_1, x_2, \ldots, x_n\right]$ be a polynomial. Let $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ be a monomial. Then, the **coefficient** of $\mathfrak{m}$ in p is the element $[\mathfrak{m}]\, p$ of R defined as follows: If we write p as

$$p = \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \qquad \left(\text{for } p_{i_1, i_2, \ldots, i_n} \in R\right),$$

then

$$[\mathfrak{m}]\, p := p_{a_1, a_2, \ldots, a_n}.$$

For example:

- For univariate polynomials, we have

$$\left[x^3\right]\left((1+x)^5\right) = \binom{5}{3} = 10 \qquad \text{and} \qquad \left[x^6\right]\left((1+x)^5\right) = 0$$

(since $(1+x)^5 = 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5$).

- For multivariate polynomials, if we set $n = 2$ and rename the variables x_1, x_2 as x, y, then we have

$$\left[x^2y^3\right]\left((x+y)^5\right) = 10$$

(since $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$) and

$$[xy]\left((x+y)^5\right) = 0$$

(for the same reason).

3.2.7. Symbols for indeterminates

The definition of a multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ that we gave above (Definition 3.2.3 in Lecture 24) depends on a ring R and the number n. The names of the indeterminates are "hardcoded" to be $x_1, x_2, \ldots, x_n$. However, it is actually better to have a more flexible definition, which allows to arbitrarily specify the names of the indeterminates. Thus, for example, we should be able to define the polynomial rings $R[x, y]$ and $R[y, z]$, which are each isomorphic to $R[x_1, x_2]$, but should not be treated as being the same ring (since the former has indeterminates x and y whereas the latter has indeterminates y and z). Distinguishing between these two isomorphic rings $R[x, y]$ and $R[y, z]$ offers several advantages, in particular allowing us to identify them with two **different** subrings of $R[x, y, z]$ (in a natural way).

This necessitates some minor changes to our definition of multivariate polynomial rings (Definition 3.2.3 in Lecture 24). Namely, instead of using the monoid

$$C^{(n)} = \left\{x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \mid (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n\right\}$$

as the set of monomials, we now need to use the monoid

$$C^{(S)} = \left\{\prod_{s\in S} s^{a_s} \mid a_s \in \mathbb{N} \text{ for each } s \in S\right\},$$

where S is our chosen (finite) set of indeterminates (for example, $S = \{x, y\}$ or $S = \{y, z\}$ or $S = \{\alpha, \mathbf{w}, \clubsuit\}$ if we have nothing better to do). A monomial in this monoid $C^{(S)}$ is a "formal" product of the form $\prod\limits_{s\in S} s^{a_s}$ (with each factor being a formal power of one of our indeterminates), and stands for a family $(a_s)_{s\in S} \in \mathbb{N}^S$ of nonnegative integers. Two such monomials are multiplied by the rule

$$\left(\prod_{s\in S} s^{a_s}\right)\cdot\left(\prod_{s\in S} s^{b_s}\right) = \prod_{s\in S} s^{a_s+b_s}.$$

The polynomial ring in the set S of indeterminates is then defined as the monoid ring $R\left[C^{(S)}\right]$ of this monoid $C^{(S)}$. We shall refer to such a ring as a **multivariate polynomial ring with named variables**, and just call it $R[S]$.

Thus, for a three-element set $S = \{x, y, z\}$, we have $R[S] = R[x, y, z]$, which is the polynomial ring over R in three variables that are named x, y, z. For instance, $x^2 + 7y^3z - xyz$ is a polynomial in this ring $R[x, y, z]$. As we said, $R[x, y, z]$ is isomorphic to $R[x_1, x_2, x_3]$ as an R-algebra (via the isomorphism that sends each monomial $x^a y^b z^c$ to $x_1^a x_2^b x_3^c$); thus, named variables do not introduce anything genuinely new to our theory as long as we are studying a single polynomial ring at a time. But their flexibility is helpful when working with several polynomial rings, e.g., by allowing us to treat $R[x]$ and $R[y]$ as two different subrings of $R[x, y]$.

We will be cavalier about all of this in the following, sometimes renaming variables at will (we will often rename x_1, x_2 as x, y or rename x_1, x_2, x_3 as x, y, z for no other reasons than brevity).

3.3. Univariate polynomials

Let us now take a closer look at univariate polynomial rings, as they have several special properties that multivariate polynomial rings do not share.

3.3.1. Degrees and coefficients

By its definition, the univariate polynomial ring $R[x]$ has the basis $(x^0, x^1, x^2, \ldots)$ (as an R-module).

Recall that if $p \in R[x]$ is a polynomial, and if $i \in \mathbb{N}$, then $[x^i]\, p$ is the coefficient of x^i in p. That is, if p is written as $p = \sum_{j \in \mathbb{N}} p_j x^j$ with $p_j \in R$, then $[x^i]\, p = p_i$.

Definition 3.3.1. Let $p \in R[x]$ be a univariate polynomial.

(a) If $p \neq 0$, then the **degree** of p is defined to be the largest $i \in \mathbb{N}$ such that $[x^i]\, p \neq 0$. The degree of the zero polynomial $0 \in R[x]$ is defined to be $-\infty$ (a symbol that is understood to be smaller than any integer).

The degree of p is denoted by $\deg p$.

(b) If $p \neq 0$, then the **leading coefficient** of p is defined to be $[x^{\deg p}]\, p \in R$.

(c) The polynomial p is said to be **monic** if its leading coefficient is 1.

For example, the polynomial

$$5x^3 + 2x + 1 \in \mathbb{Q}[x]$$

has degree 3 and leading coefficient 5. Hence, it is not monic (since $5 \neq 1$). The polynomial

$$\overline{5}x^3 + \overline{2}x + \overline{1} \in (\mathbb{Z}/n)[x] \qquad \text{(for a given integer } n > 0\text{)}$$

has

- degree 3 if $n > 5$;
- degree 1 if $n = 5$ (since the $\overline{5}x^3$ term disappears when $n = 5$);
- degree 3 if $n = 2, 3, 4$;
- degree $-\infty$ if $n = 1$.

Remark 3.3.2. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}
&\{f \in R[x] \mid \deg f \leq n\} \\
&= \left\{f \in R[x] \mid f = a_0x^0 + a_1x^1 + \cdots + a_nx^n \text{ for some } a_i \in R\right\} \\
&= \operatorname{span}\left(x^0, x^1, \ldots, x^n\right).
\end{aligned}$$

In particular, this is an R-submodule of $R[x]$.

Corollary 3.3.3. Let $p, q \in R[x]$. Then,

$$\begin{aligned}
&\deg(p+q) \leq \max\{\deg p, \deg q\} \qquad \text{and} \\
&\deg(p-q) \leq \max\{\deg p, \deg q\}.
\end{aligned}$$

Remark 3.3.4. The polynomials of degree ≤ 0 are just the constant polynomials.

So much for degrees of sums and differences. What can we say about the degree of a product?

Proposition 3.3.5. Let $p, q \in R[x]$. Then:
(a) We have $\deg(pq) \leq \deg p + \deg q$.
(b) We have $\deg(pq) = \deg p + \deg q$ if $p \neq 0$ and the leading coefficient of p is a unit.
(c) We have $\deg(pq) = \deg p + \deg q$ if R is an integral domain.
(d) If $n, m \in \mathbb{N}$ satisfy $n \geq \deg p$ and $m \geq \deg q$, then

$$\left[x^{n+m}\right](pq) = \left[x^n\right](p) \cdot \left[x^m\right](q).$$

(e) If $pq = 0$ and $p \neq 0$ and if the leading coefficient of p is a unit, then $q = 0$.

Proof. See Proposition 4.3.5 in the text for proofs. □

Corollary 3.3.6. If R is an integral domain, then the polynomial ring $R[x]$ is also an integral domain.

Proof. Follows from Proposition 3.3.5 **(c)** (since $\deg 0 = -\infty$). □

Remark 3.3.7. If R is not an integral domain, then polynomials over R can behave rather strangely. For example, if $R = \mathbb{Z}/4$, then

$$\left(\overline{1} + \overline{2}x\right)^2 = \overline{1} + \overline{4}x + \overline{4}x^2 = \overline{1} \qquad \left(\text{since } \overline{4} = \overline{0}\right).$$

So the degree of a polynomial can decrease when it is squared!

3.3.2. Division with remainder

Just like integers, univariate polynomials can be divided with remainder, as long as the polynomial you are dividing by has an invertible (i.e., unit) leading coefficient:

Theorem 3.3.8 (Division-with-remainder theorem for polynomials)**.** Let $b \in R[x]$ be a nonzero polynomial whose leading coefficient is a unit. Let $a \in R[x]$ be any polynomial.

(a) Then, there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

(b) Moreover, this pair satisfies $\deg q \leq \deg a - \deg b$.

Proof. See Theorem 4.3.7 in the text. □

The polynomials q and r in Theorem 3.3.8 are called the **quotient** and the **remainder** obtained when dividing a by b. Note that if $\deg a < \deg b$, then the quotient q is 0 whereas the remainder r is a. The quotient and the remainder become interesting when $\deg a \geq \deg b$.

Don't forget the condition "the leading coefficient of b is a unit" in Theorem 3.3.8. This condition is automatically satisfied if b is monic (since 1 is a unit), and it is also automatically satisfied if R is a field (since any nonzero element of a field is a unit). But there are examples for $R = \mathbb{Z}$ where it is not satisfied. (See Exercises 5 and 6 on homework set #6 for some examples.)

Recall from elementary number theory that a positive integer b divides an integer a if and only if the remainder that a leaves when divided by b is 0. Here is an analogue of this fact for univariate polynomials:

Proposition 3.3.9. Let $b \in R[x]$ be a nonzero polynomial whose leading coefficient is a unit. Let $a \in R[x]$ be any polynomial. Let q and r be the quotient and the remainder obtained when dividing a by b. Then, we have $b \mid a$ in $R[x]$ if and only if $r = 0$.

Proof. See Proposition 4.3.12 in the text (or figure it out on your own – it is easy). □