# Math 332 Winter 2023, Lecture 29: Polynomials

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

## 5. Polynomials II

In this last lecture, we will catch a very brief glimpse of the study of multivariate polynomials. The material that I will show (without proofs) is at the spring of several renowned fields of mathematics (algebraic geometry, Gröbner bases, combinatorial commutative algebra) and deserves a whole course of its own. Alas, now that the quarter is almost over, all I can give are a few basic results and pose a few questions. More can be found in Chapter 6 of the text, in de Graaf's notes [deGraa20], or in the book [CoLiOs15] (listed here roughly in the order of increasing comprehensiveness, although I am not saying that each source is fully contained in the next).

**Convention 5.0.1.** Again, for this entire chapter, we fix a **commutative** ring $R$.

As we saw last time (§3.5 in Lecture 28), univariate polynomials are very well-behaved as long as their leading coefficients are invertible. If $b \in R[x]$ is a degree-$m$ polynomial with this property, then $R[x]/b$ is a free $R$-module with basis $\left(\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}\right)$. Furthermore, in this case, each polynomial in $R[x]$ can be divided with remainder by $b$, and thus divisibility by $b$ can be easily checked. Also, if $F$ is a field, then the polynomial ring $F[x]$ is a Euclidean domain (by Theorem 3.3.16 in Lecture 26), thus a PID, so that all its ideals are principal, and therefore the quotient rings of $F[x]$ always have the form $F[x]/b$ for some single polynomial $b$.

Everything becomes more complicated once we pass to multivariate polynomials. I will just outline some of the main questions and a few of the simplest results. Generally, the study of ideals and quotient rings of multivariate polynomial rings is one of the main topics in **algebraic geometry**.

### 5.1. Non-principal ideals

If $R$ is a field, then the ring $R[x]$ is a PID, but the ring $R[x,y]$ is not. Here is the simplest example of a non-principal ideal: Let $P = R[x,y]$. Then, the ideal $xP + yP$ of $P$ can be rewritten as follows:

$$\begin{aligned} xP + yP &= \{\text{all multiples of } x\} + \{\text{all multiples of } y\} \\ &= \{\text{all polynomials whose constant term is } 0\} \qquad (\text{why?}) \\ &= \{f \in P \mid f[0,0] = 0\} \qquad (\text{since } f[0,0] \text{ is the constant term of } f). \end{aligned}$$

If $R$ is nontrivial, then this ideal $xP + yP$ of $P$ is not principal (i.e., not of the form $uP$ for some $u \in P$).

The quotient ring $P/(xP + yP)$ is quite simple: It is isomorphic to $R$ (as an $R$-algebra). Specifically, the map

$$\begin{aligned} P/(xP + yP) &\to R, \\ \overline{f} &\mapsto f[0,0] \end{aligned}$$

is an $R$-algebra isomorphism. (This is not hard to check.)

For comparison,

$$P/(xP) = P/x \cong R[y],$$

via the $R$-algebra isomorphism

$$\begin{aligned} P/x &\to R[y], \\ \overline{f} &\mapsto f[0,y]. \end{aligned}$$

This should be quite intuitive: If we quotient out $x$ from the polynomial ring $P = R[x,y]$, we should be left with the other indeterminate $y$.

Here is a slightly trickier version of this isomorphism: We have

$$P/(x+y) \cong R[x],$$

via the $R$-algebra isomorphism

$$\begin{aligned} P/(x+y) &\to R[x], \\ \overline{f} &\mapsto f[x,-x]. \end{aligned}$$

Intuitively, this is because quotienting out $x + y$ from the polynomial ring $P = R[x,y]$ means that we are "setting $y := -x$", so that we are left with only one free variable $x$.

Note, in particular, that $P/(x+y)$ is not the same as $P/(xP + yP)$, since the principal ideal $(x+y)P$ is not the same as $xP + yP$. (For instance, $2x + 3y \notin (x+y)P$.)

## 5.2. More interesting example: $R[x,y]/\left(x^2+y^2-1\right)$

How does the quotient ring $R[x,y]/\left(x^2+y^2-1\right)$ look like? For $R = \mathbb{R}$ in particular, it is known as the **ring of trigonometric polynomials**, since there is an $\mathbb{R}$-algebra morphism

$$\begin{aligned} \mathbb{R}[x,y]/\left(x^2+y^2-1\right) &\to \underbrace{\mathbb{R}^{\mathbb{R}}}_{\substack{\text{ring of functions } \mathbb{R}\to\mathbb{R} \\ \text{(with pointwise addition} \\ \text{and multiplication and} \\ \text{scaling)}}}, \\ \overline{f} &\mapsto f[\sin t, \cos t]. \end{aligned}$$

It can be shown that this map is injective (not obvious!), so that $\mathbb{R}[x,y] / \left(x^2+y^2-1\right)$ is isomorphic to a subring of $\mathbb{R}^{\mathbb{R}}$. It can also be shown that $\mathbb{R}[x,y] / \left(x^2+y^2-1\right)$ is an integral domain. But, for instance, $(\mathbb{Z}/2)[x,y] / \left(x^2+y^2-1\right)$ is not an integral domain, because over $\mathbb{Z}/2$, we have

$$x^2+y^2-1 = (x+y-1)^2 \qquad \text{(check this!)},$$

so that the nonzero residue class $\overline{x+y-1}$ is nilpotent in $(\mathbb{Z}/2)[x,y] / \left(x^2+y^2-1\right)$.

Another question: As an $R$-module, is $R[x,y] / \left(x^2+y^2-1\right)$ free? Equivalently, is there a unique division-with-remainder procedure in the ring $R[x,y]$ by the polynomial $x^2+y^2-1$ ?

There are two answers to this question, one more specific to this polynomial, and one more general.

For the more specific answer, we note the following:

**Proposition 5.2.1.** We have

$$R[x,y] \cong (R[x])[y] \qquad \text{as } R\text{-algebras.}$$

More concretely, the map

$$R[x,y] \to (R[x])[y],$$
$$\sum_{i,j\in\mathbb{N}} a_{i,j}x^i y^j \mapsto \sum_{j\in\mathbb{N}} \left(\sum_{i\in\mathbb{N}} a_{i,j}x^i\right) y^j$$

is an $R$-algebra isomorphism.

This isomorphism sends $x^2+y^2-1 \in R[x,y]$ to $x^2+y^2-1 = y^2+\left(x^2-1\right) \in (R[x])[y]$, which is a monic polynomial in $y$ of degree 2 over the ring $R[x]$. Hence, by what we know about monic polynomials (specifically, Theorem 3.5.2 in Lecture 28), we can divide with remainder by $y^2+\left(x^2-1\right)$, and the quotient ring $(R[x])[y] / \left(y^2+\left(x^2-1\right)\right)$ is a free $R[x]$-module with basis $\left(\overline{y^0}, \overline{y^1}\right) = \left(\overline{1}, \overline{y}\right)$. Now, unapplying the isomorphism from Proposition 5.2.1, we conclude that the quotient ring $R[x,y] / \left(x^2+y^2-1\right)$ is a free $R[x]$-module with basis $\left(\overline{1}, \overline{y}\right)$, therefore a free $R$-module with basis

$$\left(\overline{x^0}, \overline{x^1}, \overline{x^2}, \ldots, \overline{x^0y}, \overline{x^1y}, \overline{x^2y}, \ldots\right).$$

Note that Proposition 5.2.1 can be generalized to many variables:

**Proposition 5.2.2.** For any $n > 0$, we have

$$R[x_1, x_2, \ldots, x_n] \cong (R[x_1, x_2, \ldots, x_{n-1}])[x_n] \text{ as } R[x_1, x_2, \ldots, x_{n-1}]\text{-algebras.}$$

By applying this proposition iteratively, we obtain

$$R[x_1, x_2, \ldots, x_n] \cong (((R[x_1])[x_2])[x_3]) \cdots [x_n] \text{ as } R\text{-algebras.}$$

In other words, a multivariate polynomial ring can be constructed by introducing the variables "one at a time".

The variables in a multivariate polynomial ring can also be reordered arbitrarily: e.g., we have $R[x, y, z, w] \cong R[y, z, x, w]$. Thus, while Proposition 5.2.1 gives an isomorphism $R[x, y] \cong (R[x])[y]$, we can just as easily obtain an isomorphism $R[x, y] \cong (R[y])[x]$. As a consequence, a polynomial in $x$ and $y$ can be regarded as a univariate polynomial in two ways: either as a univariate polynomial in $y$ over $R[x]$ (using the isomorphism $R[x, y] \cong (R[x])[y]$), or as a univariate polynomial in $x$ over $R[y]$ (using the isomorphism $R[x, y] \cong (R[y])[x]$). By viewing our polynomial $x^2 + y^2 - 1$ in the former way, we obtained the basis

$$\left(\overline{x^0}, \overline{x^1}, \overline{x^2}, \ldots, \overline{x^0 y}, \overline{x^1 y}, \overline{x^2 y}, \ldots\right)$$

of $R[x, y] / \left(x^2 + y^2 - 1\right)$. Likewise, viewing it in the latter way, we can obtain the basis

$$\left(\overline{y^0}, \overline{y^1}, \overline{y^2}, \ldots, \overline{xy^0}, \overline{xy^1}, \overline{xy^2}, \ldots\right)$$

of $R[x, y] / \left(x^2 + y^2 - 1\right)$. There are, of course, many other bases.

## 5.3. Trickier examples

Now we understand the $R$-modules $R[x, y] / y$ and $R[x, y] / \left(x^2 + y^2 - 1\right)$ well enough. What about $R[x, y] / (xy)$ ?

Our above method does not help us here, since the polynomial $xy$ neither has an invertible leading coefficient when considered as a polynomial in $x$ (over $R[y]$) nor when considered as a polynomial in $y$ (over $R[x]$). We need a new idea.

However, $xy$ is just a monomial, so that it is pretty clear what happens when we quotient it out: All monomials $x^i y^j$ with $i > 0$ and $j > 0$ are equated to 0 (since they are multiples of $xy$), whereas all the other monomials (i.e., the monomials $1, x, x^2, x^3, \ldots, y, y^2, y^3, \ldots$) remain $R$-linearly independent (since no $R$-linear combination of them is a multiple of $xy$, except for the trivial combination 0). Thus, the $R$-module $R[x, y] / (xy)$ is free with basis

$$\left(\overline{1}, \overline{x}, \overline{x^2}, \overline{x^3}, \ldots, \overline{y}, \overline{y^2}, \overline{y^3}, \ldots\right).$$

As an $R$-algebra, it is not an integral domain, since $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{0}$.

So we were lucky again. But what about $R[x, y] / (xy(x - y))$ ? None of our above tricks can help us now.

## 5.4. Degrees and the deg-lex order

It is time for a general method, or at least as general as we can hope for. In the univariate case, we were able to answer many questions about $R[x]/b$ using division with remainder. So let us try to extend division with remainder to the multivariate case. The first question is: What is a leading coefficient?

For example, in the polynomial

$$(x+y+1)^2 = x^2 + 2xy + y^2 + 2x + 2y + 1,$$

the terms $x^2$, $2xy$ and $y^2$ have the largest degrees. It makes sense for one of them to count as the leading term. But which one? We clearly need a systematic method to break ties.

First, we get some basic terminology in place:

**Convention 5.4.1.** As we said, $R$ is a fixed commutative ring.

Now we also fix $n \in \mathbb{N}$. We let $P$ be the polynomial ring $R[x_1, x_2, \ldots, x_n]$.

As we recall, a **monomial** is an element of the free abelian monoid $C^{(n)}$ with $n$ generators $x_1, x_2, \ldots, x_n$, and has the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ for some $a_1, a_2, \ldots, a_n \in \mathbb{N}$.

We have already used the notion of a degree of such a monomial, but let us define it formally:

**Definition 5.4.2.** The **degree** of a monomial $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is defined to be $a_1 + a_2 + \cdots + a_n \in \mathbb{N}$. It is called $\deg \mathfrak{m}$.

**Definition 5.4.3.** A monomial $\mathfrak{m}$ is said to **appear** in a polynomial $f \in P$ if $[\mathfrak{m}] f \neq 0$. (Recall that $[\mathfrak{m}] f$ denotes the coefficient of $\mathfrak{m}$ in $f$.)

**Definition 5.4.4.** The **degree** of a nonzero polynomial $f \in P$ is the largest degree of a monomial that appears in $f$.

For example, the polynomial $(x+y+1)^3 - (x+y)^3 \in \mathbb{Q}[x,y]$ has degree 2, since it equals $3x^2 + 3y^2 + 6xy + 3x + 3y + 1$. But the polynomial $\left(x+y+\overline{1}\right)^3 - (x+y)^3 \in (\mathbb{Z}/3)[x,y]$ has degree 0, since it equals $\overline{1}$.

The following proposition is the multivariate analogue to parts **(a)** and **(c)** of Proposition 3.3.5 in Lecture 25:

**Proposition 5.4.5** (degree-of-a-product formula)**.** Let $p, q \in P$ be nonzero. Then:

**(a)** We have $\deg(pq) \leq \deg p + \deg q$.

**(b)** We have $\deg(pq) = \deg p + \deg q$ if $R$ is an integral domain.

Part **(a)** of this proposition is easy (since $\deg(\mathfrak{mn}) = \deg\mathfrak{m} + \deg\mathfrak{n}$ for any monomials $\mathfrak{m}$ and $\mathfrak{n}$). But why should part **(b)** be true? It is no longer clear what a "leading term" should be, so what guarantees us that there is not some "magic" cancellation in the highest degree when we multiply $p$ with $q$?

There are, in fact, many different ways to define leading terms. Here is the simplest:

**Definition 5.4.6.** Let $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $\mathfrak{n} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ be two monomials. We write $\mathfrak{m} \prec \mathfrak{n}$ (and say that $\mathfrak{m}$ is **smaller than** $\mathfrak{n}$ **in deg-lex order**) if and only if

- either $\deg\mathfrak{m} < \deg\mathfrak{n}$
- or $\deg\mathfrak{m} = \deg\mathfrak{n}$ and the smallest $i \in \{1, 2, \ldots, n\}$ that satisfies $a_i \neq b_i$ satisfies $a_i < b_i$.

Thus, the deg-lex order is a way to compare two monomials $\mathfrak{m}$ and $\mathfrak{n}$, and it compares them as follows: If their degrees are different, then the monomial with smaller degree is automatically declared to be smaller. If their degrees are equal, then the exponents on each variable are compared, starting with $x_1$ and moving up the list of variables. The first time the exponents differ on some variable, the monomial having the smaller exponent is declared to be smaller.

For example, writing $x_1, x_2, x_3$ as $x, y, z$, we have $x^3y^2z^1 \prec z^8$ (since $\deg\left(x^3y^2z^1\right) < \deg\left(z^8\right)$) and $x^3y^1z^2 \prec x^3y^2z^1$ (since $\deg\left(x^3y^1z^2\right) = \deg\left(x^3y^2z^1\right)$ and $3 = 3$ and $1 < 2$) and

$$x^2 \prec y^2z \prec xyz \prec x^2z \prec y^4 \prec x^2y^2 \prec x^3y \prec \cdots.$$

This deg-lex order ("deg-lex" is short for "degree-lexicographic") has some nice properties, including (most importantly) the fact that if two monomials $\mathfrak{m}$ and $\mathfrak{n}$ satisfy $\mathfrak{m} \prec \mathfrak{n}$, then $\mathfrak{mp} \prec \mathfrak{np}$ for any further monomial $\mathfrak{p}$. (See §6.2.2 in the text for more details.)

Now, we can define use the deg-lex order to define leading coefficients for multivariate polynomials:

**Definition 5.4.7.** Let $p \in P$ be a nonzero polynomial. Then:

**(a)** The **leading monomial** of $p$ is defined to be the largest monomial $\mathfrak{m}$ (largest with respect to deg-lex order) that appears in $p$. We denote this leading monomial by $\operatorname{LM} p$.

**(b)** The **leading coefficient** of $p$ is defined to be the coefficient $[\operatorname{LM} p]\, p$ of $p$. It is denoted by $\operatorname{LC} p$.

**(c)** The **leading term** of $p$ is defined to be $\operatorname{LC} p \cdot \operatorname{LM} p$.

For example, the leading monomial of $(x+y+3)^2 \in \mathbb{Q}[x,y]$ is $x^2$, and the leading coefficient is 1. For another example, the leading monomial of

$(2x+3y)^2 \in \mathbb{Q}[x,y]$ is $x^2$, the leading coefficient is 4, and the leading term is $4x^2$.

Thanks to the above $\mathfrak{mp} \prec \mathfrak{np}$ property of deg-lex order, leading monomials behave well: In particular, when we multiply two nonzero polynomials $p, q \in P$, their leading terms get multiplied, unless the coefficients multiply to 0. This yields Proposition 5.4.5 **(b)**. As a consequence, we conclude:

**Corollary 5.4.8.** If $R$ is an integral domain, then the multivariate polynomial ring $P = R[x_1, x_2, \ldots, x_n]$ is an integral domain as well.

(Alternatively, this can also be proved using Proposition 5.2.2, since we know how to prove the univariate case already.)

## 5.5. Division with remainder

So the deg-lex order is a nice and consistent way to break ties when deciding what monomial of a polynomial is leading. It is not the only such way, and in fact, the existence of many possible "monomial orders" that each fit the bill is more of a blessing than a curse, since it allows you to pick and choose in specific problems. There is no single best order, although the deg-lex order is perhaps the simplest to work with. See §6.3.3 in the text for another important monomial order (the lex order, which does **not** take degrees into account before comparing exponents), and see [CoLiOs15, §2.2] for a general theory of monomial orders.

Having a monomial order in place, we can try to imitate the standard "long division" (i.e., division-with-remainder) algorithm for univariate polynomials with multivariate polynomials. We obtain the following generalization of the univariate division-with-remainder theorem (Theorem 3.3.8 in Lecture 25):

**Theorem 5.5.1** (Division-with-remainder theorem for multivariate polynomials)**.** Let $b \in P$ be a nonzero polynomial whose leading coefficient is a unit of $R$. Let $a \in P$ be any polynomial.

Then, there is a **unique** pair $(q, r)$ of polynomials in $P$ such that

$$a = qb + r$$

and such that no multiples of the leading monomial of $b$ appear as monomials in $r$.

*Proof.* Much like the univariate case. Note that the "no multiples of the leading monomial of $b$ appear as monomials in $r$" condition is a multivariate analogue of the "$\deg r < \deg b$" condition from the univariate case. See Theorem 6.3.1 in the text for some examples.

(But note that the uniqueness is only relative to the choice of monomial order. A different monomial order can lead to a different pair $(q, r)$.) □

**Corollary 5.5.2.** Let $b \in P$ be a nonzero polynomial whose leading coefficient is a unit of $R$. Then, the $R$-module $P/b$ is free with basis

$$(\overline{\mathfrak{m}})_{\mathfrak{m} \text{ is a monomial that is not a multiple of the leading monomial of } b}.$$

This answers (at least under the "leading coefficient is a unit" condition) the question of how a quotient ring of $P$ by a single polynomial looks like.

## 5.6. What about non-principal ideals?

But recall that $P$ has non-principal ideals, too (if $n > 1$). What happens if we quotient $P$ by a non-principal ideal? In other words, what if we want to equate several polynomials with 0 at the same time?

Here, the theory becomes really interesting. You can try dividing with remainder by several polynomials, but the remainder will often be non-unique. There is a way to make remainders unique by bringing the list of polynomials to a special form, called a **Gröbner basis**. A taste of Gröbner bases can be found in §6.3 of the text, and a systematic introduction is given in [CoLiOs15] and in [deGraa20]. Let me mention that, at least when $R$ is a field, the whole theory is algorithmic, and the algorithms are available in most computer algebra packages. For example:

**Example 5.6.1.** Let $R = \mathbb{Q}$ and $n = 3$, and write $x, y, z$ for $x_1, x_2, x_3$. Let $I = b_1 P + b_2 P + b_3 P$, where

$$\begin{aligned} b_1 &= x^2 + xy, \\ b_2 &= y^2 + yz, \\ b_3 &= z^2 + zx. \end{aligned}$$

Does $z^4$ belong to $I$ ? Direct division with remainder does not help, at least not if you are using the deg-lex order, since none of the leading monomials of $b_1, b_2, b_3$ or any of their multiples appear in $z^4$ (keep in mind that the leading monomial of $b_3$ is $zx$, not $z^2$). However, if you first compute the Gröbner basis of $I$, and then divide $z^4$ with remainder by that Gröbner basis, then you obtain the remainder 0, which shows that $z^4$ does belong to $I$.

For example, the SageMath computer algebra system computes the Gröbner basis to be

$$\left(x^2 + xy,\ \ y^2 + yz,\ \ xz + z^2,\ \ yz^2 - z^3,\ \ z^4\right),$$

which makes it particularly clear that $z^4 \in I$.

# References

[CoLiOs15] David A. Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, 4th edition, Springer 2015.
https://dx.doi.org/10.1007/978-3-319-16721-3

[deGraa20] Willem de Graaf, *Computational Algebra*, 5 August 2021.
https://www.science.unitn.it/~degraaf/algnotes/compalg.pdf