Computational Methods

These notes are written by Federico Galetto (Cleveland State University) for the mini-course on Computational Methods in Commutative Algebra at the Séminaire de Mathématiques Supérieures (SMS) 2025: An Introduction to Recent Trends in Commutative Algebra. The author wishes to thank all students who participated in the 2025 SMS for their feedback on earlier versions of these notes; a special thanks to Silas Vriend for catching a number of typos and for many helpful comments. You can contact the author at f.galetto@csuohio.edu.

References

- Cox, Little, O'Shea - *Ideals, Varieties and Algorithms*
- Eisenbud - *An Introduction to Commutative Algebra with a View Towards Algebraic Geometry*
- Kreuzer, Robbiano - *Computational Algebra 1*
- Ene, Herzog - *Gröbner Bases in Commutative Algebra*
- Adams, Loustaunau - *An Introduction to Gröbner Bases*

Day 1

Motivational problems

Let $R = \Bbbk[x_1, \dots, x_n]$ be a polynomial ring over a field $\Bbbk$. Let $I = \langle f_1, \dots, f_r \rangle \subseteq R$ be an ideal. We are interested in the following problems.

Ideal membership and equality

- Given $f \in R$, determine if $f \in I$.
- If $f \in I$, find $q_1, \dots, q_r \in R$ such that $f = \sum_{i=1}^{r} q_i f_i$.
- Given an ideal J of R, determine if $I = J$.

Let $\mathbb{V}(I)$ denote the vanishing locus of I in the affine space $\mathbb{A}^n_{\Bbbk}$. Knowing that $f \in I$ tells us that f vanishes on all points of $\mathbb{V}(I)$. Checking ideal equality is useful when the same ideal is given two different generating sets. Also, $I = J$ implies the equality of vanishing loci $\mathbb{V}(I) = \mathbb{V}(J)$ (the converse is false).

Quotient representations

- Given $f \in R$, how should we represent the coset $f + I$ in the quotient ring R/I?
- Given $f, g \in R$, determine if $f + I = g + I$.
- Find a basis of R/I as a $\Bbbk$-vector space.

For example, the classes in the quotient ring $\mathbb{Z}/\langle m\rangle$ can be represented by the integers $0, \ldots, m-1$. Geometrically, a polynomial $f \in R$ determines a polynomial function $\mathbb{V}(I) \to \Bbbk$. When $f + I = g + I$, the polynomials f and g determine the same function on $\mathbb{V}(I)$. Finding bases of R/I allows us to use linear algebra to study geometric properties of $\mathbb{V}(I)$ such as dimension and degree.

Univariate case

Before tackling these problems in full generality, it useful to focus on the one variable case $\Bbbk[x]$. In this case, we can use the fact that $\Bbbk[x]$ is a Euclidean domain.

Theorem

For every $f, g \in \Bbbk[x]$ with $g \neq 0$, there exist unique $q, r \in \Bbbk[x]$ (called *quotient* and *remainder*, respectively) such that $f = qg + r$ and $r = 0$ or $\deg(r) < \deg(g)$.

Here $\deg(g)$ denotes the largest power of the variable x appearing in g with a nonzero coefficient. In other words, if $\deg(g) = d$, then

$$g = \sum_{i=1}^{d} c_i x^i$$

with $c_d \neq 0$. We call $c_d x^d$ the *leading* or *initial term* of g and we call c_d the *leading coefficient*.

The *long division algorithm* gives an effective way to construct q and r given f and g. From here, we can solve the problems above. For example, letting $I = \langle g\rangle$, we have:

- $f \in I$ if and only if $r = 0$;
- if $f \in I$, then $f = qg$ where the unique q can be found explicitly;
- $f + I = r + I$, so we can choose the remainder as the standard representative modulo I;
- assuming $\deg(g) = d$, the elements $1 + I, x + I, x^2 + I, \ldots, x^{d-1} + I$ form a $\Bbbk$-basis of $\Bbbk[x]/I$.

Monomial orderings

The first thing we do when dividing f by g is line out their terms from highest to lowest degree. A multivariate division algorithm would require a similar step, but how should we order terms of a polynomial in two or more variables?

A *monomial* in $R = \Bbbk[x_1, \ldots, x_n]$ is an element of the form $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ with $a = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$ (note: $0 \in \mathbb{N}$). We set $|a| = a_1 + a_2 + \cdots + a_n$, so $\deg(x^a) = |a|$. Some sources say *term* instead of monomial; other sources use the word term for polynomials cm where $0 \neq c \in \Bbbk$ and m is a monomial.

Definition

A *monomial ordering* on the polynomial ring $R = \Bbbk[x_1, \ldots, x_n]$ is an order (meaning reflexive, antisymmetric, and transitive) relation $<$ on the set of monomials in R satisfying the following

properties.

1. It is total: for all monomials $m_1 \neq m_2$, we have $m_1 < m_2$ or $m_2 < m_1$.
2. It is compatible with multiplication: for all monomials m_1, m_2, m_3, if $m_1 < m_2$, then $m_1 m_3 < m_2 m_3$.
3. Has 1 as its minimum: for all monomials $m \neq 1$, we have $1 < m$.

Here are a few notable monomial orderings.

Example: Lexicographic Order (Lex)

We write $x^a >_{\text{Lex}} x^b$ in the lexicographic order if the first nonzero entry of the vector $a - b$ is positive. When we use different letters such as x, y, z for variables, the lexicographic order is simply the alphabetical order, so $x > y > z$. However, as a result, the lexicographic order ignores degrees, so you end up with $x > y^{100}$.

Example: Graded Lexicographic Order (GLex)

We write $x^a >_{\text{GLex}} x^b$ in the graded lexicographic order if $|a| > |b|$, or $|a| = |b|$ and $x^a >_{\text{Lex}} x^b$. Thus, the graded lexicographic order prioritizes degree, and then uses the lexicographic order to break ties.

Example: Graded Reverse Lexicographic Order (GRevLex)

We write $x^a >_{\text{GRevLex}} x^b$ in the graded reverse lexicographic order if $|a| > |b|$, or $|a| = |b|$ and the rightmost nonzero entry of the vector $a - b$ is negative. The name is related to the fact that on monomials of the same degree this is the reverse of the (graded) lexicographic order if the order of the variables is reversed.

Here is the same polynomial written from largest to smallest term in the orders above.

- Using Lex: $x^4 + x^3y^2z^4 + xy^5z^3$
- Using GLex: $x^3y^2z^4 + xy^5z^3 + x^4$
- Using GRevLex: $xy^5z^3 + x^3y^2z^4 + x^4$

Although Lex and GLex seem a little more natural and have their applications, there are practical reasons for working with GRevLex (which is the default in software like Macaulay2).

Fix a monomial ordering on $R = \mathbb{k}[x_1, \ldots, x_n]$ and let $f \in R$.

- The largest monomial appearing with a nonzero coefficient in a polynomial f is called its *leading monomial*; we denote it $\text{LM}(f)$.

- The coefficient of the leading monomial is called the *leading coefficient* of f; we denote it $\mathrm{LC}(f)$.
- The product of the leading coefficient and the leading monomial gives the *leading term* of f; we denote it $\mathrm{LT}(f)$, so we have $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$.

The words monomial and term are some times interchanged in the literature; also, some sources refer to leading terms/monomials as *initial* or *head* terms/monomials.

Multivariate division

Theorem

Consider an ordered collection of polynomials $F = (f_1, \ldots, f_s) \in R^s$ where $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. For every $f \in R$, there exist $q_1, \ldots, q_s, r \in R$ such that $f = \sum_{i=1}^{s} q_i f_i + r$, and $r = 0$ or r is a $\Bbbk$-linear combination of monomials none of which are divisible by any of $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s)$.

The element r is known as the *normal form* of f upon division by F.

Division algorithm

To construct $q_1, \ldots, q_s$ and r, we initially set them equal to 0, then proceed as follows.

1. Find the smallest i such that $\mathrm{LM}(f_i)$ divides $\mathrm{LM}(f)$, if any, then go to step 2; otherwise, go to step 3.
2. Replace q_i by $q_i + \mathrm{LT}(f)/\mathrm{LT}(f_i)$ and f by $f - (\mathrm{LT}(f)/\mathrm{LT}(f_i))f_i$, then go to step 4.
3. Replace r by $r + \mathrm{LT}(f)$ and f by $f - \mathrm{LT}(f)$, then go to step 4.
4. If $f = 0$, then stop and return $q_1, \ldots, q_s, r$; otherwise, go back to step 1.

For example, suppose we want to divide $f = x^2y^2 - y^3$ by $f_1 = y^2 - x$ and $f_2 = xy - 1$ in GLex. We can write out the division algorithm using the format of long division. We highlight terms added to r.

Therefore, we get $q_1 = x^2 - y$, $q_2 = -1$, and $r = x^3 - 1$. However, notice what happens if we swap f_1 and f_2.

In this case, we get $q_1 = xy$, $q_2 = -y$, and $r = 0$; it follows that $f = xyf_2 - yf_1 \in \langle f_1, f_2 \rangle$. This shows the remainder is not uniquely determined, so it cannot be used to test ideal membership. As it turns out, the fault for this behavior is not in the remainder or in the algorithm, but in the tuple F we are dividing by.

Gröbner bases

We adopt the following working definition. We will later provide equivalent characterizations.

Definition

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. A tuple $G = (g_1, \ldots, g_s) \in R^s$ of nonzero elements is a *Gröbner basis* if for every $f \in R$ there is a unique $r \in R$ with the following properties:

- $f = \sum_{i=1}^{s} q_i g_i + r$ for some $q_1, \ldots, q_s \in R$;
- $r = 0$ or no term of r is divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$.

If $I = \langle g_1, \ldots, g_s \rangle$ is the ideal generated by the elements in G, we call G a Gröbner basis of I.

The r in this definition can be computed using the division algorithm. Since R contains infinitely many elements, the definition above is hard to use in practice, so we need a different way to recognize a Gröbner basis.

Definition

Consider nonzero polynomials $f, g \in R = \Bbbk[x_1, \ldots, x_n]$. The *S-polynomial* of f and g is

$$S(f, g) = \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g$$

where lcm denotes the least common multiple.

The S-polynomial $S(f, g)$ is designed to produce a cancellation of leading terms. Notice also that $S(f, g) \in \langle f, g \rangle$.

For example, consider the polynomials $f_1 = y^2 - x$ and $f_2 = xy - 1$ in GLex. We have $\mathrm{lcm}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)) = \mathrm{lcm}(y^2, xy) = xy^2$. Therefore, the S-polynomial of f_1, f_2 is

$$S(f_1, f_2) = \frac{xy^2}{y^2}(y^2 - x) - \frac{xy^2}{xy}(xy - 1) = xy^2 - x^2 - xy^2 + y = -x^2 + y.$$

Theorem (Buchberger's Criterion)

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. A tuple $G = (g_1, \ldots, g_s) \in R^s$ of nonzero elements is a Gröbner basis if and only if for all $i \neq j$ the remainder of $S(g_i, g_j)$ upon division by G is zero.

The previous computation shows that $F = (f_1, f_2)$ is not a Gröbner basis because the remainder of $S(f_1, f_2)$ upon division by F is nonzero. However, if we let $f_3 = S(f_1, f_2)$, we can use Buchberger's criterion to show that $G = (f_1, f_2, f_3)$ is a Gröbner basis of $\langle f_1, f_2 \rangle$.

Buchberger's Algorithm

To construct a Gröbner basis of $I = \langle f_1, \ldots, f_s \rangle$, set $G = (f_1, \ldots, f_s)$ and proceed as follows.

1. For each pair $\{p, q\}$ in G with $p \neq q$, compute the remainder of $S(p, q)$ upon division by G. Go to step 2.
2. If all remainders computed in step 1 are zero, stop and return G; otherwise, add all nonzero remainders to G and go back to step 1.

Buchberger's Criterion ensures that this algorithm returns a Gröbner basis. Of course, one should still prove that this algorithm terminates in a finite number of steps. The algorithm above is designed to be simple but is not very efficient; however, one can introduce several optimizations. In addition, there are other algorithms that can be used to compute Gröbner bases (Hilbert drives, Faugère's F_4, signature-based) and algorithms that convert Gröbner bases between different monomial orders (FGLM, Gröbner walk). There are also algorithms that will compute Gröbner bases of special families of ideals, such as the Buchberger-Möller algorithm for ideals of points.

Special generation

We conclude this discussion with another property that characterizes Gröbner bases. This property will be analyzed further on Day 3.

Consider again the polynomials $f_1 = y^2 - x$ and $f_2 = xy - 1$ in GLex. We observed that

$$f = -x^2 + y = xf_1 - yf_2 \in \langle f_1, f_2 \rangle.$$

One would hope that $\mathrm{LM}(f)$ is equal to either $\mathrm{LM}(xf_1)$ or $\mathrm{LM}(yf_2)$. However, we have $\mathrm{LM}(f) = x^2$ and $\mathrm{LM}(xf_1) = \mathrm{LM}(yf_2) = xy^2$; in fact, $f = S(f_1, f_2)$ so it is designed to produce a cancellation of leading terms. This cannot occur with a Gröbner basis.

Theorem

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. A tuple $G = (g_1, \ldots, g_s) \in R^s$ of nonzero elements is a Gröbner basis if and only if for every nonzero $f \in \langle G \rangle$ there exist $q_1, \ldots, q_s \in R$ such that $f = \sum_{i=1}^{s} q_i g_i$ and

$$\mathrm{LM}(f) = \max\{\mathrm{LM}(q_i g_i) \,|\, i \in \{1, \ldots, s\}, q_i g_i \neq 0\}$$

where the maximum is taken with respect to the chosen monomial ordering.

Thus, a Gröbner basis of an ideal I can be seen as special set of generators that satisfies the property in the theorem.

Day 1 problems

Problems 1, 3, 9, 11, 12, and 13 are easier to start with. Everyone should try at least one of the problems that ask to compute a Gröbner basis (11, 12, and 13 are more hands-on; 14 and 15 are a bit more abstract). Problem 4 is also strongly recommended as the results will be used on Day 2.

Problem 1

Show that there is only one monomial order on $\Bbbk[x]$.

Problem 2

- We say a monomial ordering $\geqslant$ is *degree compatible* if $x^a \geqslant x^b$ implies $\deg(x^a) \geqslant \deg(x^b)$. For example, GLex and GRevLex are degree compatible by definition. Show that there are exactly two degree compatible monomial orderings on $\Bbbk[x,y]$.
- Show that there is only one monomial ordering on $\Bbbk[x,y]$ such that $x > y^i$ for all $i \geqslant 2$.

For more on the classification of monomial orderings for a small number of variables see Tutorial 10 in Kreuzer, Robbiano.

Problem 3

Write in increasing order the 20 smallest monomials in $\Bbbk[x,y,z]$ equipped with Lex. Do the same for GLex and GRevLex.

Problem 4

Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}^n$ and fix a monomial ordering $>$ on $\Bbbk[x_1, \ldots, x_n]$. Given monomials x^a and x^b , define $x^a >_{\mathbf{u}} x^b$ if and only if:

- $\mathbf{u} \cdot a > \mathbf{u} \cdot b$ (where $\cdot$ denotes the dot product of vectors), or
- $\mathbf{u} \cdot a = \mathbf{u} \cdot b$ and $x^a > x^b$ (in the monomial ordering fixed at the beginning).

We call $>_{\mathbf{u}}$ the *weight order* determined by $\mathbf{u}$ and $>$.

- Show that $>_{\mathbf{u}}$ is a monomial ordering.
- Assume $>$ is Lex and find $\mathbf{u}$ such that $>_u$ is GLex.
- Consider a positive integer $m \leqslant n$ and let $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$ with m 1's and $n - m$ 0's. Let $>$ be GRevLex. Show that $>_{\mathbf{u}}$ has the following property: any monomial divisible by one of $x_1, \ldots, x_m$ is greater than all monomials in $\Bbbk[x_{m+1}, \ldots, x_n]$.

Problem 5

Let M be an $n \times n$ nonsingular matrix with integer entries and denote M^T its transpose. Given monomials $x^a, x^b \in \Bbbk[x_1, \ldots, x_n]$, define $x^a \geqslant_M x^b$ if and only if the first nonzero entry of $(a-b)M^T$ is positive, where $(a-b)M^T$ is the product of the row vector $a-b$ with the matrix M^T.

- Prove that $\geqslant_M$ is a total order.

- Prove that $\geqslant_M$ is a monomial order if and only if the first nonzero entry of each column of M is positive.
- Find a matrix M such that $\geqslant_M$ is Lex. Do the same for GLex and GRevLex.

Problem 6

Let $>$ be a total order compatible with multiplication on the set of monomials of $\Bbbk[x_1, \ldots, x_n]$ (see our definition of monomial ordering). Recall that a *well-ordering* is a total order such that every nonempty subset contains a least element. Show that $>$ has the monomial 1 as its minimum element if and only if it is a well-ordering. [Hint: for the $\Rightarrow$ implication, use Hilbert's Basis Theorem or Dickson's Lemma.]

Problem 7

Given monomials $x^a, x^b \in \Bbbk[x_1, \ldots, x_n]$, define $x^a \geqslant x^b$ if and only if $a = b$ or the rightmost nonzero entry of the vector $a - b$ is negative; we call this relation RevLex.

- Show that RevLex is a total order compatible with multiplication.
- Show that RevLex is not a monomial ordering.

Problem 8

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R.

- Show that $\operatorname{LM}(fg) = \operatorname{LM}(f)\operatorname{LM}(g)$ for all nonzero $f, g \in R$.
- Show that $\operatorname{LM}(f + g) \leqslant \max\{\operatorname{LM}(f), \operatorname{LM}(g)\}$ for all nonzero $f, g \in R$ such that $f + g \neq 0$. Show that when $\operatorname{LM}(f) \neq \operatorname{LM}(g)$ the equality is achieved.

Problem 9

This problem gives another example where the remainder of division depends on the order of the divisors. Consider $\mathbb{Q}[x, y]$ with the Lex order. Let $f = x^5 - 1$, $g_1 = -x^2 + xy^2$ and $g_2 = x^2y - y^2$.

- Divide f by the tuple (g_1, g_2).
- Divide f by the tuple (g_2, g_1).

Problem 10

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. Consider $f, g \in R$ whose leading monomials are relatively prime, meaning that $\operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g)) = \operatorname{LM}(f)\operatorname{LM}(g)$.

- Show that $S(f, g) = pg - qf$ where $p = f - \operatorname{LT}(f)$ and $q = g - \operatorname{LT}(g)$.
- Assuming f and g have at least two terms, show that $\operatorname{LM}(S(f, g)) = \max\{\operatorname{LM}(pg), \operatorname{LM}(qf)\}$.
- Deduce that the remainder of $S(f, g)$ upon division by the pair (f, g) is zero.

Problem 11

Consider $R = \mathbb{Q}[x, y]$ with the lexicographic ordering. Is the tuple $F = (y^2 - x, xy - 1)$ a Gröbner basis? If not, find a Gröbner basis of the ideal $\langle F \rangle$.

Problem 12

For a little more practice with the Buchberger algorithm, compute a Gröbner basis of the ideal $\langle 2z - x^3, y - x^2 \rangle$ in $\mathbb{Q}[x, y, z]$ with the GRevLex (or with Lex if you want to see a few more steps). What are some obvious ways to improve upon the algorithm as outlined above?

Problem 13

Here is an example where the result changes with the characteristic of the field. Find a Gröbner basis of $\langle x^2 + 1, x^2 y + x - y \rangle$ in $\Bbbk[x, y]$ with GRevLex, when $\Bbbk = \mathbb{Q}$ and when $\Bbbk = \mathbb{Z}/2$.

Problem 14

Let $A = (a_{i,j})$ be an $m \times n$ matrix with entries in $\Bbbk$. Let

$$f_i = a_{i,1} x_1 + a_{i,2} x_2 + \cdots + a_{i,n} x_n$$

be the linear polynomial in $\Bbbk[x_1, \ldots, x_n]$ determined by the i-th row of A, and consider the ideal $I = \langle f_1, \ldots, f_m \rangle$. Let B be the reduced row echelon form of A and let $g_1, \ldots, g_t$ be the linear polynomials determined by the nonzero rows of B (so $t \leqslant m$). Prove that $\{g_1, \ldots, g_t\}$ is a Gröbner basis of I.

Problem 15

A binomial in $R = \Bbbk[x_1, \ldots, x_n]$ is a polynomial of the form $\alpha x^a - \beta x^b$ for some nonzero $\alpha, \beta \in \Bbbk$ and two different exponent vectors $a, b \in \mathbb{N}^n$. A binomial ideal in R is an ideal that has a generating set consisting entirely of binomials.

- Show that the S-polynomial of two binomials is a binomial.
- Show that the remainder of a binomial upon division by a tuple of binomials is a binomial.
- Deduce that a binomial ideal has a Gröbner basis consisting entirely of binomials.

Day 2

Reduced Gröbner bases

If you compute Gröbner bases by hand and compare with others or with a computer, you may obtain different results.

ⓘ Definition

A Gröbner basis G is called *reduced* if for all g in G:

1. $\mathrm{LC}(g) = 1$;
2. no monomial of g is divisible by the leading term of any other element of G.

Reduced Gröbner bases are important for the following reason.

Theorem

Let $R = \mathbb{k}[x_1, \ldots, x_n]$ and fix a monomial ordering on R. Every nonzero ideal I in R has a unique reduced Gröbner basis.

If a Gröbner basis G of I is known, then it is easy to produce the reduced Gröbner basis of I by normalizing coefficients and eliminating unnecessary terms. This gives us a new method to test ideal equality.

Corollary

Two ideals I, J in R are equal if and only if they have the same reduced Gröbner basis for some (hence any) monomial ordering.

We also notice that (1) is the reduced Gröbner basis of the ideal $\langle 1 \rangle = \mathbb{k}[x_1, \ldots, x_n]$ in any monomial ordering. The vanishing locus in the affine space $\mathbb{A}^n_{\mathbb{k}}$ of the ideal $\langle 1 \rangle$ is clearly empty. Conversely, by the weak Nullstellensatz, if $\mathbb{k}$ is algebraically closed and $I \subseteq \mathbb{k}[x_1, \ldots, x_n]$ is an ideal such that $\mathbb{V}(I) = \varnothing$, then $I = \langle 1 \rangle$. This leads to the following criterion which allows us to check when a system of polynomial equations has a solution.

Corollary

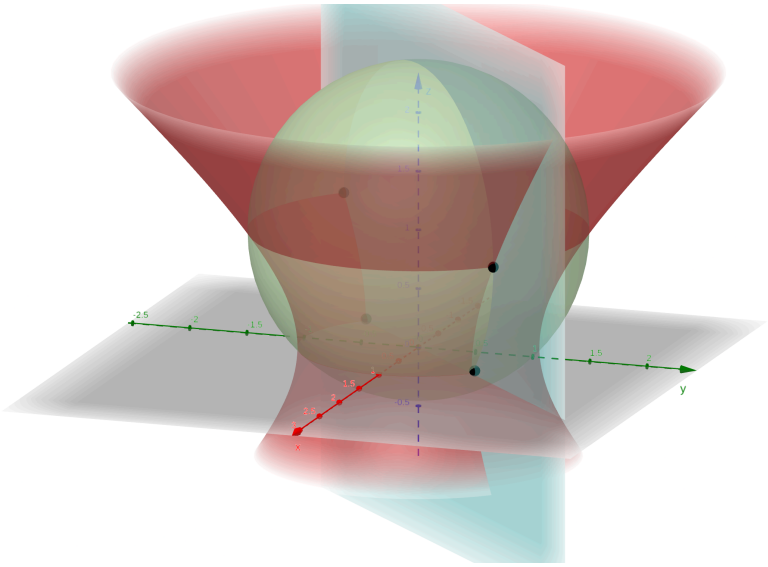
Let I be an ideal in $\mathbb{k}[x_1, \ldots, x_n]$ with $\mathbb{k}$ algebraically closed. Then $\mathbb{V}(I) = \varnothing$ if and only if the reduced Gröbner basis of I in one (hence any) monomial ordering is (1).

It is not possible to work computationally over an algebraically closed field. However, the construction of a Gröbner basis as described in Buchberger's Algorithm can be carried out over a subfield that can be represented in a computer algebra system.

Solving systems of equations

Gröbner bases may help solve systems of polynomial equations. Consider the following example, which describes the intersection of a sphere, a hyperboloid, and a plane.

$$\begin{cases} x^2 + y^2 + (z-1)^2 = 2 \\ x^2 + y^2 - z^2 = 1 \\ x = y \end{cases}$$



In Macaulay2, we set up a ring $R = \mathbb{Q}[x, y, z]$ with the lexicographic order and define the ideal

$$I = \langle x^2 + y^2 + (z-1)^2 - 2, x^2 + y^2 - z^2 - 1, x - y \rangle$$

with generators corresponding to the equations of the system.

```
R=QQ[x,y,z,MonomialOrder=>Lex]
I=ideal(x^2+y^2+(z-1)^2-2, x^2+y^2-z^2-1, x-y)
```

Observe how M2 expands all operations and arranges monomials according to the chosen ordering. Next, we compute a Gröbner basis using Macaulay2.

```
G=gb I
gens G
```

The `gb` command runs the Gröbner basis computation, then we can use `gens` to display the result as a one-row matrix. Notice that the leading terms of the elements in the Gröbner basis are arranged in increasing order: $z^2 < 2y^2 < x$. Because we chose to use Lex and the smallest leading term is a power of the smallest variable z, it follows that the other terms in the first polynomial must be smaller

than z^2 and, therefore, they cannot involve other variables. Thus, we get an equivalent system

$$\begin{cases} z^2 - z = 0 \\ 2y^2 - z - 1 = 0 \\ x - y = 0 \end{cases}$$

where the first equation is univariate. This system can be solved from top to bottom by finding roots of one equation and substituting into the next. The solutions are the four points

$$\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right), \qquad \left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right), \qquad (1,1,1), \qquad (-1,-1,1).$$

In this particular example, the default ordering (GRevLex) also leads to a system with a univariate equation, but that may not always be the case.

The Gröbner basis `G` we obtained for the ideal `I` is not reduced but only because of the coefficient in $2y^2$; this choice allows M2 to avoid denominators over $\mathbb{Q}$. We can check that the paraboloid $z = x^2 + y^2 - 1$ passes through the four points by checking it belongs to `I` or, equivalently, that its remainder modulo `G` is zero.

```
f=x^2+y^2-1-z
f%G
```

To express the polynomial `f` as a linear combination of `G` we can compute the quotients of division as follows.

```
f//(gens G)
```

We can also express `f` as a linear combination of the original generators of `I`.

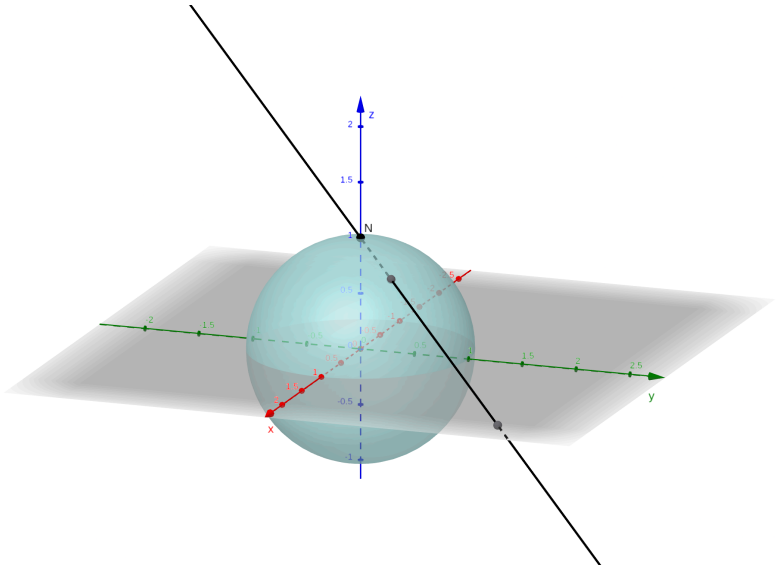
```
f//(gens I)
```

Elimination

Gröbner bases can also be used to find implicit equations for varieties parametrized by rational functions. In other words, we can use Gröbner bases to eliminate parameters. The stereographic projection from the north pole gives the rational parametrization of the sphere

$$x = \frac{2u}{1+u^2+v^2}, \qquad y = \frac{2v}{1+u^2+v^2}, \qquad z = \frac{-1+u^2+v^2}{1+u^2+v^2}.$$

depending on two parameters u, v.



In Macaulay2, we set up a ring $R = \mathbb{Q}[u, v, x, y, z]$ and define the ideal

$$I = \langle (1 + u^2 + v^2)x - 2u, (1 + u^2 + v^2)y - 2v, (1 + u^2 + v^2)z + 1 - u^2 - v^2 \rangle$$

with generators obtained by clearing denominators in the parametrization. We are formally interested in the so-called *elimination ideal* $I \cap \mathbb{Q}[x, y, z]$ in the subring $\mathbb{Q}[x, y, z]$. We could take the Lex order with $u > v > x > y > z$. Another option, which is typically more efficient, is to use a so-called *elimination order* designed to eliminate the first two variables u, v.

```
R=QQ[u,v,x,y,z,MonomialOrder=>Eliminate 2]
I=ideal((1+u^2+v^2)*x-2*u,
    (1+u^2+v^2)*y-2*v,
    (1+u^2+v^2)*z+1-u^2-v^2)
```

Next, we compute a Gröbner basis and display its elements.

```
G=gb I
gens G
```

The elements of this Gröbner basis involving only x, y, z give us implicit equations for the sphere. To extract these elements, we can use the command `selectInSubring`.

```
selectInSubring(1,gens G)
```

When we set up the ring with the elimination order, M2 creates two blocks of variables: u, v and x, y, z; the first argument informs M2 that we want to eliminate the variables in the first block. Another way to obtain an elimination ideal in M2 is to use the command `eliminate`.
Notice that our parametrization of the sphere misses the point $(0, 0, 1)$, so it only covers a subset U of the sphere which is open in the Zariski topology. The elimination ideal vanishes on the closure of U which is the whole sphere.

The ideas illustrated in this example can be generalized as follows.

Definition

Given an ideal I in the polynomial ring $\Bbbk[x_1, \ldots, x_n]$, the m-th *elimination ideal* I_m is the ideal of the subring $\Bbbk[x_{m+1}, \ldots, x_n]$ defined by $I_m = I \cap \Bbbk[x_{m+1}, \ldots, x_n]$.

Definition

A monomial ordering on $\Bbbk[x_1, \ldots, x_n]$ is of *m-elimination type* if every monomial involving one of $x_1, \ldots, x_m$ is greater than all monomials in $\Bbbk[x_{m+1}, \ldots, x_n]$.

With the definitions above, we have the following result.

Theorem

If I is an ideal in $\Bbbk[x_1, \ldots, x_n]$ and G is a Gröbner basis of I with respect to a monomial ordering of m-elimination type, then $G \cap \Bbbk[x_{m+1}, \ldots, x_n]$ is a Gröbner basis of the m-th elimination ideal $I_m = I \cap \Bbbk[x_{m+1}, \ldots, x_n]$.

Day 2 problems

Problem 16 is about reduced Gröbner bases and can be done by hand. The other problems showcase a variety of applications of Gröbner bases in the spirit of the Day 2 notes; use of a computer algebra system like Macaulay2 is highly recommended. Problem 21 is strongly recommended for anyone who has not seen it before.

Problem 16

If you found Gröbner bases by hand in problems 11 or 12, your results are likely not reduced. Find the reduced Gröbner bases for the ideals in those problems.

Problem 17

Consider the following system of polynomial equations.

$$\begin{cases} x^2 + y^2 + z^2 = 9 \\ 3x^2 = y^2 z \\ x^2 z + 2 = 2y^2 \end{cases}$$

How many rational, real, and complex solutions does it have?

Problem 18

A finite graph is *3-colorable* if every vertex can be assigned one of 3 different colors in such a way that vertices connected by an edge have different colors. If w denotes a primitive cubic root of unity, then we can use the complex numbers $1, w, w^2$ to represent 3 different colors. If we denote $x_1, \ldots, x_n$ the vertices of our graph, assigning a color to each vertex means that each variable x_i must be assigned one of the values $1, w, w^2$. Then, the equations

$$x_i^3 - 1 = 0$$

must be satisfied for all $i \in \{1, \ldots, n\}$. If x_i and x_j are connected by an edge, then $x_i \neq x_j$. Given that $x_i^3 = 1 = x_j^3$ and $x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2)$, an equation of the form

$$x_i^2 + x_i x_j + x_j^2 = 0$$

must be satisfied for each edge in the graph. It follows that the graph is 3-colorable if and only if $\mathbb{V}(I) \neq \varnothing$ where I is the ideal of $\mathbb{k}[x_1, \ldots, x_n]$ generated by all the equations above. Now, we can use Gröbner bases to solve the following.

- Show that K_5, the complete graph on 5 vertices, is not 3-colorable.
- Let G be the graph obtained from K_5 by removing two non-incident edges. Show that G is 3-colorable.

To work over an extension of $\mathbb{Q}$ containing a primitive cubic root of unity, you can use the following Macaulay2 code. Note that $x^2 + x + 1$ is the minimal polynomial of w.

```
kk=toField( QQ[w] / ideal(w^2+w+1))
R=kk[x_1..x_5]
```

Problem 19

Shidoku is a smaller relative of Sudoku. You play on the 4×4 grid

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

and you replace each letter with an integer from 1 to 4 in a way that every row, column, and 2×2 corner block contains each of the number 1, 2, 3, and 4 exactly once. This problem shows how you can represent and solve Shidoku puzzles using Gröbner bases.

- Each letter in the grid must satisfy an equation of the form

  $$(w - 1)(w - 2)(w - 3)(w - 4) = 0$$

  to ensure that it can only be equal to 1, 2, 3, or 4.

- The only way to choose four numbers w, x, y, z from the set $\{1, 2, 3, 4\}$ is for them to add up to 10 and multiply to 24; in other words, they must satisfy the equations:

$$w + x + y + z - 10 = 0, \qquad wxyz - 24 = 0.$$

- Form the ideal I in $\mathbb{Q}[a, \ldots, p]$ generated by the conditions above for all variables and all choices of rows, columns, and 2×2 corner blocks. Your ideal should have 40 generators. The ideal I represents all possible Shidoku boards.
- Now, consider a particular board; for example:

			4
4		2	
	3		1
1			

  We can represent this board by adding new equations such as $d = 4$ and so on for all other values present on the board. Let J be the ideal generated by the elements of I and these new equations.
- Find a Gröbner basis of J to determine if the board above admits a unique solution. If so, use the Gröbner basis to solve the puzzle.

For more information and for more ideas on how to represent Sudoku boards algebraically, consult the article "Gröbner Basis Representations of Sudoku" by Elizabeth Arnold, Stephen Lucas, and Laura Taalman.

Problem 20

Consider the surface S in $\mathbb{R}^3$ formed by the union of all lines joining the points

$$(u^2, -u^3, u), \qquad (-u^2, u^3, 1 - u)$$

for $u \in \mathbb{R}$; this is an example of a *ruled surface*.

- Write a parametrization of S.
- Use elimination to find a polynomial $f \in \mathbb{R}[x, y, z]$ such that S is contained in the set of points satisfying the implicit equation $f = 0$.

Problem 21

Consider the polynomial rings $R = \Bbbk[w, x, y, z]$ and $S = \Bbbk[s, t]$. Consider the ring homomorphism $\varphi\colon R \to S$ defined on the variables as follows:

$$\varphi(w) = s^3, \qquad \varphi(x) = s^2t, \qquad \varphi(y) = st^2, \qquad \varphi(z) = t^3.$$

The kernel of φ is the vanishing ideal of the *twisted cubic* in $\mathbb{P}^3$, an object of interest to geometers. The homomorphism φ corresponds to a parametrization of the twisted cubic, so we can use elimination to compute this kernel. Define the ideal

$$I = \langle w - s^3, x - s^2t, y - st^2, z - t^3 \rangle$$

in $\Bbbk[s,t,w,x,y,z]$.

- Show that $\ker \varphi = I \cap R$.
- Use Gröbner bases to find generators of $\ker \varphi$.

Problem 22

The trigonometric parametrization

$$\begin{cases} x = (2 + \cos(t))\cos(u) \\ y = (2 + \cos(t))\sin(u) \\ z = \sin(t) \end{cases}$$

describes a torus in $\mathbb{R}^3$. We show this torus lies in an affine variety by eliminating the parameters t and u to produce a polynomial equation. The trigonometric functions prevent us from using elimination directly, so set

$$a = \cos(t), \qquad b = \sin(t), \qquad c = \cos(u), \qquad d = \sin(u)$$

to replace the parametrization above with an algebraic one. However, these new variables are not independent as they must satisfy $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$. Now, form an ideal I in $\mathbb{Q}[a,b,c,d,x,y,z]$ generated by the parametrization and the relations among the new variables. Finally, use elimination to find the equation for the torus.

Problem 23

You may remember when a quadratic equation has a double root, but what about a cubic equation? Consider the polynomial $p(x) = ax^3 + bx^2 + cx + d$ for some $a, b, c, d \in \Bbbk$, where $\Bbbk$ is a field of characteristic not equal to 2 or 3, and $a \neq 0$. Recall that x_0 is a double root of $p(x)$ if and only if $(x - x_0)^2$ divides $p(x)$.

- Show that x_0 is a double root of $p(x)$ if and only if $p(x_0) = 0$ and $\frac{dp}{dx}(x_0) = 0$.
- Consider the ideal $I = \langle p, \frac{dp}{dx} \rangle$ of $\Bbbk[x,a,b,c,d]$. Find $I \cap \Bbbk[a,b,c,d]$ and use it to determine when p has a double root in terms of a, b, c, d.
- Similarly, find conditions on a, b, c, d guaranteeing $p(x)$ has a triple root.

Problem 24

Consider the polynomial

$$f(x,y) = y^2 - (x^3 + ax + b),$$

where $a, b \in \Bbbk$ and $\Bbbk$ is a field of characteristic not equal to 2 or 3. The points $(x,y) \in \Bbbk^2$ that satisfy $f(x,y) = 0$ define a plane cubic curve. A point $P = (x_0, y_0)$ on this curve is called *singular* if the tangent vector at P

$$\left(\frac{\partial f}{\partial x}\bigg|_P, \frac{\partial f}{\partial y}\bigg|_P \right)$$

is zero; we say the curve is *smooth* if it has no singular points. To determine when the curve has singular points proceed as follows. Consider the ideal $I = \langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \rangle$ of $\Bbbk[x, y, a, b]$, then eliminate x and y to find relations between a, b. The plane cubic will be smooth, also known as an *elliptic curve*, when those relations are nonzero.

Problem 25

Fix $a \in \mathbb{C}$. The minimal polynomial of a over $\mathbb{Q}$ is the monic polynomial p with rational coefficients of the smallest degree such that $p(a) = 0$, where *monic* means it has leading coefficient is 1. For example, the minimal polynomials of $a = \sqrt{2}$, $b = \sqrt[3]{5}$, and $i = \sqrt{-1}$ are, in order, $a^2 - 2$, $b^3 - 5$, and $i^2 + 1$. This problem shows how to use elimination to find the minimal polynomial of a complex number living in a particular field extension of $\mathbb{Q}$. For example, consider

$$x = \frac{b^2 - i}{a} = \frac{\sqrt[3]{25} - i}{\sqrt{2}} \in \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}, i\right).$$

By clearing the denominator, we obtain the algebraic relation $ax - b^2 + i = 0$. We take the ideal of $\mathbb{Q}[a, b, i, x]$ generated by this relation and the minimal polynomials of a, b, and i:

$$I = \langle ax - b^2 + i, a^2 - 2, b^3 - 5, i^2 + 1 \rangle.$$

Next, we use an elimination order to compute $I \cap \mathbb{Q}[x]$. Since this elimination ideal lives in $\mathbb{Q}[x]$, it can be generated by a single monic polynomial, which is the minimal polynomial of x. Find this minimal polynomial.

Problem 26

A polynomial $f \in \Bbbk[x_1, \ldots, x_n]$ is called *symmetric* if

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

for every permutation σ of $\{1, \ldots, n\}$. We can use elimination orderings to identify symmetric polynomials as follows. For $1 \leqslant k \leqslant n$, we define the *elementary symmetric polynomial* of degree k as

$$e_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \cdots x_{i_k};$$

in other words, e_k is the sum of all squarefree monomials of degree k. In the ring $R = \Bbbk[x_1, \ldots, x_n, y_1, \ldots, y_n]$ with a monomial ordering of n-elimination type, let G be a Gröbner basis of the ideal $I = \langle e_1 - y_1, \ldots, e_n - y_n \rangle$. Given $f \in \Bbbk[x_1, \ldots, x_n] \subseteq R$, let g be the remainder upon division of f by G. Then:

1. f is symmetric if and only if $g \in \Bbbk[y_1, \ldots, y_n]$;
2. if f is symmetric, then $f = g(e_1, \ldots, e_n)$ and this is the unique expression of f as a polynomial in $e_1, \ldots, e_n$.

Now, for $i \geqslant 0$, define the *power sum symmetric polynomial*

$$p_i = x_1^i + \cdots + x_n^i$$

and the *complete homogeneous symmetric polynomial*

$$h_i = \sum_{a_1+\cdots+a_n=i} x_1^{a_1} \cdots x_n^{a_n}.$$

For $n = 4$, use the ideas above to verify that $p_1, \ldots, p_4$ and $h_1, \ldots, h_4$ are symmetric, and express them as polynomials in $e_1, \ldots, e_4$.

Problem 27

Let I and J be ideals in $\Bbbk[x_1, \ldots, x_n]$.

- Show that $(tI + (1-t)J) \cap \Bbbk[x_1, \ldots, x_n] = I \cap J$. Here, tI is the ideal of $\Bbbk[t, x_1, \ldots, x_n]$ generated by $\{tf_1, \ldots, tf_r\}$ where $\{f_1, \ldots, f_r\}$ is a set of generators of I; the ideal $(1-t)J$ is constructed similarly.
- Use elimination to compute $I \cap J$ where $I = \langle x^2y - z, xy + 1\rangle$ and $J = \langle x - y, z^2 - x\rangle$ are ideals of $\Bbbk[x, y, z]$.

Problem 28

Let I and J be ideals in $R = \Bbbk[x_1, \ldots, x_n]$. The *ideal quotient* $I : J$, also known as a *colon ideal*, is defined as

$$I : J = \{f \in R \,|\, \forall g \in J, fg \in I\}.$$

Ideals quotients are useful when studying differences of algebraic sets.

- Show that $I : J$ is an ideal of R.
- Show that if $J = \langle g_1, \ldots, g_s\rangle$, then

$$I : J = \bigcap_{i=1}^{s} I : \langle g_i\rangle.$$

- Show that if $g \in R$ is nonzero, then

$$I : \langle g\rangle = \frac{1}{g}(I \cap \langle g\rangle).$$

- Combine the previous observations to compute $I : J$ for the ideals $I = \langle x(x+y)^2, y\rangle$ and $J = \langle x^2, x + y\rangle$ in $\mathbb{Q}[x, y]$. You can use Problem 27 to compute intersections or you can just use the Macaulay2 method `intersect`.

Day 3

Leading terms

Recall that having fixed a monomial ordering on the polynomial ring $R = \Bbbk[x_1, \ldots, x_n]$, the largest monomial appearing with a nonzero coefficient in a polynomial f is called its *leading monomial*; we denote it $\mathrm{LM}(f)$. The coefficient of the leading monomial is called the *leading coefficient* of f; we

denote it $\mathrm{LC}(f)$. The product of the two gives the *leading term* of f; we denote it $\mathrm{LT}(f)$, so we have $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$.

Definition

Let I in $R = \Bbbk[x_1, \ldots, x_n]$ be a nonzero ideal and fix a monomial ordering on R. Denote $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I. We call $\langle \mathrm{LT}(I) \rangle$ the *ideal of leading terms* of I.

The ideal of leading terms is, by construction, a monomial ideal of R, i.e., an ideal that has a generating set consisting entirely of monomials. Although $\mathrm{LT}(I)$ is an infinite set, $\langle \mathrm{LT}(I) \rangle$ admits a finite generating set (consisting of monomials) by Hilbert's Basis Theorem. One can also show directly that a monomial ideal admits a finite generating set; this result is known as Dickson's Lemma.

One would hope that if $I = \langle f_1, \ldots, f_r \rangle$, then $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r) \rangle$; however, this is false in general. For example, consider the polynomials $f_1 = y^2 - x$ and $f_2 = xy - 1$ in GLex. On Day 1, we showed that

$$-x^2 + y = S(f_1, f_2) \in \langle f_1, f_2 \rangle.$$

However, $x^2 \notin \langle y^2, xy \rangle$.

Theorem

Let I in $R = \Bbbk[x_1, \ldots, x_n]$ be a nonzero ideal and fix a monomial ordering on R. A tuple $G = (g_1, \ldots, g_s) \in R^s$ is a Gröbner basis of I if and only if $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.

Since it is an equivalent characterization, this is often taken as the definition of a Gröbner basis. As it turns out, this characterization has many useful applications.

Quotient representations

We are finally able to solve our other motivational problems, namely how to represent and compare elements in the quotients of a polynomial ring.

Let $R = \Bbbk[x_1, \ldots, x_n]$ and fix a monomial ordering on R. Let I in R be an ideal and let $G = (g_1, \ldots, g_s)$ be a Gröbner basis of I. Given any polynomial $f \in R$, we can use the division algorithm to write $f = \sum_{i=1}^{s} q_i g_i + r$, where r is a $\Bbbk$-linear combination of monomials not divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$. Since G is a Gröbner basis of I, we have:

- $I = \langle g_1, \ldots, g_r \rangle$ so $f + I = r + I$;
- r is uniquely determined (it depends only on f, I, and the monomial ordering);
- no term of r is divisible by any monomial in $\langle \mathrm{LT}(I) \rangle$.

We can combine these observations into the following result.

🕮 Theorem (Macaulay's Basis Theorem)

Let I in $R = \Bbbk[x_1, \ldots, x_n]$ be a nonzero ideal and fix a monomial ordering on R. The monomials of R not belonging to $\langle \mathrm{LT}(I) \rangle$ form a basis of R/I as a $\Bbbk$-vector space. In particular, if $G = (g_1, \ldots, g_s)$ is a Gröbner basis of I, then the monomials of R not divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$ form a basis of R/I as a $\Bbbk$-vector space.

The monomials of R not contained in $\langle \mathrm{LT}(I) \rangle$ are sometimes called the *standard monomials* modulo I.

Hilbert functions and polynomials

Recall that a polynomial $f \in R = \Bbbk[x_1, \ldots, x_n]$ is called *homogeneous of degree* d if

$$f(tx_1, \ldots, tx_n) = t^d f(x_1, \ldots, x_n)$$

for all $t \in \Bbbk \setminus \{0\}$ or, equivalently, if all terms of f have degree d. For $d \in \mathbb{N}$, denote R_d the $\Bbbk$-vector subspace of R spanned by all homogeneous polynomials of degree d, which we call the *graded component* of R of degree d. The ring R admits a direct sum decomposition

$$R = \bigoplus_{d \in \mathbb{N}} R_d$$

as a $\Bbbk$-vector space. Moreover, multiplication respects this decomposition in the sense that for all $f \in R_d, g \in R_e$ we have $fg \in R_{d+e}$. An ideal I of R is called *homogeneous* if it has a generating set consisting entirely of homogeneous polynomials. For example, monomial ideals are homogeneous. For $d \in \mathbb{N}$, let I_d be the $\Bbbk$-vector subspace of I spanned by all homogeneous polynomials of degree d in I, which we call the *graded component* of I of degree d. A homogeneous ideal I admits a direct sum decomposition

$$I = \bigoplus_{d \in \mathbb{N}} I_d$$

as a $\Bbbk$-vector space. Moreover, multiplication is compatible with this decomposition in the sense that for all $f \in I_d, g \in R_e$ we have $fg \in I_{d+e}$. When I is a homogeneous ideal, the quotient ring R/I inherits a grading

$$R/I = \bigoplus_{d \in \mathbb{N}} (R/I)_d$$

by letting $(R/I)_d$ be the span of all cosets $f + I$ with $f \in R_d$. As a $\Bbbk$-vector space, we have $(R/I)_d = R_d/I_d$. Quotients of a polynomial ring by a homogeneous ideal arise naturally as "coordinate rings" of projective varieties, so we will focus on them for the rest of this section. An analogous discussion can be had in the nonhomogeneous (i.e., affine) case.

Definition

Let I be a homogeneous ideal of the polynomial ring $R = \mathbb{k}[x_1, \ldots, x_n]$. The *Hilbert function* of R/I is the function $H_{R/I}\colon \mathbb{N} \to \mathbb{N}$ defined by $H_{R/I}(d) = \dim_{\mathbb{k}}(R/I)_d$, i.e., the dimension of the graded component of degree d of R/I as a $\mathbb{k}$-vector space.

As a simple example, observe that when $I = \{0\}$ we have $R/I \cong R$ and

$$H_R(d) = \dim_{\mathbb{k}} R_d = \binom{n-1+d}{d}.$$

Fixing a monomial ordering on R, we have a basis of $(R/I)_d$ consisting of all monomials of degree d not contained in $\langle \mathrm{LT}(I) \rangle$. This shows the dimension of $(R/I)_d$ is always finite and gives us a practical way to compute it.

For example, consider the homogeneous ideal

$$I = \langle w^2 + x^2 + y^2 + z^2, w(x+y+z) \rangle$$

in $R = \mathbb{Q}[w, x, y, z]$ with the GRevLex ordering. We can use the following Macaulay2 code to produce the ideal of leading terms of I.

```
R=QQ[w,x,y,z]
I=ideal(w^2+x^2+y^2+z^2,w*(x+y+z))
leadTerm I
```

As a result, we get that $\langle \mathrm{LT}(I) \rangle = \langle wx, w^2, x^3 \rangle$. From here, we see that

$$H_{R/I}(0) = 1, \qquad H_{R/I}(1) = 4, \qquad H_{R/I}(2) = 8$$

because all monomials of degree 0 and 1 survive in the quotient, but 2 of the 10 monomials of degree 2 are congruent to zero. For larger d, the computation is a little more involved. For example, when $d = 3$ the monomials not in $\langle wx, w^2, x^3 \rangle$ are

$$wy^2, wyz, wz^2, xy^2, xyz, xz^2, x^2y, x^2z, y^3, y^2z, yz^2, z^3$$

so that $H_{R/I}(3) = 12$. In fact, for $d \geqslant 3$ the monomials not in $\langle wx, w^2, x^3 \rangle$ are:

- $wy^{d-1}, wy^{d-2}z, \ldots, wyz^{d-2}, wz^{d-1}$ (d monomials),
- $xy^{d-1}, xy^{d-2}z, \ldots, xyz^{d-2}, xz^{d-1}$ (d monomials),
- $x^2y^{d-2}, x^2y^{d-3}z, \ldots, x^2yz^{d-3}, x^2z^{d-2}$ ($d-1$ monomials),
- and $y^d, y^{d-1}z, \ldots, yz^{d-1}, z^d$ ($d+1$ monomials).

Therefore, for $d \geqslant 3$ we have

$$H_{R/I}(d) = d + d + (d-1) + (d+1) = 4d.$$

We can also use Macaulay2 to compute individual values of the Hilbert function and to get bases for the graded components.

```
Q=R/I
for i to 10 do print hilbertFunction(i,Q)
basis(2,Q)
```

The behavior observed in this example generalizes.

Theorem

Let I be a homogeneous ideal in $R = \mathbb{k}[x_1, \ldots, x_n]$. There is a polynomial $P_{R/I}(t) \in \mathbb{Q}[t]$ such that for all d sufficiently large we have $H_{R/I}(d) = P_{R/I}(d)$.

The polynomial $P_{R/I}$ is called the *Hilbert polynomial* of R/I and it carries useful information. If the leading term of $P_{R/I}$ is ct^d, then

- $\dim(R/I) = 1 + d$, where $\dim(R/I)$ denotes the Krull dimension of R/I;
- $\deg(R/I) = cd!$, where $\deg(R/I)$ denotes the degree or multiplicity of R/I.

The dimension and the degree of R/I allow us to measure how big and complicated the vanishing locus of I is in projective space. In the example above, we have $\dim(R/I) = 2$ so the vanishing locus of I is a curve (the Krull dimension of the coordinate ring is one more than the dimension of the projective variety); also, $\deg(R/I) = 4$, so this is a curve of degree 4. To compute the Hilbert polynomial in the format above using Macaulay2 you can use the following code.

```
hilbertPolynomial(Q,Projective=>false)
```

The connection between the algebra and the geometry goes even deeper. Suppose I is a homogeneous ideal and $G = (g_1, \ldots, g_s)$ is a Gröbner basis of I. For $1 \leqslant i \leqslant s$, define polynomials

$$h_i = g_i - \mathrm{LT}(g_i)$$

obtained by removing the leading term from each g_i, and let

$$G_{i,t} = \mathrm{LT}(g_i) + th_i$$

where t is a parameter. Altogether, the polynomials $G_{i,t}$ define a family of ideals

$$I_t = \langle G_{1,t}, \ldots, G_{s,t} \rangle$$

depending on the parameter t. Note that $I_1 = I$ and $I_0 = \langle \mathrm{LT}(I) \rangle$. Our previous discussion allows us to observe that $\dim_{\mathbb{k}}(R/I_1)_d = \dim_{\mathbb{k}}(R/I_0)_d$ for all $d \in \mathbb{N}$, so that R/I_1 and R/I_0 have the same Hilbert function and, therefore, they have the same Hilbert polynomial, dimension and degree. In fact, the quotients R/I_t have the same Hilbert function for all values of the parameter t. For $t \neq 0$, the vanishing locus of I_t may look like some deformation of the vanishing locus of I. However, for $t = 0$,

$I = I_0$ is a monomial ideal and its vanishing locus reduces to a union of linear subspaces; this is typically different from the vanishing locus of I but it may be easier to understand. The process of deforming the vanishing locus of I to that of I_0 is sometimes referred to as a Gröbner degeneration.

Syzygies

Finally, let us return to the division algorithm. We observed that when dividing by the terms of a Gröbner basis the remainder is unique, in particular it does not depend on the order of the divisors. However, quotients are generally not uniquely determined.

Consider the polynomials $f_1 = y^2 - x, f_2 = xy - 1, f_3 = -x^2 + y$. As we observed on Day 1, (f_1, f_2, f_3) is a Gröbner basis. We have

$$xy^2 = xf_1 - f_3 + y = (x-1)f_1 + xf_2 + (y-1)f_3 + y,$$

where the first equality was obtained using the division algorithm and y is the remainder. Thus, we have at least two different sets of coefficients $(x, 0, -1)$ and $(x-1, x, y-1)$ for f_1, f_2, f_3 that could act as "quotients" upon division of xy^2 by (f_1, f_2, f_3).

Let $R = \mathbb{k}[x_1, \ldots, x_n]$ and fix a monomial ordering on R. Consider a tuple $F = (f_1, \ldots, f_s) \in R^s$ of nonzero elements. Given $f, r \in R$, suppose there are two different tuples $(q_1, \ldots, q_s), (\tilde{q}_1, \ldots, \tilde{q}_s) \in R^s$ such that

$$f = \sum_{i=1}^{s} q_i f_i + r = \sum_{i=1}^{s} \tilde{q}_i f_i + r.$$

Then, we have

$$\sum_{i=1}^{s} (q_i - \tilde{q}_i) f_i = 0.$$

We can study the tuples $(h_1, \ldots, h_s) \in R^s$ such that $\sum_{i=1}^{s} h_i f_i = 0$ as a way to measure the failure of uniqueness of the quotients upon division by F.

Definition

Let $R = \mathbb{k}[x_1, \ldots, x_n]$ and consider a tuple $F = (f_1, \ldots, f_s) \in R^s$ of nonzero elements. A tuple $H = (h_1, \ldots, h_s) \in R^s$ such that

$$\sum_{i=1}^{s} h_i f_i = 0$$

is called a *syzygy* of F. We denote $\mathrm{Syz}(F)$ the set of all syzygies of F.

The universally beloved word syzygy comes from the greek word for yoke. It is used in astronomy to describe an alignment of celestial objects. It is also the name of a few music bands and the title of

several short films, TV show and podcast episodes, including an episode of the 90's cult TV show The X-Files.

The set $\mathrm{Syz}(F)$ is closed under sums and multiplication by elements of R; in other words, $\mathrm{Syz}(F)$ is a submodule of R^s. If we let

$$\mathbf{e}_i = (0, \ldots, 0, \underbrace{1}_{i\text{-th position}}, 0, \ldots, 0) \in R^s,$$

then we can write

$$(h_1, \ldots, h_s) = \sum_{i=1}^{s} h_i \mathbf{e}_i.$$

For all choices of indices $1 \leqslant i < j \leqslant s$, we have

$$f_j \mathbf{e}_i - f_i \mathbf{e}_j \in \mathrm{Syz}(F).$$

Are there other syzygies and, if so, can we find them all? Since R is Noetherian and R^s is a finitely generated R-module, the submodule $\mathrm{Syz}(F)$ is also finitely generated. Thus, to describe all syzygies it is enough to find a finite generating set.

Going back to our example, we know that f_3 is the S-polynomial of f_1 and f_2:

$$S(f_1, f_2) = \frac{xy^2}{y^2}(y^2 - x) - \frac{xy^2}{xy}(xy - 1) = -x^2 + y = f_3,$$

where xy^2 is the least common multiple of the leading monomials of f_1 and f_2. We know that the S-polynomial is designed to cancel the leading terms of its arguments, a fact which we can write as follows.

$$S(\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = \frac{xy^2}{y^2} y^2 - \frac{xy^2}{xy} xy = x(y^2) - y(xy) = 0$$

If we let $\mathrm{LT}(F) = (\mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(f_3))$, the above equality can be reintepreted using the language of syzygies: $(x, -y, 0) \in \mathrm{Syz}(\mathrm{LT}(F))$.

As observed in our example, S-polynomials give rise to syzygies of leading terms. In fact, every syzygy among leading terms arises as an R-linear combination of these.

Theorem

Let $R = \mathbb{k}[x_1, \ldots, x_n]$ and consider a tuple $F = (f_1, \ldots, f_s) \in R^s$ of nonzero elements. Fix a monomial ordering on R and write $\mathrm{LT}(F)$ for the tuple $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)) \in R^s$. The elements

$$\sigma_{ij} = \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)}\mathbf{e}_i - \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_j)}\mathbf{e}_j$$

for $1 \leqslant i < j \leqslant s$ generate the submodule $\mathrm{Syz}(\mathrm{LT}(F))$ of R^s.

In our ongoing example, we have:

$$\sigma_{12} = (x, -y, 0), \qquad \sigma_{13} = (x^2, 0, y^2), \qquad \sigma_{23} = (0, x, y).$$

Notice that $\sigma_{13} = x\sigma_{12} + y\sigma_{23}$, so σ_{13} is a redundant generator. We can also see that σ_{13} is related to one of the "obvious" syzygies of F:

$$\tau_{13} = -f_3\mathbf{e}_1 + f_1\mathbf{e}_3 = (x^2 - y, 0, y^2 - x) = \sigma_{13} - (y, 0, x).$$

The tuple $(y, 0, x)$ happens to contain the quotients of division of $S(f_1, f_3)$ upon division by F:

$$S(f_1, f_3) = -x^3 + y^3 = y \cdot f_1 + 0 \cdot f_2 + x \cdot f_3.$$

In this case, we say that σ_{13} "lifts" to a syzygy of F. Replicating these steps with σ_{12} and σ_{23}, we get the quotient tuples

$$\begin{aligned} S(f_1, f_2) &= -x^2 + y = 0 \cdot f_1 + 0 \cdot f_2 + 1 \cdot f_3 \leftrightsquigarrow (0, 0, 1), \\ S(f_2, f_3) &= y^2 - x = 1 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 \quad \leftrightsquigarrow (1, 0, 0), \end{aligned}$$

so σ_{12} and σ_{23} lift to the following syzygies of F:

$$\begin{aligned} \tau_{12} &= (x, -y, 0) - (0, 0, 1) = (x, -y, -1), \\ \tau_{23} &= (0, x, y) - (1, 0, 0) = (-1, x, y). \end{aligned}$$

Here is the crucial observation: in order to write every S-polynomial $S(f_i, f_j)$ as a linear combination of F we want the remainder of $S(f_i, f_j)$ upon division by F to be zero; in other words, we want F to be a Gröbner basis!

Theorem

Let $R = \mathbb{k}[x_1, \ldots, x_n]$ and fix a monomial ordering on R. A tuple $G = (g_1, \ldots, g_s) \in R^s$ of nonzero elements is a Gröbner basis if and only if every homogeneous element of $\mathrm{Syz}(\mathrm{LT}(G))$ lifts to an element of $\mathrm{Syz}(G)$. In this case, if $\sigma_1, \ldots, \sigma_m$ are homogeneous elements generating $\mathrm{Syz}(\mathrm{LT}(G))$, then their lifts $\tau_1, \ldots, \tau_m$ generate $\mathrm{Syz}(G)$.

We can formalize the process for finding generators of $\mathrm{Syz}(G)$ in the following algorithm.

Lifting syzygies

To find a generating set of $\mathrm{Syz}(G)$ where $G = (g_1, \ldots, g_s)$ is a Gröbner basis, proceed as follows.

1. For all indices $1 \leqslant i < j \leqslant s$, compute
$$\sigma_{ij} = \frac{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_i)}\mathbf{e}_i - \frac{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_j)}\mathbf{e}_j.$$
2. For all indices $1 \leqslant i < j \leqslant s$, find $(c_{ij1}, \ldots, c_{ijs}) \in R^s$ such that
$$S(g_i, g_j) = \sum_{k=1}^{s} c_{ijk} g_k.$$
3. For all indices $1 \leqslant i < j \leqslant s$, compute
$$\tau_{ij} = \sigma_{ij} - \sum_{k=1}^{s} c_{ijk}\mathbf{e}_k.$$
4. Return the set $\{\tau_{ij} \mid 1 \leqslant i < j \leqslant s\}$.

Macaulay2 can find syzygies using the command `syz`.

```
R=QQ[x,y,MonomialOrder=>GLex]
I=ideal(y^2-x,x*y-1)
--syzygies of the leading terms
LTG=leadTerm I
syz LTG
--syzygies of the Gröbner basis
G=gens gb I
syz G
```

Day 3 problems

Problem 29

Consider the ideal in Problem 12.

- Find the initial ideal with respect to GRevLex.
- Find the initial ideal with respect to Lex.

Problem 30

Consider the ideal of $R = \mathbb{Q}[x, y, z]$ generated by the equations in Problem 17. Fix a monomial ordering on R.

- Find a basis of R/I as a $\mathbb{Q}$-vector space and show it is finite dimensional.

- If you previously solved Problem 17, how does the dimension of R/I relate to the total number of solutions of the system?

Problem 31

Let $R = \mathbb{C}[x, y, z]$ and

$$I = \langle y^2z - yz^2, xyz, x^2z - xz^2, x^2y - xy^2 \rangle.$$

- Verify that the generators of I form a Gröbner basis with respect to GRevLex.
- Use the initial ideal of I to find the Hilbert polynomial of R/I.
- Find the dimension and degree of R/I, then use them to give a geometric description of $\mathbb{V}(I)$ in $\mathbb{P}^2$.

Problem 32

Let $R = \Bbbk[w, x, y, z]$ and let J be the defining ideal of the twisted cubic in $\mathbb{P}^3$ that you constructed in Problem 21.

- Find a Gröbner basis G of J with respect to GRevLex.
- Use G to find the initial ideal of J and, from there, the Hilbert polynomial of R/J.
- Find the dimension of R/I to confirm that $\mathbb{V}(I)$ is a curve (remember the dimension of the ring is the dimension of the projective variety plus one).
- Find the degree of R/I to confirm that $\mathbb{V}(I)$ is a cubic.
- Show that $\mathrm{Syz}(G)$ is generated by two linear syzygies.

Problem 33

This problem is about studying a non-homogeneous ideal by making it homogeneous. We start with a brief review of projective space.

The projective space $\mathbb{P}^n$ over the field $\Bbbk$ is made up of points $[x_0 : x_1 : \cdots : x_n]$ with at least one $x_i \neq 0$, and these points are defined up to nonzero scalars, meaning that for every $0 \neq \lambda \in \Bbbk$ we have

$$[x_0 : x_1 : \cdots : x_n] = [\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n].$$

A homogeneous polynomial f of degree d has the property that

$$f(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_0, x_1, \ldots, x_n)$$

so the vanishing of a homogeneous polynomial at a point of $\mathbb{P}^n$ is well-defined. The affine space $\mathbb{A}^n$ over $\Bbbk$ embeds embeds in $\mathbb{P}^n$ by sending $(x_1, \ldots, x_n)$ to $[1 : x_1 : \cdots : x_n]$. Now, if $X \subseteq \mathbb{A}^n$ is a variety, the smallest subvariety of $\mathbb{P}^n$ that contains the image of X under this embedding is called the *projective closure* of X.

If $X \subseteq \mathbb{A}^n$ is the vanishing locus of an ideal $I = \langle f_1, \ldots, f_r \rangle \subseteq \Bbbk[x_1, \ldots, x_n]$, the first thing you might try to do is multiply the terms in the generators f_i by powers of the variable x_0 so that the resulting

polynomials f_i^h are homogeneous (see the example below). The following exercises show that this approach can fail even in simple situations.

- Let $I = \langle f_1, f_2 \rangle \subseteq \mathbb{C}[x, y]$ where $f_1 = y^2 - x$ and $f_2 = xy - 1$. Show that the vanishing locus of I in $\mathbb{A}^2$ contains exactly three points. We can denote these points (a_i, b_i) for $i \in \{1, 2, 3\}$.
- When we homogenize f_1 and f_2 with respect to a new variable z, we get $f_1^h = y^2 - xz$ and $f_2^h = xy - z^2$. Show that the vanishing locus of the homogeneous ideal $\langle f_1^h, f_2^h \rangle \subseteq \mathbb{C}[x, y, z]$ in $\mathbb{P}^2$ contains $[a_i : b_i : 1]$ for $i \in \{1, 2, 3\}$, and one additional point $[a_4 : b_4 : 0]$.

Here is how we remedy the situation.

- Compute a Gröbner basis G of I with respect to a degree compatible monomial ordering such as GLex or GRevLex.
- If $G = (g_1, \ldots, g_s)$, then we form the ideal $I^h = \langle g_1^h, \ldots, g_s^h \rangle$ of $\mathbb{C}[x, y, z]$ generated by the homogenizations of the elements in G with respect to z.
- Show that the vanishing locus of I^h in $\mathbb{P}^2$ contains only the points $[a_i : b_i : 1]$ for $i \in \{1, 2, 3\}$.

The general theory says that if $G = \langle g_1, \ldots, g_s \rangle$ is a Gröbner basis of an ideal $I \subseteq \Bbbk[x_1, \ldots, x_n]$ with respect to a degree compatible monomial ordering, then the projective closure of $\mathbb{V}(I)$ in $\mathbb{P}^n$ is the vanishing locus of $I^h = \langle g_1^h, \ldots, g_s^h \rangle \subseteq \Bbbk[x_0, x_1, \ldots, x_n]$.

Problem 34

This is a continuation of Problem 19 on Shidoku puzzles. Let $I \subseteq \mathbb{Q}[a, \ldots, p]$ be the ideal representing all possible Shidoku boards.

- Find I^h using the method described in Problem 31. Macaulay2 has the `homogenize` method that you can use to homogenize a polynomial or an ideal with respect to a variable (you will need to work in a larger polynomial ring that contains one extra variable).
- Show that R/I^h has dimension one. This tells you that the projective variety defined by I^h has dimension zero or, equivalently, that it is a finite set of points (whose coordinates are the entries of all the possible Shidoku boards).
- Find the degree of R/I^h. This will tell you the number of points in the vanishing locus of I^h, which is also the total number of possible Shidoku boards.
- Use similar methods to find the number of possible solutions for the following board.

			4
		2	
	3		
1			

Problem 35

Let $R = \mathbb{Q}[w, x, y, z]$. The tuple

$$G = (x^2 + yz, wx + yz, w^2 + yz, wyz - xyz) \in R^4$$

is a Gröbner basis with respect to GRevLex.

- Construct all the generators σ_{ij} of $\mathrm{Syz}(\mathrm{LT}(G))$.
- Remove all non-minimal σ_{ij} (this will reduce computations in the next steps).
- Find lifts τ_{ij} of the minimal σ_{ij} to construct a generating set of $\mathrm{Syz}(G)$.

Problem 36

This problem tries to clarify what it means to "lift" a syzygy.

Let $R = \Bbbk[x_1, \ldots, x_n]$ and consider a tuple $G = (g_1, \ldots, g_s) \in R^s$ of nonzero elements. Fix a monomial ordering on R and write $\mathrm{LT}(G)$ for the tuple $(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)) \in R^s$. A tuple of terms $(t_1, \ldots, t_s) \in R^s$ is *homogeneous* of degree $a \in \mathbb{N}^n$ relative to G if $\mathrm{LM}(g_i)\,\mathrm{LM}(t_i) = x^a$ for all $i \in \{1, \ldots, s\}$ such that $t_i \neq 0$.

- Show that for $1 \leqslant i < j \leqslant s$ the element

$$\sigma_{ij} = \frac{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_i)}\mathbf{e}_i - \frac{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_j)}\mathbf{e}_j \in R^s$$

  is homogeneous of degree a relative to G where $x^a = \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$.

Every element of R^s decomposes as a sum of homogeneous elements of possibly different degrees relative to G.

- For example, consider the tuple

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

  of polynomials in $\mathbb{Q}[x, y]$ with GLex. Decompose

$$H = (x^3y - xy^2, x^3 + y^3, xy^3 - x^2y)$$

  into a sum of homogeneous elements relative to G.

Given $H \in R^s$, we write $H = \sum_{a \in \mathbb{N}^n} H_a$ with H_a homogeneous of degree a relative to G. We define the *leading form* of H relative to G as $\mathrm{LF}_G(H) = H_d$ where

$$x^d = \max\{x^a \mid H_a \neq 0\}$$

taken with respect to the monomial ordering.

- Find $\mathrm{LF}_G(H)$ for the triples G and H above.
- In general, show that if $H \in \mathrm{Syz}(G)$, then $LF_G(H) \in \mathrm{Syz}(\mathrm{LT}(G))$.

Thus, the operator LF_G defines a function from R^s to R^s that sends the submodule $\mathrm{Syz}(G)$ to $\mathrm{Syz}(\mathrm{LT}(G))$. Finally, we say that $H \in R^s$ is a *lifting* of $\overline{H} \in R^s$ if $\mathrm{LF}_G(H) = \overline{H}$.

- For the triple G above, find a lifting of

$$\overline{H} = (x^4y^2, x^3y^3, x^2y^4).$$

Not every element $\overline{H} \in R^s$ has a lifting. However, if G is a Gröbner basis and $\overline{H}$ is homogeneous, then $\overline{H}$ has a lifting.