Exercise List 1

Polynomials, monomial orderings, monomial ideals, and a division algorithm

The first part of this exercise list is a warm-up and focuses on understanding varieties as solutions of polynomial equations. We next consider monomial orderings and monomial ideals, which will play a crucial role later in the course, for example in the theory of Gröbner bases. We conclude with the introduction of the multivariate division algorithm, which is based on the concept of monomial orderings, and we learn how to do it both by hand and in the computer algebra system `OSCAR`.

References are given from the book

[CLO1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra* 4th edition. Springer.

When writing §X.Y we mean Chapter X, Section Y. Throughout k denotes an arbitrary field.

Polynomials and varieties.

Exercise 1 ([CLO1] §1.2, Lemma 2)**.** For $V = \mathbf{V}(f_1, \dots, f_s)$ and $W = \mathbf{V}(g_1, \dots, g_r)$, with $f_1, \dots, f_s, g_1, \dots, g_r \in k[x_1, \dots, x_n]$, show that it holds

$$V \cap W = \mathbf{V}(f_1, \dots, f_s, g_1, \dots, g_r), \qquad V \cup W = \mathbf{V}(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq r).$$

Exercise 2. Sketch the following affine varieties in $\mathbb{R}^2$:
(a) $\mathbf{V}(xy - 1)$
(b) $\mathbf{V}(x^2 + y^2 - 4)$
(c) $\mathbf{V}(xy - 1, x^2 + y^2 - 4)$
(d) $\mathbf{V}(x^3y - x^2 + xy^3 - 4xy - y^2 + 4)$

Hint: Use Exercise 1.

Exercise 3 ([CLO1] §1.2, Ex 6, 8)**.** Decide which of the following sets are affine varieties:
(a) a set containing exactly one point $(a_1, \dots, a_n) \in k^n$.
(b) a finite subset of k^n.
(c) $\{(x, x) \mid x \in \mathbb{R}, x \neq 1\} \subseteq \mathbb{R}^2$.

Hint: In (c) consider the polynomial $g(t) := f(t, t) \in \mathbb{R}[t]$.

Exercise 4. Prove that any variety in $\mathbb{R}^n$ can be written as the set of zeros of a single polynomial.

Bonus challenge: Prove that this holds over any non-algebraically-closed field.

Exercise 5 ([CLO1] §1.4, Ex 1)**.** Consider the equations

$$\begin{aligned} x^2 + y^2 - 4 &= 0, \\ xy - 1 &= 0, \end{aligned}$$

which describe the variety from Exercise 2(c).
(a) Use algebra to eliminate y from the above equations.
(b) Show that the polynomial found in part (a) lies in the ideal $\langle x^2 + y^2 - 4, xy - 1 \rangle$.
(c) Use the polynomial found in part (a) to find the points in $\mathbf{V}(x^2 + y^2 - 4, xy - 1)$.

Monomial orders.

Exercise 6 ([CLO1] §2.2, Ex 1)**.** Rewrite each of the following polynomials, ordering the terms using the lex order, the grlex order, and the grevlex order, giving $\mathrm{LM}(f), \mathrm{LT}(f)$, and $\mathrm{multideg}(f)$ in each case. We consider $x > y > z$.
(a) $f(x,y,z) = 2x + 3y + z + x^2 - z^2 + x^3$,
(b) $f(x,y,z) = x + x^2y + xy^2 + yz^2 + y$,
(c) $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.

Exercise 7 ([CLO1] §2.2, Ex 4 and 5)**. (a)** Show that the graded lex order (grlex) and the graded reverse lex order (grevlex) are monomial orders.
(b) Show that the "reverse lex order", defined by $\alpha > \beta$ if and only if the leftmost entry of $\alpha - \beta$ is negative is not a monomial order. Which property fails? Is it a total order on $\mathbb{Z}^n_{\geq 0}$?
(c) Show that for $n = 2$, grlex and grevlex agree.

Exercise 8. Let M be an $m \times n$ real matrix, and write the rows of M as $w_1, \ldots, w_m$. Define the relation $>_M$ as follows:

$$\alpha >_M \beta \quad \Leftrightarrow \quad \text{there exists } \ell \leq m \text{ such that } w_i \cdot \alpha = w_i \cdot \beta,\ i = 1, \ldots, \ell - 1, \text{ and } w_\ell \cdot \alpha > w_\ell \cdot \beta.$$

(a) Show that if all entries of M are nonnegative and $\ker(M) \cap \mathbb{Z}^n = \{0\}$, then $>_M$ is a monomial order.
(b) Find matrices M such that the orders lex, grlex and grevlex arise in this form.

Exercise 9 ([CLO1] §2.4 Ex 11.a)**.** Fix a monomial order $\prec$ on $k[x_1, \ldots, x_n]$. For a vector $w \in \mathbb{R}^n$ define a relation on $\mathbb{Z}^n_{\geq 0}$ as

$$\alpha \succ_w \beta \qquad \Longleftrightarrow \qquad w \cdot \alpha > w \cdot \beta \quad \text{or} \quad (w \cdot \alpha = w \cdot \beta \quad \text{and} \quad \alpha \succ \beta).$$

(a) Show that $\prec_w$ is a total order satisfying $\alpha + \gamma \succ_w \beta + \gamma$ for all $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ with $\alpha \succ_w \beta$.
(b) Show that $\prec_w$ is a monomial order, if $w \in \mathbb{R}^n_{\geq 0}$.
(c) Find w such that grlex is $\prec_w$ when the monomial order $\prec$ is lex.
(d) Is grevlex an order $\prec_w$ for some w and monomial order $\prec$?

Exercise 10 ([CLO1] §2.2, Ex 13)**.** Prove that $1 < x < x^2 < \ldots$ is the unique monomial order on $k[x]$.

Exercise 11 ([CLO1] §2.2, Ex 12)**.** Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero. Show that
(a) $\mathrm{multideg}(f \cdot g) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$.
(b) If $f + g \neq 0$, then $\mathrm{multideg}(f + g) \leq \max\big(\mathrm{multideg}(f), \mathrm{multideg}(g)\big)$. If in addition $\mathrm{multideg}(f) \neq \mathrm{multideg}(g)$, then equality occurs.

Exercise 12 ([CLO1] §2.2, Ex 13)**.** Show that $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$ if and only if every strict decreasing sequence $\alpha_1 > \alpha_2 > \ldots > \alpha_r > \ldots$ in $\mathbb{Z}^n_{\geq 0}$ is finite.

Monomial ideals.

Exercise 13 ([CLO1] §2.4, Ex 3.a)**.** Let $I = \langle x^6, x^2y^3, xy^7\rangle \subseteq k[x, y]$ be a monomial ideal. Sketch with a drawing the set of exponent vectors (m, n) of monomials $x^m y^n$ appearing in elements of I.

Exercise 14. Let $f \in k[x_1, \dots, x_n]$ be nonzero. Show that the only term of f that belongs to $\langle \mathrm{LM}(f)\rangle$ is $\mathrm{LT}(f)$.

Exercise 15 ([CLO1] §2.4, Ex 1)**.** Let $I \subset k[x_1, \dots, x_n]$ be an ideal with the property that for every $f = \sum c_\alpha x^\alpha \in I$, every monomial x^α appearing in f is also in I. Show that I is a monomial ideal.

Exercise 16 (Minimal basis of monomial ideals)**.** Show that for a monomial ideal $I \subseteq k[x_1, \dots, x_n]$, there exists a unique basis $\{x^{\alpha_1}, \dots, x^{\alpha_s}\}$ such that x^{α_i} does not divide x^{α_j} for any $i \neq j$.

Exercise 17 ([CLO1] §2.4, Ex 5)**.** Suppose that $I = \langle x^\alpha \mid \alpha \in A\rangle$ is a monomial ideal in $k[x_1, \dots, x_n]$, and let S be the set of all monomials of I. Let $>$ be a monomial order, and let x^μ be the smallest element of S with respect to $>$. Prove that μ must lie in A. (In other words, the smallest monomial of a monomial ideal must be in any generating set.)

Multivariate division algorithm. Given polynomials $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ and a monomial order $>$, the goal of a multivariate division algorithm is to obtain polynomials $q_1, \dots, q_s, r \in k[x_1, \dots, x_n]$ such that

$$f = q_1 f_1 + \dots q_s f_s + r,$$

satisfying:

(i) No term of r is divisible by $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)$.

(ii) $\mathrm{multideg}(q_i f_i) \leq \mathrm{multideg}(f)$, for any $i \in \{1, \dots, s\}$ such that $q_i f_i \neq 0$.

The univariate division algorithm can be adapted to the multivariate case as follows:

Initialize $q_1 := 0, \dots, q_s := 0, r := 0$, and $p := f$.
WHILE $p \neq 0$ DO
    IF (exists i such that $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$) THEN
        $i :=$ the smallest i such that $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$
        $q_i := q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}, \quad p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$
    ELSE
        $r := r + \mathrm{LT}(p), \quad p := p - \mathrm{LT}(p)$

Exercise 18. Apply the multivariate division algorithm with the polynomials $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$, using the lex order in $\mathbb{Q}[x, y]$ with $x > y$. Would the answer be different using the grlex order (graded lexicographic order)?

Exercise 19. In the Jupyter notebook `Division_algorithm.ipynb` you find how to perform the division algorithm in `OSCAR`. Spend some time learning how the commands work, and then do the following exercises:

(a) Consider the polynomials in the file, namely $f = x^2 + xy^2 + y$, $f_1 = x + xy$, $f_2 = x + y$, and the lexicographic order with $x > y$. Find the remainder of f divided by f_2 and f_1 (that is, change the order of the list of polynomials we divide with). Is the answer the same?

(b) Check your answer from Exercise 18.

Exercise 20 ([CLO1] §2.3, Ex 5)**.** We will study the division of $f = x^3 - x^2y - x^2z + x$ by $f_1 = x^2y - z$ and $f_2 = x\,y - 1$. Throughout we consider the grlex ordering on $\mathbb{Q}[x, y, z]$.

(a) Compute $r :=$ remainder of f on division by (f_1, f_2), and $r' :=$ remainder of f on division by (f_2, f_1).

(b) Show that $g := r - r'$ belongs to the ideal $\langle f_1, f_2\rangle$ by finding explicit $A, B \in \mathbb{Q}[x, y]$ such that $g = Af_1 + Bf_2$. *Hint:* Use the quotients you found in (a).

(c) Compute the remainder of g on division by (f_1, f_2). Why could you have predicted your answer before doing the division?

(d) Find another polynomial $h \in \langle f_1, f_2\rangle$ such that the remainder on division of h by (f_1, f_2) is nonzero.

(e) Does the division algorithm give us a solution for the ideal membership problem for the ideal $\langle f_1, f_2\rangle$? Explain your answer.

(f) Think in general about what you found in this exercise: What polynomials $h \in \langle f_1, f_2\rangle$ have the property that the remainder on division by (f_1, f_2) is nonzero?

Exercise 21 ([CLO1] §2.4, Ex 8)**.** If $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\rangle \subseteq k[x_1, \dots x_n]$ is a monomial ideal, prove that a polynomial f is in I if and only if the remainder of f on division by $(x^{\alpha(1)}, \dots, x^{\alpha(s)})$ is zero.

Hint: Use Lemma 2 and 3 from [CLO1] §2.4.

Exercise 22 ([CLO1] §2.3, Ex 1)**.** Consider the polynomials $f = x^7y^2+x^3y^2-y+1$, $f_1 = xy^2-x$, and $f_2 = x - y^3$ in $\mathbb{Q}[x, y]$.

(a) Use `OSCAR` to divide f by both (f_1, f_2) and (f_2, f_1), with respect to the lex ordering.

(b) Now do the same with respect to the grlex ordering. Compare with the result from (a).

Exercise 23. Show that the algorithm given above terminates after finitely many steps, and that the output has the property that $\text{multideg}(q_i f_i) \leq \text{multideg}(f)$, for any $i \in \{1, \dots, s\}$ such that $q_i f_i \neq 0$.