Exercise List 3: Elimination, extension and implicitization

Week 3

This exercise list focuses on the Elimination and the Extension theorem and its applications, including implicitization.

References are given from the books

[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.

[LOU] P. Loustaunau, and W. W. Adams. *An introduction to Gröbner bases.* 1994. Graduate Studies in Mathematics, Vol 3. American Mathematical Society.

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

Exercise 1 ([CLO1] §3.1, Ex 4)**.** Find bases for the elimination ideals I_1 and I_2 for the ideal I determined by the equations:

$$\begin{aligned} &x^2 + y^2 + z^2 = 4, \\ &x^2 + 2y^2 = 5, \\ &xz = 1. \end{aligned}$$

How many rational (i.e., in $\mathbb{Q}^3$) solutions are there?

Exercise 2 ([CLO1] §2.8, Ex 3, Ex 4)**.** Use Gröbner bases to find the points in $\mathbb{C}^3$ on the variety

(a) $\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z)$,

(b) $\mathbf{V}(x^2y - z^3, 2xy - 4z - 1, z - y^2, x^3 - 4zy)$.

Exercise 3 ([CLO1] §3.2, Ex 4)**.** To see how the Closure Theorem can fail over $\mathbb{R}$, consider the ideal

$$I = \langle x^2 + y^2 + z^2 + 2, 3x^2 + 4y^2 + 4z^2 + 5\rangle.$$

Let $V = \mathbf{V}(I)$, and let π_1 be the projection taking (x, y, z) to (y, z).

(a) Working over $\mathbb{C}$, prove that $\mathbf{V}(I_1) = \pi_1(V)$.

(b) Working over $\mathbb{R}$, prove that $V = \emptyset$ and that $\mathbf{V}(I_1)$ is infinite. Thus, $\mathbf{V}(I_1)$ may be much larger than the smallest variety containing $\pi_1(V)$ when the field is not algebraically closed.

Exercise 4 ([CLO1] §3.3, Ex 6)**.** Let S be the parametric surface defined by

$$x = u\,v, \qquad y = u^2, \qquad z = v^2.$$

(a) Find the equation of the smallest variety V that contains S.

(b) Over $\mathbb{C}$, use the extension theorem to prove that $S = V$.

(c) Over $\mathbb{R}$, show that S only covers "half" of V. What parametrization would cover the other "half"?

Exercise 5 ([CLO1] §3.3, Ex 8)**.** The *Enneper surface* is defined parametrically by

$$x = 3u + 3u\,v^2 - u^3, \qquad y = 3v + 3u^2v - v^3, \qquad z = 3u^2 - 3v^2.$$

(a) Find the equation of the smallest variety V that contains the Enneper surface (it will be a very complicated equation!)

(b) Over $\mathbb{C}$, use the extension theorem to prove that V equals the image of the parametrization.

Note for (b): there are a lot of polynomials in the Gröbner bases, keep looking! Alternatively, recall that the Extension Theorem does not require a Gröbner basis.

Exercise 6 ([CLO1] §3.3, Ex 14)**.** The *folium of Descartes* can be parametrized by

$$x = \frac{3t}{1+t^3}, \qquad y = \frac{3t^2}{1+t^3}.$$

(a) Find the equation of the folium of Descartes.
(b) Over $\mathbb{C}$ or $\mathbb{R}$, show that the parametrization fills up all the entire curve.

Exercise 7 (Smooth del Pezzo)**.** Consider the family of varieties defined by the equations

$$x_1x_2 - x_3x_4 = 0, \qquad a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5(1 - x_1 - x_2 - x_3 - x_4)^2 = 0.$$

(this is the affine version of the so-called del Pezzo surfaces of degree 4). The variety is said to be smooth, if the Jacobian matrix of the two equations evaluated at all points of the variety has rank 2.

Determine for what values of the parameters $a_1, \ldots, a_5$ the variety is smooth.

Note: To find the Jacobian matrix, use the command `derivative` to find each entry.

Exercise 8 ([CLO1] §3.1, Ex 6)**. (a)** Fix an integer $1 \leq \ell \leq n$, and define the order $>_\ell$ as follows: if $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, then $\alpha >_\ell \beta$ if

$$\alpha_1 + \cdots + \alpha_\ell > \beta_1 + \cdots + \beta_\ell, \qquad \text{or} \qquad \alpha_1 + \cdots + \alpha_\ell = \beta_1 + \cdots + \beta_\ell \quad \text{and} \quad \alpha >_{grevlex} \beta.$$

Prove that $>_\ell$ is a monomial order and is of ℓ-elimination type (that is, any monomial involving at least one of $x_1, \ldots, x_\ell$ is larger than any monomial only in $x_{\ell+1}, \ldots, x_n$.)

(b) If G is a Gröbner basis for $I \subset k[x_1, \ldots, x_n]$ for the monomial order of part (a), explain why $G \cap k[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis with respect to grevlex.

Exercise 9 ([CLO1] §3.3, Ex 10)**.** Consider the curve in $\mathbb{C}^n$ parametrized by $x_i = f_i(t)$, where $f_1, \ldots, f_n \in \mathbb{C}[t]$. This gives the ideal

$$I = \langle x_1 - f_1(t), \ldots, x_n - f_n(t) \rangle \subseteq \mathbb{C}[t, x_1, \ldots, x_n].$$

(a) Prove that the parametric equations fill up all of the variety $V(I_1) \subseteq \mathbb{C}^n$.
(b) Show that the conclusion of part (a) might fail over $\mathbb{R}$.
(c) Show that the conclusion of part (a) may fail if we let $f_1, \ldots, f_n$ be rational functions in t.

Exercise 10. Given a set $S \subseteq k^n$, show that $V(I(S))$ is the smallest variety containing S.

Exercise 11 ([CLO1] §3.2, Ex 5)**.** Suppose that $I \subseteq \mathbb{C}[x, y]$ is an ideal such that $I_1 \neq \{0\}$. Prove that $\mathbf{V}(I_1) = \pi_1(V)$, where $V = \mathbf{V}(I)$ and π_1 is the projection onto the y-axis.

Hint: Recall that the only varieties contained in $\mathbb{C}$ are either $\mathbb{C}$ or finite subsets of $\mathbb{C}$.

Exercise 12 (Deciding surjectivity)**.** Propose an algorithm to decide whether a polynomial map

$$F \colon \mathbb{C}^r \to \mathbb{C}^m$$
$$x = (x_1, \ldots, x_r) \mapsto (F_1(x), \ldots, F_m(x))$$

with $F_i \in \mathbb{C}[x_1, \ldots, x_r]$, is surjective.

Exercise 13 (Intersection of ideals)**.** In this exercise we will find an algorithm to compute the **intersection ideal** $I \cap J$ of two ideals I and J of $k[x_1, \dots, x_n]$, provided we have bases for I and J. So let $I = \langle f_1, \dots, f_s \rangle$ and $J = \langle g_1, \dots, g_\ell \rangle$ be ideals in $k[x_1, \dots, x_n]$. Consider the ideal

$$A := \langle tf_1, \dots, tf_s, (1-t)g_1, \dots, (1-t)g_\ell \rangle \subseteq k[t, x_1, \dots, x_n].$$

(a) Show that $I \cap J \subseteq A \cap k[x_1, \dots, x_n]$.

(b) Show that $A \cap k[x_1, \dots, x_n] \subseteq I \cap J$. To this end, write $f \in A \cap k[x_1, \dots, x_n]$ in terms of the generators of A, and evaluate t at 0 and 1.

Note: In general, it holds that $I \cap J = (tI + (1-t)J) \cap k[x_1, \dots, x_n]$, where $f(t)I$ for $f \in k[t]$ is the ideal generated by $f(t)g$ for all $g \in I$. Try to prove this, or read the relevant paragraph in [CLO1] §4.3.

Exercise 14 ([CLO1] §3.1, Ex 7)**.** Consider the equations

$$\begin{aligned} t^2 + x^2 + y^2 + z^2 &= 0, \\ t^2 + 2x^2 - xy - z^2 &= 0, \\ t + y^3 - z^3 &= 0. \end{aligned}$$

We want to eliminate t. Let $I = \langle t^2 + x^2 + y^2 + z^2, t^2 + 2x^2 - xy - z^2, t + y^3 - z^3 \rangle$ be the corresponding ideal. Do the computations of this exercise in `OSCAR`.

(a) Using lex order with $t > x > y > z$, compute the reduced Gröbner basis for I, and then find a basis for $I \cap \mathbb{Q}[x, y, z]$. You should get four generators, one of which has total degree 12.

(b) Compute the reduced grevlex Gröbner basis for $I \cap \mathbb{Q}[x, y, z]$. You will get a simpler set of two generators.

(c) Combine the answer to part (b) with the polynomial $t + y^3 - z^3$ and show that this gives a Gröbner basis for I with respect to the elimination order $>_1$ (this is $>_\ell$ with $\ell = 1$) of Exercise 8. Note that this Gröbner basis is much simpler than the one found in part (a).

Hint: c) Each monomial order can be represented by a matrix, see [CLO1, §2.4]. The grevlex order is represented by the matrix `[1 1 1 1; 0 0 0 -1; 0 0 -1 0;0 -1 0 0]`. To represent the elimination order $>_1$, you can put the row `[1 0 0 0]` to the top of this matrix. In `OSCAR`, you can write `matrix_ordering(gens(R), [1 0 0 0; 1 1 1 1; 0 0 0 -1; 0 0 -1 0; 0 -1 0 0])` whenever you need to use the elimination order $>_1$.

Exercise 15. Using the methods from Exercise 12 and 13, solve the following problems:

(a) Decide whether the following two polynomial maps are surjective:

(i) $F\colon \mathbb{C}^4 \to \mathbb{C}^3$ with $F(x_1, x_2, x_3, x_4) = (x_1^2 - x_2, x_2x_3 + x_4, x_4^2 - x_1x_3)$.

(ii) $F\colon \mathbb{C}^3 \to \mathbb{C}^3$ with $F(x_1, x_2, x_3) = (x_1^2 - x_2, x_2x_3, x_1^4x_2x_3 - 2x_1^2x_2^2x_3 + x_2^3x_3 + x_2^2x_3^3)$.

(b) Find a basis of $I \cap J$ in the following two cases:

(i) $I = \langle x^2y \rangle$, $J = \langle xy^2 \rangle$ in $\mathbb{Q}[x, y]$.

(ii) $I = \langle x^2 - y + z, x - z^2 \rangle$, $J = \langle x^2 + 2y^2, xz - 1 \rangle$ in $\mathbb{Q}[x, y]$.

Exercise 16 (Binomial model in statistics)**.** In this exercise we see an application of implicitization in statistics. You will also use the ideal membership and ideal equality tests.

Consider the binomial random variable, with probabilities

$$p_j = p_j(\theta) = \binom{m}{j} \theta^j (1-\theta)^{m-j}, \qquad j = 0, \dots, m, \quad \theta \in (0,1).$$

Each p_j gives the probability of observing j instances of an event occurring in a trial with probability θ, if we make m trials.

We let $m = 4$.

(a) Give equations of the minimal variety $V \subseteq \mathbb{R}[p_0, \dots, p_4]$ containing $(p_0(\theta), \dots, p_4(\theta)) \subseteq \mathbb{R}^5$, $\theta \in \mathbb{R}$.

(b) Show that the polynomial $p_0p_2 - \frac{3}{8}p_1^2$ vanishes on the variety.

(c) Show that the minimal variety found in (a) can be described by the ideal $I \cap \mathbb{R}[p_0, \dots, p_4]$ where

$$I = \langle p_0p_2 - \tfrac{3}{8}p_1^2, p_1p_3 - \tfrac{4}{9}p_2^2, p_2p_4 - \tfrac{3}{8}p_3^2, p_0 + p_1 + p_2 + p_3 + p_4 - 1, 1 - (p_0p_1p_2p_3p_4)t \rangle.$$

Do you get the same result if you remove the last two polynomials? What do they encode?

(d) Can the probability vector $p = (\frac{16}{81}, \frac{32}{81}, \frac{8}{27}, \frac{8}{81}, \frac{1}{81})$ describe the probabilities of a binomial random variable with 4 trials? And the probability vector $p = (\frac{13}{81}, \frac{29}{81}, \frac{8}{27}, \frac{11}{81}, \frac{4}{81})$?

(e) Discuss how the equations found in (c) can be used to assess whether some collected data follows a binomial distribution and the difficulties of implementing this approach.

Note: A huge research field called *Algebraic Statistics* uses computational algebra to address model selection and other questions where polynomial models arise. This exercise showed a basic example, and the conclusions of (c) hold for general m, by considering the polynomials $p_{j-1}p_{j+1} - \frac{j(m-j)}{(j+1)(m-j+1)}p_j^2$ for $j = 1, \dots, m-1$. Algebraic statistics has found a particular application in *phylogenetics*, the theory that aims at inferring species trees out of (genomic) data. In this field, a question of interest is to find good "invariants", meaning good generators of the ideal of interest, as we did in (c).

Exercise 17 (Double roots and discriminants)**.** Given a degree 2 univariate polynomial $p = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$, it is well known that p has a double root if and only if the discriminant $\Delta = a_1^2 - 4a_0a_2$ vanishes.

(a) Fix n. Devise a method, based on elimination, to find necessary relations on the coefficients of a generic degree n univariate polynomial $p = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ for the polynomial to have a double root. Think about what type of answer your method gives depending on whether the field is $\mathbb{R}$ or $\mathbb{C}$. Check your method with $n = 2$.

(b) Apply the method to find the equations that the coefficients of polynomials of degree $n = 3$ (resp. $n = 4$) need to satisfy to have a double root. Are the conditions also sufficient in $\mathbb{C}$? And in $\mathbb{R}$? Use the command `derivative` in `Oscar`.

(c) For what values of a does the polynomial $p = 4a\,x^3 - (a+1)x^2 + a + 1$ have a double root?

(d) The variety defined by the conditions is called the *discriminant*! In Oscar, the command `discriminant` computes these equations. Check out the syntax at `https://docs.oscar-system.org/v0.11/AbstractAlgebra/polynomial/#discriminant-Tuple{PolyElem}` and verify you get the same answer as in the previous questions.

Exercise 18 (Minimal Polynomials of algebraic numbers)**.** An algebraic number α (over $\mathbb{Q}$) is a number $\alpha \in \mathbb{C}$ that is a root of a polynomial in $\mathbb{Q}[x]$. Then the minimal polynomial of α is defined to be the monic polynomial $f \in \mathbb{Q}[x]$ of smallest degree, such that $f(\alpha) = 0$. The set of all algebraic numbers forms a field $\overline{\mathbb{Q}}$, called the *algebraic closure of* $\mathbb{Q}$. Therefore, sums and products of algebraic numbers are algebraic.

`OSCAR` and many other computer algebra systems represent an algebraic number as a root of its minimal polynomial, and hence, to represent sums and products of algebraic numbers on a computer, we have to find their minimal polynomials. This can be done algorithmically using Gröbner bases.

Given two algebraic numbers α_1, α_2 with minimal polynomials f_1, f_2, consider the algebraic number $\alpha_1 + \alpha_2$. Let $I = \langle f_1(x), f_2(y), z - x - y\rangle \subseteq \mathbb{Q}[x, y, z]$.

(a) Show that $(\alpha_1, \alpha_2, \alpha_1 + \alpha_2) \in V(I)$.

(b) Show that if $f \in I \cap \mathbb{Q}[z]$, then f vanishes on $z = \alpha_1 + \alpha_2$.

(c) Find polynomials over $\mathbb{Q}$ that vanish on the following algebraic numbers: $\sqrt{2} + \sqrt{3}$ and $\sqrt[3]{7} + \sqrt[4]{5}$.

(d) Extend the argument to the product of algebraic numbers, and find a polynomial over $\mathbb{Q}$ that vanishes on $\sqrt[3]{7}\sqrt[4]{5}$.

Note: The polynomials of minimal degree computed here are the minimal polynomials of the algebraic numbers $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$. This follows from a general theorem [LOU, Thm. 2.6.3].

Exercise 19 (Plücker relations)**.** Consider an $m \times n$ matrix A with coefficients in a field k, such that $m \leq n$. The collection of all maximal minors (determinants of all square submatrices of A of size m) satisfy polynomial equations, called the *Plücker relations*. So, the value of some of the maximal minors determines the rest.

(a) Use implicitization to find generators of the ideal defined by the Plücker relations when $m = 2, n = 4$. How many minors should you know at least, to be able to deduce the value of all?

(b) Repeat with $m = 2, n = 5$. Do you see a pattern?

If you have a background in algebraic geometry, search for *Plücker embedding* to read a bit more on these relations.

Hint: Some useful commands in `OSCAR`: To enter a matrix whose entries are polynomials in $x1, \ldots, x8$, create a polynomial ring with these variables and use `M = matrix([[x1,x2,x3,x4],[x5,x6,x7,x8]])`. To compute all the maximal minors of M, use `minors(M,2)`.

Exercise 20 (Invariants for reaction networks)**.** Elimination theory has found application in the field of biochemical reaction networks. In this exercise, we see an example of that. For a certain biochemical reaction network and modeling assumptions, the set of equilibria is given as the positive solutions of the following system of polynomial equations:

$$\begin{aligned} -\kappa_4 x_2 x_3 + \kappa_3 x_4 + \kappa_5 x_5 &= 0 \\ \kappa_1 x_1 x_3 - \kappa_2 x_4 - \kappa_3 x_4 &= 0 \\ \kappa_4 x_2 x_3 - \kappa_5 x_5 - \kappa_6 x_5 &= 0. \end{aligned}$$

Here, $\kappa_1, \ldots, \kappa_6$ are parameters, which are positive (they are reaction rate constants), and x_1, x_2, x_3, x_4, x_5 are concentrations of the proteins in the network.

(a) Show that at any positive solution to the system ($x_i > 0$ for $i = 1, \ldots, 5$), x_1 and x_2 lie on a line (make sure your Gröbner bases hold for all parameter values!). The exact equation of the line depends on the parameter values, but the fact that there is a line, does not.

(b) Assume that x_1, x_2 can be measured at equilibrium, and that different initial concentrations lead to different equilibria. Discuss a method to disregard or verify that the proposed model fits the observed data.