1. Division Algorithm

Let K be a field and $R := K[x_1, \dots, x_n]$. Similar to ordinary division in Euclidean domains, there is a general concept of dividing a polynomial $f \in R$ by a finite set of polynomials $\{f_1, \dots, f_s\} \subseteq R$.

1. Elaborate the necessary theory.
2. Implement an algorithm which computes the normed reduced Gröbner basis of a finite set of polynomials with respect to an admissible ordering together with the additional information of representation. You may choose $K = \mathbb{Q}$ for your implementation.

   Input: A vector of polynomials $S = (f_1, \dots, f_s)^{\mathrm{T}} \in R^s$ and an admissible ordering $<$.

   Output: The normed reduced Gröbner basis $G \in R^t$ of the ideal $\langle S \rangle_R$ with respect to the ordering $<$ and a matrix $M \in R^{t \times s}$ such that $G = MS$.

References: Winkler [Win96], Becker and Weispfenning [BW93], Cox, Little and O'Shea [CLO15].

2. Zero-dimensional Systems

In applications it is quite often the case that a system of polynomial equations has only finitely many solutions.

1. Determine criteria when a system of polynomial equations in several variables with coefficients in an algebraically closed field (characteristic zero) has finitely many solutions. Present the necessary theory.
2. Implement an algorithm which decides whether such a system has finitely many solutions and—in the affirmative case—determine all solutions. You may compute the solutions numerically.

   Input: A (finite) sequence of polynomials $f_1, \dots, f_s \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$.

   Output: The list of solutions of $f_1 = \dots = f_s = 0$ in $\overline{\mathbb{Q}}^n$ or `INFINITE` if the system has infinitely many solutions.

References: Winkler [Win96], Becker and Weispfenning [BW93], Cox, Little and O'Shea [CLO15], Tran and Winkler [TW00].

3. Basis Conversion

The concept of Gröbner basis depends heavily on the chosen admissible ordering. Besides that different bases may look quite disparate, Gröbner bases with respect to different orderings serve different needs.

Instead of computing a Gröbner basis of an ideal for several admissible orderings separately, it is possible to convert one into another.

1. Present the theory of converting Gröbner bases of zero-dimensional ideals with respect to a given admissible ordering into lexicographic Gröbner bases.
2. Let $R := \overline{\mathbb{Q}}[x_1, \dots, x_n]$. Implement an algorithm which performs this basis conversion.

   Input: A Gröbner basis $G = \{g_1, \dots, g_s\} \subseteq R$ of the zero-dimensional ideal $\langle G \rangle_R$ with respect to an admissible ordering $<$ and a permutation π of $\{1, \dots, n\}$.

   Output: The normed reduced Gröbner basis of $\langle G \rangle_R$ with respect to the lexicographic ordering with $x_{\pi(1)} > \cdots > x_{\pi(n)}$.

References: Faugère et al. [Fau+93], Hofmann [Hof89].

4. Implicitization of Rational Varieties

Algebraic varieties are sometimes described by parametric equations. The implicitization problem is to convert such a parametrization into implicit defining equations.

1. Work out the theory of implicitizing rational algebraic varieties by Gröbner bases.
2. Let K be an infinite field and $R := K[t_1, \dots, t_s]$. Implement an algorithm which computes the implicit representation of a rationally parametrized algebraic variety. You may chose $K = \mathbb{Q}$ or $K = \overline{\mathbb{Q}}$ for your implementation.

   Input: A rational parametrization

   $$\begin{cases} x_1 &= \frac{f_1(t_1,\dots,t_s)}{g_1(t_1,\dots,t_s)} \\ \vdots &= \quad\vdots \\ x_n &= \frac{f_n(t_1,\dots,t_s)}{g_n(t_1,\dots,t_s)} \end{cases},$$

   where $f_1, \dots, f_n \in R$ and $g_1, \dots, g_n \in R \setminus \{0\}$.

   Output: An implicit representation, viz. a set of polynomials $S \subseteq K[x_1, \dots, x_n]$, of the smallest algebraic variety described by this parametrization.

References: Winkler [Win96], Cox, Little and O'Shea [CLO15], Cox, Little and O'Shea [CLO05].

5. Universal Gröbner Bases

Let $R := K[x_1, \dots, x_n]$ and $G \subseteq R$ be a finite subset. The set G is called a universal Gröbner basis of the ideal $I = \langle G \rangle_R$ if G is a Gröbner basis of I with respect to **every** admissible ordering of $[x_1, \dots, x_n]$.

1. Work out the theory of universal Gröbner bases.
2. Provide several non-trivial examples of universal Gröbner bases.

References: A good starting point is the book by Becker and Weispfenning [BW93]. There is also plenty of literature on this topic available online.

6. Square-free Factorization

An algorithm for computing the square-free factors of univariate integer polynomials is discussed in the lecture notes. This algorithm can be generalized to the multivariate case.

1. Elaborate the theory of square-free factorization in unique factorization domains.
2. Write a program that computes the square-free factors of a multivariate polynomial with rational coefficients.

   Input: A polynomial $f \in \mathbb{Q}[x_1, \dots, x_n] \setminus \{0\}$.

   Output: The list of square-free factors of f.

References: Winkler [Win96], Becker and Weispfenning [BW93].

7. Linear Algebra over Polynomial Rings

Let K be a field, $R := K[x_1, \dots, x_n]$, and consider the vector of polynomials $(f_1, \dots, f_s)^{\mathrm{T}} \in R^s$. A solution $(z_1, \dots, z_s)^{\mathrm{T}} \in R^s$ of the homogeneous linear equation $z_1 f_1 + \dots + z_s f_s = 0$ is called a *syzygy* of the polynomials $f_1, \dots, f_s$.

1. Work out the theory of syzygies over polynomial rings.
2. Implement an algorithm that computes solutions of linear equations over R. You may chose $K = \mathbb{Q}$ for your implementation.

   Input: Polynomials $g, f_1, \dots, f_s \in R$.

   Output: The general solution $(z_1, \dots, z_s)^{\mathrm{T}} \in R^s$ of the equation $z_1 f_1 + \dots + f_s z_s = g$.

References: Winkler [Win96], Becker and Weispfenning [BW93], Eisenbud [Eis95].

8. Modular GCD Computation

The aim of this project is to study the modular GCD algorithms from the lecture notes in more detail.

1. Examine the theory at the basis of modular GCD computations in detail.
2. Implement the modular GCD algorithm for integer polynomials.

   Input: Integer polynomials $a, b \in \mathbb{Z}[x] \setminus \{0\}$.

   Output: The greatest common divisor of a and b in $\mathbb{Z}[x]$.
3. Extend your program to multivariate modular GCD computations.

References: Winkler [Win96].

9. Hilbert Function

The Hilbert function is a measure for the growth of the dimension of the homogeneous parts of an algebra.

1. Develop the theory of Hilbert functions for graded modules over $K[x_1, \dots, x_n]$, where K is a field. Explain the concept of Hilbert series/Hilbert polynomial and its relation to the Hilbert function. Study methods for computing these objects.
2. Use your knowledge about Hilbert functions to determine essential data such as degree, dimension, etc. of some interesting algebraic varieties.

References: Cox, Little and O'Shea [CLO15], Eisenbud [Eis95].

10. Geometric Theorem Proving

Many geometric theorems from plane geometry (Thales's theorem, Desargues's theorem, etc.) can be expressed by polynomial equations.

1. Elaborate the theory of proving theorems of plane geometry by using Gröbner bases: translation of geometric statements into polynomial equations, definition of a strict/generic consequence from a set of hypotheses, sufficient conditions for being a strict/generic consequence.
2. Write an algorithm that detects whether a given geometric statement follows (strictly or generically) from a given system of geometric statements.
3. Prove a non-trivial geometric theorem of your choice along these lines.

References: Cox, Little and O'Shea [CLO15].

11. Robotics and Motion Planning

An interesting application of Gröbner bases is the study of possible configurations of mechanical linkages such as robot arms.

1. Work out the theory of planar robots (joint space, configuration space, forward/inverse kinematic problem).
2. Demonstrate the theory by means of a planar robot with a fixed segment 1 and with n revolute joints linking segments of length $l_2, \dots, l_n$. The "hand" is segment $n+1$, attached to segment n by joint n. Determine the position of the hand as a function of joint settings.
3. Consider a concrete planar robot with 3 revolute joints linking 4 segments of length 1, followed by one prismatic joint taking length values from the interval $[0, 1]$, linking the 4-th segment to the hand. Solve the inverse kinematic problem for this robot. Describe possible kinematic singularities.

References: Cox, Little and O'Shea [CLO15], Lozano-Pérez [Loz87].

References

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer-Verlag New York, 1993.

[CLO05] David A. Cox, John Little and Donal O'Shea. *Using Algebraic Geometry*. 2nd ed. Vol. 185. Graduate Texts in Mathematics. Springer-Verlag New York, 2005.

[CLO15] David A. Cox, John Little and Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4th ed. Undergraduate Texts in Mathematics. Springer International Publishing, 2015.

[Eis95] David Eisenbud. *Commutative Algebra. with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. Springer-Verlag New York, 1995.

[Fau+93] Jean-Charles Faugère et al. 'Efficient computation of zero-dimensional Gröbner bases by change of ordering'. In: *Journal of Symbolic Computation* 16.4 (1993), pp. 329–344.

[Hof89] Christoph M. Hofmann. *Geometric and Solid Modeling: An Introduction*. Morgan Kaufmann Pub, 1989.

[Loz87] Tomás Lozano-Pérez. 'A simple motion-planning algorithm for general robot manipulators'. In: *IEEE Journal on Robotics and Automation* 3.3 (1987), pp. 224–238.

[TW00] Quoc-Nam Tran and Franz Winkler. ‘Applications of the Gröbner basis method’. In: *Journal of Symbolic Computation* 30.4 (2000).

[Win96] Franz Winkler. *Polynomial Algorithms in Computer Algebra*. Texts & Monographs in Symbolic Computation. Springer-Verlag Wien, 1996.