ENS de Lyon Géométrie Algébrique
M1 2025-2026

TD3 : The Nullstellensatz in explicit cases
Playing with parametrizations

Exercises with a  are algebraic geometry exercices which will be corrected during the exercise session, if time allows it. Exercises with a  are important exercices of commutative algebra.

Exercise 1. (*Equation from a parametrization*) —

1. Let $\phi : \mathbb{R} \to \mathbb{R}^2$ be given by $t \mapsto (t^2, t^3)$. Prove that any $f \in \mathbb{R}[X, Y]$ vanishing on $\phi(\mathbb{R})$ is divisible by $Y^2 - X^3$. Which property of the field $\mathbb{R}$ did you use ?

2. Do the same work with $t \mapsto (t^2 - 1, t^3 - t)$.

3. (bonus) Redo the previous questions using explicit computations.

Exercise 2. (*A theorem of Liouville*) — Let k be a field of zero characteristic and $n \geq 3$. Show that the equation $P^n + Q^n + R^n = 0$ has no solution for $P, Q, R \in k[X]$, unless if P, Q, R are all k-collinear. And for $n = 2$?

Exercise 3. (*Resultant and Bézout's theorem*) —

Resultant

Let A be a commutative ring. Let $n, m > 0$, P and Q such that $\deg(P) \leq n$ and $\deg(Q) \leq m$. Define

$$\phi_{P,Q}^{n,m} : \left| \begin{array}{ccc} A_{m-1}[X] \times A_{n-1}[X] & \longrightarrow & A_{n+m-1}[X] \\ (U, V) & \longmapsto & UP + QV. \end{array} \right.$$

Call $\mathrm{Sylv}^{n,m}(P, Q)$ its matrix in the bases $((X^{m-1}, 0), \ldots, (1, 0), (0, X^{n-1}), \ldots, (0, 1))$ and $(X^{n+m-1}, \ldots, 1)$.

Call $\mathrm{Res}^{n,m}(P, Q)$ the determinant of this matrix.

The Sylvester matrix of (P, Q) is defined as $\mathrm{Sylv}^{\deg(P),\deg(Q)}(P, Q)$ and the Resultant of (P, Q) is defined as $\mathrm{Res}^{\deg(P),\deg(Q)}(P, Q)$.

1. Draw $\mathrm{Sylv}(P, Q)$.

2. Let $f : A \to B$ a morphism of rings. Show that f commutes with $\mathrm{Sylv}^{n,m}$ and $\mathrm{Res}^{n,m}$. Formulate a result where f commutes with Sylv and Res.

3. Let A be integral. Suppose that P and Q have a non constant common divisor. Show that $\mathrm{Res}(P, Q) = 0$. (what can you show if A is a general commutative ring ?)

4. If $k = A$ is a field, show that $\dim \ker \mathrm{Sylv}(P, Q) = \deg(P \wedge Q)$.

An application

5. Let x and y be algebraic on $\mathbb{Q}$ (resp. integral on $\mathbb{Z}$) which minimal polynomials are known, say P and Q. Describe an algorithm which computes a polynomial in $\mathbb{Q}$ (resp. in $\mathbb{Z}$ and monic) vanishing at $x+y$. Do the same with xy. Do the same with x^{-1} for the algebraic case. *Idea : use previous facts with the ring* $A = \mathbb{Q}[Y]$*. Evaluating a polynomial is the same as applying a morphism of rings. Use some nice resultant of two elements of* $A[X]$*, and notice that such a resultant is a polynomial in* Y*.*

Towards Bézout's theorem

Let $P, Q \in k[X,Y]$. Let $E \subset k^2$ be the set of common solutions of P and Q. We want to bound $\#E$. Write $n = \deg(P)$ and $m = \deg(Q)$.

6. Show that there exists some $R(X) \in k[X]$ such that $\forall (x,y) \in k^2$, $R(x) = 0$. (*) Show that its degree is $\leq mn$.

7. Deduce that $\#E \leq (mn)^2$. Can you refine how you use the previous question to show that $\#E \leq mn$?

The strong version of Bézout's theorem says that the number of common roots in $\mathbb{P}^2(k)$, where k is algebraicly closed, is exactly nm (counting multiplicities).

Exercise 4. (*Jacobson rings, fixed version*) — For the sequel, recall : (Krull's Theorem) Denote Spec$A$ the set of prime ideals of A. Then

$$\bigcap_{\mathfrak{p} \in \mathrm{Spec} A} \mathfrak{p} = \sqrt{(0)}.$$

Let A be a commutative ring and $I \subset A$ an ideal. The *Jacobson radical* $J(I)$ of I is defined as the intersection of all the maximal ideals of A containing I.

First manipulations.

1. Show that $J((0)) = \{x \in A \mid \forall y \in A, 1 - xy \in A^\times\}$.

A is called a *Jacobson ring* if for all ideal I of A, $J(I) = \sqrt{I}$.

2. Show that the following rings are Jacobson : $\mathbb{Z}$, fields, and the rings $k[T]$ where k is a field.

3. Show that the quotient of a Jacobson ring is again Jacobson.

4. Show that a ring is Jacobson if and only if for all prime ideal $\mathfrak{p}$, $\mathfrak{p} = J(\mathfrak{p})$.

5. Show that $A[T]$ being Jacobson implies A being Jacobson.

Polynomial rings over Jacobson rings.

6. (prelude) Let A be an integral domain, $\mathfrak{p}$ a non zero prime ideal of $A[T]$.

a. Let $f, g \in A[T]$, f of non-zero leading coefficient a. Show that there exists $n \in \mathbb{N}$, $q, r \in A[T]$ with $r = 0$ or $\deg(r) < \deg(f)$, such that $a^n g = qf + r$.

b. Let $f \in \mathfrak{p} - \{0\}$ of minimal degree and a its leading coefficient. Show that $\forall h \in \mathfrak{p}, \exists n \in \mathbb{N}, a^n h \in fA[T]$.

c. If $g \in A[T] - \mathfrak{p}$, prove that $(\mathfrak{p} + (g)) \cap A \neq 0$.

7. Let A an integral Jacobson ring. Let's show that $A[T]$ is Jacobson also.

a. Let $\mathfrak{p}$ a *non zero* prime ideal in $A[T]$ that intersects A trivially. Let $g \in J(\mathfrak{p})$, suppose it's not in $\mathfrak{p}$. Show that there exists $b \in (\mathfrak{p} + (g)) \cap A - \mathfrak{p}$.

b. Use again the notations f and a from the previous question. Show that there is some maximal ideal $\mathfrak{m}_0$ of A not containing b such that $a \notin \mathfrak{m}_0 A[T] + \mathfrak{p}$.

c. Show that there exists some maximal ideal $\mathfrak{m}$ of $A[T]$ containing $\mathfrak{m}_0 A[T] + \mathfrak{p}$. Show that there is a contradiction.

d. Deduce that for all prime ideals $\mathfrak{p}$ in $A[T]$ such that $A \cap \mathfrak{p} = 0$, we have $\mathfrak{p} = J(\mathfrak{p})$.

8. Let A be a general Jacobson ring, prove that $A[T]$ is Jacobson.

Generalized Nullstellensatz.

9. Let A be an integral domain. Let $\mathfrak{m}$ be maximal in $A[T]$. Suppose that $A \cap \mathfrak{m} = 0$. Let again the notations f and a from the previous questions.

a. Let $\mathfrak{m}_0$ be any non zero maximal ideal in A. Let $b \in \mathfrak{m}_0 - \{0\}$. Explain why there exist $g \in A[T]$, $h \in \mathfrak{m}$ such that $1 = h + gb$.

b. Apply Euclidean division of some $a^n g$ by f, denote the remainder r. Show that $a^n - br \in \mathfrak{m}$. Deduce that $a \in \mathfrak{m}_0$.

10. Let A be an integral domain which is Jacobson. Show that A is a field if and only if there exists a maximal ideal $\mathfrak{m}$ of $A[T]$ such that $\mathfrak{m} \cap A = 0$.

11. Show that the following are equivalent :

(1). A is Jacobson

(2). For all maximal ideal $\mathfrak{m}$ of $A[T]$, $\mathfrak{m} \cap A$ is a maximal ideal in A.

12. (Generalized Nullstellensatz) Let A a Jacobson ring and B a commutative A-algebra of finite type.

a. Show that B is a Jacobson ring.

b. If $\mathfrak{m}$ is a maximal ideal of B, show that $A \cap \mathfrak{m}$ is maximal.

c. Show furthermore that

$$A/A \cap \mathfrak{m} \to B/\mathfrak{m}$$

is a finite extension of fields (a theorem from a previous sheet may be used).

13. How is this theorem related to the Hilbertscher Nullstellensatz ?