ENS de Lyon — Géométrie Algébrique
M1 — 2025-2026

# TD3 : The Nullstellensatz in explicit cases
## Playing with parametrizations

**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 ?

*Correction.* $\mathbb{R}$ is infinite to whenever $\forall t \in \mathbb{R}$, $Q(t^2, t^3) = 0$, you can just say that $Q(T^2, T^3) = 0$ as a polynomial. Perform an euclidean division of $Q(X, Y)$ by $Y^2 - X^3$ and manage to survive.

**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 $n = 2$ ?

*Correction.* You will find it in Cassini books (Francinou-Gianella-Nicolas) or on the website agreg-maths.

**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 $\leq mn$.

*Correction.* This is know as "weak Bézout", you can find a proof named "Bézout faible" in the website agreg-maths.

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

*Correction.* Prove the following : $\forall x \in A$, $x \notin A^\times$ iff $\exists \mathfrak{m}$ maximal in $A$ such that $x \in \mathfrak{m}$. □

$A$ 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.

*Correction.* They are factorial so non zero ideals can be characterized simply. Beware : you have to treat the zero ideal separately, one way of concluding is by showing that whenever a ring is factorial, it contains an infinite number of prime elements. Just copy Euclid's proof for infinity of prime numbers. □

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

*Correction.* The ideals of $A/I$ are the $J/I$ for $J$ ideal of $A$ containing $I$. □

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

*Correction.* This is absolutely non trivial unless... you use Krull's theorem we saw in TD1 ! □

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

*Correction.* This question is a joke. Either you don't see it... either you see that $A$ is just the quotient of $A[T]$ by $(T)$. □

**Polynomial rings over Jacobson rings.**

**6.** (prelude : about prime ideals in $A[T]$) 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 $a^n g = qf + r$.

*Correction.* You should try to show it directly by copying the proof of the existence of euclidean division (this will give an algorithm to compute this question). I'll write here a quicker proof. Let $B = A[a^{-1}]$ ($A$ being integral, this is just a subring of the fraction field), the rings whose elements are or the form $\frac{u}{a^n}$ for $u \in A, n \in \mathbb{N}$. Then the leading coefficient of $f$ is invertible in $B$. Hence $\frac{1}{a}f$ is monic so it's easy to see that euclidean division exists (this is a basic theorem you should know : the proof goes by trying to kill all monomials of $g$ using multiples of $f$, starting by the leading one). Now you have something like $g = qf/a + r$, $q, r \in B[X]$, $\deg(r) < \deg(f)$. Multiply by a good power of $a^n$ to force $q, r$ to be in $A[X]$. □

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

*Correction.* Let $h \in \mathfrak{p}$. Write $a^n h = qf + r$ as before, with $\deg(r) < \deg(f)$. Notice that $r \in \mathfrak{p}$. Thus $r = 0$ by minimality of degrees. This concludes. □

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

*Correction.* Let $k$ the fraction field of $A$. Let's show that $g$ and $f$ are coprime in $k[T]$ because it looks like a Bézout's relation. The key point is that $f$ is irreducible in $k[T]$. Let $f = UV$ a decomposition in $k[T]$. Multiplying by the denominators, you get $\alpha, \beta \in A - \{0\}$ such that $\alpha U, \beta V \in A[T]$. Thus $\alpha U \beta V = \alpha\beta f \in \mathfrak{p}$. $\mathfrak{p}$ is prime so say that $\alpha U \in \mathfrak{p}$. But the degree of $f$ is minimal in $\mathfrak{p} - \{0\}$ so $\deg U = \deg f$. Hence $f$ is irreducible.

Now, let's show that $f$ does not divide $g$ in $k[T]$ : suppose it was the case with $fh = g$, $h \in k[T]$. Again, you can write $f\alpha h = \alpha g$ with $\alpha \in A - \{0\}$ and $\alpha h \in A[T]$. Hence $\alpha g \in \mathfrak{p}$ so $\alpha \in \mathfrak{p}$. This is possible but then we would be done with this question.

Now we can assume that $f$ does not divide $g$ in $k[T]$. $f$ is irreducible hence $f$ and $g$ are coprime hence we can find $U, V \in k[T]$ such that $fU + gV = 1$. Again, multiply by the denominators to force $U, V \in A[T]$, and now $fU + gV \in A - \{0\}$. □

**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 $b \in (\mathfrak{p} + (g)) \cap A - \{0\}$.

*Correction.* Yes, we just proved it. It's just that $\mathfrak{p}$ is prime and non zero so we deduced that $(\mathfrak{p} + (g)) \cap A - \{0\}$ is not empty. □

**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 $a \notin \mathfrak{m}_0 A[T] + \mathfrak{p}$.

*Correction.* We certainly want to find $\mathfrak{m}_0$ not containing $a$ nor $b$. As $A$ is a domain, $ab \notin \sqrt{(0)}$. As $A$ is Jacobson, $ab \notin \bigcap_{\mathfrak{m}} \mathfrak{m}$ hence there exists $\mathfrak{m}_0$ not containing $ab$. Hence $a \notin \mathfrak{m}_0$ and $b \notin \mathfrak{m}_0$.

Suppose that $a \in \mathfrak{m}_0 A[T] + \mathfrak{p}$. The elements of $\mathfrak{m}_0 A[T]$ are of the form $\sum_i m_i g_i$ for $m_i \in \mathfrak{m}_0$, $g_i \in A[T]$. Hence there is a relation of the form $a = \sum_i m_i g_i + p$, $p \in \mathfrak{p}$. The

trick here is to work inside $A/\mathfrak{m}_0[T]$ because it's a nice-looking ring (polynomials over a field) and we don't know anything about the $g_i$. In $A/\mathfrak{m}_0[T]$, one has $\overline{a} = \overline{p}$. Hence the polynomial $\overline{p} \in A/\mathfrak{m}_0[T]$ is constant non zero. But we know that there is some $n$ such that $a^n p = fh$, for some $h \in A[T]$. Hence $\overline{fh}$ is constant and non zero. So, looking at the degrees, $\overline{f}$ and $\overline{h}$ should also be constant. $f$ is not constant, hence its leading coefficient, $a$, lies in $\mathfrak{m}_0$. Impossible. Hence the result. □

**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.

*Correction.* $\mathfrak{m}_0 A[T] + \mathfrak{p}$ is proper so by Zorn's lemma, there is $\mathfrak{n}$ maximal in $A[T]$ containing it. Notice that $\mathfrak{m}_0 \cap \mathfrak{n} \cap A$. $\mathfrak{n} \cap A$ is proper because it does not contain 1. Hence, by maximality, $\mathfrak{m}_0 = \mathfrak{n} \cap A$. Also, $g \in J(\mathfrak{p})$ and $\mathfrak{n}$ contains $\mathfrak{p}$. Hence, $g \in \mathfrak{n}$.

Now, we have $b \in (\mathfrak{p} + (g)) \cap A \subset \mathfrak{n} \cap A = \mathfrak{m}_0$, which is impossible.

**Remark**. Why does it work ? We want to show that $g \in \mathfrak{p}$. If it's not the case, we notice that some Bézout relation implies the existence of this $b$. Now, to make good use of $g \in J(\mathfrak{p})$, one has to build maximal ideals $\mathfrak{n}$ of $A[T]$ containing $\mathfrak{p}$, but we want to have some insight of what we can find in $\mathfrak{n}$. A magic trick that may be hard for intuition may be the moment when we notice that $\mathfrak{n} \cap A = \mathfrak{m}_0$ : this allows us to know that $b \notin \mathfrak{n}$. □

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

*Correction.* The joke is that we are just left to prove the case when $\mathfrak{p} = 0$. The joke is that we will use the previous cases. Let $g \in J(0)$, show that $g = 0$.

Let $k$ be the fraction field of $A$. Let $p$ be a prime element of $k[T]$. Then $(p)$ is a maximal ideal of $k[T]$ hence $\mathfrak{p} := A[T] \cap (p)$ is prime (not always maximal, beware). $\mathfrak{p}$ is non zero because you can multiply $p$ by elements of $A$ to get an element of $A[T]$. Now, $(p)$ is a proper ideal of $k[T]$ hence does not contain any constant. Then $\mathfrak{p} \cap A \subset (p) \cap A = 0$. Hence $\mathfrak{p} = J(\mathfrak{p})$.

Finally, we have $g \in J(0) \subset J(\mathfrak{p}) = \mathfrak{p}$. This means that $g \in (p)$. Hence $g$ is divisible by all primes of $k[T]$. All the maximal ideals of $k[T]$ are of the form $(p)$ hence $g \in \bigcap_{\mathfrak{m} \subset k[T]} \mathfrak{m} = 0$ because $k[T]$ is a Jacobson domain as we saw.

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

*Correction.* Let $\mathfrak{p}$ be prime in $A[T]$. Let $B = A/(\mathfrak{p} \cap A)$. $B$ is a domain and $\mathfrak{p}$ descends to a prime ideal $\overline{\mathfrak{p}}$ in $B[T]$ that intersects $B$ trivially. Then $\overline{\mathfrak{p}} = J(\overline{\mathfrak{p}})$. It's easy to deduce that $\mathfrak{p} = J(\mathfrak{p})$. Hence $A[T]$ 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 $f \in \mathfrak{m}$ 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 $1 = h + gb$.

*Correction.* $b \in \mathfrak{m}_0 \cap A$ so, as $A \cap \mathfrak{m} = 0$, we have $b \notin \mathfrak{m}$. Hence $\mathfrak{m} \subsetneq (\mathfrak{m}, b)$. By maximality of $\mathfrak{m}$ amongst proper ideals, $(\mathfrak{m}, b) = A[T]$. This set contains 1 as a consequence. □

**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 $a \in \mathfrak{m}_0$.

*Correction.* Write $a^n g = qf + r$. Thus $a^n bg = qfb + rb$. Hence $a^n - ha^n = qfb + rb$. Hence $a^n - rb = qfb + ha^n \in \mathfrak{m}$. The degree of $a^n - rb$ is the one of $r$ but it's strictly

smaller than $\deg(f)$, so by minimality, $a^n - rb = 0$. Hence $a^n \in \mathfrak{m}_0$ hence $a \in \mathfrak{m}_0$. $\square$

**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 $\mathfrak{m} \cap A = 0$.

*Correction.* If $A$ is a field, then $(T)$ is a maximal ideal of $A[T]$ because $A[T]/(T) = A$ is a field and $(T) \cap A = 0$. Now, suppose that $A$ is not a field. Let $\mathfrak{m}$ be a maximal ideal of $A[T]$ such that $\mathfrak{m} \cap A = 0$, and bring back notations $f, a$. Then it should have a maximal ideal $\mathfrak{m}_0$. $A$ is not a field so $\mathfrak{m}_0$ is not 0. The previous question yields $a \in \mathfrak{m}_0$. Hence $a \in \bigcap_{\mathfrak{m}_0 \subset A} \mathfrak{m}_0 = 0$ because $A$ is a Jacobson domain. This is impossible. $\square$

**11.** Let $A$ be a commutative ring. 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 $A$.

*Correction.* (2) implies (1) : let $\mathfrak{p}$ be prime in $A$. Let $x \in J(\mathfrak{p}) - \mathfrak{p}$. Build a maximal ideal of $A[T]$ to deduce an interesting maximal ideal of $A$. Do it this way : $A[T]/(\mathfrak{p}, (1 - Tx)) = A/\mathfrak{p}[T]/(1 - Tx) = A/\mathfrak{p}[x^{-1}]$. (won't be corrected today).

(1) implies (2) : Suppose $A$ Jacobson and let $\mathfrak{m}$ a maximal ideal of $A[T]$. Then $\mathfrak{p} := \mathfrak{m} \cap A$ is prime then $B := A/\mathfrak{p}$ is a Jacobson domain. $\overline{\mathfrak{m}}$ is a maximal ideal of $B[T]$. Furthermore, if $x \in \overline{\mathfrak{m}} \cap B$, then $x$ is a constant polynomial in $B[T]$ so can be lifted to a constant in $A[T]$ that lies in $\mathfrak{m}$. But $\mathfrak{m} \cap A = \mathfrak{p}$ so $x = 0$. Then $\overline{\mathfrak{m}} \cap B = 0$. The previous question gets us that $B$ is a field so $\mathfrak{p}$ is maximal 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).

*Correction.* Let's do everything together. Let $b_1, \ldots, b_n$ be generators of the $A$-algebra $B$. Then we have a morphism $\phi : A[X_1, \ldots, X_n] \hookrightarrow B$. Denote its kernel $I$. Then $B \simeq A[X_1, \ldots, X_n]/I$. By previous questions and recursion, $A[X_1, \ldots, X_n]$ is Jacobson, and $B$ is a quotient of it so $B$ is Jacobson.

If $\mathfrak{m}$ is maximal in $B$, then it rises up to a maximal ideal $\mathfrak{n}$ in $A[X_1, \ldots, X_n]$. Then, by the previous question, $\mathfrak{n} \cap A[X_1, \ldots, X_{n-1}]$ is maximal, thus $\mathfrak{n} \cap A[X_1, \ldots, X_{n-2}]$ also, all the way down to $\mathfrak{n} \cap A$. This implies $\phi(\mathfrak{n} \cap A)$ to be maximal in $\phi(A)$, but this is precisely $\phi(A) \cap \mathfrak{m}$, that we identify with $A \cap \mathfrak{m}$.

The last fact is an easy consequence of the not easy exercise 2 in TD1.

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

*Correction.* We just did prove this theorem by not using anything related to the nullstellensatz. Let's use it to give a new proof of the nullstellensatz. As we saw in TD1, the nullstellensatz is a direct computational consequence of the weak form of it. Suppose $k$ algebraicly closed. Then $A = k[X_1, \ldots, X_n]$ is Jacobson by the previous question. The nullstellensatz is trivial for $n = 1$, let's assume it's true for $n - 1$, and show it for $n$. Let $\mathfrak{m}$ be a maximal ideal of $A$. Then $\mathfrak{m} \cap k[X_1, \ldots, X_{n-1}]$, by our

previous question, is maximal, so it should be of the form $\mathfrak{m}_1 = (X_1 - a_1, \ldots, X_{n-1} - a_{n-1})$.

$\mathfrak{m}$ is maximal and $\mathfrak{m}_1$ is not so we have $\mathfrak{m}_1 \subset \mathfrak{m}$. So the natural morphism

$$k[X_n] \simeq k[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_{n-1} - a_{n-1}) = A/\mathfrak{m}_1 \twoheadrightarrow A/\mathfrak{m}$$

has a non trivial prime kernel (because the destination ring is a domain). $k$ being algebraicly closed, this kernel is of the form $(X_n - a_n)$, and we are done proving that $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$.

Note : the nullstellensatz implies easy the fact that $k[X_1, \ldots, X_n]$ is Jacobson. This motivates the Jacobson theory, and why we got lead to this generalization.