Sur un théorème de Kronecker concernant les variétés algébriques

Thierry Coquand (*)

31 mars 2005

Résumé Un résultat classique de Kronecker, énoncé à la fin de la section 10 de [5], est que le radical d'un idéal de type fini dans un anneau de polynômes à n variables est le radical d'un idéal engendré par $n+1$ éléments. Nous présentons une preuve constructive et élémentaire d'une généralisation de ce théorème due à Heitmann [3] : dans un anneau de dimension de Krull $\leq n$ tout radical d'un idéal de type fini est le radical d'un idéal engendré par $n+1$ éléments.

Abstract A classical result of Kronecker, stated at the end of the section 10 of [5], is that any radical of a finitely generated ideal in a polynomial ring of n variables over a field is the radical of an ideal generated by $n+1$ elements. We give a constructive and elementary proof of a generalisation presented in [3] : in a ring of Krull dimension $\leq n$ a radical of a finitely generated ideal is the radical of an ideal generated by $n+1$ elements.

MSC 2000 : 13C15, 03F65, 13A15, 13E05

Mots clés : Dimension de Krull, Bord d'une sous-variété, Mathématiques constructives.

Key words : Krull dimension, Boundary of a subvariety, Constructive Mathematics.

Abridged english version

On a theorem of Kronecker about algebraic sets

1 Zariski spectrum and Krull dimension

Let R be a commutative ring with unit. Following Joyal [4], we define the Zariski spectrum of R as the distributive lattice generated by symbols $Z(f),\ f \in R$ and relations

$$Z(0) = 1 \qquad Z(1) = 0 \quad Z(fg) = Z(f) \vee Z(g) \qquad Z(f) \wedge Z(g) \leq Z(f+g)$$

We write $Z(f_1, \ldots, f_m)$ for $Z(f_1) \wedge \ldots \wedge Z(f_m)$. It can be shown directly that

$$Z(f_1, \ldots, f_m) \leq Z(g_1) \vee \ldots \vee Z(g_n)$$

holds if, and only if, the monoid generated by $g_1, \ldots, g_n$ meets the ideal generated by $f_1, \ldots, f_m$ [1]. Thus $Z(f_1, \ldots, f_m)$ can be defined as the radical of the ideal generated by $f_1, \ldots, f_m$ (with

* Chalmers, University of Göteborg, Sweden, email : coquand@cs.chalmers.se

reverse inclusion as ordering), and we have a point-free and elementary description of the basic closed sets of the Zariski spectrum of R.

In the case where R is a polynomial ring over a field K, $Z(f_1, \dots, f_m)$ can be thought of as the sets of common zeros of $f_1, \dots, f_m$ in an algebraic closure of K. This is the content of the Nullstellensatz theorem. But our elementary presentation is actually closer to the one of Kronecker, for which the common zeros were symbols in a suitable extension of K.

In [2] we present the following elementary caracterisation of Krull dimension. If $a \in R$ we define the *boundary* of a as being the ideal N_a generated by a and the elements b such that ab is nilpotent (or equivalently $Z(a) \vee Z(b) = 1$). Thus an element in N_a can be written $at + b$ with ab nilpotent.

Théorème 1.1 *The Krull dimension of R is $\leq n+1$ if, and only if, for all $a \in R$ the Krull dimension of R/N_a is $\leq n$.*

This can actually be taken as a constructive definition of Krull dimension, if we define further R to be of dimension ≤ -1 if, and only if, $R = 0$. This inductive definition of being of dimension $\leq n$ is then equivalent to the usual definition that there is no strictly increasing chain of prime ideals of length $n+1$ [2]. In [1] it is shown, in an elementary and constructive way, that the dimension of a polynomial ring with n variables over a discrete field is $\leq n$.

2 Kronecker's theorem

Théorème 2.1 *If the dimension of R if $\leq n$ and $k > n+1$ then for any $a_1, \dots, a_k$ there exist $b_2, \dots, b_k$ such that $Z(a_1, \dots, a_k) = Z(a_2 + a_1 b_2, \dots, a_k + a_1 b_k)$.*

Proof.
The proof is by induction on n. Let I be the ideal boundary of a_k. We have $a_k \in I$ and the dimension of R/I is $\leq n-1$. By induction, we can find $b_2, \dots, b_{k-1}$ such that

$$Z(a_1, \dots, a_{k-1}) = Z(a_2 + a_1 b_2, \dots, a_{k-1} + a_1 b_{k-1})$$

in R/I. This is clearly equivalent to

$$Z(a_2 + a_1 b_2, \dots, a_{k-1} + a_1 b_{k-1}) \leq Z(a_1)$$

so that a_1 is in the radical of the ideal $J = <a_2 + a_1 b_2, \dots, a_{k-1} + a_1 b_{k-1}>$ in the ring R/I. By definition of the boundary this means that there exists b_k such that $a_k b_k$ is nilpotent and that a_1 is in the radical of the ideal $J + <a_k, b_k>$. So, in R/J, we have $Z(a_k, b_k) \leq Z(a_1)$. We claim that we have $Z(a_k + a_1 b_k) \leq Z(a_1)$ in R/J. Indeed, we have both

$$Z(a_k + a_1 b_k) \wedge Z(b_k) = Z(a_k, b_k) \leq Z(a_1)$$

and

$$Z(a_k + a_1 b_k) \wedge Z(a_k) = Z(a_1 b_k, a_k) \leq Z(a_1)$$

hence the result since $Z(a_k) \vee Z(b_k) = 1$. It follows that we have

$$Z(a_2 + a_1 b_2, \dots, a_{k-1} + a_1 b_{k-1}, a_k + a_1 b_k) \leq Z(a_1)$$

in R, which is equivalent to $Z(a_1, \dots, a_k) = Z(a_2 + a_1 b_2, \dots, a_k + a_1 b_k)$. $\square$

Corollaire 2.2 *If the dimension of R is $\leq n$, then any radical of a finitely generated ideal is the radical of an ideal requiring at most $n+1$ generators. In fact, we can write $Z(a_1,\ldots,a_{n+1},u_1,\ldots,u_m) = Z(c_1,\ldots,c_{n+1})$ with $c_i = a_i + \Sigma r_{ij}u_j$*

The proof being constructive can be thought of as an algorithm that produces explicitely these $n+1$ generators. Notice that we don't have any noetherianity hypothesis.

As an application, since we know, in a constructive way, that $K[X_1,\ldots,X_n]$, with K discrete, has dimension $\leq n$, we get an explicit version of Kronecker's theorem that any radical of a finitely generated ideal is the radical of an ideal requiring at most $n+1$ generators. More generally, if $R = K[X_1,\ldots,X_n]/I$ with I finitely generated, then using Noether's normalisation algorithm, R can be written as a finite integral extension of a polynomial ring $K[Y_1,\ldots,Y_r]$, and it follows from [1] that R is of dimension $\leq r$, so that any radical of a finitely generated ideal is the radical of an ideal requiring at most $r+1$ generators.

Another direct application, in the case where $<a_1,\ldots,a_k>$ is R, is Bass' Stable Range Theorem. It follows then for instance directly that a stably free module of rank $\geq n+1$ over a ring of dimension $\leq n$ is free [6], without any noetherianity hypotheses.

---

l'article en français

1 Le spectre de Zariski et la dimension de Krull

Soit R un anneau commutatif unitaire. Suivant Joyal [4], nous définissons le spectre de Zariski de R comme étant le treillis distributif engendré par les symboles $Z(f)$, $f \in R$ et les relations

$$Z(0) = 1 \qquad Z(1) = 0 \quad Z(fg) = Z(f) \vee Z(g) \qquad Z(f) \wedge Z(g) \leq Z(f+g)$$

Nous écrivons $Z(f_1,\ldots,f_m)$ pour $Z(f_1) \wedge \ldots \wedge Z(f_m)$. On peut montrer directement que l'on a

$$Z(f_1,\ldots,f_m) \leq Z(g_1) \vee \ldots \vee Z(g_n)$$

si et seulement si le monoide engendré par $g_1,\ldots,g_n$ rencontre l'idéal engendré par $f_1,\ldots,f_m$ [1]. Donc $Z(f_1,\ldots,f_m)$ peut être défini comme le radical de l'idéal engendré par $f_1,\ldots,f_m$, et nous avons une description élémentaire "sans points" des fermés de base du spectre de Zariski de R.

Dans le cas où R est un anneau de polynômes sur un corps K, on peut penser à $Z(f_1,\ldots,f_m)$ comme l'ensemble des zéros communs à $f_1,\ldots,f_m$ dans une clôture algébrique de K. C'est le contenu du théorème de Nullstellensatz. Mais notre description élémentaire est en fait plus proche de celle de Kronecker, pour lequel les zéros communs étaient seulement des objets symboliques dans un surcorps convenable de K.

Dans [2] nous présentons la caractérisation suivante de la dimension de Krull. Si $a \in R$ on définit le *bord* de a comme l'idéal N_a engendré par a et les éléments b tels que ab est nilpotent (ou, de manière équivalente $Z(a) \vee Z(b) = 1$). Un élément de N_a peut donc s'écrire $at+b$ où ab est nilpotent.

Théorème 1.1 *La dimension de R est $\leq n+1$ si et seulement si pour tout $a \in R$ la dimension de R/N_a est $\leq n$.*

Ceci peut en fait être vu comme une définition constructive de la dimension de Krull, si nous ajoutons que R est de dimension ≤ -1 si et seulement si R est l'anneau trivial. Cette définition d'être de dimension $\leq n$ est alors équivalente à la définition usuelle qu'il n'y a pas de chaîne d'idéaux premiers strictement croissante de longueur $n+1$ [2]. Dans [1] nous montrons ainsi que la dimension d'un anneau de polynômes à n variables sur un corps discret est $\leq n$.

2 Le théorème de Kronecker

Théorème 2.1 *Si la dimension de R est $\leq n$ et $k > n+1$ alors pour tout $a_1, \ldots, a_k$ il existe $b_2, \ldots, b_k$ tels que $Z(a_1, \ldots, a_k) = Z(a_2 + a_1 b_2, \ldots, a_k + a_1 b_k)$.*

Preuve.
La preuve est par induction sur n. Soit I l'idéal bord de a_k. On a $a_k \in I$ et la dimension de R/I est $\leq n-1$. Par induction, on trouve $b_2, \ldots, b_{k-1}$ tels que

$$Z(a_1, \ldots, a_{k-1}) = Z(a_2 + a_1 b_2, \ldots, a_{k-1} + a_1 b_{k-1})$$

dans R/I. Ceci est équivalent à

$$Z(a_2 + a_1 b_2, \ldots, a_{k-1} + a_1 b_{k-1}) \leq Z(a_1)$$

et donc a_1 est dans le radical de l' idéal $J = <a_2 + a_1 b_2, \ldots, a_{k-1} + a_1 b_{k-1}>$ dans l'anneau R/I. Par définition du bord, ceci veut dire qu'il existe b_k tel que $a_k b_k$ est nilpotent et que a_1 est dans le radical de l'idéal $J + <a_k, b_k>$. Donc, dans R/J, on a $Z(a_k, b_k) \leq Z(a_1)$. Alors, on a $Z(a_k + a_1 b_k) \leq Z(a_1)$ dans R/J. En effet, on a

$$Z(a_k + a_1 b_k) \wedge Z(b_k) = Z(a_k, b_k) \leq Z(a_1)$$

et

$$Z(a_k + a_1 b_k) \wedge Z(a_k) = Z(a_1 b_k, a_k) \leq Z(a_1)$$

d'où le résultat puisque $Z(a_k) \vee Z(b_k) = 1$. On en déduit

$$Z(a_2 + a_1 b_2, \ldots, a_{k-1} + a_1 b_{k-1}, a_k + a_1 b_k) \leq Z(a_1)$$

dans R, ce qui est équivalent à $Z(a_1, \ldots, a_k) = Z(a_2 + a_1 b_2, \ldots, a_k + a_1 b_k)$. □

Corollaire 2.2 *Si la dimension de R est $\leq n$, alors tout radical d'un idéal de type fini est le radical d'un idéal engendré par au plus $n+1$ éléments. En fait, on peut écrire $Z(a_1, \ldots, a_{n+1}, u_1, \ldots, u_m) = Z(c_1, \ldots, c_{n+1})$ avec $c_i = a_i + \Sigma r_{ij} u_j$*

Puisque cette preuve est constructive, on peut la voir comme un algorithme qui construit explicitement ces $n+1$ générateurs. On notera qu'il n'y a aucune hypothèse noethérienne.

Comme application, puisque l'on a que $K[X_1, \ldots, X_n]$, avec K corps discret, a une dimension $\leq n$, on obtient une version constructive du théorème de Kronecker disant qu'un radical d'un idéal de type fini est le radical d'un idéal engendré par au plus $n+1$ éléments.

Une autre application est le théorème de "Stable Range" de Bass dans le cas où l'idéal $<a_1, \ldots, a_k>$ est R. On en déduit par exemple directement qu'un module stablement libre de rang $\geq n+1$ sur un anneau de dimension $\leq n$ est libre [6], sans hypothèse noethérienne.

En conclusion, je voudrais remercier Henri Lombardi et Claude Quitté pour leurs commentaires sur une version préliminaire de cette note.

Références

[1] Th. Coquand and H. Lombardi. Hidden constructions in abstract algebra (3) Krull dimension. dans *Commutative ring theory and applications.* Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499.

[2] Th. Coquand, H. Lombardi and M-F. Roy. Une caractérisation élémentaire de la dimension de Krull. Prépublication 2003.

[3] R. Heitmann. Generating non-Noetherian modules efficiently. *Michigan Math. J.* 31 (1984), no. 2, 167–180.

[4] A. Joyal. Le théorème de Chevalley-Tarski. *Cahiers de Topologie et Géométrie Différentielle* 16, 256–258 (1975).

[5] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. reine angew. Math.* 92, 1-123 (1882). Réimprimé dans *Leopold Kronecker's Werke*, II, 237–387.

[6] T.Y. Lam. Serre's conjecture. Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978.