A Nilregular Element Property[*]

Thierry Coquand[1], Henri Lombardi[2], and Peter Schuster[3]

[1] Computing Science, Chalmers University of Technology
412 96 Göteborg, Sweden
`coquand@cs.chalmers.se`
[2] Equipe de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques
Université de Franche-Comté, 25 030 Besançon cedex, France
`henri.lombardi@univ-fcomte.fr`
[3] Mathematisches Institut, Universität München
Theresienstraße 39, 80333 München, Germany
`peter.schuster@mathematik.uni-muenchen.de`

Abstract. An element or an ideal of a commutative ring is nilregular if and only if it is regular modulo the nilradical. We prove that if the ring is Noetherian, then every nilregular ideal contains a nilregular element. In constructive mathematics, this proof can then be seen as an algorithm to produce nilregular elements of nilregular ideals whenever the ring is coherent, Noetherian, and discrete. As an application, we give a constructive proof of the Eisenbud–Evans–Storch theorem that every algebraic set in n–dimensional affine space is the intersection of n hypersurfaces. The input of the algorithm is an arbitrary finite list of polynomials, which need not arrive in a special form such as a Gröbner basis. We dispense with prime ideals when defining concepts or carrying out proofs.

Keywords. commutative Noetherian rings, constructive algebra

1 Introduction

With this paper we contribute to a partial realisation of Hilbert's programme in commutative algebra. Any talk of complexity aside, our method differs in spirit from computational approaches such as the one based on the concept of Gröbner basis (see, for example, [1]). One difference is that the algorithms which can be read from our constructive proofs (that is, proofs done with intuitionistic logic [12]) can essentially be run on the objects of customary mathematics; they do not expect their data to be of a special form. For instance, a finitely generated polynomial ideal may be given by an arbitrary finite list of generators, which need not be (transformed into) a Gröbner basis.

Our objective is to reveal the constructions hidden in abstract algebra. Also, we aim at constructive proofs carried out at the same type level at which the

---

[*] The original article will appear in *Arch. Math. (Basel)*. Birkhäuser-Verlag has kindly permitted the earlier publication of this enriched version.

theorems are formulated. To this end we make prime ideals unnecessary wherever they occur only as tools, to define concepts or to carry out proofs. Prime ideals are subsets of the given ring; whence their type level is in general higher than the one of (finite sequences of) ring elements. As we eventually want to transform a finite list of polynomials into another one (Theorem 3), it makes sense to keep away from arbitrary (prime) ideals on the way to this result.

How can one do without prime ideals when dealing with commutative rings? A simple example is the nilradical, which should rather be defined as the set of all nilpotent ring elements than as the intersection of all (minimal) prime ideals. A less trivial example is the concept of Krull dimension, which is usually defined as the greatest possible length of a chain of prime ideals. It equals the Krull dimension of the Zariski spectrum: that is, the greatest possible length of a chain of inhabited irreducible closed subspaces.

A recently given inductive characterisation of Krull dimension without primes [5] is equally intuitive, but more effective than Krull's. It carries over to the algebraic setting the inductive concept of dimension for topological spaces which is due to Brouwer, Menger, and Urysohn. The idea is that a topological space is zero–dimensional if and only if each point has a basis of neighbourhoods with empty boundaries, while for $n \geq 0$ a topological space has dimension $\leq n$ precisely when each point has a basis of neighbourhoods with boundaries of dimension $\leq n - 1$. This inductive characterisation made possible an elementary constructive proof [2] of a theorem due to Kronecker whose geometric interpretation is that every algebraic subset of n–dimensional space is the intersection of $n + 1$ hypersurfaces.

Moreover, the new characterisation of Krull dimension enables us to perform the task of this paper, to give a constructive proof of the theorem of Eisenbud–Evans and Storch. As this is the ideal–theoretic version of the statement that every algebraic subset of of n–dimensional space is in fact the intersection of n hypersurfaces, it improves on Kronecker's theorem. After giving a topological proof of a variant of the regular element property (Section 1), we show how to constructively interpret this proof without prime ideals (Section 2), and finally apply this interpretation to achieve the desired result (Section 3).

2   The Nilregular Element Property

Let R be a commutative ring with unit and N its nilradical. We define an element a (respectively, an ideal I) of R to be *nilregular* if and only if $x \in N$ whenever $ax \in N$ (respectively, $ax \in N$ for all $a \in I$). So an ideal I is nilregular precisely when the transporter ideal $(N : I) = \{x \in R : xI \subseteq N\}$ is contained in N. To find nilregular elements of nilregular ideals when R is Noetherian, we interpret first the property of being nilregular in a topological way.

As usual, let $\mathfrak{D}(a)$ be the set of prime ideals $\mathfrak{p}$ of R such that $a \notin \mathfrak{p}$, and let $\mathfrak{D}(a_1, \ldots, a_n)$ stand for the union of $\mathfrak{D}(a_1), \ldots, \mathfrak{D}(a_n)$. The intersection of $\mathfrak{D}(a)$ and $\mathfrak{D}(b)$ is $\mathfrak{D}(ab)$, and $\mathfrak{D}(a)$ is a subset of $\mathfrak{D}(a_1, \ldots, a_n)$ if and only if a belongs

to the radical of the ideal $(a_1, \ldots, a_n)$ generated by $a_1, \ldots, a_n$. In particular, $\mathfrak{D}(a) = \emptyset$ precisely when $a \in N$.

Lemma 1. *We have* $\mathfrak{D}(a + b, ab) = \mathfrak{D}(a, b)$ *for all* $a, b \in R$. *If, in particular,* $\mathfrak{D}(a)$ *and* $\mathfrak{D}(b)$ *are disjoint, then* $\mathfrak{D}(a + b) = \mathfrak{D}(a, b)$.

It is well–known that the $\mathfrak{D}(a)$ with $a \in R$ form a basis of opens for the Zariski topology on the prime spectrum (the set of all prime ideals) of R.

Remark 1. $\mathfrak{D}(a_1, \ldots, a_n)$ is dense if and only if $(a_1, \ldots, a_n)$ is a nilregular ideal.

Theorem 1. *Let R be Noetherian. If $\mathfrak{D}(a_1, \ldots, a_n)$ is dense for $a_1, \ldots, a_n \in R$, then the ideal $(a_1, \ldots, a_n)$ contains a nilregular element.*

Proof. If $\mathfrak{D}(x) \neq \emptyset$, then there exists i such that $\mathfrak{D}(xa_i) \neq \emptyset$, because $\mathfrak{D}(a_1, \ldots, a_n)$ is dense. Hence if the ring is nontrivial, then we can inductively build a sequence $b_0, b_1, \ldots$ of elements of R in the following way: b_0 is one a_i such that $\mathfrak{D}(b_0) \neq \emptyset$; if $\mathfrak{D}(b_0, \ldots, b_k)$ is not dense, then b_{k+1} is a multiple of one a_j such that $\mathfrak{D}(b_{k+1}) \neq \emptyset$ and $\mathfrak{D}(b_{k+1})$ is disjoint from $\mathfrak{D}(b_0, \ldots, b_k)$. Since R is Noetherian, this procedure has to stop, and we eventually find p such that $\mathfrak{D}(b_0, \ldots, b_p)$ is dense and $\mathfrak{D}(b_i) \cap \mathfrak{D}(b_j) = \emptyset$ whenever $i \neq j$. By Lemma 1, we have

$$\mathfrak{D}(b_0, \ldots, b_p) = \mathfrak{D}(b_0 + \cdots + b_p)$$

and $b_0 + \cdots + b_p$ is a nilregular element in $(a_1, \ldots, a_n)$.

As in [2] we define the *ideal boundary* N_a of $a \in R$ to be the ideal generated by a and the elements x of R such that ax is nilpotent; in other words, $N_a = aR + (N : a)$.

Lemma 2. *Every ideal boundary is a nilregular ideal.*

Corollary 1. *If R is Noetherian, then every ideal boundary contains a nilregular element.*

Throughout this section we could only have required that the topological space $\mathrm{Spec}(R)$ rather than the ring R be Noetherian.

3   Constructive Interpretation

We interpret the previous argument in the framework of constructive mathematics [10,11]. Let $L(R)$ be the lattice of *radically finitely generated* ideals of R: that is, the radicals of finitely generated ideals [3]. Following Joyal [8], the lattice $L(R)$, with inclusion as ordering, can also be defined as the distributive lattice generated by the symbols $D(a)$ with $a \in R$, and equipped with the relations

$$D(0) = 0, \quad D(1) = 1, \quad D(ab) = D(a) \wedge D(b), \quad D(a + b) \leq D(a) \vee D(b)$$

for $a, b \in A$. Writing $D(a_1, \ldots, a_m)$ for $D(a_1) \vee \cdots \vee D(a_m)$, it can be shown [3] that
$$D(b_1) \wedge \cdots \wedge D(b_n) \leq D(a_1, \ldots, a_m)$$
if and only if the monoid generated by $b_1, \ldots, b_n$ meets the ideal generated by $a_1, \ldots, a_m$. So $D(a_1, \ldots, a_m)$ can indeed be identified with the radical of the ideal $(a_1, \ldots, a_m)$, and $D(a) = 0$ precisely when a is nilpotent.

Lemma 3. *If R is coherent, Noetherian, and discrete, then one can decide whether a given element of R is nilpotent.*

Proof. Let $a \in R$. Every annihilator $(0 : a^p)$ is a finitely generated ideal with $(0 : a^p) \subseteq (0 : a^{p+1})$. Since R is Noetherian, there exists n such that $(0 : a^n) = (0 : a^{n+1})$. We even have $(0 : a^n) = (0 : a^{n+k})$ for all k. (Indeed, if $a^{n+k+1}b = 0$, then $a^k b$ annihilates a^{n+1} and thus also a^n, so that $a^{n+k}b = 0$.) Hence a is nilpotent if and only if $a^n = 0$.

Corollary 2. *If R is coherent, Noetherian, and discrete, then equality to 0 is decidable in $L(R)$.*

If R is coherent and Noetherian, then $L(R)$ is a Heyting algebra [3].

Remark 2. $\neg D(a_1, \ldots, a_n) = 0$ if and only if $(a_1, \ldots, a_n)$ is a nilregular ideal.

Lemma 4. *If R is coherent, Noetherian, and discrete, for given $b_0, \ldots, b_k \in R$ we can decide whether $\neg D(b_0, \ldots, b_k) = 0$; if indeed $\neg D(b_0, \ldots, b_k) \neq 0$, then we can compute $b_{k+1} \in R$ such that $D(b_{k+1}) \neq 0$ and $D(b_{k+1}) \wedge D(b_0, \ldots, b_k) = 0$.*

Proof. Write $\neg D(b_0, \ldots, b_k) = D(c_1, \ldots, c_m)$, and apply Lemma 3 successively to the c_j. If $c_j \notin N$ for some j, then $b_{k+1} = c_j$ is as desired.

Corollary 3. *If R is coherent, Noetherian and discrete, then we can decide whether an element b of R is nilregular, and if this is not the case, then we can compute an element $x \notin N$ such that $bx \in N$.*

In this context, $\neg D(b_0, \ldots, b_k) = 0$ precisely when $D(b_0, \ldots, b_k)$ is dense. Reasoning as in the previous section (Theorem 1), we can now conclude.

Theorem 2. *Let R be coherent, Noetherian, and discrete. If $\neg D(a_1, \ldots, a_n) = 0$ for $a_1, \ldots, a_n \in R$, then the ideal $(a_1, \ldots, a_n)$ contains a nilregular element.*

This result seems closely connected to the regular element property proved constructively in [11]. The hypothesis is a little weaker (we don't assume the ring to contain an infinite field), but the statement is a priori different unless the ring is reduced (we use 'nilregular' instead of 'regular'). In view of Lemma 2, Corollary 1 can be rephrased as follows.

Corollary 4. *If R is coherent, Noetherian, and discrete, then every ideal boundary contains a nilregular element.*

In terms of $L(R)$, this means that for every $a \in R$ there is $s \in R$ with $\neg D(s) = 0$ and $D(s) \leq D(a) \vee \neg D(a)$; observe that $D(N_a) = D(a) \vee \neg D(a)$.

4   Application

The motivation of this work was to give a constructive proof of the Eisenbud–Evans–Storch theorem that every algebraic set in n–dimensional affine space is the intersection of n hypersurfaces [6,13]. In [2,3,5] a constructive approach to the theory of Krull dimension is given with $\mathsf{Kdim}R \leq -1$ if and only if R is trivial, and $\mathsf{Kdim}R \leq n+1$ if and only if $\mathsf{Kdim}(R/N_a) \leq n$ for all $a \in R$. This inductive definition of being of Krull dimension $\leq n$ is then classically equivalent to the usual definition that there is no strictly increasing chain of prime ideals of length $> n$ [3,5]. We also say that two rings R_1 and R_2 *have the same Krull dimension* if and only if $\mathsf{Kdim}R_1 \leq n$ is equivalent to $\mathsf{Kdim}R_2 \leq n$ for every $n \geq -1$.

Lemma 5. *If I is an ideal of R with $I \subseteq N$, then R and R/I have the same Krull dimension.*

Corollary 5. *If $\mathsf{Kdim}R \leq n+1$ and $s \in R$ is nilregular, then $\mathsf{Kdim}(R/sR) \leq n$*

Lemma 6. *If R is reduced, then R is von Neumann regular if and only if $\mathsf{Kdim}R \leq 0$.*

Corollary 6. *If R is reduced and $\mathsf{Kdim}R \leq 0$, then every finitely generated ideal of $R[X]$ is principal. If we assume only $\mathsf{Kdim}R \leq 0$, then every radically finitely generated ideal of $R[X]$ is radically generated by one element.*

Theorem 3. *Let R be coherent, Noetherian, and strongly discrete. If $\mathsf{Kdim}R \leq d$, then for every $g_1, \ldots, g_m \in R[X]$ there exists $f_0, \ldots, f_d \in R[X]$ such that $D(g_1, \ldots, g_m) = D(f_0, \ldots, f_d)$.*

Proof. We prove this by induction on d. The statement is clear from Corollary 6 if $d = 0$. Let S be the multiplicative monoid of nilregular elements. Corollary 4 shows that the ring of fractions R_S is of Krull dimension ≤ 0. Hence, using Corollary 6 again, we can find $f \in R[X]$ such that $D(f) = D(g_1, \ldots, g_m)$ in $R_S[X]$. In $R[X]$ this means that there exists $s \in S$ such that

$$D(f) \wedge D(s) \leq D(g_1, \ldots, g_m) \quad \text{and} \quad D(g_i) \wedge D(s) \leq D(f)\,.$$

We now set $f_0 = sf$ and thus arrive at

$$D(s) \wedge D(g_1, \ldots, g_m) \leq D(f_0) \leq D(g_1, \ldots, g_m)$$

in $R[X]$. Since $s \in S$, we have $\mathsf{Kdim}(R/sR) \leq d-1$ by Corollary 5. By induction,

$$D(h_1, \ldots, h_d) = D(g_1, \ldots, g_m)$$

for suitable $h_1, \ldots, h_d$ in $(R/sR)[X]$. (Induction is possible, because if R is coherent, Noetherian, and strongly discrete, then so is R/I for every finitely generated ideal I of R [10, III.2].) This means

$$D(s, h_1, \ldots, h_d) = D(s, g_1, \ldots, g_m)$$

in $R[X]$; whence
$$h_j^{n_j} = a_j s + \sum_i c_{ij} g_i$$
for $j = 1, ..., d$ and suitable integers $n_j \geq 1$. For each $j \geq 1$, we now set
$$f_j = h_j^{n_j} - a_j s$$
and get $D(f_j, s) = D(h_j, s)$ with $D(f_j) \leq D(g_1, ..., g_m)$; whence
$$D(s, f_1, ..., f_d) = D(s, g_1, ..., g_m)$$
and thus $D(f_0, f_1, ..., f_d) \leq D(g_1, ..., g_m)$. For each $i \leq m$, moreover, $D(g_i) \leq D(s, f_1, ..., f_d)$ implies $D(g_i) \leq D(sg_i, f_1, ..., f_d)$; since also $D(sg_i) \leq D(f_0)$, we get $D(g_i) \leq D(f_0, f_1, ..., f_d)$. We finally arrive at $D(f_0, f_1, ..., f_d) = D(g_1, ..., g_m)$ as desired.

In this proof we apply Corollary 6 also to certain quotient rings of R (for instance, to R/sR for some nilregular element s). We thus need to know that *all* these rings are discrete, which is guaranteed by the assumption that R be *strongly* discrete. Note that if R is coherent, Noetherian, and strongly discrete, then $L(R)$ is discrete [3].

In [3] it is shown, in an elementary and constructive way, that the Krull dimension of a polynomial ring in n variables over a discrete field is $\leq n$. By Hilbert's basis theorem [10, VIII.1.5], any such ring is coherent, Noetherian, and strongly discrete.

Corollary 7. *If K is a discrete field and $d \geq 1$, then for all $g_1, \ldots, g_m \in K[X_1, \ldots, X_d]$ there exist $f_1, \ldots, f_d \in K[X_1, \ldots, X_d]$ such that $D(g_1, \ldots, g_m) = D(f_1, \ldots, f_d)$.*

Kronecker proved this result with $d+1$ polynomials instead of d polynomials [2]. Our argument, being constructive, can be read as an algorithm that produces $f_1, \ldots, f_d$ for given $g_1, \ldots, g_m$.

5   Conclusion

The fresh perspective on Krull dimension which we needed also in this paper (Section 3) made it further possible to generalise some results providing bounds for numbers of generators. For instance, a generalisation of the theorem of Forster and Swan works in the non–Noetherian case as well [4]. The clue is to switch to Heitmann's notion of dimension [7], which gives the Krull dimension of the maximal spectrum in the Noetherian case.

Before, the local–global principle of commutative algebra was understood in a point–free way by means of finite open coverings [9]. This requires Joyal's presentation of the Zariski spectrum as a distributive lattice, which was indispensable also in the present paper (Section 2): the points of the Zariski spectrum are nothing but the prime ideals of the given commutative ring. The other ideals that have occurred in this paper are (radicals of) finitely generated ideals; whence each of them can be seen as a finite list of ring elements.

References

1. Th. Becker and V. Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra.* In cooperation with H. Kredel. Springer, New York (1993).

2. T. Coquand. Sur un théorème de Kronecker concernant les variétés algébriques. *C. R. Math. Acad. Sci. Paris*, Ser. I, 338 (2004), 291–294.

3. T. Coquand and H. Lombardi. Hidden constructions in abstract algebra (3): Krull dimension of distributive lattices and commutative rings. In: M. Fontana et al., eds., *Commutative Ring Theory and Applications.* Lecture Notes Pure Appl. Math. 131, Dekker, New York (2002), 477–499.

4. T. Coquand, H. Lombardi, and C. Quitté. Generating non–Noetherian modules constructively. *Manuscripta Math.* 115 (2004), 513–520.

5. T. Coquand, H. Lombardi, and M.–F. Roy. An elementary characterisation of Krull dimension. In: L. Crosilla, P. Schuster, eds., *From Sets and Types to Topology and Analysis.* Oxford University Press, forthcoming.

6. D. Eisenbud and E. G. Evans, Jr. Every algebraic set in n–space is the intersection of n hypersurfaces. *Invent. Math.* 19 (1973), 107–112.

7. R. Heitmann. Generating non–Noetherian modules efficiently. *Michigan Math. J.* 31 (1984), 167–180.

8. A. Joyal. Le théorème de Chevalley–Tarski. *Cah. Topol. Géom. Différ. Catég.* 16 (1975), 256–258.

9. H. Lombardi and C. Quitté. Constructions cachées en algèbre abstraite (2). Le principe local–global. In: M. Fontana et al., eds., *Commutative Ring Theory and Applications.* Lecture Notes Pure Appl. Math. 131, Dekker, New York (2002), 461–476.

10. R. Mines, F. Richman, W. Ruitenburg. *A Course in Constructive Algebra.* Springer, New York (1987).

11. F. Richman. The regular element property. *Proc. Amer. Math. Soc.* 126 (1998), 2123–2129.

12. F. Richman. Intuitionism as generalization. *Philos. Math.* 5 (1990), 124–128.

13. U. Storch. Bemerkung zu einem Satz von M. Kneser. *Arch. Math. (Basel)* 23 (1972), 403–404.