Some remarks about normal rings

Thierry Coquand* and Henri Lombardi†

Abstract

We give a constructive proof that $R[X]$ is normal when R is normal. We apply this result to an operation needed for studying the henselization of a local ring. Our proof is based on the case where R is without zero divisors, which is more involved than the case where R is an integral domain. We have to use a constructive deciphering technique that replaces the use of minimal primes (in classical mathematics) by suitable explicit localizations in a suitable tree.

Kewwords: Normal ring, pf-ring, constructive mathematics, gcd-tree.

MSC2010: 13B22, 13B30, 13B40, 03F65

An *integrally closed domain* R is an integral domain whose integral closure in its field of fraction is R itself. An element b is *integral* over an ideal I iff b satisfies an integral relation

$$b^n + u_1 b^{n-1} + \cdots + u_n = 0$$

with u_l in I^l. We can reformulate the definition of being integrally closed by stating that whenever b is integral over $\langle a \rangle$ then b belongs to $\langle a \rangle$. In this form, this definition makes sense even if R is an arbitrary ring (not necessarily a domain) and this characterizes the notion of *normal* ring. It can be checked that this is equivalent to the following: any localization of R at a prime ideal is an integrally closed integral domain [Ducos et al., 2004, Proposition 6.4].

This paper is mainly concerned with the analysis of the following classical result: if R is an integrally closed domain then so is $R[X]$. We first recall a proof which reduces this result to Kronecker's Theorem [Lombardi and Quitté, 2015, Theorem 3.3]. Interestingly, the argument depends in a crucial how we interpret constructively the notion of "integral domain". Logically, to be an integral domain can be stated as

(1) $$\forall x.\forall y.\ xy = 0 \rightarrow [x = 0 \vee y = 0]$$

which is classically, but not constructively, equivalent to

(2) $$\forall x.\ x = 0 \vee [\forall y.xy = 0 \rightarrow y = 0].$$

On this form, this means that any element is 0 or is regular. This Definition (2) is actually the usual definition of integral domain in constructive mathematics Lombardi and Quitté [2015], Mines et al. [1988]. With this definition the argument using Kronecker's Theorem makes sense constructively.

*Department of Computer Science, Chalmers, University of Göteborg, 41296 Göteborg, Sweden. Thierry.Coquand@cse.gu.se

†Laboratoire de Mathématiques. Université de Franche-Comté. F-25030 Besançon Cedex. henri.lombardi@univ-fcomte.fr

The definition (1) also has been considered in constructive algebra: a ring satisfying this condition is called a ring *without zero divisors* Lombardi and Quitté [2015]. The main part of this paper presents a proof that if R is a normal ring without zero divisors than so is $R[X]$. What is surprising is that this proof seems to require a technique which is used for analyzing argument involving *minimal* prime ideal [Lombardi and Quitté, 2015, Section XV-7]. Furthermore, the proof involves the introduction of the notion of *gcd tree* of two polynomials, which is important in other context Alonso et al. [2014]. Going from Definition (2) to Definition (1), classically equivalent, requires a much more complex argument.

The advantage of Definition (2) is that it is now relatively easy to conclude from this that, more generally, if R is normal (without any integrality condition) then so is $R[X]$. The last section analyzes a connected operation useful for studying the henselization of a local ring.

1 Constructible and Gcd trees

Given a reduced ring R we define the notion of *constructible tree* for R. This is a binary tree. To each node of this tree is associated a reduced ring, and R is associated to the root of the tree. Such a tree can only grow in the following way: we choose a leaf, and an element a of the ring S associated to this leaf. We add then two sons to this node: to the left branch we associate the ring $S[1/a]$ and to the right branch the ring $S/\sqrt{\langle a\rangle}$. Any such tree defines a partition of the constructible spectrum of R Johnstone [1986].

If we look at the leftmost branch of this tree, the leaf is of the form $R[1/(a_1 \cdots a_n)]$ and so is a localization of the ring R.

The main proofs in this note will be by induction on the size of a given constructible tree.

If we have two polynomials P and Q in $R[X]$ we can associate a constructible tree which corresponds to the formal computation of the gcd of P and Q. To each leaf S are also associated polynomials A, B, G, P_1, Q_1 in $S[X]$, with G monic, which witness the computation of the gcd of P and Q

$$AP_1 + BQ_1 = 1 \qquad P = GP_1 \qquad Q = GQ_1.$$

Notice that for building this tree, R does not need to be discrete (i.e. to have a decidable equality). Here is a simple example: $P = X^2$ and $Q = aX + b$. We start by the two branches $S_0 = R[1/a]$ and $S_1 = R/\sqrt{\langle a\rangle}$. Over S_0 we have the two branches $S_{00} = S_0[1/b]$ and $S_{01} = S_0/\sqrt{\langle b\rangle}$. Over S_1 we have the two branches $S_{10} = S_1[1/b]$ and $S_{11} = S_1/\sqrt{\langle b\rangle}$. The gcd is 1 over S_{00} and S_{10}, and is X over S_{01} and is X^2 over S_{11}.

This tree is called the *gcd tree* of P and Q.

If one of the polynomial is monic, one can reduce the size of this tree by using subresultants Apéry and Jouanoulou [2006].

2 Kronecker's Theorem

We shall only need a simple case of Kronecker's Theorem [Lombardi and Quitté, 2015, Theorem 3.3].

Theorem 2.1 *Let R be a ring, if $X^m + a_1X^{m-1} + \cdots + a_m$ divides a polynomial of the form $X^n + b_1X^{n-1} + \cdots + b_n$ in $R[X]$ then $a_1, \ldots, a_m$ are integral over the subring of R generated by $b_1, \ldots, b_n$.*

Proof. We introduce the splitting algebra[1] T of $X^n + b_1X^{n-1} + \cdots + b_n$ Lombardi and Quitté [2015] so that $X^n + b_1X^{n-1} + \cdots + b_n = (X - t_1)\cdots(X - t_n)$ in $T[X]$. The ring R embeds in T and a_i is a polynomial in $t_1, \ldots, t_n$. □

Corollary 2.2 *Let R be a ring, if $Y + a_0X^m + \cdots + a_m$ divides a polynominal of the form $Y^n + b_1Y^{n-1} + \cdots + b_n$ in $R[X, Y]$ then all coefficients $a_0, \ldots, a_m$ are roots of polynomials of the form $Z^l + p_1Z^{l-1} + \cdots + p_l$ where p_i is a homogeneous polynomial of degree i in $b_1, \ldots, b_n$ where b_j has weight j.*

Proof. It is enough to look at the case where $a_0, \ldots, a_m$ are indeterminates, and R is a polynomial ring on $a_0, \ldots, a_m$ and some other indeterminates. By replacing Y by X^N for N big enough, we get that each $a_0, \ldots, a_m$ is integral over $\mathbb{Z}[b_1, \ldots, b_n]$ and hence each a_k is root of a polynomial of the form $Z^l + p_1Z^{l-1} + \cdots + p_l$ where p_i is a polynomial in $b_1, \ldots, b_n$. By replacing Y by Y/c where c is another indeterminate, we get that p_i is homogeneous of degree i in $b_1, \ldots, b_n$ where b_j has weight j. □

Corollary 2.3 *Let R be a normal integral domain, then $R[X]$ is a normal integral domain.*

Proof. We assume given P and Q in $R[X]$ such that P is integral over $\langle Q\rangle$ and we want to show that P is in $\langle Q\rangle$ in $R[X]$. Let K be the total fraction field of R. Since R is an integral domain, we can consider R to be a subring of K. Since $K[X]$ is euclidean, we know that P is in $\langle Q\rangle$ in $K[X]$ and we have $cP = HQ$ for some regular element c. Since P is integral over $\langle Q\rangle$ we have a relation

$$P^n + A_1QP^{n-1} + \cdots + A_nQ^n = 0$$

with $A_1, \ldots, A_n$ in $R[X]$ and so we can write

$$Y^n + A_1cY^{n-1} + \cdots + A_nc^n = (Y - H)S(X, Y)$$

where $S(X, Y)$ is a monic polynomial in $R[X][Y]$. Using Corollary 2.2, it follows that all coefficients of H are integral over $\langle c\rangle$ and hence are in $\langle c\rangle$ since R is normal. We can then write $H = cH_1$ and so $c(P - QH_1) = 0$ in $R[X]$. It follows that we have $P = QH_1$ and hence P is in $\langle Q\rangle$ in $R[X]$. □

This is the argument we are going to adapt in the case where R is normal and without zero divisors.

3 Polynomial ring

We assume that R is normal without zero divisors and we show that $R[X]$ is normal. We assume given P and Q in $R[X]$ such that P is integral over $\langle Q\rangle$ and we want to show that P is in $\langle Q\rangle$ in $R[X]$.

Lemma 3.1 *If R is normal then R is reduced.*

Proof. If $b^2 = 0$ then b is integral over $\langle 0\rangle$ and so is in $\langle 0\rangle$. □

Lemma 3.2 *If R is normal then so is $R[1/a]$.*

[1] $T = R[X_1, \ldots, X_n]/J(f) = R[x_1, \ldots, x_n]$ where $J(f)$ is the ideal of symmetric relators necessary to identify $\prod_{j=1}^{n}(X - x_j)$ with $f(X)$ in $T[X]$. We let $x = x_1$ and the quotient ring $R[x] = R[X]/\langle f\rangle$ is identified with a subring of T. If $g(X, Y) = \frac{f(X)-f(Y)}{X-Y}$ then $g(x_1, X) = \prod_{i=2}^{n}(X - x_i)$ in $T[X]$ and $g(x_1, x_j) = 0$ for $j \geq 2$.

Proof. For c and b in R, if c is integral over $\langle b\rangle$ in $R[1/a]$ we have a relation $(a^N c)^n + u_1 b(a^N c)^{n-1} + \cdots + u_n b^n = 0$ with $u_1, \ldots, u_n$ in R. Since R is normal we have $a^N c$ in $\langle b\rangle$. □

Lemma 3.3 *If R is without zero divisors then so is $R[1/a]$.*

Proof. We take two elements $v = b/a^n$ and $w = c/a^m$ of $R[1/a]$ with b and c in R. If we have $vw = 0$ in $R[1/a]$ we have $a^p bc = 0$ in R for some $p \geqslant 0$. We have then $a^p b = 0$ in R or $a^p c = 0$ in R, which implies that $v = 0$ or $w = 0$ in $R[1/a]$. □

From now on in this section, we assume R to be a normal ring without zero divisors.

Lemma 3.4 *If P is integral over $\langle Q\rangle$ and is in $\langle Q\rangle$ in $R[1/a][X]$ then $a = 0$ or P is in $\langle Q\rangle$ in $R[X]$.*

Proof. We have H in $R[X]$ such that $a^N P = QH$ for some N. We write $c = a^N$. Since P is integral over $\langle Q\rangle$ we have a relation

$$P^n + A_1 Q P^{n-1} + \cdots + A_n Q^n = 0$$

with $A_1, \ldots, A_n$ in $R[X]$ and so

$$Q^n(H^n + A_1 c H^{n-1} + \cdots + A_n c^n) = 0$$

in $R[X]$. Hence either $Q = 0$ in which case $P = 0$ is in $\langle Q\rangle$ or we can write

$$Y^n + A_1 c Y^{n-1} + \cdots + A_n c^n = (Y - H) S(X, Y)$$

where $S(X, Y)$ is a monic polynomial in $R[X][Y]$. Using the corollary of Kronecker's Theorem 2.2, it follows that all coefficients of H are integral over $\langle c\rangle$ and hence are in $\langle c\rangle$ since R is normal. We can then write $H = cH_1$ and so $c(P - QH_1) = 0$ in $R[X]$. It follows that we have $c = 0$, that is equivalent to $a = 0$, or $P = QH_1$ and hence P is in $\langle Q\rangle$ in $R[X]$. □

Lemma 3.5 *If we have P and Q in $R[X]$ and a constructible tree for R such as, at all leaves S of this tree, we have P in $\langle Q\rangle$ in $S[X]$. Then P is in $\langle Q\rangle$ in $R[X]$.*

Proof. We look at the leftmost branch of this tree, indexed by elements $a_1, \ldots, a_l$, so that $S = S'[1/a_l]$ where $S' = R[1/(a_1 \cdots a_{l-1})]$ is without zero divisors by Lemma 3.3 and is normal by Lemma 3.2. Using Lemma 3.4 we get that $a_l = 0$ in S' or P is in $\langle Q\rangle$ in $S'[X]$. In the second case, we can shorten the leftmost branch to $a_1, \ldots, a_l$ and get a smaller tree. In the first case where $a_l = 0$ in S', this means that the right son $S'/\langle a\rangle$ of S' is equal to S' and we also can shorten the tree. We conclude by tree induction. □

Theorem 3.6 *If R is normal and without zero divisors then so is $R[X]$.*

Proof. We take P and Q in $R[X]$ and we assume that we have a relation

$$P^n + A_1 Q P^{n-1} + \cdots + A_n Q^n = 0$$

with $n \geqslant 1$ and $A_1, \cdots, A_n$ in $R[X]$. We have to show that P is in $\langle Q\rangle$ in $R[X]$.

We look now at the gcd tree of P and Q as defined in the first section. At all leaves S of this tree, we have P_1, Q_1, G, A, B in $S[X]$ satisfying

$$P = GP_1, \quad Q = GQ_1, \quad AP_1 + BQ_1 = 1$$

in $S[X]$ and G is monic. Since G is monic and

$$P^n + A_1QP^{n-1} + \cdots + A_nQ^n = G^n(P_1^n + A_1Q_1P_1^{n-1} + \cdots + A_nQ_1^n) = 0$$

we have

$$P_1^n + A_1Q_1P_1^{n-1} + \cdots + A_nQ_1^n = 0$$

and Q_1 divides P_1^n. With $AP_1 + BQ_1 = 1$ this implies that Q_1 is a unit and so P is in $\langle Q \rangle$ in $S[X]$. We can now apply Lemma 3.5. □

4 Normal ring

We say that the ring is *locally* without zero divisors [Lombardi and Quitté, 2015, Lemma VIII-3.2] if, and only if, whenever $ab = 0$ then there exists u such that $ua = 0$ and $(1-u)b = 0$. These rings are often called pf-rings. In this note, only the notion of rings without zero divisors and locally without zero divisors will play a role.

Lemma 4.1 *If R is normal then R is locally without zero divisors.*

Proof. If $ab = 0$ then $b^2 - (a+b)b = 0$ so b is integral over $\langle a+b \rangle$ and so is in $\langle a+b \rangle$. We can write $b = (a+b)u$ and so $ua = (1-u)b$. This implies $ua^2 = (1-u)ba = 0$ and so $ua = (1-u)b = 0$ since R is reduced. □

Theorem 4.2 *If R is normal then so is $R[X]$.*

Proof. By Lemma 4.1, R is locally without zero divisors. Assume then that a polynomial $P \in R[X]$ is integral over $\langle Q \rangle$ in $R[X]$. Following the proof of Theorem 3.6, each time we use $ab = 0 \to a = 0$ or $b = 0$, we split the "current ring $R[1/v]$" in two rings $R[1/vu]$ and $R[1/v(1-u)]$ by using an u such that $ua = 0$ and $(1-u)b = 0$. We find finally $u_1, \ldots, u_m$ in R such that $\langle u_1, \ldots, u_m \rangle = 1$ and P belongs to $\langle Q \rangle$ in each $R[1/u_j][X]$. It follows that P is in $\langle Q \rangle$ as required. □

5 The ring $R_{\{f\}}$

Let f be a monic polynomial in $R[X]$. We can consider the extension $S = R[X]/\langle f \rangle$ where f has a root x. We let f_X be the formal derivative of f w.r.t. X, and we define $R_{\{f\}}$ to be the localization $S[1/f_X(x)]$. This construction is important to study the properties of henselization of a local ring Raynaud [1970].

The goal of this section is to show that $R_{\{f\}}$ is normal whenever R is normal. As in the previous section, we can first assume that R is without zero divisors, and then use that a normal ring is locally without zero divisors to conclude. So in the rest of the section, we assume that R is a normal ring without zero divisors.

If $f = gh$ is the product of two monic polynomials g and h we have $R_{\{f\}}$ isomorphic to $R_{\{g\}}[1/h(x)] \times R_{\{h\}}[1/g(x)]$. This remark is important since by using Lemma 3.2 we can reason by induction on the degree of f to show that $R_{\{f\}}$ is normal if R is normal.

Lemma 5.1 *If R is normal without zero divisors, and a in R and $T = R[1/a]$ and $f = gf_1$ with g and f_1 monic in $T[X]$ then we have g and f_1 in $R[X]$ or $a = 0$.*

Proof. Using Kronecker's Theorem 2.1, each coefficient of g and f_1 is integral over R. Since R is normal and without zero divisors, this implies that $a = 0$ or g and f_1 are in $R[X]$. □

We have the trace map $\mathsf{tr} : S \to R$. If we introduce the splitting algebra [Lombardi and Quitté, 2015, Definition III-4.1] of f and write $f = (X - x_1) \cdots (X - x_n)$ with $x = x_1$ then the trace of $h(x) \in S$ is $h(x_1) + \cdots + h(x_n)$. If $v = h(x)$ in S is integral over $\langle a \rangle_S$ with a in R then all elements $h(x_1), \ldots, h(x_n)$ are integral over $\langle a \rangle_R$ and so $\mathsf{tr}(v)$ is also integral over $\langle a \rangle_X$ and so is in $\langle a \rangle_X$ since R is normal. Also if we write $f(X) - f(Y) = (X - Y)g(X, Y) = \sum_i g_i(Y)X^i$, we have $f_X(T) = g(T, T)$ and $g(x_1, x_j) = 0$ for $j \neq 1$. So we get for all $v = h(x) = h(x_1)$ in S

$$f_X(x)h(x) = g(x_1, x_1)h(x_1) = \sum\nolimits_i g_i(x_1)h(x_1)\ x_1^i$$

and for $j \neq 1$

$$0 = g(x_1, x_j)h(x_j) = \sum\nolimits_i g_i(x_j)h(x_j)\ x_1^i$$

so that, by summation, we get Tate's formula [Raynaud, 1970, Chapter VII, 1]

$$f_X(x)v = \sum\nolimits_i \mathsf{tr}(g_i(x)v)\ x^i.$$

Since each $g_i(x)$ is integral over R, we can state the following lemma.

Lemma 5.2 *If R is normal, if a in R and if v in S is integral over $\langle a \rangle_S$ then $f_X(x)v$ is in $\langle a \rangle_S$.*

Theorem 5.3 *If R is normal then $R_{\{f\}}$ is normal.*

Proof. We assume given p, q in $R[X]$ such that $p(x)$ is integral over $\langle q(x) \rangle$ in S so that we have a relation $p(x)^n + u_1(x)q(x)p(x)^{n-1} + \cdots + u_n(x)q(x)^n = 0$. The goal is to show that $p(x)$ is in $q(x)S[f_X(x)^{-1}]$.

We look at the gcd tree of q and f, and the leftmost branch of this tree. At the leaf of this branch we have a list of elements that we force to be invertible $a_1, \ldots, a_n$ and q_1, f_1, g, A, B in $R[a^{-1}]$ with $a = a_1 \ldots a_n$ such that

$$f = gf_1 \qquad q = gq_1 \qquad 1 = Af_1 + Bq_1.$$

Furthermore g and hence f_1 are monic since f is monic.

If $f = f_1$ we have $g = 1$ and $q = q_1$. In this case we have $c = Af + Bq$ where $c = (a_1 \ldots a_n)^m$ for some m and so we have $c = B(x)q(x)$ in $S = R[X]/\langle f \rangle$. We then have a relation

$$(p(x)B(x))^n + u_1(x)c(p(x)B(x))^{n-1} + \cdots + u_n(x)c^n = 0$$

and hence, by Lemma 5.2, we get that $p(x)B(x)$ is in $\langle c \rangle$ in $S[f_X(x)^{-1}]$. Hence we have $l(x)$ in S and N such that

$$f_X(x)^N p(x)B(x) = cl(x) = q(x)B(x)l(x)$$

and so

$$c(p(x)f_X(x)^N - l(x)q(x)) = 0.$$

We have then $c = 0$ or $p(x)$ is in $\langle q(x) \rangle$ in $R[f_X(x)^{-1}]$. So either we have the desired conclusion that $p(x)$ is in $\langle q(x) \rangle$ or we have $a_n = 0$ in $R[1/(a_1 \cdots a_{n-1})]$ and we can shorten the computation tree of the gcd of f and q.

If f and f_1 have not the same degree, we have found a proper decomposition $f = gf_1$ of f in $R[1/a]$ with $a = a_1 \cdots a_n$. In this case, since R is normal, by Lemma 5.1, we have two subcases

- either g and f_1 are in $R[X]$ and we can conclude by induction on the degree of f, using that $R_{\{f\}}$ isomorphic to $R_{\{g\}}[1/f_1] \times R_{\{f_1\}}[1/g]$,

- or $a = 0$ and as in the previous case, we can shorten the computation tree of the gcd of f and q.

□

As in [Lombardi and Quitté, 2015, VIII-4.4], we say that a ring is a Prüfer ring if it is arithmetic and reduced. A coherent Prüfer ring is an arithmetic *pp*-ring.

Corollary 5.4 *If R is a Prüfer ring of Krull dimension $\leqslant 1$ then so is $R_{\{f\}}$.*

Proof. We use the fact that a ring is normal coherent ring of Krull dimension $\leqslant 1$ if, and only if, it is Prüfer and of Krull dimension $\leqslant 1$ Ducos et al. [2004]. We have shown that $R_{\{f\}}$ is normal. Since $S = R[X]/\langle f\rangle$ is an integral extension of R it is also of Krull dimension $\leqslant 1$ Coquand et al. [2009] and so is its localization $R_{\{f\}}$. Finally, S is a finite free R-module, and so it is coherent if R is coherent and so is its localization $R_{\{f\}}$. □

This gives an alternative proof to the main result of Coquand et al. [2010], that $R_{\{f\}}$ is Prüfer when $R = k[X]$, in the case where f is monic in Y. It is possible however to reduce the general case to this case, by a change of variables.

References

M. E. Alonso, T. Coquand, and H. Lombardi. Revisiting Zariski main theorem from a constructive point of view. *J. Algebra*, 406:46–68, 2014. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2014.02.003. URL http://dx.doi/10.1016/j.jalgebra.2014.02.003. 2

François Apéry and Jean-Pierre Jouanoulou. *Élimination: le cas d'une variable.* Hermann, Paris, 2006. 2

Thierry Coquand, Lionel Ducos, Henri Lombardi, and Claude Quitté. Constructive Krull dimension. I. Integral extensions. *J. Algebra Appl.*, 8(1):129–138, 2009. ISSN 0219-4988. doi: 10.1142/S0219498809003199. URL http://dx.doi/10.1142/S0219498809003199. 7

Thierry Coquand, Henri Lombardi, and Claude Quitté. Curves and coherent Prüfer rings. *J. Symbolic Comput.*, 45(12):1378–1390, 2010. ISSN 0747-7171. doi: 10.1016/j.jsc.2010.06.016. URL http://dx.doi/10.1016/j.jsc.2010.06.016. 7

L. Ducos, H. Lombardi, C. Quitté, and M. Salou. Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind. *J. Algebra*, 281(2):604–650, 2004. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2004.06.030. URL http://dx.doi/10.1016/j.jalgebra.2004.06.030. 1, 7

Peter T. Johnstone. *Stone spaces*, volume 3 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. ISBN 0-521-33779-8. Reprint of the 1982 edition. 2

Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods*, volume 20 of *Algebra and Applications*. Springer, Dordrecht, revised edition, 2015. ISBN 978-94-017-9943-0; 978-94-017-9944-7. doi: 10.1007/978-94-017-9944-7. URL http://dx.doi/10.1007/978-94-017-9944-7. Finite projective modules, Translated from the French by Tania K. Roblot. 1, 2, 3, 5, 6, 7

Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra*. Universitext. Springer-Verlag, New York, 1988. ISBN 0-387-96640-4. doi: 10.1007/978-1-4419-8640-5. URL http://dx.doi/10.1007/978-1-4419-8640-5. 1

Michel Raynaud. *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin-New York, 1970. 5, 6