ELSEVIER Journal of Pure and Applied Algebra 103 (1995) 303–311

JOURNAL OF PURE AND APPLIED ALGEBRA

Elasticity for integral-valued polynomials

Paul-Jean Cahen[a,*], Jean-Luc Chabert[b]

[a] Service 322, Faculté des Sciences de Saint-Jérôme, 13397 Marseille Cedex 20, Université d'Aix-Marseille III-URA 225, France

[b] Institut Supérieur des Sciences et Techniques, Université de Picardie, 48 rue Raspail, 02109 Saint Quentin, France

Communicated by C.A. Weibel; received 11 October 1993, revised 25 April 1994

Abstract

The elasticity of a domain is the upper bound of the ratios of lengths of two decompositions in irreducible factors of nonzero nonunit elements. We show that for a large class of Noetherian domains, including any domain contained in a number field (but not a field), the elasticity of the ring of integral-valued polynomials is infinite.

0. Introduction

A domain D is said to be *atomic* if every nonzero nonunit element of D can be decomposed into products of irreducible elements (*atoms*); this is for example the case for Noetherian domains and more generally for domains which satisfy the ascending chain condition on principal ideals (or ACCP). If the decomposition is unique, D is a *unique factorization domain* (in short a UFD), but it may not be, it may even happen that two decompositions of the same element do not have the same number of irreducible factors. The *elasticity* of D is then defined as $\rho(D) = \mathrm{Sup}\{m/n \mid x_1 \cdots x_m = y_1 \cdots y_n$, for x_i, y_j irreducible elements of $D\}$. This concept was introduced by Valenza [15] for rings of integers in an algebraic number field, then was studied by Steffan [14] for a Dedekind domain with finite divisor class group and by Anderson and others [1–3] in more general settings.

In this paper D is an integral domain with quotient field K, and we study the elasticity of the ring $\mathrm{Int}(D)$ of *integral-valued polynomials* over D, i.e. $\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subset D\}$. Integral-valued polynomials over rings of integers in an algebraic number field have been studied by Polya [12] and Ostrowsky [11], over Dedekind domains by Brizolis [5], by the authors in various general situations [6–10] and by others in quite a few recent papers. We show that the elasticity of $\mathrm{Int}(D)$ is infinite in most cases; in particular the ring $\mathrm{Int}(\mathbb{Z})$ of integral-valued polynomials with rational coefficients provides quite a natural and easy example of infinite elasticity.

SSDI 0022-4049(94)00108-1

In Section 1 we recall a few results on the ascending chain condition on principal ideals. They give a fairly large class of domains (including in particular Noetherian domains) such that Int(D) is atomic and for which it is relevant to study elasticity. Finally we give a straightforward proof that the elasticity of Int($\mathbb{Z}$) is infinite.

In Section 2 we study the irreducibility of polynomials in Int(D): in particular it is enough that f be irreducible in $K[X]$ and not divisible in Int(D) by any nonunit element of D; we also give examples of polynomials which are irreducible in Int(D) but not in $K[X]$.

In the last section we finally give (technical but quite general) sufficient conditions for the elasticity of Int(D) to be infinite: it is enough that D be a Noetherian domain with a principal ideal Dt such that the quotient D/Dt is finite. This applies in particular to any domain (which is not a field) contained in a number field or a function field over a finite field. In fact we could not provide any example where the elasticity of Int(D) is finite, except when Int(D) is *trivial*, i.e. equal to the ring $D[X]$ of polynomials with coefficients in D.

1. Atomicity

Let D be a domain with quotient field K. Recall that D is said to be *atomic* if every nonzero nonunit element can be decomposed into products of irreducible elements. In this paper we are interested in irreducible elements of Int(D) and we first record a lemma (the proof of which is immediate).

Lemma 1.1. (i) *The units of* Int(D) *are the units of D.*
(ii) *An element of D is irreducible in* Int(D) *if and only if it is irreducible in D.*

From this we get immediately:

Proposition 1.2. *If* Int(D) *is atomic then D is atomic.*

Note that (conversely) Roitman [13] has shown how to construct an atomic integral domain D such that $D[X]$ is not atomic; such a D can be chosen so that $\text{Int}(D) = D[X]$.

A domain D which satisfies ACCP (i.e. the ascending chain condition on principal ideals) is atomic. For the sake of completeness, we then prove the following that is a particular case of Corollary 7.6 in [1]:

Theorem 1.3. *The ring* Int(D) *satisfies ACCP if and only if D satisfies ACCP.*

Proof. The condition is necessary: let a_nD be in increasing sequence of principal ideals of D; by hypothesis the sequence $a_n\text{Int}(D)$ is stationary, hence there exists n_0 such that, for $n \geq n_0$, $a_n\text{Int}(D) = a_{n_0}\text{Int}(D)$, thus $a_n = \lambda_n a_{n_0}$, where λ_n is a unit of

$\mathrm{Int}(D)$ (hence a unit of D) and $a_n D = a_{n_0} D$. The condition is sufficient: let $f_n \,\mathrm{Int}(D)$ be an increasing sequence of (nonzero) principal ideals of $\mathrm{Int}(D)$; the sequence $f_n K[X]$ of principal ideals of $K[X]$ is stationary and there exists n_0 such that, for $n \geq n_0$, $f_n K[X] = f_{n_0} K[X]$, hence $f_n = \lambda_n f_{n_0}$, where λ_n is a nonzero element of K. If ever $D = K$, then $\mathrm{Int}(D) = K[X]$ and we are done. If $D \neq K$, then D is infinite and there exists an element a of D such that $f_{n_0}(a) \neq 0$. The sequence $f_n(a)D$ is increasing, thus stationary by hypothesis. Hence there exists $m_0 \geq n_0$ such that, for $n \geq m_0$, $f_n(a) = \mu_n f_{m_0}(a)$, where μ_n is a unit of D. Hence $f_n = \mu_n f_{m_0}$ and thus $f_n \,\mathrm{Int}(D) = \mu_n f_{m_0} \,\mathrm{Int}(D)$. □

Thus, if D satisfies ACCP (and in particular if D is Noetherian), $\mathrm{Int}(D)$ is atomic.

Assuming that $\mathrm{Int}(D)$ is atomic we shall then be interested in the elasticity of $\mathrm{Int}(D)$, i.e. the upper bound $\mathrm{Sup}\{m/n \mid f_1 \cdots f_m = g_1 \cdots g_n,$ for f_i, g_j irreducible elements of $\mathrm{Int}(D)\}$. Here is an other immediate consequence to Lemma 1.1:

Proposition 1.4. *The elasticity of* $\mathrm{Int}(D)$ *is greater or equal to the elasticity of* D.

If, for each nonzero nonunit element α of D, there is a bound $L_D(\alpha)$ on the lengths of factorizations of α into products of irreducible elements, the domain D is said to be a *bounded factorization domain* (or a BFD [2]). It is known that $\mathrm{Int}(D)$ is a BFD if and only if D is a BFD [1, Corollary 7.6]. More precisely we may record the following:

Proposition 1.5. *Let D be a* BFD, *Then, for each $f \in \mathrm{Int}(D)$ and each $\alpha \in D$*:

$$L_{\mathrm{Int}(D)}(f(X)) \leq L_{K[X]}(f(X)) + L_D(f(\alpha)) \leq \deg(f(X)) + L_D(f(\alpha))$$

with the following convention: $L_D(\alpha) = 0$ if α is a unit in D and $L_D(0) = \infty$.

Proof. First we note that the hypothesis on D implies the ascending chain condition on principal ideals of D hence, by Theorem 1.3, the atomicity of $\mathrm{Int}(D)$. If $f = \lambda_1 \cdots \lambda_s \cdot g_1 \cdots g_t$ where the λ_i are nonzero nonunit elements of D and the g_j are nonconstant elements of $\mathrm{Int}(D)$, then obviously $t \leq L_{K[X]}(f(X)) \leq \deg(f(X))$ and $s \leq L_D(\lambda_1 \cdots \lambda_s) \leq L_D(f(\alpha))$ for each $\alpha \in D$ since $\lambda_1 \cdots \lambda_s$ divides $f(\alpha)$ in D. □

In the last section we shall see that, in most cases, the elasticity of $\mathrm{Int}(D)$ turns out to be infinite; but before going into these general results we give here a straightforward proof of this fact, for the principal ideal domain $\mathbb{Z}$ whose elasticity is one.

Theorem 1.6. *The elasticity of* $\mathrm{Int}(\mathbb{Z})$ *is infinite.*

Proof. Recall that the binomials

$$\binom{X}{n} = 1/n! \prod_{i=0}^{n-1} (X - i)$$

are integral-valued (and form a basis of $\text{Int}(\mathbb{Z})$ as a $\mathbb{Z}$-module). Write

$$n!\binom{X}{n} = \prod_{i=0}^{n-1} (X - i);$$

it is clear that $(X - i)$ is irreducible (and will follow from more general results below, Example 2.3), hence there are n irreducible factors on the right-hand side whereas, on the left-hand side, $n!$ admits as many irreducible factors in $\text{Int}(\mathbb{Z})$ as it does in $\mathbb{Z}$ (Lemma 1.1). We conclude with a proof that this number of factors may eventually be greater than nm, whatever m. Let $n = p!$, where p is prime. Among the factors $1, 2, \ldots, n$ of $n!$, there are $n/2$ multiples of 2, $n/3$ multiples of 3, $n/5$ multiples 5, and so on up to p, hence $n!$ admits (at least) $n(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p})$ irreducible factors. We are done, since the series of the inverses of primes is divergent. □

2. Irreducible polynomials

In this section we describe irreducible elements of $\text{Int}(D)$: on the one hand there are the elements of D (constant polynomials) which are irreducible in D [Lemma 1.1], on the other hand the next proposition and its corollaries will provide examples of nonconstant irreducible polynomials.

Proposition 2.1. *Let f be a polynomial of* $\text{Int}(D)$ *which is irreducible in* $K[X]$. *Then the following assertions are equivalent:*

(i) *f is irreducible in* $\text{Int}(D)$.

(ii) *For each $a \in D$, $(f/a) \in \text{Int}(D)$ if and only if a is a unit of D.*

Proof. If f is irreducible in $\text{Int}(D)$ and $g = (f/a) \in \text{Int}(D)$, then $f = ag$ and thus a is a unit since g is not (g is nonconstant). Conversely, if f is irreducible in $K[X]$ and if $f = gh$ in $\text{Int}(D)$, necessarily one factor, say h, is in D; letting $a = h$, then $(f/a) = g \in \text{Int}(D)$ and condition (ii) implies that a is a unit. □

Corollary 2.2. *Let f be a polynomial of* $\text{Int}(D)$ *such that*

(i) *f is irreducible in $K[X]$,*

(ii) *for every maximal ideal $\mathfrak{M}$ of D, there exists $\alpha \in D$ such that $f(\alpha) \notin \mathfrak{M}$.*

Then f is irreducible in $\text{Int}(D)$.

Proof. Let $a \in D$ and suppose that $(f/a) \in \text{Int}(D)$. For very maximal ideal $\mathfrak{M}$ of D, there exists $\alpha \in D$ such that $f(\alpha) \notin \mathfrak{M}$; hence $a \notin \mathfrak{M}$, since $(f(\alpha)/a) \in D$. Therefore a is a unit of D and f is irreducible in $\text{Int}(D)$ from the previous proposition. □

Example 2.3. For each $a \in D$, $(X - a)$ is irreducible in $\text{Int}(D)$.

Remark 2.4. In contradiction to condition (ii) of the previous proposition, condition (ii) of Corollary 2.2 is not necessary as the next example shows.

Example 2.5. Assume D is a Dedekind domain with a maximal ideal $\mathfrak{M} = (u, v)$ which is not principal but generated by two elements u and v. If moreover $D/\mathfrak{M}$ is finite, then $\mathrm{Int}(D)$ is not *trivial*, i.e. $\mathrm{Int}(D) \neq D[X]$ [8, p. 304]). Let $f = uX + v$, clearly, f is irreducible in $K[X]$. Moreover if $a \in D$ and $(f/a) \in \mathrm{Int}(D)$, then $f(0)/a = v/a$ and $f(1)/a = (u+v)/a$ are in D; thus a divides u and v and the principal ideal Da contains $\mathfrak{M} = (u, v)$. In conclusion a is a unit and therefore f is irreducible in $\mathrm{Int}(D)$ (Proposition 2.1). However, for each $\alpha \in D, f(\alpha) = u\alpha + v$, hence $f(\alpha) \in \mathfrak{M}$.

The next corollary is a particular case of Corollary 2.2 or Proposition 1.5:

Corollary 2.6. *Let f be a polynomial* $\mathrm{Int}(D)$ *such that*
(i) *f is irreducible in $K[X]$,*
(ii) *there exists $\alpha \in D$ such that $f(\alpha)$ is a unit of D.*
Then f is irreducible in $\mathrm{Int}(D)$.

The next proposition is the key to the general results of the last section; it gives more examples of irreducible polynomials under the hypothesis there exists a (nontrivial) discrete valuation v on the field K. Clearly this implies the existence of an element b of D such that $v(b) \neq 0$ (if not v would be null on every element of K).

Proposition 2.7. *Assume there exists a discrete valuation v on K. Then, for each $a \in D$, each $b \in D$ such that $v(b) \neq 0$ and each positive integer m prime to $v(b)$, the polynomial $f = (X - a)^m + b$ is irreducible in* $\mathrm{Int}(D)$.

Proof. We prove first that f is irreducible in $K[X]$. Let x be a root of f in an algebraic closure of K, and v' a valuation extending v to $K(x)$, then $mv'(x - a) = v(b)$. From Bezout there are integers α and β such that $\alpha v(b) - \beta m = 1$. Let t in $K(x)$ be such that $v'(t) = 1$ and consider $y = (x - a)^\alpha / t^\beta$; then one has $v'(y) = \alpha v'(x - a) - \beta v(t) = (\alpha/m)v(b) - \beta = 1/m$. Therefore the ramification index of v' over v is m, $K(x)$ is an extension of degree m of K and f is the minimal polynomial of x. We can conclude that f is irreducible in $\mathrm{Int}(D)$ from Corollary 2.2. Indeed, for every maximal ideal $\mathfrak{M}$ of D, there exists α in D such that $f(\alpha) \notin \mathfrak{M}$: either $b \in \mathfrak{M}$, then choose α such that $(\alpha - a) \notin \mathfrak{M}$, or $b \notin \mathfrak{M}$, then choose α such that $(\alpha - a) \in \mathfrak{M}$. □

We conclude this section with examples of polynomials which are irreducible in $\mathrm{Int}(D)$ *but not* in $K[X]$.

Example 2.8. For each $n \geq 1$,

$$\binom{X}{n} = 1/n! \prod_{i=0}^{n-1} (X - i)$$

is irreducible in Int($\mathbb{Z}$). Recall indeed that if $f \in$ Int($\mathbb{Z}$) is of degree at most n, then $(n!)f \in \mathbb{Z}[X]$. So if

$$\binom{X}{n} = gh,$$

with g and h respectively of degree r and s, then

$$(r!)(s!)\binom{X}{n} \in \mathbb{Z}[X],$$

and thus

$$\frac{(r!)(s!)}{n!} \in \mathbb{Z}.$$

Therefore

$$\binom{n}{r} = 1,$$

hence $r = 0$ or $r = n$ and g or h is in $\mathbb{Z}$. Say g in $\mathbb{Z}$, then $(n!)h \in \mathbb{Z}[X]$ and the leading coefficient of

$$n!\binom{X}{n} = n!gh$$

is 1, hence $g = \pm 1$.

3. Pseudo-principal ideals and elasticity

We start this section with an easy, although technical lemma which is really the key of next results:

Lemma 3.1. *Assume there is a (nontrivial) discrete valuation v on K and an ideal $\mathfrak{q}$ of D such $D/\mathfrak{q}$ is finite. Then, for every integer $n \geq 1$, there exists a product of q irreducible elements of* Int(D) *with values in $\mathfrak{q}^n$, where q is the cardinal of $D/\mathfrak{q}$.*

Proof. First, there exists $b \in \mathfrak{q}$ such that $v(b) \neq 0$. Indeed there exists $x \in D$ such that $v(x) \neq 0$, so consider any $y \in \mathfrak{q}$: either $v(y) \neq 0$, then we are done with $b = y$, or $v(y) = 0$, then take $b = xy$. Let then $u_0, u_1, \ldots, u_{q-1}$ be a set of representatives of $D/\mathfrak{q}$. If m is an integer prime to $nv(b)$, the polynomials $f_i = (X - u_i)^m + b^n$ are irreducible (Proposition 2.7); if moreover $m > n$, the product $\prod_{i=0}^{q-1} f_i$ takes its values in $\mathfrak{q}^n$ since, for any $\alpha \in D$, there is i, $1 \leq i \leq q-1$, such that $(\alpha - u_i) \in \mathfrak{q}$, hence $f_i(\alpha) \in \mathfrak{q}^n$. □

Recall that an ideal $\mathfrak{q}$ of a ring D is said to be *pseudo-principal* if there is an integer k and a nonunit $t \in D$, such that $\mathfrak{q}^k \subset Dt$ (7, Definition 5.1); the following will lead to various generalizations of Theorem 1.6:

Theorem 3.2. *Let D be a domain with quotient field K such that*
(i) $\text{Int}(D)$ *is atomic*,
(ii) *there is a (nontrivial) discrete valuation v on K*,
(iii) *there is a pseudo-principal ideal* $\mathfrak{q}$ *of D such that* $D/\mathfrak{q}$ *is finite.*
Then the elasticity of $\text{Int}(D)$ *is infinite.*

Proof. Let n be any integer. There exist a nonunit t in D and an integer k such that $\mathfrak{q}^k \subset Dt$, hence $\mathfrak{q}^{kn} \subset Dt^n$. From Lemma 3.1 there is a product $\prod_{i=0}^{q-1} f_i$ of irreducible factors of $\text{Int}(D)$ with values in $\mathfrak{q}^{kn}$, thus $h = 1/t^n \prod_{i=0}^{q-1} f_i$ is integral valued; writing $t^n h = \prod_{i=0}^{q-1} f_i$, there are (at least) $n+1$ factors on the left-hand side and exactly q irreducible factors on the right. □

The first two conditions of Theorem 3.2 are satisfied for Krull or Noetherian domains, hence we derive:

Corollary 3.3. *Let D be a Krull or a Noetherian domain with a pseudo-principal ideal* $\mathfrak{q}$ *such that* $D/\mathfrak{q}$ *is finite. Then the elasticity of* $\text{Int}(D)$ *is infinite.*

Krull and Noetherian domains are particular cases of Mori domains (i.e. domains which satisfy the ascending chain condition on divisorial ideals) which in turn satisfy the ascending chain condition on principal ideals, then we ask:

Question 1. Is there always a (non trivial) discrete valuation on the field of fractions of a Mori domain or more generally of a domain which satisfies ACCP?

Remark 3.4. In the Noetherian case, if $\mathfrak{q}$ is an ideal such that $D/\mathfrak{q}$ is finite, then $D/\mathfrak{q}^k$ is finite for every integer k; so if $\mathfrak{q}$ is pseudo-principal, i.e. $\mathfrak{q}^k \subset Dt$, the principal ideal Dt is itself such that D/Dt is finite. The next example shows however that, in general, there may be a pseudo-principal ideal with finite quotient ring, but no principal ideal with the same property.

Example 3.5. Let k be a finite field, L an infinite extension of k and $V = L[[t]]$, the ring of formal power series with coefficients in L. Consider the "$D + M$" construction $R = k + tL[[t]]$. Since V satisfies the ascending chain condition on principal ideals (indeed V is a discrete valuation domain) and k is a field, it is easily seen (and classical, see for example [4, Theorem 12]) that R itself satisfies the ascending chain condition on principal ideals (indeed if two principal ideals of R are such that $Ra \subseteq Rb$, then $Ra = Rb$ if and only if $Va = Vb$). The maximal ideal $\mathfrak{M} = tL[[t]]$, shared by R and V, is such that $R/\mathfrak{M} = k$ is finite and $\mathfrak{M}^2 \subset Rt$; hence $\mathfrak{M}$ is a pseudo-principal ideal with finite residue field. Therefore the elasticity of $\text{Int}(R)$ is infinite [Theorem 3.2], whereas the elasticity of R is 1 (by Example 3.7 of [1]). However, for every nonunit $x \in R$, i.e. $x \in \mathfrak{M}$, R/Rx is infinite: indeed if $\lambda \in L$ and $\mu \in L$, then $\lambda x \in R$ and $\mu x \in R$; but

$(\lambda x - \mu x) \in Rx$ if and only if $(\lambda - \mu) \in k$; thus the cardinal of R/Rx is at least the cardinal of L/k.

From Corollary 3.3, we get the following generalization of Theorem 1.6:

Corollary 3.6. *Let D be a one-dimensional Noetherian domain with finite residue fields. Then the elasticity of* $\mathrm{Int}(D)$ *is infinite.*

Proof. For any nonzero nonunit $t \in D$, Dt contains a power of its radical hence a product of finitely many maximal ideals with finite residue fields, therefore D/Dt is finite. □.

Corollary 3.7. *Let D be a domain, which is not a field, contained in an algebraic number field or a function field over a finite field. Then the elasticity of* $\mathrm{Int}(D)$ *is infinite.*

The hypotheses of Corollary 3.6. are certainly too strong, indeed it would be enough to suppose there exists *one* nonunit $t \in D$ such that D/tD is finite. In fact we ask:

Question 2. Is there any one dimensional Noetherian domain D such that one residue field at least is finite and the elasticity of $\mathrm{Int}(D)$ is finite? More generally, is there any example of a domain D such that $\mathrm{Int}(D) \neq D[X]$ and the elasticity of $\mathrm{Int}(D)$ is finite?

We conclude with principal ideal domains for which we have a complete characterization:

Corollary 3.8. *Let D be a principal ideal domain. If there is a maximal ideal* $\mathfrak{M}$ *of D such that* $D/\mathfrak{M}$ *is finite, then the elasticity of* $\mathrm{Int}(D)$ *is infinite otherwise the elasticity of* $\mathrm{Int}(D)$ *is* 1.

Proof. If every residue field of D is infinite, then $\mathrm{Int}(D) = D[X]$ is a unique factorization domain, otherwise there is a principal ideal with finite residue ring and the elasticity of $\mathrm{Int}(D)$ is infinite [Corollary 3.3]. □

Acknowledgements

The authors thank the referee for his useful comments.

References

[1] D.D. Anderson, D.F. Anderson, and M. Zafrullah, Rings between $D[X]$ and $K[X]$, Houston J. Math. 17 (1991) 109–129.

[2] D.D. Anderson and D.F. Anderson, Elasticity of factorizations in integral domains, J. Pure Appl. Algebra 80, (1992) 217–235.
[3] D.D. Anderson, D.F. Anderson, S. Chapman and W. Smith, Rational elasticity of factorizations in Krull domains, Proc. Amer. Math. Soc. 117 (1993) 37–43.
[4] V. Barucci, D. Dobbs and M. Fontana, Conducive integral domains as pullbacks, Manuscripta Math. 54 (1986) 261–277.
[5] D. Brizolis, Ideals in rings of integer values polynomials, J. Reine Angew. Math. 285 (1976) 28–52.
[6] P-J. Cahen, Polynômes à valeurs entières, Canad. J. Math 24 (1972) 747–754.
[7] P-J. Cahen, Dimension de l'anneau des polynômes à valeurs entières, Manuscripta Math. 67 (1990) 333–343.
[8] P-J. Cahen and J-L. Chabert, Coefficients et valeurs d'un polynôme, Bull. Sci. Math. (2) 95 (1971) 295–304.
[9] P-J. Cahen and Y. Haouat, Polynômes à valeurs entières sur un anneau de pseudovaluation, Manuscripta Math. 61 (1988) 23–31.
[10] J-L. Chabert, Les idéaux premisers de l'anneau des polynômes à valeurs entières, J. Reine Angew. Math. 293/294, (1977) 275–283.
[11] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, J. Reine Angew. Math. 149 (1919) 117–124.
[12] G. Polya, Uber ganzwertige Polynome in algebraischen Zahlkörpern, J. Reine Angew. Math. 149 (1919) 97–116.
[13] M. Roitman, Polynomial extensions of atomic domains, J. Pure Appl. Algebra 87 (1993) 187–199.
[14] J. Steffan, Longueur des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind, J. Algebra 102 (1986) 229–236.
[15] R.J. Valenza, Elasticity of factorizations in number fields, J. Number Theory 36 (1990) 212–218.