C. R. Acad. Sci. Paris, Ser. I 351 (2013) 5–8

Contents lists available at SciVerse ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Algebra

Some remarks on non-commutative principal ideal rings

Sylvain Carpentier [a], Alberto De Sole [b], Victor G. Kac [c]

[a] École normale supérieure, 75005 Paris, France
[b] Dipartimento di matematica, University of Rome-1, "La Sapienza", 00185 Roma, Italy
[c] Department of Mathematics, M.I.T., Cambridge, MA 02139, USA

ARTICLE INFO

Article history:
Received 10 January 2013
Accepted 18 January 2013
Available online 4 February 2013

Presented by Michèle Vergne

ABSTRACT

We prove some algebraic results on the ring of matrix differential operators over a differential field in the generality of non-commutative principal ideal rings. These results are used in the theory of non-local Poisson structures.

RÉSUMÉ

Nous démontrons quelques résultats algébriques sur l'anneau des matrices d'opérateurs différentiels sur un corps différentiel dans le cas général des anneaux principaux non commutatifs. Ces résultats sont utilisés dans la théorie des structures de Poisson non locales.

© 2013 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

1. Introduction

In our previous two papers [1,2] we established some algebraic properties of the ring of matrix differential operators over a differential field. The problems naturally arose in the study of non-local Poisson structures [3,4].

Eventually we realized that the proofs of [2] can be simplified, so that our results hold in the full generality of left and right principal ideal rings.

The new result which is not contained in our previous paper is Theorem 3.3, which is used in the theory of the non-local Lenard–Magri scheme in [4].

2. General facts about principal ideal rings

Let R be a unital associative (not necessarily commutative) ring. Recall that a *left* (resp. *right*) *ideal* of R is an additive subgroup $I \subset R$ such that $RI = I$ (resp. $IR = I$). The left (resp. right) *principal* ideal generated by $a \in R$ is, by definition, Ra (resp. aR).

Throughout the paper, we assume that the ring R is both a left and a right *principal ideal ring*, meaning that every left ideal of R and every right ideal of R is principal.

Example 2.1. Let $\mathcal{K}$ be a differential field with a derivation ∂, and let $\mathcal{K}[\partial]$ be the ring of differential operators over $\mathcal{K}$. It is well known that $\mathcal{K}[\partial]$ is a left and right principal ideal domain, see e.g. [1]. Let $\mathcal{R} = \mathrm{Mat}_{\ell\times\ell}(\mathcal{K}[\partial])$ be the ring of $\ell \times \ell$ matrices with coefficients in $\mathcal{K}[\partial]$. By Theorem 2.2(a) below, the ring $\mathcal{R}$ is a left and right principal ideal ring as well. Note also that $\mathcal{K}^\ell$ is naturally a left $\mathcal{R}$-module.

E-mail addresses: sylvain.carpentier@ens.fr (S. Carpentier), desole@mat.uniroma1.it (A. De Sole), kac@math.mit.edu (V.G. Kac).

1631-073X/$ – see front matter
http://dx.doi.org/10.1016/j.crma.2013.01.006

Given an element $a \in R$, an element $d \in R$ is called a *right* (resp. *left*) *divisor* of a if $a = a_1 d$ (resp. $a = da_1$) for some $a_1 \in R$. An element $m \in R$ is called a *left* (resp. *right*) *multiple* of a if $m = qa$ (resp. $m = aq$) for some $q \in R$.

Given elements $a, b \in R$, their *right* (resp. *left*) *greatest common divisor* is the generator d of the *left* (resp. *right*) ideal generated by a and b: $Ra + Rb = Rd$ (resp. $aR + bR = dR$). It is uniquely defined up to multiplication by an invertible element. It follows that d is a right (resp. left) divisor of both a and b, and we have the *Bezout identity* $d = ua + vb$ (resp. $d = au + bv$) for some $u, v \in R$.

Similarly, the *left* (resp. *right*) *least common multiple* of a and b is an element $m \in R$, defined, uniquely up to multiplication by an invertible element, as the generator of the intersection of the left (resp. right) principal ideals generated by a and by b: $Rm = Ra \cap Rb$ (resp. $mR = aR \cap bR$).

We say that a and b are *right* (resp. *left*) *coprime* if their *right* (resp. *left*) greatest common divisor is 1 (or invertible), namely if the *left* (resp. *right*) ideal that they generate is the whole ring R: $Ra + Rb = R$ (resp. $aR + bR = R$). Clearly, this happens if and only if we have the Bezout identity $ua + vb = 1$ (resp. $au + bv = 1$) for some $u, v \in R$.

An element $k \in R$ is called a *right* (resp. *left*) *zero divisor* if there exists $k_1 \in R \backslash \{0\}$ such that $k_1 k = 0$ (resp. $kk_1 = 0$). Note that, if d is a right (resp. left) divisor of a, and d is a left (resp. right) zero divisor, then so is a. In particular, if either a or b is not a left (resp. right) zero divisor, then their right (resp. left) greatest common divisor d is also not a left (resp. right) zero divisor. A non-zero element $b \in R$ is called *regular* if it is neither a left nor a right zero divisor.

The following results summarize some important properties of principal ideal rings that will be used in this paper. Since a principal ideal ring is obviously Noetherian, one can use the powerful theory of non-commutative Noetherian rings (see [6]).

Theorem 2.2. *Let R be a left and right principal ideal ring. Then*:

(a) *The ring* $\mathrm{Mat}_{\ell\times\ell}(R)$ *of $\ell \times \ell$ matrices with entries in R is a left and right principal ideal ring.*
(b) *The sets of left and right zero divisors of R coincide. Hence, an element of R is regular if and only if it is not a left (or a right) zero divisor.*
(c) *The set of regular elements of R satisfies the left (resp. right) Ore property: for $a, b \in R$ with b regular, there exist $a_1, b_1 \in R$, with b_1 regular, such that $ba_1 = ab_1$ (resp. $a_1 b = b_1 a$).*
(d) *There exists the* ring of fractions $Q(R)$ *containing R, consisting of left fractions ab^{-1} (or, equivalently, right fractions $b^{-1}a$), with $a, b \in R$ and b regular.*
(e) *Given $a, b \in R$ with b regular, there exists $q \in R$ such that $a + qb$ (resp. $a + bq$) is regular.*
(f) *Suppose that the ring R contains a central regular element $r \in R$ such that $r - 1$ is regular too. Given $a_1, a_2, b_1, b_2 \in R$ with b_1, b_2 regular, there exists $q \in R$ such that $a_1 + qb_1$ and $a_2 + qb_2$ (resp. $a_1 + b_1 q$ and $a_2 + b_2 q$) are both regular.*

Proof (*by J.T. Stafford*)**.** Statement (a) is in [6, Prop. 3.4.10]. For part (b) [6, Cor. 4.1.9] shows that R is a direct sum $R = A \oplus B$ of an Artinian ring A and a Noetherian semiprime ring B. Obviously the regular elements of A are just the units. By Goldie's Theorem the right regular elements of B are the same as the left regular elements, i.e. the regular elements (see [6, Props. 2.3.4 and 2.3.5]). Since an element $(a, b) \in R = A \oplus B$ is regular if and only if a and b are both regular the same conclusion holds for R. This proves (b). The equivalence of (c) and (d) is Ore's Theorem [6, Thm. 2.1.12]. Part (c) then follows from Goldie's Theorem. It is routine to see that the regular elements of $A \oplus B$ form an Ore set if this is true for both A and B. Of course this result is vacuously true for A while Goldie's Theorem does it for B. Part (e) follows from [7, Cor. 2.5], and part (f) is in [8]. $\square$

Remark 2.3. As T. Stafford pointed out, the ring $R = \mathbb{Z}/2\mathbb{Z}$ does not satisfy the property in part (f).

Remark 2.4. From the above theorem we immediately get the following simple observations.

(a) By Theorem 2.2(b) we have that if $a = bc$, then a is regular if and only if b and c are regular. In particular, any left or right divisor of a regular element is regular.
(b) If b is regular and a arbitrary, then we can write their right (resp. left) least common multiple as $ab_1 = ba_1$ with b_1 regular. This follows from the Ore property in Theorem 2.2(c). Indeed, let $I = \{b' \in R \mid ab' \in bR\}$. It is clearly a right ideal of R. Hence, $I = b_1 R$ for some b_1. Clearly, $m = ab_1$ is the right least common multiple of a and b. By the Ore property, there exists a regular element $\tilde{b} \in I$. Hence, $\tilde{b} = b_1 c$, and therefore b_1 is regular too.
(c) It follows from the above observation that, if a and b are regular, so is their right (resp. left) least common multiple.
(d) If $a = a_1 d$, $b = b_1 d$ (resp. $a = da_1$, $b = db_1$), and a_1 and b_1 are right (resp. left) coprime, then d is the right (resp. left) greatest common divisor of a and b. Indeed, by the Bezout identity we have $ua_1 + vb_1 = 1$ (resp. $a_1 u + b_1 v = 1$), which implies $ua + vb = d$ (resp. $au + bv = d$). But then $Rd = Ra + Rb$ (resp. $dR = aR + bR$), proving the claim.
(e) Conversely, if $a = a_1 d$, $b = b_1 d$ (resp. $a = da_1$, $b = db_1$), and d is the right (resp. left) greatest common divisor of a and b, then, assuming that d is regular, we get that a_1 and b_1 are right (resp. left) coprime. Indeed, by the Bezout identity we have $d = ua + vb = (ua_1 + vb_1)d$ (resp. $d = au + bv = d(a_1 u + b_1 v)$), and since by assumption d is regular it follows that $ua_1 + vb_1 = 1$.

3. Some arithmetic properties of principal ideal rings

Theorem 3.1. *Let R be a left and right principal ideal ring and let $Q(R)$ be its ring of fractions. Let $f = ab^{-1} = a_1 b_1^{-1} \in Q(R)$ (resp. $f = b^{-1}a = b_1^{-1}a_1 \in Q(R)$), with $a, a_1, b, b_1 \in R$ and b, b_1 regular, and assume that a_1 and b_1 are right (resp. left) coprime. Then there exists a regular element $q \in R$ such that $a = a_1 q$ and $b = b_1 q$ (resp. $a = qa_1$ and $b = qb_1$).*

Proof. By assumption a_1 and b_1 are right coprime, hence we have the Bezout identity $ua_1 + vb_1 = 1$, for some $u, v \in R$. Let $q = ua + vb$. We have

$$b_1 q = b_1(ua + vb) = b_1\big(uab^{-1} + v\big)b = b_1\big(ua_1 b_1^{-1} + v\big)b = b_1(ua_1 + vb_1)b_1^{-1}b = b,$$

and

$$a_1 q = a_1 b_1^{-1} b_1 q = a_1 b_1^{-1} b = ab^{-1}b = a.$$

Finally, q is regular since $q = b_1^{-1}b$ is invertible in $Q(R)$. □

Corollary 3.2. *For every $f \in Q(R)$ there is a "minimal" right (resp. left) fractional decomposition $f = ab^{-1}$ (resp. $f = b^{-1}a$) with a, b right (resp. left) coprime. Any other right (resp. left) fractional decomposition is obtained from it by simultaneous multiplication of a and b on the right (resp. left) by some regular element $q \in R$.*

Proof. It follows immediately from Remark 2.4(d) and Theorem 3.1. □

Theorem 3.3. *Let R be a left and right principal ideal ring, and let V be a left module over R. Assume that the ring R contains a central regular element $r \in R$ such that $r - 1$ is regular too. Let $a, b \in R$, with b regular, be left coprime. Let $m = ab_1 = ba_1$ be their right least common multiple. Then, for every $x, y \in V$ such that $ax = by$, there exists $z \in V$ such that $x = b_1 z$ and $y = a_1 z$. In particular, $aV \cap bV = mV$.*

Proof. We first reduce to the case when a is regular. Indeed, let, by Theorem 2.2(e), $q \in R$ be such that $a + bq$ is regular. Then it is immediate to check that the right least common multiple of $a + bq$ and b is $(a + bq)b_1 = b(a_1 + qb_1)$. Moreover, since by assumption $ax = by$, we have $(a + bq)x = b(y + qx)$. Therefore, assuming that the theorem holds for regular a, there exists $z \in V$ such that $x = b_1 z$ and $y + qx = (a_1 + qb_1)z$, which implies $y = a_1 z$, proving the claim.

Next, let us prove the theorem under the assumption that both a and b are regular. Since $m = ab_1 = ba_1$ is the right least common multiple of a and b, it follows that a_1 and b_1 are right coprime, and therefore we have the Bezout identity

$$ub_1 + va_1 = 1, \tag{3.1}$$

for some $u, v \in R$. After replacing u by $u + qa$ and v by $v - qb$, Eq. (3.1) still holds. Hence, by Theorem 2.2(f), we can assume, without loss of generality, that u and v are both regular. Moreover, by Remark 2.4(c), since by assumption both a and b are regular, their right least common multiple is regular too, and therefore a_1 and b_1 are regular too. Multiplying in $Q(R)$ both sides of Eq. (3.1) on the left by u^{-1} and on the right by a_1^{-1}, we get

$$a^{-1}b = (a_1 u)^{-1}(1 - a_1 v), \tag{3.2}$$

and similarly, multiplying (3.1) on the left by v^{-1} and on the right by b_1^{-1}, we get

$$b^{-1}a = (b_1 v)^{-1}(1 - b_1 u). \tag{3.3}$$

Since, by assumption, a and b are left coprime, both fractions $a^{-1}b$ and $b^{-1}a$ are in their minimal fractional decomposition. Hence, by Eqs. (3.2) and (3.3), there exist $p, q \in R$ such that

$$1 - a_1 v = pb, \qquad a_1 u = pa, \tag{3.4}$$

$$1 - b_1 u = qa, \qquad b_1 v = qb. \tag{3.5}$$

Applying the first equation in (3.4) to $y \in V$ and using the assumption $ax = by$ and the second equation of (3.4), we get

$$y = a_1 vy + pby = a_1 vy + pax = a_1(vy + ux),$$

and, similarly, applying the first equation in (3.5) to $x \in V$ and using the second equation of (3.5), we get

$$x = b_1 ux + qax = b_1 ux + qby = b_1(ux + vy).$$

Hence, the statement holds with $z = ux + vy$. □

If V is a left R-module and $a \in R$, we denote $\operatorname{Ker} a = \{x \in V \mid ax = 0\}$.

Remark 3.4. If d is the right greatest common divisor of a and b in R, then $\operatorname{Ker} a \cap \operatorname{Ker} b = \operatorname{Ker} d$. Indeed, by the Bezout identity we have $b_1 a + a_1 b = d$. Therefore $\operatorname{Ker} a \cap \operatorname{Ker} b \subset \operatorname{Ker} d$. The reverse inclusion is obvious.

Corollary 3.5. *Let R be as in Theorem 3.3, and let V be a left R-module. Let $\sigma : R \to R$ be an anti-automorphism of the ring R. Let $a, b \in R$, with b regular, be right coprime, and suppose that $\sigma(a)b = \epsilon\sigma(b)a$, for some invertible central element $\epsilon \in R$. Let $x, y \in V$ be such that $\sigma(a)x = \epsilon\sigma(b)y$. Then there exists $z \in V$ such that $x = bz$ and $y = az$.*

Proof. First, since b is regular and σ is an anti-automorphism, $\sigma(b)$ is regular too. Moreover, since by assumption a and b are right coprime and σ is an anti-automorphism, it follows that $\sigma(a)$ and $\sigma(b)$ are left coprime.

We claim that the left least common multiple of a and b is equal to the right least common multiple of $\sigma(a)$ and $\sigma(b)$, and it is given by $m = \sigma(a)b = \epsilon\sigma(b)a$. Indeed, clearly m is a common right multiple of $\sigma(a)$ and $\sigma(b)$. It is therefore a right multiple of the minimal one: $m_1 = \sigma(a)b_1 = \sigma(b)a_1$. Namely, there exists $q \in R$ such that $b = b_1q$ and $a = \epsilon^{-1}a_1q$. But by assumption a and b are right coprime. Hence, q must be invertible, proving that m is the right least common multiple of $\sigma(a)$ and $\sigma(b)$. The same argument proves that m is also the left least common multiple of a and b.

We can now apply Theorem 3.3 to $\sigma(a)$ and $\sigma(b)$, to deduce that there exists $z \in V$ such that $x = bz$ and $\epsilon y = \epsilon az$, hence $y = az$. $\square$

As in [2], Corollary 3.5 implies the following maximal isotropicity property important for the theory of Dirac structures [5,3].

Corollary 3.6. *Let R be as in Theorem 3.3, and let V be a left R-module and let $(\cdot,\cdot) : V \times V \to A$ be a non-degenerate symmetric bi-additive pairing on V with values in an abelian group A. Let $*$ be an anti-involution of R such that $(ax, y) = (x, a^*y)$ for all $a \in R$ and $x, y \in V$. Extend the pairing $(\cdot,\cdot)$ to a pairing $\langle\cdot \mid \cdot\rangle$ on $V \oplus V$ with values in A, given by*

$$\langle x_1 \oplus x_2 \mid y_1 \oplus y_2\rangle = (x_1, y_2) + (x_2, y_1),$$

for every $x_1, x_2, y_1, y_2 \in V$. Given two elements $a, b \in R$, we consider the following additive subgroup of $V \oplus V$:

$$\mathcal{L}_{a,b} = \{bx \oplus ax \mid x \in V\} \subset V \oplus V. \tag{3.6}$$

(a) *The subgroup $\mathcal{L}_{a,b} \subset V \oplus V$ is isotropic with respect to the pairing $\langle\cdot \mid \cdot\rangle$ if and only if $a^*b + b^*a$ acts as 0 on V.*
(b) *If b is regular, a and b are right coprime, and $a^*b + b^*a = 0$, then the subgroup $\mathcal{L}_{a,b} \subset V \oplus V$ is maximal isotropic.*

Proof. Part (a) is straightforward and part (b) follows immediately from Corollary 3.5 with $\sigma(a) = a^*$ and $\epsilon = -1$. $\square$

Corollary 3.7. *Let R be as in Theorem 3.3, and let V be a left R-module. Let $a, b \in R$, with b regular, be left coprime. Let $m = ab_1 = ba_1$ be their right least common multiple. Then* $\operatorname{Ker} b = a_1(\operatorname{Ker} b_1)$.

Proof. If $k_1 \in \operatorname{Ker} b_1$, then $b(a_1k_1) = ab_1k_1 = 0$. Therefore, $a_1(\operatorname{Ker} b_1) \subset \operatorname{Ker} b$. We need to prove the opposite inclusion. If $k \in \operatorname{Ker} b$, we have $a0 = 0 = bk$. Hence, by Theorem 3.3, there exists $z \in V$ such that $0 = b_1z$ and $k = a_1z$. Namely, $k \in a_1(\operatorname{Ker} b_1)$. $\square$

Remark 3.8. In the ring $\mathcal{R} = \mathrm{Mat}_{\ell\times\ell}\mathcal{K}[\partial]$ of $\ell \times \ell$ matrix differential operators over a differential field $\mathcal{K}$, the above Corollary 3.7 implies that if $b^{-1}a = a_1b_1^{-1}$ is a rational matrix pseudodifferential operator in its minimal left and right fractional decompositions, then $\deg(b) = \deg(b_1)$ (where $\deg(b)$ is the degree of the Dieudonné determinant of b). Indeed, the fractional decomposition $b^{-1}a$ being minimal means that a and b are left coprime. Hence, by Corollary 3.7 we have that $\dim(\operatorname{Ker} b) = \dim(a_1 \operatorname{Ker} b_1)$ in any differential field extension of $\mathcal{K}$. Moreover, the fractional decomposition $a_1b_1^{-1}$ being minimal means that $\operatorname{Ker} a_1 \cap \operatorname{Ker} b_1 = 0$ in any differential field extension of $\mathcal{K}$. The claim follows by the fact that $\deg b$ is equal to the dimension of $\operatorname{Ker} b$ in the linear closure of $\mathcal{K}$ [2].

Acknowledgements

We wish to thank Toby Stafford and Lance Small for very useful correspondence. In particular, Toby Stafford provided us a proof of Theorem 2.2.

References

[1] S. Carpentier, A. De Sole, V.G. Kac, Some algebraic properties of matrix differential operators and their Dieudonné determinant, J. Math. Phys. 53 (2012) 063501.
[2] S. Carpentier, A. De Sole, V.G. Kac, Rational matrix pseudodifferential operators, preprint, arXiv:1206.4165, 2012.
[3] A. De Sole, V.G. Kac, Non-local Poisson structures and applications to the theory of integrable systems I, preprint, arXiv:1210.1688, 2012.
[4] A. De Sole, V.G. Kac, Non-local Poisson structures and applications to the theory of integrable systems II, preprint, arXiv:1211.2391, 2012.
[5] I.Ya. Dorfman, Dirac Structures and Integrability of Nonlinear Evolution Equations, Nonlinear Sci. Theory Appl., Wiley & Sons, New York, 1993.
[6] J.C. McConnell, J.C. Robson, Non-Commutative Noetherian Rings, Grad. Stud. Math., vol. 30, American Mathematical Society, Providence, RI, 2001.
[7] L.W. Small, J.T. Stafford, Regularity of zero divisors, Proc. Lond. Math. Soc. (3) 44 (3) (1982) 405–419.
[8] J.T. Stafford, private communication, 2012.