

## COMMUTATOR AUTOMORPHISMS OF FORMAL POWER SERIES RINGS

JOSEPH GUBELADZE AND ZAZA MUSHKUDIANI

(Communicated by Bernd Ulrich)

**ABSTRACT.** For a big class of commutative rings  $R$ , every continuous  $R$ -automorphism of  $R[[X_1, \dots, X_n]]$  with the linear part the identity is in the commutator subgroup of  $\text{Aut}(R[[X_1, \dots, X_n]])$ . An explicit bound for the number of commutators involved and a  $K$ -theoretic interpretation of this result are provided.

### 1. INTRODUCTION

**1.1. Motivation.** A  $K$ -theoretical framework for some well-known conjectures on automorphisms and idempotent endomorphisms of polynomial rings was initiated at the end of the 1970s in the works [BW, C1, C2, CW]. However, the development since then has been blocked due to the intractability of these conjectures. Recent evidence of this intractability is provided by [SU].

There are two natural variations of the mentioned nonlinear  $K$ -theory that makes things easier and tractable. One variant corresponds to extending polynomial algebras to *polytopal algebras* – essentially affine cones over projective toric varieties – and restricting homomorphisms to graded homomorphisms. A systematic theory in this direction, including higher groups, is developed in [BrG1, BrG2, BrG3, BrG4].

Here we consider the other variation that corresponds to the completion process and leads to the category of formal power series and their continuous homomorphisms. For higher groups this approach leads to a challenging conjectural homological computation – the isomorphisms (1) below for which supporting low dimensional results are obtained in this paper.

The freeness of projective objects in the context of complete algebras was proved in [T], as an application of a technique designed to study retracts of polynomial algebras, and also in [P], in the general context of projective algebras over nilpotent algebraic theories. One should also mention the work [K], establishing an analogue of the  $K$ -theoretical local-global principle for complete algebras.

Below we show (Theorem 1.1) how the standard method of ‘indeterminate coefficients’ implies the aforementioned result on retracts of  $R[[X_1, \dots, X_n]]$ . Furthermore, the same method almost immediately yields the corresponding  $K_1$ -analogue for the group  $\text{Aut}(R[[X_1, \dots, X_n]])$  if the ground ring  $R$  contains  $\mathbb{Q}$  (Theorem 1.2).

---

Received by the editors January 16, 2004 and, in revised form, January 3, 2005.

2000 *Mathematics Subject Classification.* Primary 13J10, 13F25, 19A99, 19B99.

*Key words and phrases.* Formal power series ring, retraction, automorphism, commutator.

©2005 American Mathematical Society  
Reverts to public domain 28 years from publication

The main emphasis in this paper is on the derivation of a similar result on the automorphism group when the coefficient ring is an algebra over a finite field (Theorem 1.3). Here things are a bit complicated. One needs to invoke a complex induction on the coefficient indices, depending on the residues modulo the characteristic. The main difficulty to make the indeterminate coefficients method work has been guessing how many auxiliary automorphisms yield feasible systems of equations. Also, one needs to treat separately the univariate case and the passage to the multivariate case. For a variant of the result in the case  $n = 1$  and  $R = \mathbb{Z}_p$ , where  $p$  is a prime number  $\neq 2, 3$ , see [Ca1]. The corresponding groups of automorphisms are related to *Nottingham groups* – objects of recent active investigation [Ca2].

We have not been able to involve algebras over  $\mathbb{Z}_2$  and  $\mathbb{Z}_3$  in our consideration.

The higher  $K$ -theory machinery of symmetric monoidal categories [Gr] explains what the direct higher analogue of the main result (after interpreting it as a claim on the fundamental group of certain  $K$ -theoretic spaces) should be. We conjecture the isomorphisms of integral homologies

$$(1) \quad H_i(E(R), \mathbb{Z}) = H_i([\text{GA}^c(R), \text{GA}^c(R)], \mathbb{Z}), \quad i \geq 2,$$

where  $E(R)$  is the stable group of elementary matrices and  $\text{GA}^c(R)$  stands for the formal nonlinear analogue of the general linear group  $GL(R)$ . These isomorphisms seem to be highly nontrivial already for  $i = 2$ . In this particular case, a theory of universal Steinberg relations should be possible, generalizing Milnor’s  $K_2$ . In the polytopal  $K$ -theory this is done in [BrG3].

**1.2. Main results.** Throughout the paper  $R$  is a commutative ring.

$\text{Mod}(R)$  denotes the category of  $R$ -modules, and  $\mathbb{P}(R)$  denotes the full subcategory of finitely generated projective modules. Let  $\text{Alg}^c(R)$  be the category of augmented  $R$ -algebras, complete in the additive topology of the augmentation ideal. For  $A \in \text{Alg}^c(R)$  let  $I(A) = \text{Ker}(A \rightarrow R)$ . The coproduct of two algebras in  $\text{Alg}^c(R)$  is given by the additive completion of the tensor product:  $A \sqcup B = (A \otimes_R B)_{I(A \otimes B)}^\wedge$ ,  $I(A \otimes B) = \text{Im}((I(A) \otimes B) \oplus (A \otimes I(B)) \rightarrow A \otimes B)$ . This makes  $\text{Alg}^c(A)$  a symmetric monoidal category. We have the functors:

$$\hat{S} : \text{Mod}(R) \rightarrow \text{Alg}^c(R), \quad \hat{S}(M) = (R \oplus M \oplus S^2(M) \oplus \dots)_{0 \oplus M \oplus S^2(M) \oplus \dots}^\wedge,$$

$$I/I^2 : \text{Alg}^c(R) \rightarrow \text{Mod}(R), \quad I/I^2(A) = I(A)/I^2(A).$$

Let  $\overline{X} = (X_1, \dots, X_n)$ . A *retract* of  $R[[\overline{X}]]$  is an algebra  $A \in \text{Alg}^c(R)$  for which there are morphisms  $A \rightarrow R[[\overline{X}]] \rightarrow A$  whose composite is  $1_A$ .

**Theorem 1.1.** *Any retract of  $R[[\overline{X}]]$  is of type  $\hat{S}(P)$  for some  $P \in \mathbb{P}(R)$ .*

Denote by  $\text{GA}_n^c(R)$  the group of augmented continuous  $R$ -automorphisms of the formal power series ring  $R[[\overline{X}]]$ , where ‘augmented’ and ‘continuous’ are understood with respect to the ideal  $(\overline{X})R[[\overline{X}]] \subset R[[\overline{X}]]$  and the corresponding additive topology on  $R[[\overline{X}]]$ . Such an automorphism is determined by its values on the variables

$$X_i \mapsto h_i^{(1)} + h_i^{(2)} + \dots, \quad i = 1, \dots, n,$$

where  $h_i^{(j)} \in R[[\overline{X}]]$  is a homogeneous polynomial of degree  $j$  for  $i = 1, \dots, n$ .

The surjective group homomorphism  $\text{GA}_n^c(R) \rightarrow \text{Aut}(\mathfrak{M}/\mathfrak{M}^2) = GL_n(R)$  is split by the natural embedding  $GL_n(R) \rightarrow \text{GA}_n^c(R)$  whose image consists of the linear transformations of the  $X_i$ . Let  $\text{GI}_n^c(R)$  and  $\text{GE}_n^c(R)$  denote respectively the preimages of the trivial and elementary subgroups:  $\{1\} \subset E_n(R) \subset GL_n(R)$ .

For a natural number  $k$  and a group  $\Gamma$  we let  $[\Gamma, \Gamma]^{(k)}$  denote the subset

$$\{[\beta_1, \gamma_1] \cdots [\beta_k, \gamma_k] : \beta_1, \gamma_1, \dots, \beta_k, \gamma_k \in \Gamma\} \subset [\Gamma, \Gamma]$$

where  $[-, -]$  refers to the commutator.

**Theorem 1.2.** *If there exist  $b, c \in U(R)$  such that  $(b^m - 1)R + (c^m - 1)R = R$  for all natural numbers  $m$ , then  $GI_n^c(R) \subset [GA_n^c(R), GA_n^c(R)]^{(1)}$ .*

The class of rings in Theorem 1.2 contains all  $\mathbb{Q}$ -algebras.

Let  $p$  be a prime number  $\geq 5$ .

**Theorem 1.3.** (a) *If  $\mathbb{Z}_p \subset R$ , then  $GI_1^c(R) = [GA_1^c(R), GA_1^c(R)]^{(2)}$ .*

(b) *If  $\mathbb{Z}_p \subset R$  and  $n \geq 2$ , then  $GI_n^c(R) \subset [GA_n^c(R), GA_n^c(R)]^{(n(n+3))}$ .*

(c) *If  $R$  is a field of characteristic  $p$ , then  $GI_n^c(R) \subset [GA_n^c(R), GA_n^c(R)]^{(4n)}$ .*

*Convention.* Below  $R^n$  is thought of as the module of  $n$ -columns and  $U(R)$  refers to the group of units of  $R$ . For a univariate formal power series  $f(X) \in R[[X]]$ , its  $m$ -th coefficient is denoted by  $f(X)_m$ .

2. PROOF OF THEOREM 1.1

Let  $A \subset R[[\bar{X}]]$  be an  $R$ -subalgebra for which there exists an  $R$ -algebra homomorphism  $\pi : R[[\bar{X}]] \rightarrow A$  such that  $\pi|_A = \mathbf{1}_A$ . We put

$$\pi(X_i) = f_i = f_i^{(1)} + f_i^{(2)} + \dots, \quad i = 1, \dots, n,$$

where  $f_i^{(k)} \in R[\bar{X}]$  is a homogeneous polynomial of degree  $k$ . Let  $M(\pi)$  denote the  $n \times n$ -matrix whose  $i$ -th column is  $(a_{i1}, \dots, a_{in})^\top$  where  $f_i^{(1)} = a_{i1}X_1 + \dots + a_{in}X_n$ . The submodule of  $R^n$  generated by the columns of  $M(\pi)$  is naturally identified with the module  $P = (I/I^2)(A)$ . The latter is a projective  $R$ -module: we have the split epimorphism  $(I/I^2)(\pi) : R^n \rightarrow P$ . Put  $Q = \text{Ker}((I/I^2)(\pi))$  and fix an epimorphism  $\rho : R^n \rightarrow Q$  split by the embedding  $Q \subset R^n$ . Then we have the following split  $R$ -algebra epimorphism:

$$\pi \sqcup \hat{S}(\rho) : R[[\bar{X}, \bar{Y}]] \rightarrow A \sqcup \hat{S}(Q).$$

(Here  $\bar{Y} = (Y_1, \dots, Y_n)$ .) Because  $P \oplus Q \simeq R^n$  there exists  $\alpha \in \text{Aut}_R(R^{2n}) = GL_{2n}(R)$  such that  $\alpha(P \oplus Q) = R^n \oplus 0$ . Then the idempotent endomorphism  $\kappa = \hat{S}(\alpha) (\pi \sqcup \hat{S}(\rho)) \hat{S}(\alpha)^{-1} : R[[\bar{X}, \bar{Y}]] \rightarrow R[[\bar{X}, \bar{Y}]]$  is of the form

$$\begin{aligned} \kappa(X_i) &= X_i + g_i^{(2)} + g_i^{(3)} + \dots, \quad i = 1, \dots, n, \\ \kappa(Y_j) &= h_j^{(2)} + h_j^{(3)} + \dots, \quad j = 1, \dots, n, \end{aligned}$$

where  $g_i^{(k)}, h_j^{(k)} \in R[\bar{X}, \bar{Y}]$  are homogeneous polynomials of degree  $k$ . We want to show the equality

$$(2) \quad \text{Im}(\kappa) = R[[\bar{X}]].$$

First observe that  $h_j^{(2)} \in R[\bar{X}]$ ,  $j = 1, \dots, n$ . In fact, if  $h_j^{(2)} \in R[\bar{X}, \bar{Y}] \setminus R[\bar{X}]$  for some index  $j$ , then the first appearance of the  $Y$ -variables in  $\kappa^2(Y_j)$  can only be in a homogeneous summand of degree  $> 2$ , contradicting the condition  $\kappa^2 = \kappa$ .

Assume we have shown

$$(3) \quad h_j^{(2)}, h_j^{(3)}, \dots, h_j^{(k)} \in R[\bar{X}], \quad j = 1, \dots, n.$$

Applying  $\kappa^2 = \kappa$  to the variables  $X_i$  we get

$$(4) \quad g_i^{(2)}, g_i^{(3)}, \dots, g_i^{(k)} \in R[\overline{X}], \quad i = 1, \dots, n.$$

Therefore, (2) follows once it is shown that (3) implies

$$h_j^{(k+1)} \in R[\overline{X}], \quad j = 1, \dots, n.$$

Assume to the contrary that  $h_j^{(k+1)}$  involves one of the variables  $Y_1, \dots, Y_n$  for some index  $j$ . But then, in view of (3) and (4), the first appearance of the  $Y$ -variables in  $\kappa^2(Y_j)$  can only be in a homogeneous summand of degree higher than  $k + 1$ , contradicting the condition  $\kappa^2 = \kappa$ .

The following commutative diagram is a consequence of (2):

$$\begin{array}{ccccc} \hat{S}(P) \sqcup \hat{S}(Q) & \xrightarrow{\subset} & R[[\overline{X}, \overline{Y}]] & \xrightarrow{\pi \sqcup \hat{S}(\rho)} & A \sqcup \hat{S}(Q) & \xrightarrow{\subset} & R[[\overline{X}, \overline{Y}]] \\ \downarrow & & \hat{S}(\alpha) \downarrow & & \downarrow & & \hat{S}(\alpha) \downarrow \\ R[[\overline{X}]] & \xrightarrow{\subset} & R[[\overline{X}, \overline{Y}]] & \longrightarrow & R[[\overline{X}]] & \xrightarrow{\subset} & R[[\overline{X}, \overline{Y}]] \end{array}$$

where the vertical arrows represent isomorphisms, the composite of the first two upper homomorphisms is  $\pi|_{\hat{S}(P)} \sqcup \mathbf{1}_{\hat{S}(Q)}$ , and that of the first two lower homomorphisms is an isomorphism. It follows that  $\pi|_{\hat{S}(P)} : \hat{S}(P) \rightarrow A$  is also an isomorphism. □

### 3. COMPOSITE AUTOMORPHISMS

Here we prove Theorem 1.2. Let  $n$  be a fixed natural number.

Assume  $\beta, \gamma \in \text{GA}_1^c(R) = \text{Aut}(R[[X]])$ ,  $\beta(X) = b_1X + b_2X^2 + \dots$  and  $\gamma(X) = c_1X + c_2X^2 + \dots$ . We have

$$(5) \quad (\gamma\beta)(X)_m = \sum_{r=1}^m b_r \sum_{\substack{(j_1, \dots, j_r) \\ j_1 + \dots + j_r = m}} c_{j_1} \cdots c_{j_r}.$$

While there is no obvious compact multivariate analog of (5), there is some sort of control on composite automorphisms which will play a crucial rôle in the sequel.

For a natural number  $m$ , let  $\mathcal{S}_m$  denote the number of ordered partitions of  $m$  with nonnegative entries and having length  $n$ . An arbitrary continuous  $R$ -algebra endomorphism  $\alpha$  of  $R[[\overline{X}]]$  can be represented in the following way:

$$\alpha(\overline{X}) = \sum_{m=1}^{\infty} \alpha(\overline{X})_m \cdot \left( (X_1^{d_1} \cdots X_n^{d_n})_{d_1 + \dots + d_n = m} \right)^\top$$

where  $\alpha(\overline{X})_m$  is an  $n \times \mathcal{S}_m$  matrix over  $R$  and

$$\left( (X_1^{d_1} \cdots X_n^{d_n})_{d_1 + \dots + d_n = m} \right)$$

refers to the vector of monomials of total degree  $d$  whose components are ordered lexicographically with respect to  $X_1 > \dots > X_n$ .

Next we introduce the pairings

$$M_{n \times \mathcal{S}_l}(R) \times M_{n \times \mathcal{S}_m}(R) \rightarrow M_{n \times \mathcal{S}_{lm}}(R), \quad (L, M) \mapsto L \star M, \quad l, m \in \mathbb{N},$$

defined by

$$\begin{aligned} & \left( L \cdot \left( (X_1^{d_1} \cdots X_n^{d_n})_{d_1+\dots+d_n=l} \right)^\top \right) \circ \left( M \cdot \left( (X_1^{d_1} \cdots X_n^{d_n})_{d_1+\dots+d_n=m} \right)^\top \right) (\overline{X}) \\ & = (L \star M) \cdot \left( (X_1^{d_1} \cdots X_n^{d_n})_{d_1+\dots+d_n=lm} \right) \end{aligned}$$

where  $\circ$  is the composition of the two endomorphisms of  $R[[\overline{X}]]$ . The associativity of the composition yields the associativity rule  $(L \star M) \star N = L \star (M \star N)$ .

Clearly, when  $l = m = 1$  the  $\star$  operation becomes the usual matrix product of  $n \times n$  matrices.

For natural numbers  $r$  and  $m$  and a system of automorphisms  $\delta_1, \dots, \delta_r \in \text{GA}_n^c(R)$ , the components of the matrix  $(\delta_1 \cdots \delta_k)(\overline{X})_m$  are polynomial functions of the components of the matrices  $\delta_1(\overline{X})_s, \dots, \delta_k(\overline{X})_s, s = 1, 2, \dots$ , the latter being treated as variables in the next lemma.

**Lemma 3.1.** *Let  $\alpha, \beta, \gamma$  be continuous  $R$ -algebra endomorphisms of  $R[[\overline{X}]]$ .*

- (a) *The components of the matrices  $(\beta\gamma\alpha)(\overline{X})_k$  and  $(\gamma\beta)(\overline{X})_k$  do not depend on the components of the matrices  $\alpha(\overline{X})_m, \beta(\overline{X})_m$ , or  $\gamma(\overline{X})_m$  for  $k < m$ .*
- (b) *The components of the  $n \times \mathcal{S}_m$  matrices*

$$(\beta\gamma\alpha)(\overline{X})_m - \beta(\overline{X})_m \star \gamma(\overline{X})_1 \star \alpha(\overline{X})_1 - \beta(\overline{X})_1 \star \gamma(\overline{X})_m \star \alpha(\overline{X})_1$$

and

$$(\gamma\beta)(\overline{X})_m - \gamma(\overline{X})_m \star \beta(\overline{X})_1 - \gamma(\overline{X})_1 \star \beta(\overline{X})_m$$

do not depend on the components of the matrices  $\beta(\overline{X})_m$  or  $\gamma(\overline{X})_m$ .

The proof is straightforward.

Below for an element  $\alpha \in \text{GI}_n^c(R)$  we will consider the equation  $\alpha = [\gamma^{-1}, \beta^{-1}]$  to be solved for  $\beta, \gamma \in \text{GA}_n^c(R)$ . This is equivalent to the infinite system of equations

$$(\mathcal{E}_m) \quad (\beta\gamma\alpha)(\overline{X})_m = (\gamma\beta)(\overline{X})_m, \quad m \in \mathbb{N},$$

for matrices  $\beta(\overline{X})_m, \gamma(\overline{X})_m \in M_{n \times \mathcal{S}_m}(R)$  such that  $\beta(\overline{X})_1, \gamma(\overline{X})_1 \in GL_n(R)$ .

*Proof of Theorem 1.2.* Let  $b, c \in R$  be elements such that  $(b^m - 1)R + (c^m - 1)R = R$  for all natural numbers  $m$ . For an arbitrary element  $\alpha \in \text{GI}_n^c(R)$  we want to solve the infinite system  $(\mathcal{E}_m), m \in \mathbb{N}$ .

Let  $\beta(\overline{X})_1 = b \cdot \mathbf{Id}_n$  and  $\gamma(\overline{X})_1 = c \cdot \mathbf{Id}_n$ . It follows from Lemma 3.1(a) that whatever matrices  $\beta(\overline{X})_m$  and  $\gamma(\overline{X})_m, m \geq 2$ , we take (of size  $n \times \mathcal{S}_m$ ), the equality  $(\mathcal{E}_1)$  is satisfied. More generally, the same proposition implies that for an arbitrary natural number  $m \geq 2$ , the validity of  $(\mathcal{E}_k), k < m$ , only depends on the matrices  $\beta(\overline{X})_k$  and  $\gamma(\overline{X})_k, k < m$ .

Now Lemma 3.1(b) implies that for every natural number  $m \geq 2$  the equation  $(\mathcal{E}_m)$  can be rewritten as

$$\begin{aligned} (\beta\gamma\alpha)(\overline{X})_m - (\gamma\beta)(\overline{X})_m &= \beta(\overline{X})_1 \star \gamma(\overline{X})_m \star \alpha(\overline{X})_1 + \beta(\overline{X})_m \star \gamma(\overline{X})_1 \star \alpha(\overline{X})_1 \\ &\quad - \gamma(\overline{X})_m \star \beta(\overline{X})_1 - \gamma(\overline{X})_1 \star \beta(\overline{X})_m + \mathcal{M}_m, \end{aligned}$$

where  $\mathcal{M}_m$  is an  $n \times \mathcal{S}_m$  matrix that only depends on the entries of the matrices  $\alpha(\overline{X})_k, \beta(\overline{X})_k, \gamma(\overline{X})_k, k < m$ . It is, therefore, possible to find successively matrices  $\beta(\overline{X})_m$  and  $\gamma(\overline{X})_m$  with the desired properties once the following is shown. For an

arbitrary natural number  $m$  and an arbitrary  $n \times \mathcal{S}_m$  matrix  $\mathcal{A}$  there are two  $n \times \mathcal{S}_m$  matrices  $\mathcal{B}$  and  $\mathcal{C}$  such that

$$\mathcal{A} = \beta(\overline{X})_1 \star \mathcal{C} \star \alpha(\overline{X})_1 + \mathcal{B} \star \gamma(\overline{X})_1 \star \alpha(\overline{X})_1 - \mathcal{C} \star \beta(\overline{X})_1 - \gamma(\overline{X})_1 \star \mathcal{B}.$$

In view of the conditions  $\alpha(\overline{X})_1 = \mathbf{Id}$ ,  $\beta(\overline{X})_1 = b \cdot \mathbf{Id}$  and  $\gamma(\overline{X})_1 = c \cdot \mathbf{Id}$ , this equation is equivalent to  $\mathcal{A} = \mathcal{C}(b^m - b) + \mathcal{B}(c - c^m)$ . Finally, the existence of the desired matrices  $\mathcal{B}$  and  $\mathcal{C}$  follows from the condition

$$(b^{m-1} - 1)(bR) + (c^{m-1} - 1)(-cR) = (b^{m-1} - 1)R + (c^{m-1} - 1)R = R$$

being applied separately to every component. □

The proof of Theorem 1.2 implies the following useful fact to be used later.

**Corollary 3.2.** *Let  $m$  be a natural number. If there exist elements  $b, c \in U(R)$  such that  $(b^k - 1)R + (c^k - 1)R = R$  for all  $k = 1, \dots, m - 1$ , then for an arbitrary element  $\alpha \in \text{GI}_n^c(R)$  there exist elements  $\beta, \gamma \in \text{GA}_n^c(R)$  such that  $\alpha(\overline{X})_k = [\beta, \gamma](\overline{X})_k$  for  $k = 1, \dots, m$ .*

#### 4. CHARACTERISTIC $\geq 5$ : THE UNIVARIATE CASE

In this section we prove Theorem 1.3(a). The notation  $(\mathcal{E}_m)$  has the same meaning as in Section 3, only considered in the univariate case.

Let  $\mathbf{F}$  be a field contained in  $R$ ,  $\text{char } \mathbf{F} = p \geq 5$ .

Choose arbitrary elements  $b_2, b_3, c_2, c_3 \in \mathbf{F}$  such that  $c_2 - b_2 \neq 0$ . Put  $a_2 = [\gamma^{-1}, \beta^{-1}](X)_2$  and  $a_3 = [\gamma^{-1}, \beta^{-1}](X)_3$  where  $\beta, \gamma \in \text{GA}_1^c(R)$  are arbitrary automorphisms such that  $\beta(X)_1 = \gamma(X) = -1$  and  $\beta(X)_k = b_k$ ,  $\gamma(X)_k = c_k$ ,  $k = 2, 3$ . Using (5) in Section 3 one easily sees  $a_2 = 2(b_2 - c_2)$  and  $a_3 = 4(b_2 - c_2)^2$ . In particular, if  $b_2 = 1$ ,  $c_2 = 0$ , then  $a_2 = 2$  and  $a_3 = 4$ .

**Lemma 4.1.** *Let  $\alpha \in \text{GA}_1^c(R)$  be an arbitrary element such that  $\alpha(X) = X + a_2X^2 + a_3X^3 + a_4X^4 + \dots$ . Assume  $m \geq 4$  is an even natural number,  $m \not\equiv 2 \pmod{p}$ . Then for arbitrary elements  $b_k, c_k \in R$ ,  $k \geq 4$ ,  $k \neq m$ , there exist elements  $b_m, c_m \in R$  such that  $(\mathcal{E}_m)$  and  $(\mathcal{E}_{m+1})$  are satisfied for the automorphisms  $\beta, \gamma \in \text{GA}_1^c(R)$  where  $\beta(X) = -X + b_2X^2 + b_3X^3 + b_4X^4 + \dots$  and  $\gamma(X) = -X + c_2X^2 + c_3X^3 + c_4X^4 + \dots$ .*

*Proof.* Using (5) and the conditions on  $m$ , one can easily check that the system  $(\mathcal{E}_m, \mathcal{E}_{m+1})$  is independent of  $b_{m+1}$  and  $c_{m+1}$  (although the values of the  $(m + 1)$ -coefficients do depend on  $b_{m+1}$  and  $c_{m+1}$ ). Moreover, this system can be rewritten as the following system of linear equations for  $c_m$  and  $b_m$ :

$$\begin{aligned} \text{(A)} \quad & 2c_m - & & 2b_m & = \mathcal{X}, \\ & (+2a_2 - (m - 2)b_2)c_m + & & (-2a_2 + (m - 2)c_2)b_m & = \mathcal{Y} \end{aligned}$$

where  $\mathcal{X}$  and  $\mathcal{Y}$  are elements of  $R$  only depending (polynomially) on  $b_k, c_k$ ,  $k < m$ . See Remark 4.3 below. Now the determinant of (A) is  $2(m - 2)(c_2 - b_2) \in U(R)$  and, therefore, the system is (uniquely) solvable for  $b_m$  and  $c_m$ . □

**Lemma 4.2.** *Assume  $m \geq 4$  is an even natural number,  $m \equiv 2 \pmod{p}$ . Let  $b_2 = 1$ ,  $c_2 = 0$ , and  $b_3, c_3 \in \mathbf{F}$  such that  $b_3 + c_3 = 0$ . Then for arbitrary elements  $b_k, c_k \in R$ ,  $k \geq 4$ ,  $k \neq m - 1, m$ , there exist elements  $b_{m-1}, c_{m-1}, b_m, c_m \in R$  such that  $(\mathcal{E}_m)$  and  $(\mathcal{E}_{m+1})$  are satisfied for the automorphisms  $\beta, \gamma \in \text{GA}_1^c(R)$  where  $\beta(X) = -X + b_2X^2 + b_3X^3 + b_4X^4 + \dots$  and  $\gamma(X) = -X + c_2X^2 + c_3X^3 + c_4X^4 + \dots$ .*

*Proof.* We start with general elements  $b_2, c_2, b_3, c_3 \in \mathbf{F}$ . By multiple applications of (5) the system  $(\mathcal{E}_m, \mathcal{E}_{m+1})$  can be rewritten as

$$\begin{aligned}
 (\mathbf{B}) \quad & 2(c_m - b_m) + (-2a_2 + (m + 1)b_2)c_{m-1} + (-2a_2 - (m + 1)c_2)b_{m-1} = \mathcal{X}, \\
 & 2a_2(c_m - b_m) + (-3a_3 + (m - 4)b_3 + 2ma_2b_2 - 2a_2c_2 - 2b_2c_2)c_{m-1} \\
 & + (-3a_3 - (m - 4)c_3 + 2a_2b_2 - 6a_2c_2 + 2c_2b_2)b_{m-1} = \mathcal{Y}
 \end{aligned}$$

where  $\mathcal{X}, \mathcal{Y} \in R$  only depend (polynomially) on  $b_4, c_4, \dots, b_{m-2}, c_{m-2}$ . See Remark 4.3 below. We view  $(\mathbf{B})$  as a system of linear equations with respect to  $2(c_m - b_m), c_{m-1}$ , and  $b_{m-1}$ . Since the matrix of  $(\mathbf{B})$  is defined over  $\mathbf{F}$  it is enough to show that its rank equals 2. By multiplying the first row of the mentioned matrix by  $a_2$  and then subtracting the result from the second row, the condition on the rank becomes  $(m - 3)a_2(b_2 - c_2) - 4b_2c_2 + (m - 4)(b_3 + c_3) \neq 0$ . For our specific choice of  $b_2, c_2, b_3, c_3$  this is equivalent to  $m \not\equiv 3 \pmod{p}$ , which is the case as  $m \equiv 2 \pmod{p}$ .  $\square$

*Remark 4.3.* Here we explain how the coefficients in the systems  $(\mathbf{A})$  and  $(\mathbf{B})$  above are computed. We only illustrate the process on the coefficients of  $c_{m-1}$  and  $b_{m-1}$  in the second equation of  $(\mathbf{B})$ . The argument for all other coefficients is similar and substantially easier.

Put  $(\beta\gamma)(X) = X + d_2X^2 + d_3X^3 + \dots$ , the  $d_j$  being polynomial functions of  $b_2, c_2, b_3, c_3, \dots$ . Then by (5) we have

$$(\beta\gamma\alpha)(X)_{m+1} = \sum_{r=1}^{m+1} a_r \sum_{\substack{(j_1, \dots, j_r) \\ j_1 + \dots + j_r = m+1}} d_{j_1} \cdots d_{j_r},$$

where  $d_1 = 1$ . By Lemma 3.1(a), among the  $d_j$  in this equality only  $d_{m-1}, d_m$  and  $d_{m+1}$  depend on the coefficients  $c_{m-1}$  and  $b_{m-1}$ . Thus,

$$(\beta\gamma\alpha)(X)_{m+1} = (2d_2a_2 + 3a_3)d_{m-1} + 2a_2d_m + d_{m+1} + \mathcal{U}$$

where  $\mathcal{U}$  does not depend on  $c_{m-1}, b_{m-1}$ .

Again (5), together with the assumptions that  $m$  is even and  $b_1 = c_1 = -1$ , implies  $d_2 = c_2 - b_2, d_{m-1} = (-c_{m-1} - b_{m-1}) + \mathcal{U}_{m-1}, d_m = (m - 1)b_2c_{m-1} - 2c_2b_{m-1} + \mathcal{U}_m$  and  $d_{m+1} = ((m - 1)b_3 - \binom{m-1}{2}b_2^2)c_{m-1} + (2b_2c_2 + 3c_3)b_{m-1} + \mathcal{U}_{m+1}$  where  $\mathcal{U}_{m-1}, \mathcal{U}_m$  and  $\mathcal{U}_{m+1}$  do not depend on  $c_{m-1}$  and  $b_{m-1}$ . Also, the condition  $m \equiv 2 \pmod{p}$  implies  $\binom{m-1}{2} = 0 \in R$ .

Similar computations show  $(\gamma\beta)(X)_{m+1} = (3b_3 + 2b_2c_2)c_{m-1} + (m - 1)c_3b_{m-1} + \mathcal{W}$ , where  $\mathcal{W}$  does not depend on  $c_{m-1}$  and  $b_{m-1}$ . Summing up, we get the desired coefficients in the expression

$$\begin{aligned}
 & (\beta\gamma\alpha)(X)_{m+1} - (\gamma\beta)(X)_{m+1} \\
 & = (-3a_3 + (m - 4)b_3 + 2ma_2b_2 - 2a_2c_2 - 2b_2c_2)c_{m-1} \\
 & + (-3a_3 - (m - 4)c_3 + 2a_2b_2 - 6a_2c_2 + 2c_2b_2)b_{m-1} + \mathcal{V} + \mathcal{W}.
 \end{aligned}$$

*Proof of Theorem 1.3(a).* Let  $\alpha \in \text{GI}_1^c(R)$  be an arbitrary automorphism and let  $\varphi \in \text{GA}_1^c(R)$  be the automorphism  $\varphi(X) = X + 2X^2 + 4X^3$ . Since  $\text{char } \mathbf{F} \geq 5$ , the field  $\mathbf{F}$  contains an element of multiplicative order  $\geq 4$ . Then by Corollary 3.2 (and Lemma (3.1)) there exist elements  $\beta_0, \gamma_0 \in \text{GA}_1^c(R)$  such that

$$(\alpha\varphi^{-1})(X)_k = [\beta_0, \gamma_0](X)_k$$

for  $k = 2, 3$ , equivalently  $([\beta_0, \gamma_0]^{-1} \circ \alpha)(X)_2 = 2$  and  $([\beta_0, \gamma_0]^{-1} \circ \alpha)(X)_3 = 4$ . We are done because by Lemmas 4.1 and 4.2 any automorphism  $\psi \in \text{GI}_1^c(R)$ , such that  $\psi(X)_2 = 2$  and  $\psi(X)_3 = 4$ , belongs to the commutator subgroup  $[\text{GA}_1^c(R), \text{GA}_1^c(R)]^{(1)}$ .  $\square$

5. CHARACTERISTIC  $\geq 5$ : THE MULTIVARIATE CASE

In this section we assume  $n \geq 2$ .

For a power series  $g \in (X_1, \dots, \check{X}_i, \dots, X_n)^2 R[[X_1, \dots, \check{X}_i, \dots, X_n]]$  the element  $\varepsilon_i^g \in \text{Aut}(R[\check{X}])$ , defined by

$$\varepsilon_i^g(X_j) = \begin{cases} X_i + g & \text{for } j = i, \\ X_j & \text{for } j \neq i, \end{cases}$$

will be called *elementary*.

**Lemma 5.1.** *Elementary automorphisms of  $R[\check{X}]$  belong to  $[\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(1)}$ .*

*Proof.* It is enough to observe that  $\varepsilon_1^g \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(1)}$  for an arbitrary element  $g \in (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]]$ . In fact, we have  $\beta \varepsilon_1^g \gamma = \gamma \beta$  where

$$\beta(X_i) = \begin{cases} X_1 + X_2 & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n \end{cases} \quad \text{and} \quad \gamma(X_i) = \begin{cases} X_i & \text{for } i = 1, 3, \dots, n, \\ X_2 + g & \text{for } i = 2. \end{cases}$$

$\square$

**Lemma 5.2.** *Let  $\frac{1}{2} \in R$  and  $f \in (X_2, \dots, X_n)R[[X_2, \dots, X_n]]$ . Then the automorphism  $\alpha \in \text{GE}_n^c(R)$ , defined by*

$$\alpha(X_i) = \begin{cases} X_1 + X_1 f & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n, \end{cases}$$

*belongs to  $[\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(n)}$ . Moreover, if  $R$  is a field of characteristic  $\neq 2$ , then  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(1)}$ .*

*Proof.* *Step 1.* First consider the case when  $f \in (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]]$ . In this situation we have  $\alpha \beta \gamma = \gamma \beta$  where the elements  $\beta, \gamma \in \text{GA}_n^c(R)$  are defined by

$$\beta(X_i) = \begin{cases} X_1 + X_1 X_2 & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n \end{cases} \quad \text{and} \quad \gamma(X_i) = \begin{cases} X_i & \text{for } i = 1, 3, \dots, n, \\ X_2 + f + X_2 f & \text{for } i = 2. \end{cases}$$

In particular,  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(1)}$ .

*Step 2.* Now assume  $f = \xi X_2$  for some  $\xi \in R$ . Then  $\alpha^2 \gamma = \gamma \alpha$  where the automorphism  $\gamma \in \text{GA}_n^c(R)$  is given by

$$\gamma(X_i) = \begin{cases} X_i & \text{for } i = 1, 3, 4, \dots, n, \\ 2X_2 + \xi X_2^2 & \text{for } i = 2. \end{cases}$$

In particular,  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(1)}$ .

*Step 3.* In the general case  $\xi_2 X_2 + \dots + \xi_n X_n + g$  for some  $\xi_2, \dots, \xi_n \in R$  and  $g \in (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]]$ . By iterated use of the previous step (w.r.t. the variables  $X_2, \dots, X_n$ ) the automorphism  $\alpha' \in \text{GA}_n^c(R)$ , defined by

$$\alpha'(X_i) = \begin{cases} X_1(1 + \xi_2 X_2)(1 + \xi_3 X_3) \cdots (1 + \xi_n X_n) & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n, \end{cases}$$

belongs to  $[\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(n-1)}$ . Finally,  $\alpha = \alpha''\alpha'$  for the element  $\alpha'' \in \text{GA}_n^c(R)$ , defined by

$$\alpha''(X_i) = \begin{cases} X_1\vartheta & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n, \end{cases}$$

where

$$\vartheta = \frac{1 + \xi_2 X_2 + \dots + \xi_n X_n}{(1 + \xi_2 X_2)(1 + \xi_3 X_3) \dots (1 + \xi_n X_n)} \in 1 + (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]].$$

Now the case of rings containing  $1/2$  follows by Step 1.

*Step 4.* Consider the remaining case when  $R$  is a field. By Step 1 there is no loss of generality in assuming  $f = \xi_2 X_2 + \dots + x_n X_n + g$  where  $\xi_2 \in U(R)$  and  $g \in (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]]$ .

If  $\xi_2 \neq -1$ , then the exact same argument as in Step 1 works. Therefore, we can additionally assume that  $\xi_2 = -1$ . But then  $\alpha\beta_1\gamma_1 = \gamma_1\beta_1$  for the automorphisms  $\beta_1, \gamma_1 \in \text{GA}_n^c(R)$  determined by

$$\beta_1(X_i) = \begin{cases} X_1 - X_1 X_2 & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n \end{cases} \quad \text{and } \gamma_1(X_i) = \begin{cases} X_i & \text{for } i = 1, 3, 4, \dots, n, \\ X_2 + (-1 + X_2)f & \text{for } i = 2. \end{cases}$$

□

**Lemma 5.3.** *Assume  $\mathbb{Z}_p \subset R$  and  $h = (\overline{X})^2 R[[\overline{X}]]$ . Then any automorphism  $\alpha \in \text{GA}_n^c(R)$  of type*

$$\alpha(X_i) = \begin{cases} X_1 + h & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n \end{cases}$$

*belongs to  $[\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(n+3)}$ . If  $R$  is a field of characteristic  $p$ , then  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(4)}$ .*

*Proof.* We have  $h = g + X_1 f_1 + X_1^2 f_2 + X_1^3 f_3 + \dots$  for some

$$g \in (X_2, \dots, X_n)^2 R[[X_2, \dots, X_n]], \quad f_1 \in (X_2, \dots, X_n) R[[X_2, \dots, X_n]], \\ f_2, f_3, \dots \in R[[X_2, \dots, X_n]].$$

First assume  $g = 0$ . Then  $\alpha = \alpha''\alpha'$  for the automorphisms  $\alpha', \alpha'' \in \text{GA}_n^c(R)$  defined by

$$\alpha'(X_i) = \begin{cases} X_1 + X_1 f_1 & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n, \end{cases} \quad \alpha''(X_i) = \begin{cases} X_1 + X_1^2 \vartheta_2 + \dots & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n \end{cases}$$

where  $\vartheta_j = (1 + f_1)^{-1} f_j$ ,  $j = 2, 3, \dots$ . So Theorem 1.3(a) and Lemma 5.2 imply  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(n+2)}$  in general and  $\alpha \in [\text{GA}_n^c(R), \text{GA}_n^c(R)]^{(3)}$  for  $R$  a field.

If  $g \neq 0$ , then  $\alpha = \beta \varepsilon_1^g$  where  $\beta \in \text{GA}_n^c(R)$  is an automorphism of the type considered in the preceding paragraph. By Lemma 5.1 we are reduced to the previous case  $g = 0$ . □

*Proof of Theorem 1.3(b,c).* Consider an automorphism

$$\alpha \in \text{GI}_n^c(R), \quad \alpha(X_i) = X_i + h_i, \quad h_i \in (\overline{X})^2 R[[\overline{X}]], \quad i = 1, \dots, n.$$

We have the equality  $\alpha = \alpha_1\alpha_2\cdots\alpha_n$  for the recursively defined elements  $\alpha_i \in \text{GA}_n^c(R)$ :

$$\begin{aligned}\alpha_1(X_i) &= \begin{cases} X_1 + h_1 & \text{for } i = 1, \\ X_i & \text{for } i = 2, \dots, n, \end{cases} \\ \alpha_2(X_i) &= \begin{cases} X_i & \text{for } i = 1, 3, 4, \dots, n, \\ \alpha_1^{-1}(X_2 + h_2) & \text{for } i = 2, \end{cases} \\ \alpha_3(X_i) &= \begin{cases} X_i & \text{for } i = 1, 2, 4, 5, \dots, n, \\ \alpha_2^{-1}\alpha_1^{-1}(X_3 + h_3) & \text{for } i = 3, \end{cases} \\ &\dots\dots\dots \\ \alpha_n(X_i) &= \begin{cases} X_i & \text{for } i = 1, 2, \dots, n-1, \\ \alpha_{n-1}^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}(X_n + h_n) & \text{for } i = n. \end{cases}\end{aligned}$$

It only remains to note that each of these automorphisms is (up to enumeration of variables) of the type considered in Lemma 5.3.  $\square$

#### REFERENCES

- [BW] H. Bass and D. Wright, *Localisation in the K-theory of invertible algebras*, J. Pure Appl. Algebra **9** (1976/77), 89–105. MR0424789 (54:12747)
- [BrG1] W. Bruns and J. Gubeladze, *Polytopal linear groups*, J. Algebra **218** (1999), 715–737. MR1705750 (2000g:14059)
- [BrG2] W. Bruns and J. Gubeladze, *Polytopal linear retractions*, Trans. Amer. Math. Soc. **354** (2002), 179–203. MR1859031 (2002h:14086)
- [BrG3] W. Bruns and J. Gubeladze, *Polyhedral  $K_2$* , Manuscripta Math. **109** (2002), 367–404. MR1948020 (2003m:19001)
- [BrG4] W. Bruns and J. Gubeladze, *Higher polyhedral K-groups*, J. Pure Appl. Algebra **184** (2003), 175–228. MR2004974 (2004f:19002)
- [C1] E. Connell, *A K-theory for the category of projective algebras*, J. Pure Appl. Algebra **5** (1974), 281–292. MR0384803 (52:5675)
- [Ca1] R. Camina, *Some natural subgroups of the Nottingham Group*, Proc. Edin. Math Soc. **42** (1999), 333–339. MR1697402 (2001a:20043)
- [Ca2] R. Camina, *The Nottingham group*. (New horizons in pro- $p$  groups), Progr. Math., **184**, Birkhäuser, 2000, 205–221. MR1765121 (2001f:20054)
- [C2] E. Connell, *On the K-theory of algebras and polynomial extensions*, J. Pure Appl. Algebra **7** (1976), 169–17. MR0409475 (53:13230)
- [CW] E. Connell and D. Wright, *A Mayer-Vietoris sequence in nonlinear K-theory*, J. Pure Appl. Algebra **16** (1980), 149–165. MR0556157 (81e:18014)
- [Gr] D. Grayson, *Higher algebraic K-theory II* (after Quillen), Lecture Notes in Math. **551**, Springer, 1976, 217–240. MR0574096 (58:28137)
- [K] A. Kustin, *A classification of locally power series algebras*, J. Pure Appl. Algebra **17** (1980), 293–303. MR0579089 (81k:13006)
- [P] T. Pirashvili, *Projectives are free for nilpotent algebraic theories*, Algebraic K-theory and its applications, World Scientific, 1999, 589–599. MR1715892 (2000g:18003)
- [SU] I. Shestakov and U. Umirbaev, *The tame and the wild automorphisms of polynomial rings in three variables*, J. Amer. Math. Soc. **17** (2004), 197–227. MR2015334 (2004h:13022)
- [T] S. Tronin, *A construction in the theory of projective algebras*, (Russian) Mat. Zametki **35** (1984), 647–652. MR0750804 (85j:13015)

DEPARTMENT OF MATHEMATICS, SAN FRANCISCO STATE UNIVERSITY, SAN FRANCISCO, CALIFORNIA 94132

*E-mail address:* soso@math.sfsu.edu

KAVSADZE STREET 4, APART. 12, TBILISI, REPUBLIC OF GEORGIA