Mathematical
Structures and Modeling
2014. N. 3(31). PP. 27–39

UDC 512.743

A NECESSARY CONDITION FOR THE ELEMENTARY MATRIX GROUP TO BE LINEAR OVER A FIELD

G.A. Noskov
d.f.-m.n., s.r., e-mail: g.noskov@googlemail.com

Institute of Mathematics, SORAN

Abstract. We prove that if R is an associative unital ring and the elementary group $E_n(R)$ for $n \geq 3$ is linear over a field k of characteristic zero, then R has a finite index ideal which is linear over k. We prove that if A is an infinite integral domain of characteristic $p > 0$, then for every natural n the ring of Witt vectors $W_n(A)$ is not virtually linear over any field. However, somewhat paradoxically, for any field k and any $m, n \geq 1$ the group $\mathrm{GL}_m(W_n(k))$ is linear over k.

Keywords: linear group, field, affine algebraic group, associative ring, Witt ring.

Introduction

This paper is a complement to the studies reported earlier by M. Kassabov and M. Sapir [8]. Recall that a **general linear group** $\mathrm{GL}_n(R)$ over (always an associative and unital) ring R consists of all invertible $n \times n$ matrices over R with operations of matrix multiplication and inversion. A **matrix (**or **linear) group over** R is an abstract group embeddable into $\mathrm{GL}_n(R)$ for some $n \geq 1$. Similarly, a ring A is **linear over** R if it can be embedded into the ring of $n \times n$ matrices $\mathrm{M}_n(R)$ over the ring R for some $n \geq 1$. A fundamental question in group theory is to determine whether a given group G is linear over some (or certain) field or not. Here we study the case of the **elementary group** $G = \mathrm{E}_n(R)$ over a ring R. Recall that $\mathrm{E}_n(R)$ is the subgroup of $\mathrm{GL}_n(R)$ generated by all **elementary** $(n \times n)$-matrices $x_{ij}(r) = \mathrm{Id} + re_{ij}$ $(r \in R,\ 1 \leq i \neq j \leq n)$, where e_{ij} is a **standard matrix unit** with 1 in the (i, j)-position, and 0's elsewhere. The group $\mathrm{E}_n(R)$ is certainly linear over R, so the crux of the matter is whether or not $\mathrm{E}_n(R)$ is linear over some **field**. Our main result is

Theorem 1. *Let R be an associative unital ring. If group $\mathrm{E}_n(R)$ for $n \geq 3$ is linear over a field k of characteristic zero, then R is almost linear over k, i.e. R has a finite index ideal I, which is linear over k.*

The theorem should have been known for many years, but it has been proved only very recently in case $k = \mathbb{C}$ [8]. Informally, our theorem can be considered as a manifestation of the Lefschetz principle applied to the theorem by Kassabov and

Sapir. Recall that the "Lefschetz principle" states that any sentence in the first-order language of fields which is true for complex numbers is also true for every algebraically closed field of characteristic 0. The linearity of $\mathrm{E}_n(R)$ is definitely not a first-order sentence in the language of fields (although we were not able to prove this).

The study of isomorphic representability of infinite groups by matrices was initiated by Mal'cev (1940) in a paper in which he found the conditions for the representability of abelian and periodic groups (over a field) and proved a local theorem for matrix representability of bounded degree [10]. The state of art during the period 1966-1977 is surveyed in [13, 14]. A lot is known about isomorphisms between various matrix groups over (mostly commutative) rings; see [17, 22]. See also [3, 4, 6]. Moody, Long and Paton, Krammer, Bigelow made a remarkable progress in the linearity problem for braid groups [9, 16, 19, 20] . For the recent studies see [21, 23].

In the proof of Theorem 1 in [8, Thm.1] (in case $k = \mathbb{C}$) a nice topological argument plays a central role. Namely, the set $Z = 1 + Re_{1n}$ is an abelian subgroup of $\mathrm{E}_n(R)$ and at the same time Z has a natural ring structure isomorphic to R. Suppose $\mathrm{E}_n(R)$ is linear over $\mathbb{C}$. Identifying $\mathrm{E}_n(R)$ with its image in some $\mathrm{GL}_N(\mathbb{C})$, consider $\overline{Z}$ — the closure of Z in the Zariski topology on $\mathrm{GL}_N(\mathbb{C})$. The first observation is that $\overline{Z}$ possesses the structure of an associative algebraic ring with unit, which extends the R-ring structure on Z . The addition operation is given by the matrix multiplication on $\mathrm{GL}_N(\mathbb{C})$. The Zariski connected component of the additive group $\overline{Z}^0$ is a two-sided ideal in $\overline{Z}$. The key fact is that $\left(\overline{Z}^0, +\right)$ is isomorphic to $\mathbb{C}_+^m$ for some natural m. Here the authors of [8] apply topological argument, calculating the fundamental group of $\left(\overline{Z}^0, +\right)$.

In this paper, we avoid the reference to topology. With some small amount of the theory of algebraic groups, we show that $\overline{Z}^0$ is a unipotent group (see Section 1.). Moreover, to prove unipotence, we even do not use linearity of $\mathrm{E}_n(R)$ - it is enough to make use of linearity of the 2-step nilpotent Heisenberg group $\mathrm{UT}_3(R)$.

Clearly, if R is linear over a field, then the group $\mathrm{E}_n(R)$ also is linear over the same field for any $n \geq 2$. It is stated in [8, (Thm.1)] that the conclusion is true even if R is virtually linear over a field. Kassabov and Sapir also manage to build an example of a "strange" commutative ring R which is not linear over any field (even virtually) but for which $\mathrm{E}_n(R)$ is linear over field. We study their example from the scientific point of view and we show that any truncated Witt ring $W_n(k)$ satisfies the above property for every natural n.

1. The Heisenberg group over a ring

For any associative unital ring R and any natural $n \geq 2$ let $\mathrm{UT}_n(R)$ denote the upper uni-triangular group over R of the size $n \times n$. By this we mean the group

of $n \times n$ matrices

$$\mathrm{UT}_n(R) = \begin{pmatrix} 1 & R & \cdots & R \\ 0 & \ddots & & \vdots \\ 0 & 0 & \ddots & R \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In case $n = 3$ we have

$$\mathrm{UT}_3(R) = \begin{pmatrix} 1 & R & R \\ 0 & 1 & R \\ 0 & 0 & 1 \end{pmatrix}$$

and the matrix multiplication looks like this:

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & xy'+z+z' \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix},$$

where the entries $x, \ldots, z'$ are arbitrary elements of R. Identifying the first two matrices with the raws $(x, y, z), (x', y', z')$, we can rewrite the multiplication law as follows:

$$(x, y, z)(x', y', z') = (x + x', y + y', xy' + z + z').$$

The associativity can be easily verified, the triple $(0, 0, 0)$ is an identical element and the inverse is given by

$$(x, y, z)^{-1} = (-x, -y, xy - z).$$

We call $U = \mathrm{UT}_3(R)$ the **Heisenberg group** over R.

Lemma 1. *The subgroup $Z = (0, 0, R)$ is the center of U and at the same time the commutator subgroup of U. Moreover, the commutator map $U \times U \to Z$ is surjective.*

Proof. As usual, we denote by $[g, h]$ the group commutator $g^{-1}h^{-1}gh$ of the group elements g, h. It follows from the formula

$$(x, y, z)(0, 0, z') = (0, 0, z')(x, y, z) = (0, 0, z + z')$$

that Z lies in the center. On the other hand, if (x, y, z) is in the center, then

$$[(x, y, z), (1, n, 0)] = (0, 0, x - ny) = 0 \tag{1}$$

for all natural n. It follows from $x - y = 0, x - 2y = 0$ that $x = 0, y = 0$ and thus $(x, y, z) \in Z$. The commutator formula

$$[(x, y, z), (x', y', z')] = (0, 0, xy' - x'y) \tag{2}$$

shows that the commutator subgroup $[U,U]$ lies in Z. Setting $x=1, x'=0$ in the above formula, we obtain

$$[(1,y,z)\,(0,y',z')] = (0,0,y')\,, \tag{3}$$

which shows that $Z \subseteq [U,U]$ and finally $Z=[U,U]$.

■

Hence U is a 2-step nilpotent group. The sets $X=(R,0,0)\,, Y=(0,R,0)$ are abelian subgroups and XZ, XZ are normal abelian subgroups in U. We consider Z as a ring isomorphic to R.

2. Abstract linear representations of the Heisenberg group

The main result of this section is

Theorem 2. *Let R be a ring (associative, unital), k a perfect field, $m \geq 3, n \geq 2$ – the integers. Let $\rho : \mathrm{UT}_m(R) \to \mathrm{GL}_n(k)$ be an (abstract) injective homomorphism. Then for any i,j with $j-i \geq 2$, the closure of $\rho\,(x_{ij}\,(R))$ in the Zariski topology on $\mathrm{GL}_n(\overline{k})$ is a virtually unipotent k-group.*

We need some preliminaries for the proof.

A little portion of algebraic group theory ([2, 12]). Let K be an algebraically closed field. Let $K\,[X]$ be a polynomial ring in variables $X_1,\ldots,X_n$ over K. By an **affine variety** we mean a subset $A \subseteq K^n$ which is a set of zeroes of some ideal in $K\,[X]$ or equivalently it is of the form $V(S)=\{x \in K^n : f(x)= =0, \forall f \in S\}$,where S is any set of polynomials in n variables over K. We consider the **Zariski topology** on $K^n, n \geq 1$ in which the closed sets are algebraic sets.

Let k be a subfield of K. An algebraic set is k-**closed** if it is $V(S)$ for some S consisting of polynomials over k. The k-closed sets form a k-**topology** on K^n which is weaker than the original topology. If A is an arbitrary subset in K^n then the set $I\,(A)$ consisting of all polynomials vanishing on A form an ideal — the **annulator** of A in $K\,[X]$. We say that an algebraic set A is k-**defined** (or a k-**set**) if $I\,(A)$ can be generated by polynomials with coefficients in k. We shall also say that A is a k-**variety**, and denote by $k[A]$ the algebra of **regular functions** defined over k. This is the quotient of the polynomials on K^n with coefficients in k by its subideal of polynomials vanishing on A. One can clearly speak of **regular maps** (over k) between k-varieties by examining the coordinate functions.

Recall that a field k is **perfect** if every irreducible polynomial over k has distinct roots. If k is perfect then an algebraic set A is k-defined iff $A=V\,(S)$ and S consists of polynomials over k (see [12])).

An **affine algebraic group** G over K is an affine variety with group structure given by regular functions. Equivalently it is a nonsingular part of an algebraic set in $\mathrm{M}_n(K)$ – the set of $n \times n$ matrices over K. For a $k-$group G we let $G(k)=G \cap \mathrm{GL}_n(k)$ be the set of k-**rational points** of G. We say also that $G(k)$ is a k-**portion** of G.

An algebraic set A is **irreducible** if $I(S)$ is a prime ideal. In terms of Zariski topology A is irreducible if it is not empty and is not the union of two proper closed subsets. The latter condition is equivalent to the requirement that each non-empty open set be dense in A, or that each one be connected. Every algebraic set can be decomposed into a finite union of irreducible subsets, called the **components**. In case A is an algebraic group, the notions of irreducibility and connectivity are equivalent. In what follows we use only the second term, to avoid confusion with the concept of irreducibility in the sense of representation theory.

Jordan-Chevalley decomposition. Recall that a matrix $u \in \mathrm{M}_n(k)$ is called **unipotent** if $(u-1)^n = 0$. A matrix $s \in \mathrm{M}_n(k)$ is **semisimple** if any $s-$invariant subspace in k^n possesses an $s-$invariant complement subspace. In case of perfect k this is equivalent to diagonalizibility of s over the algebraic closure $\bar{k}$ [12, § 15.2.1]. The notions just introduced do not depend on the choice of a perfect field k [12, § 15.1.5]. Also these notions are invariant under conjugation by matrices from $\mathrm{GL}_n(k)$.

If k is perfect then every matrix $x \in \mathrm{GL}_n(k)$ has a unique **Jordan-Chevalley decomposition** $x = x_s x_u$ where $x_s, x_u \in \mathrm{GL}_n(k)$, x_s is semisimple, x_u is unipotent and $x_s x_u = x_u x_s$ [12, §15.3.3]. Moreover, x_s, x_u are the polynomials in x over k. We call the components of x **semisimple** and **unipotent** ones. By Mal'cev's theorem in every k-group G the components of any element belong to $G(k)$ [12, §16.1.4].

Theorem 3. [12, § 18.1.4]. *Let K be an algebraically closed extension of a perfect field k and G a commutative algebraic k-group. Then the semisimple and unipotent elements constitute the k-subgroups G_s and G_u respectively and $G = G_s \times G_u$. The same decomposition is true for $k-$portions: $G(k) = G_s(k) \times \times G_u(k)$.*

The following properties are well known.

Lemma 2. *Let k be a perfect field. (i) For any $x, y \in GL_n(k)$ we have $(yxy^{-1})_s = yx_sy^{-1}$ and $(yxy^{-1})_u = yx_uy^{-1}$, (ii) For any commuting $a, b \in GL_n(k)$ the following holds true: $(ab)_s = a_s b_s$ and $(ab)_u = a_u b_u$.*

Proof. (i) We have $yxy^{-1} = yx_sx_uy^{-1} = (yx_sy^{-1})(yx_uy^{-1})$. As yx_sy^{-1}, yx_uy^{-1} commute and are semisimple and unipotent respectively, the desired equalities follow from the uniqueness of Jordan-Chevalley decomposition. (ii) Let G be an algebraic group generated by a, b, that is the intersection of all algebraic groups containing a, b. Then G is a commutative k-group (see [2, Ch.I, § 2.4]) and the preceding Theorem shows that $G = G_s \times G_u$. It follows that $a_s a_s \in G_s, a_u b_u \in G_u$ and thus $ab = (a_s b_s)(a_u b_u)$ is a Jordan-Chevalley decomposition for ab. Whence the formulas. ■

Lemma 3. Cf. [26] *Let k be a perfect field. Let x, y, z, in $\mathrm{GL}_n(k)$ be such that $[x, y] = z$ and z commutes with both x and y. Then 1) $xy_sx^{-1} = z_s y_s$, 2)$z_s^{n!} = 1$. In particular, the element $z^{n!}$ is unipotent.*

Proof. Rewrite the equality $[x,y]=z$ in the form $xyx^{-1}=zy$. Taking the semisimple components of the last equality, and using the preceding Lemma 2, we obtain the formula $xy_sx^{-1}=z_sy_s$. Iterating this formula, we get

$$x^q y_s x^{-q} = z_s^q y_s \tag{4}$$

for all natural q. A fact from linear algebra is that any commuting set S of diagonalizable linear endomorphisms of finite-dimensional vector space V can be simultaneously diagonalized over the algebraic closure $\overline{k}$ [5, Section 6.5., Theorem 8]. Then, taking the commuting semisimple elements z_s and y_s in diagonal form

$$z_s = diag\{z_1,\dots,z_n\}, y_s = diag\{y_1,\dots,y_n\}$$

over the algebraic closure $\overline{k}$ (as we may), we see that the matrices $z_s^q y_s$ $(q\geq 0)$ are all diagonal and pairwise conjugated. Therefore, (4) implies $z_1^q y_1 = y_{j(q)}$ for some function $q\mapsto j(q)\in\{1,\dots,n\}$. It follows that $z_1^{q_1}y_1 = z_1^{q_2}y_1$ for some distinct $q_1,q_2\in[1;n+1]$. Hence $z_1^q=1$, where $1\leq q\leq n$ and so $z_1^{n!}=1$. Similarly, $z_i^{n!}=1$ for all i. Hence $z_s^{n!}=1$ and $z^{n!}$ is unipotent. ■

2.1. The proof of Theorem 2

Let K be an algebraically closed extension of a perfect field k . By assumption, $j-i\geq 2$, hence there is a natural r such that $j>r>i$. The subgroup generated by $x_{ir}(R), x_{rj}(R), x_{ij}(R)$ is naturally isomorphic to $\mathrm{UT}_3(R)$, therefore we may assume henceforth that $m=3$ and $x_{ij}(R)=Z$. To simplify notation, we assume that $U=\mathrm{UT}_3(R)$ is contained in $\mathrm{GL}_n(k)$. Of course, this embedding is assumed to be a monomorphism of **abstract** groups. In particular, apriori U may not be an algebraic subgroup in $\mathrm{GL}_n(k)$ in any reasonable sense. We denote by $\overline{G}$ the Zariski closure of a group $G\leq \mathrm{GL}_n(K)$ and we denote by G^0 the connected component of an algebraic group $G\leq \mathrm{GL}_n(K)$. Recall that G^0 is a finite index subgroup in G and if G is k-defined then G^0 is an algebraic k-defined group [2, Ch.I, §.1.2].

By Mal'cev's theorem in an algebraic group G the components g_s, g_u of any element g belong to G and, moreover, if g is k-rational then g_s, g_u are k-rational too [12, § 16.1.4] . First, note that there is a dense open subset in $\overline{Z}$ consisting of the commutators. Indeed, Lemma 1 implies that the commutator map $c: U\times U\to Z$ is surjective. It is obvious that the map c is regular, so its extension $c:\overline{U}\times\overline{U}\to\overline{Z}$ is also a regular map. We can therefore apply the Chevalley theorem [2, Theorem AG.10.2] to conclude that the image of c contains a dense open subset C in $\overline{Z}$. It follows that the intersection $C\cap\overline{Z}^0$ is a dense open subset in $\overline{Z}^0$ consisting of commutators. By Theorem 3 we have $\overline{Z}=\overline{Z}_s\times\overline{Z}_u$. We assert that $\overline{Z}_s^0=1$. Suppose not. Then setting $T_n=\left\{x\in\overline{Z}_s^0 : x^{n!}=1\right\}$, we obtain a proper closed subgroup $T_n\times\overline{Z}_u$ in a connected algebraic group $\overline{Z}^0$ hence its complement D is a dense open subset in $\overline{Z}^0$. The intersection of two open dense subsets in a connected variety is nonempty hence the intersection $C\cap D$ is nonempty and open in $\overline{Z}_s^0$ hence there is $z=z_sz_u\in C\cap D$. By Lemma 3, the element z^q is unipotent

for some q dividing $n!$. We conclude that $z_s^q = 1$ and this implies that $z \in T_n \times$ $\times \overline{Z}_u^0$, contradicting the inclusion $z \in D$. Finally, we have that $\overline{Z} = \overline{Z}_s \times \overline{Z}_u$ and the connected component $\overline{Z}_s^0$ is trivial, hence $\overline{Z}_s$ is finite and thus $\overline{Z}$ is virtually unipotent $k-$group.

■

3. Algebraic rings

Let K be an algebraically closed extension of a perfect field k. By an **algebraic k-ring** we mean an affine algebraic k-variety R over K with the k-regular maps "addition" and "multiplication", which turn R into a ring (possible non-associative and without identity). In particular this means that the additive group $(R, +)$ is an affine abelian algebraic k-group. Note that for every $r \in R$ the **left multiplication** map $R \to R$ given by $x \mapsto rx$ $(x \in R)$ is everywhere defined on R and hence it is regular, see [12, § 8.1.9]. Similarly, the right multiplication map is regular also.

Lemma 4. Cf. [8] Let R be an algebraic k-ring. Then the connected component R^0 of an additive group $(R, +)$ is a two-sided ideal in R. Moreover, R^0 is an algebraic $k-$ring.

Proof. Recall that the connected component R^0 is a subgroup of finite index in $(R, +)$ whose cosets are connected, as well as irreducible, components of $(R, +)$. Since R is defined over k, so is R^0. For any $r \in R$ the map $x \mapsto rx$ takes R^0 onto rR^0, hence rR^0 is irreducible, see [12, § 8.2.5] . As it contains $\mathbf{0}$, it is contained in R^0. This shows that R^0 is a left ideal in R. Similarly, R^0 is a right ideal. The last assertion follows directly from definitions. ■

Recall that a ring R (not necessarily associative) is an **algebra** over a field K if an operation $K \times R \to R$ is defined such that this operation together with the addition constitute a structure of $K-$vector space and the following axioms are satisfied:

$$(\lambda a)\, b = a\, (\lambda b) = \lambda\, (ab) \text{ for all } \lambda \in K, a, b \in R. \tag{5}$$

Lemma 5. *Let R be an algebraic k-ring over field K of characteristic zero. Suppose that the connected component R^0 of the group $(R, +)$ is a unipotent group. Then R^0 has a structure of finite dimensional $K-$algebra which is compatible with the ring structure on R^0. Moreover, $R^0(k)$ has a structure of a finite dimensional algebra over k which is compatible with the ring structure on $R^0(k)$.*

Proof. By assumption $(R, +)$ is a commutative unipotent group. Hence there is a k-isomorphism $R^0 \simeq K^n$. Thus we have a structure of a K-vector space on R^0 (and the induced k-vector space structure on $R^0\,(k)$). We are going to show that this structure is compatible with the ring structure on R^0 in a sense that the axioms (5) hold true. Note that the axiom $(\lambda a)\, b = \lambda\, (ab)$ means that the operator r_b of right

multiplication by b should be K-linear. But r_b is a regular endomorphism of the group $(K^n, +)$, hence it is a K-linear map (here the characteristic assumption is decisive). The second axiom can be verified similarly. Finally, the k-isomorphism $R^0 \simeq \bar{k}^n$ implies that $R^0(k) = k^n$ and the k-algebra structure on k^n is compatible with the ring structure on $R^0(k)$. ■

Theorem 4. *Let k be a field of an arbitrary characteristic and let R be a unital connected algebraic associative k-ring. Then the multiplicative group $R^\times$ of R is a linear k-group.*

Proof. The group $G = \{(x, y) \in R \times R : xy = 1\}$ is an affine algebraic k-group and thus $R^\times = G \cap (R, 1)$ is also an affine algebraic k-group. Every affine k-group is k-isomorphic to a closed subgroup, defined over k, of some $GL_n(K)$ (see [2, ch. I Prop. 1.10], and [12, § 31.23]), hence also is linear over k. ■

4. The proof of Theorem 1

We follow the scheme outlined in [8], overcoming some technical difficulties. Suppose that $\mathrm{E}_3(R)$ is linear over k. To simplify the notation we assume that $\mathrm{E}_3(R)$ is contained in $\mathrm{GL}_n(k)$. Let Z denote $x_{13}(R)$. The Zariski closure $\bar{Z}$ in $\mathrm{GL}_n(K)$ is a commutative algebraic k-group. Henceforth we use an additive notation for this group operation. By Theorem 2, the group $\bar{Z}^0$ is unipotent.

In order to define the multiplication on $\bar{Z}$ we need to use the following monomial matrices in $\mathrm{E}_3(R)$:

$$u = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

They satisfy the following key properties (we denote conjugation by ${}^u x = uxu^{-1}$):

$${}^u x_{13}(r) = x_{23}(r) \quad \text{and} \quad {}^v x_{13}(r) = x_{12}(r).$$

Recall again that we consider $\mathrm{E}_3(R)$ as a subgroup in $\mathrm{GL}_n(K)$. The conjugacy operations $g \mapsto {}^u g, g \mapsto {}^v g$ are $k-$regular maps on $\mathrm{GL}_n(K)$. Let us define a k-regular map $\cdot$ from $\bar{Z} \times \bar{Z}$ to $\mathrm{GL}_n(K)$ as follows:

$$x \cdot y := [{}^v x, {}^u y] \left(x, y \in \bar{Z}\right).$$

Since $\cdot$ takes $Z \times Z$ into Z, it also takes $\bar{Z} \times \bar{Z}$ into $\bar{Z}$ ([2, ch. I, sec.6.6.]). Moreover, the commutator relation $[x_{12}(r), x_{23}(s)] = x_{13}(rs), (r, s \in R)$ implies that the restriction of $\cdot$ to $R \subset \bar{Z}$ coincides with the original multiplication on R. The element $1 \in R$ is a unit in R hence it is unit (with respect to $\cdot$) in its closure $\bar{R} = \bar{Z}$. Similarly, since R is associative, $\bar{R} = \bar{Z}$ is associative also. We have introduced an associative unital ring structure on $\bar{Z} \supset R$ extending the original ring structure on R. By Lemma 5, the group $\bar{Z}^0(k)$ is a two-sided ideal in $\bar{Z}(k)$ and $\bar{Z}^0(k)$ is linear over k hence $\bar{Z}^0(k) \cap R$ is a two-sided ideal in R which is linear over k. The proof of Theorem 1 is complete.

5. Nonlinear Witt rings R with linear $GL_n(R)$

The analog of Theorem 4 is not true in the case of positive characteristic. Here is one simple example given in [8] (it is somewhat similar to the example from [1]): Let K be an infinite field of characteristic 2 and let us give $R = K \times K$ the following operations:

$$(a,b)+(c,d)=(a+c,ac+b+d), \qquad (a,b)\times(c,d)=(ac,bc^2+a^2d). \tag{6}$$

One can verify directly that R becomes a commutative local ring with the maximal ideal $M=(0,K)$ and residue field $R/M \simeq K$. Therefore R does not have proper ideals of finite index. This ring is not linear over any field since all elements of the form (a,b), $a \neq 0$, have "additive" order 4. Hence R is not virtually linear. Rather surprisingly, $GL_n(R)$ is linear for all $n \geq 2$! Thus, there exists a (strange) ring R which is not (virtually) linear over any field, but the group $EL_n(R)$ is linear ! In this section we show that the all truncated Witt rings $W_n(k)$ over infinite perfect field of finite characteristic possess this property.

5.1. Witt rings are strange

Our basic reference for this section is Serre [Ser] (see also [7,24]). From now on, we let p be a fixed prime number. For $n \geq 0$ define the **n-th Witt polynomial** to be

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \in \mathbb{Z}[X_0, X_1, \ldots, X_n]. \tag{7}$$

Thus

$$\begin{aligned} W_0 &= X_0 \\ W_1 &= X_0^p + pX_1 \\ W_2 &= X_0^{p^2} + pX_1^p + p^2X_2 \\ &\cdots\cdots\cdots\cdots \\ W_n &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^nX_n. \end{aligned}$$

If we extend the coefficient ring to $\mathbb{Z}\left[\frac{1}{p}\right]$ or even to a larger ring A, then the equations can be inverted:

$$X_0 = W_0, X_1 = p^{-1}(W_1 - W_0^p), \ldots, \text{etc.} \tag{8}$$

Theorem 5. *There exist unique sequences* $(S_0,\ldots,S_n,\ldots),(P_0,\ldots,P_n,\ldots)$ *of polynomials in* $\mathbb{Z}[X_0,\ldots,X_n,\ldots;Y_0,\ldots,Y_n,\ldots]$*, such that:*

$$W_n(S_0,\ldots,S_n) = W_n(X_0,\ldots,X_n) + W_n(Y_0,\ldots,Y_n),$$

$$W_n(P_0,\ldots,P_n) = W_n(X_0,\ldots,X_n)\,W_n(Y_0,\ldots,Y_n)$$

for all $n = 0,1\ldots$.

Example 1.

$$S_0 = X_0 + Y_0, \qquad S_1 = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p},$$

$$P_0 = X_0 Y_0, \qquad P_1 = X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1.$$

Let A be a unital commutative ring. We have the usual, product ring structure on A^{n+1}. Define a new addition and multiplication in A^{n+1} by

$$a \dot{+} b = \left(S_0(a,b), \ldots, S_n(a,b)\right),$$

$$a \cdot b = \left(P_0(a,b), \ldots, P_n(a,b)\right).$$

These laws of composition make A^{n+1} into a commutative unital ring, called the **ring of (truncated) Witt vectors** and denoted $W_n(A)$. The zero and unit elements of $W_n(A)$ are $0 = (0, ..., 0)$ and $1 = (1, 0, ..., 0)$ respectively. In case $n = 1$ we have a ring isomorphism $W_0(A) \simeq A$. The map

$$W_* : W_n(A) \to A^{n+1}$$

which assigns to a Witt vector $a = (a_0, \ldots, a_n)$ the element

$$\left(W_0(a_0), W_1(a_0, a_1), \ldots, W_n(a_0, \ldots, a_n)\right)$$

of the product ring A^{n+1}, is a ring homomorphism by the very definition of the polynomials S and P. It follows also that the projection map $(a_0, \ldots, a_n) \mapsto a_0$ is a ring homomorphism from $W_n(A)$ to A.

Example 2. The ring structure $W_1(A)$ is defined on A^2 according formulas (8), so in coordinates $x = (x_0, x_1), y = (y_0, y_1)$ it looks as follows:

$$\begin{aligned} \left(x \dot{+} y\right)_0 &= x_0 + y_0, \left(x \dot{+} y\right)_1 = x_1 + y_1 + \frac{1}{p}\left(x_0^p + y_0^p - (x_0 + y_0)^p\right), \\ (x \cdot y)_0 &= x_0 y_0, \qquad (x \cdot y)_1 = x_0^p y_1 + x_1 y_0^p + p x_1 y_1. \end{aligned}$$

In case $p = 2$ we obtain

$$\begin{aligned} \left(x \dot{+} y\right)_0 &= x_0 + y_0, \left(x \dot{+} y\right)_1 = x_1 + y_1 + x_0 y_0, \\ (x \cdot y)_0 &= x_0 y_0, \qquad (x \cdot y)_1 = x_0^2 y_1 + x_1 y_0^2, \end{aligned}$$

which coincides with the Kassabov-Sapir structure given by 6.

Proposition 1. *Let K be any algebraically closed field and k its prime subfield. The Witt ring $W_n(K)$ is a unital commutative algebraic k-ring. Moreover, the set of k-rational points is canonically isomorphic to the ring $W_n(k)$.*

Proof. The ring $W_n(K)$ is algebraic because the underlying k-variety is K^{n+1} and ring operations are polynomial over the prime subfield. The k-points are $k^{n+1} \subseteq K^{n+1}$ and the operations are given by the same polynomials as in the definition of $W_n(k)$. ■

"Verschiebung" V and Frobenius F. One defines the **Verschiebung** (=shift) **map** $V : W_n(A) \to W_n(A)$ by

$$(x_0, x_1, ..., x_n) \to (0, x_0, ..., x_{n-1}).$$

This map is additive (in Witt ring structure). In case A is the ring of characteristic p the **Frobenius map** $F : W_n(A) \to W_n(A)$ is defined by

$$(x_0, x_1, ..., x_n) \to (x_0^p, x_1^p, ..., x_n^p).$$

These maps satisfy identities $VF = FV = p$, where p denotes the p-power map on the additive group of $W_n(k)$.

Theorem 6. *Let A be an infinite integral domain of characteristic $p > 0$. The ring $W_0(A)$ is linear over the quotient field K of A. For every natural n the Witt ring $W_n(A)$ is not virtually linear over any field.*

Proof. As we know, $W_0(A) \simeq A$, and A is clearly linear over K. When $n \geq 1$ we first show that $W_n(k)$ has an additive exponent p^{n+1} and, moreover, all Witt vectors $(x_0, ..., x_n)$ with $x_0 \neq 0$ have an additive order p^{n+1}. Iterating the formula $VF = FV = p$, we obtain $(VF)^k = (FV)^k = p^k$ for any natural k. Hence

$$p^k (x_0, \ldots, x_n) = \left(0, \ldots, 0, x_0^{p^k}, \ldots, x_{n-k}^{p^k}\right),$$

from which it follows that $p^{n+1}x = 0$ for each $x \in W_n(A)$. Moreover, if $x_0 \neq 0$ then $p^n (x_0, \ldots, x_n) = \left(0, \ldots 0, x_0^{p^n}\right) \neq 0$.

Finalizing the proof, let I be an ideal of finite index in $W_n(A)$, which is linear over some field L. The ideal I can not lie entirely in the ideal $M = (0, A, \ldots, A)$, since $W_n(A)/M \simeq k$ is infinite by assumption. Hence, there is $x = (x_0, ..., x_n) \in I$ with $x_0 \neq 0$ but then $p^{n+1}x = 0$ and $p^n x \neq 0$, which can not happen in an L-algebra. ■

Theorem 7. *For any field k and any $m, n \geq 1$ the group $\mathrm{GL}_m(W_n(k))$ is linear over k.*

Proof. Since $W_n(k)$ is algebraic, the full matrix ring $R = \mathrm{M}_m(W_n(k))$ is an algebraic k-ring. By theorem 4 the multiplicative group $R^\times$ is linear over k. Hence its subgroup $\mathrm{GL}_m(W_n(k))$ is linear over k also. ■

6. Questions

1. It is proved in [8] that any ring homomorphism of a free associative ring $\mathbb{Z}\langle x, y\rangle$ into an algebraic ring R has a non-trivial kernel. Is it possible to embed $F_p\langle x, y\rangle$ into an algebraic ring over a field of positive characteristic? (see Remark 16 in [8]).

2. What is the structure of affine (non-commutative) algebraic rings?

3. What is the structure of (not necessarily affine) algebraic rings? The complement by George M. Bergman to the book [18] hopefully might be helpful.

4. Let R be an almost linear ring over a field k. Is it true that $\mathrm{E}_n(R)$ is a linear group over k ?

Acknowledgements

This research was partially supported by DFG through SFB 701 of Bielefeld University and by RFFI-grant 14-01-00068.

References

1. Bergman George M. Some examples in PI ring theory. Israel J. Math. 18 (1974). P. 257–277.
2. Borel Armand. Linear Algebraic Groups (2nd ed.,GTM 126). New York: Springer-Verlag, 1991.
3. Borel Armand, Tits, Jacques. Homomorphismes "abstraits" de groupes algebriques simples. Ann. of Math. (2) 97 (1973). P. 499–571.
4. Hahn Alexander J., James Donald G., Weisfeiler Boris. Homomorphisms of algebraic and classical groups: a survey. Quadratic and Hermitian forms (Hamilton, Ont., 1983), 249–296, CMS Conf. Proc., 4, Amer. Math. Soc., Providence, RI, 1984.
5. Hoffman Kenneth, Kunze Ray. Linear algebra. Second edition. Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.
6. James D., Waterhouse W., Weisfeiler B. Abstract homomorphisms of algebraic groups: problems and bibliography. Communications in Algebra, 9:1 (1981). P. 95–114.
7. Jacobson N. Basic Algebra II. 2nd edn., Freeman, San Fransisco, 1989.
8. Kassabov M., Sapir M. Nonlinearity of matrix groups. J. Topol. Anal. 1 (2009), N. 3. P. 251–260.
9. Long D.D., Paton M. The Burau representation is not faithful for $n \geq 6$, Topology 32 (1993).
10. Mal'cev A.I. On isomorphic matrix representations of infinite groups. Rec. Math. [Mat. Sbornik] N.S., 8(50):3 (1940). P. 405–422.
11. Mal'cev A.I. The elementary properties of linear groups. 1961 Certain Problems in Mathematics and Mechanics (In Honor of M.A. Lavrent'ev). P. 110–132. Izdat. Sibirsk. Otdel. Akad. Nauk SSSR, Novosibirsk.
12. Merzlyakov Yu.I. Rational groups. 2nd ed., Nauka, Moscow 1987. (Russian).
13. Merzlyakov Yu.I. Linear groups. Itogi nauki i tehniki. Algebra. Topologia. Geometria. 1970. M., 1971. P. 75–110.
14. Merzlyakov Yu.I. Linear groups. Itogi nauki i tehniki. Algebra. Topologia. Geometria. M., 1978. P. 35–89.
15. Milnor J. Introduction to algebraic K-theory. Annals of Mathematics Studies, N. 72. Princeton University Press, Princeton, N.J., 1971.
16. Moody J.A.The faithfulness question for the Burau representation. Proc. Amer. Math. Soc., 119(2):671–679, 1993.

17. Mostow G.D. Strong rigidity of locally symmetric spaces. Annals of Mathematics Studies, N. 78. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1973.
18. Mumford David. Lectures on Curves on Algebraic Surfaces (with George Bergman). Princeton University Press, 1964.
19. Bigelow S. Braid groups are linear8.J. Amer. Math. Soc. 14 (2001). P. 471–486.
20. Krammer D. Braid groups are linear. Ann. Math. 155 (2002). P. 131–156.
21. Olshanskii A.Yu. Linear Automorphism Groups of Relatively Free Groups. Turk. J. Math. 31 (2007) , Suppl. P. 105–111.
22. O'Meara O.T. Lectures on linear groups. Expository Lectures from the CBMS Regional Conference held at Arizona State University, Tempe, Ariz., March 26–30, 1973. Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, N. 22. American Mathematical Society, Providence, R.I., 1974.
23. Platonov V.P. Linear representations of automorphisms groups of free solvable groups (in Russian). Doklady RAN, 406 (2006), N. 4. P. 462–463.
24. Rabinoff J. The Theory of Witt Vectors. `http://www.math.harvard.edu/~rabinoff/misc/witt.pdf`
25. Serre J-P. Local fields. Berlin, New York: Springer-Verlag, 1980.
26. Steinberg R. Some consequences of the elementary relations in SL_n. In: Finite Groups-Coming of Age (Montreal, 1982), Amer. Math. Soc., Providence, RI, 1985. P. 335–350.

НЕОБХОДИМОЕ УСЛОВИЕ ЛИНЕЙНОСТИ НАД ПОЛЕМ ДЛЯ ЭЛЕМЕНТАРНОЙ МАТРИЧНОЙ ГРУППЫ

Г.А. Носков
д.ф.-м.н., с.н.с., e-mail: g.noskov@googlemail.com

Институт Математики им. С.Л. Соболева СОРАН

Аннотация. Мы доказываем, что если R есть ассоциативное кольцо с единицей, и элементарная матричная группа $E_n(R)$ при $n \geq 3$ линейна над полем k нулевой характеристики, то в R имеется идеал конечного индекса, линейный над k. Доказывается, что, если A является коммутативным целостным кольцом ненулевой характеристики, то для любого натурального n кольцо векторов Витта $W_n(A)$ не является почти линейным ни над каким полем. В то же время, несколько парадоксально, общая линейная группа $\mathrm{GL}_m(W_n(k))$ линейна над k в случае произвольного поля k.

Ключевые слова: линейная группа, поле, аффинная алгебраическая группа, ассоциативное кольцо, кольцо Витта.