Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 49 (2008), No. 1, 1-31.

Automorphisms of Verardi Groups: Small Upper Triangular Matrices over Rings

Theo Grundhöfer **Markus Stroppel**

*Mathematisches Institut, Universität Würzburg
Am Hubland, D-97074 Würzburg, Germany*

*Institut für Geometrie und Topologie, Universität Stuttgart
D-70550 Stuttgart, Germany*

Abstract. Verardi's construction of special groups of prime exponent is generalized, and put into a context that helps to decide isomorphism problems and to determine the full group of automorphisms (or at least the corresponding orbit decomposition). The groups in question may be interpreted as groups of unitriangular matrices over suitable rings. Finiteness is not assumed.

1. Introduction

We are going to discuss (and generalize) a class of special p-groups that was introduced by L. Verardi in [34], using finite group rings of odd characteristic. An attempt to discuss automorphisms of Verardi's examples was made in [26]. We take the opportunity to correct several errors in [26]: Corollary 2.3, Proposition 2.4(a,b,d) and Theorem 2.5 in that paper are false. See 5.4, 7.6, and 9.12 below. Actually, Verardi's groups may be interpreted as unipotent subgroups of algebraic groups over rings, see 6.1 below. However, it turns out that an interpretation as (generalized) Heisenberg groups is better suited for our interest in automorphisms.

Recall that a non-commutative p-group P is called *special* if its commutator subgroup P' and its center $\mathrm{Z}(P)$ both coincide with the Frattini subgroup $\Phi(P)$

0138-4821/93 \$ 2.50

(that is, the intersection of all maximal subgroups of P). Every special p-group has exponent dividing p^2, and is nilpotent of class at most 2. The obvious remark that a commutative group P with $P' = \mathrm{Z}(P)$ is trivial shows that, in assuming non-commutativity, we concentrate on the interesting case.

Throughout the present paper, let $\mathbb{F}$ denote a commutative field. Note that a not necessarily commutative field $\mathbb{K}$ is considered in Section 8 and in Section 9. Characteristic 2 will almost always be excluded explicitly, because we want to secure that the nilpotent groups that we construct are not commutative. Instead of group rings over $\mathbb{F}$, we will consider more general rings whenever this seems reasonable.

We briefly state our main results, details and proofs will be given below:

Theorem 1.1. *Let R be a ring such that 2 is invertible in R, and let V_R be the corresponding Verardi group (see 4.2 for the definition). By $\mathrm{Hom}(R^2, R)$ we denote the set of all additive maps from R^2 to R.*

1. *If R is commutative then $\mathrm{Aut}(\mathrm{V}_R)$ is isomorphic to the semidirect product $\Gamma\mathrm{L}(2, R) \ltimes \mathrm{Hom}(R^2, R)$. See 7.2.*
2. *If R is a local ring (for instance, the group ring of a finite p-group over a field of characteristic p) then $\mathrm{Aut}(\mathrm{V}_R)$ is known, see 9.2.*
3. *Assume $\mathrm{char}\,\mathbb{F} = p > 0$, let $G = \langle g \rangle$ be cyclic of order p^n, and put $R := \mathbb{F}[G]$. Then $\mathrm{Aut}(\mathrm{V}_R)$ is isomorphic to a semidirect product $\Gamma\mathrm{L}(2, R) \ltimes \mathrm{Hom}(\mathbb{F}^{p^{2n}}, \mathbb{F}^{p^n})$. See 9.10.*
4. *Let $\mathbb{K}$ be a (not necessarily commutative) field, let $n \geq 2$ be an integer, and put $R := \mathbb{K}^{n\times n}$. Then $\mathrm{Aut}(\mathrm{V}_R)$ is determined in 8.5, representatives for the orbits are given in 8.8. The case $n = 1$ for $\mathbb{K}$ not commutative is treated in 11.1.*

In most of these cases, the results also allow to determine the orbits under $\mathrm{Aut}(\mathrm{V}_R)$. In fact, partial information about these orbits often plays a crucial role in the determination of the automorphism group, see 5.13.

2. Heisenberg groups

The Verardi groups that we are going to study are isomorphic to groups of triangular 3×3 matrices over rings, see 6.1 below. However, the matrix description effectively hides most of the automorphisms. The present section provides the basis for a description that is better suited to our purposes.

Up to isomorphism, every special p-group of prime exponent $p > 2$ is obtained as a special case of the following construction, see 2.5 and 2.7 below.

Definition 2.1. *Let A be a commutative ring, let V and Z be modules over A, and let $\beta : V \times V \to Z$ be a bilinear map. Then*

$$(v, x) \circ_\beta (w, y) := \big(v + w, x + y + (v, w)^\beta\big)$$

defines a group multiplication on the set $V \times Z$. *We denote this group by* $\mathrm{B}(V, Z, \beta) = (V \times Z, \circ_\beta)$.
If β *is alternating (that is,* $(v, v)^\beta = 0$*), we write* $\langle v, w\rangle \coloneqq (v, w)^\beta$*, and* $\mathrm{GH}(V, Z, \beta) := \mathrm{B}(V, Z, \beta)$. *These groups are called (generalized) Heisenberg groups.*

Remarks 2.2. If all else fails, we consider abelian groups as modules over the ring $\mathbb{Z}$.

We will see in 2.4 below that $\mathrm{B}(V, Z, \alpha)$ is isomorphic to a Heisenberg group whenever 2 is invertible in A.

If V and Z are elementary abelian p-groups (i.e., vector spaces of characteristic p) then the group $\mathrm{B}(V, Z, \alpha)$ has exponent p or 4, and its commutator group is contained in the normal subgroup $\{0\} \times Z$, which in turn is contained in the center.

Remarks 2.3. If β is alternating, then the operation $*_\beta$ coincides with addition on each cyclic submodule of $V \times Z$. Consequently, the group $\mathrm{GH}(V, Z, \beta)$ is divisible if $A = \mathbb{F}$ is a field with $\operatorname{char} \mathbb{F} = 0$, and $\operatorname{char} A = e$ implies that $\mathrm{GH}(V, Z, \beta)$ has exponent e.

Every alternating bilinear map β is skew-symmetric. Conversely, a skew-symmetric bilinear map over a ring in which 2 is a unit is alternating. Sometimes, alternating maps are also called symplectic, but we reserve this terminus for maps preserving an alternating form.

Putting $[(v, x), (w, y)] := (0, \langle v, w\rangle) = (v, x)^{-1} *_\beta (w, y)^{-1} *_\beta (v, x) *_\beta (w, y)$ we obtain a Lie bracket on the module $V \times Z$; this defines a Lie algebra called $\mathfrak{gh}(V, Z, \beta)$. If $A = \mathbb{R}$ and $\mathfrak{gh}(V, Z, \beta)$ has finite dimension then $\mathrm{GH}(V, Z, \frac{1}{2}\beta)$ is the corresponding simply connected group, modeled on $V \times Z$ by Baker-Campbell-Hausdorff multiplication. Note that $(v, x) \mapsto (v, \frac{1}{2}x)$ is an isomorphism from $\mathrm{GH}(V, Z, \beta)$ onto $\mathrm{GH}(V, Z, \frac{1}{2}\beta)$.

Actually, the Baker-Campbell-Hausdorff series on $\mathfrak{gh}(V, Z, \beta)$ makes sense over any commutative ring such that 2 is invertible: all commutators belong to the center of $\mathfrak{gh}(V, Z, \beta)$, and the series reduces to the polynomial $X + Y + \frac{1}{2}[X, Y]$. See [18] §9.2, §10 for a discussion of the Baker-Campbell-Hausdorff series in arbitrary nilpotent groups. If A has prime characteristic $p > 2$ then $\mathfrak{gh}(V, Z, \beta)$ is the associated Lie ring for the p-group $\mathrm{GH}(V, Z, \beta)$ in the sense of Zassenhaus [35]; cf. [13] Section 5.6, or [18] Chapter 6.

Heisenberg groups are "standard forms" of the groups $\mathrm{B}(V, Z, \beta)$ constructed in 2.1.

Theorem 2.4. *Let* V, Z *be modules over a commutative ring* A*, and let* $\alpha : V \times V \to Z$ *be any bilinear map. If 2 is invertible in* A*, then*

$$\breve{\alpha} : V \times V \to Z : (v, w) \mapsto \langle v, w\rangle := \frac{1}{2}\left((v, w)^\alpha - (w, v)^\alpha\right)$$

is an alternating map, and the following hold:

1. *The map* $\eta : \mathrm{B}(V,Z,\alpha) \to \mathrm{GH}(V,Z,\breve{\alpha}) : (v,x) \mapsto \left(v, x - \frac{1}{2}(v,v)^\alpha\right)$ *is an isomorphism of groups. Note also that* $(v,x) \mapsto (v,2x)$ *is an isomorphism from* $\mathrm{GH}(V,Z,\breve{\alpha})$ *onto* $\mathrm{GH}(V,Z,2\breve{\alpha})$.
2. *The set of commutators in* $\mathrm{GH}(V,Z,\breve{\alpha})$ *is* $C := \{\left(0,\langle v,w\rangle\right) \mid v,w \in V\}$, *and this is also the set of commutators in* $\mathrm{B}(V,Z,\alpha)$. *In fact, in each of the groups, the commutator of* (v,x) *and* (w,y) *equals* $(0,\langle v,w\rangle)$.
3. *The center of* $\mathrm{GH}(V,Z,\breve{\alpha})$ *is* $\{(v,x) \in V \times Z \mid \forall w \in V : \langle v,w\rangle = 0\}$, *and this is also the center of* $\mathrm{B}(V,Z,\alpha)$.
4. *The Frattini subgroup of* $\mathrm{GH}(V,Z,\breve{\alpha})$ *coincides with* $\mathrm{GH}(V,Z,\breve{\alpha})' = \langle C\rangle$, *and this is also the Frattini subgroup of* $\mathrm{B}(V,Z,\alpha)$.
5. *Now assume that* A *is a field. Then* $\mathrm{GH}(V,Z,\breve{\alpha})$ *is isomorphic to* $T \times \mathrm{GH}(W,\langle C\rangle,\beta) \times U$, *where* W *is a vector space complement for* $T := \{v \in V \mid \forall w \in V : \langle v,w\rangle = 0\}$ *in* V, *the subspace* U *is a complement for* $\langle C\rangle$ *in* Z, *and* $\beta : W \times W \to \langle C\rangle$ *is the restriction of* $\breve{\alpha}$.

Proof. It is obvious that $\breve{\alpha}$ is alternating, and that the map η is a bijection. Using bi-additivity of α, we compute $\left((v,x) \circ_\alpha (w,y)\right)^\eta = (v,x)^\eta *_{\breve{\alpha}} (w,y)^\eta$. The rest of assertion 1 is verified easily.

In $\mathrm{GH}(V,Z,\breve{\alpha})$, we have $[(v,x),(w,y)] = (v,x)^{-1} *_{\breve{\alpha}} (w,y)^{-1} *_{\breve{\alpha}} (v,x) *_{\breve{\alpha}} (w,y) = \left(0,\langle v,w\rangle\right)$. Thus C is the set of commutators in $\mathrm{GH}(V,Z,\breve{\alpha})$, and $C^\eta = C$ yields the assertion for $\mathrm{B}(V,Z,\alpha)$.

Clearly, the set C is contained in the center of $\mathrm{GH}(V,Z,\breve{\alpha})$. The commutator $(0,\langle v,w\rangle)$ is trivial just if v is orthogonal to w with respect to $\breve{\alpha}$. This gives the center of $\mathrm{GH}(V,Z,\breve{\alpha})$, and of $\mathrm{B}(V,Z,\alpha)$, as well.

Finally, let M be a maximal subgroup of $H := \mathrm{GH}(V,Z,\beta)$. The quotient MH'/H' is a maximal subgroup in the vector space H/H' if, and only if, the commutator subgroup $H' = \langle C\rangle$ is contained in M. Thus $\Phi(H/H') = \{0\}$ implies $\Phi(H) \le H'$. If H' is not contained in M, we obtain $H = MH'$. The fact that H' is contained in the center of H gives $M' = (MH')' = H'$, yielding a contradiction.

The last assertion is checked by routine computations. □

Excluding fields or rings of even characteristic will occur as a standard assumption in the present paper. A main reason is that groups of exponent 2 are abelian. Nonabelian special 2-groups (in the sense used in the introduction) are groups of exponent 4, and have to be treated by methods different from those used here.

The following variant of 2.4 even more motivates our interest in Heisenberg groups, and shows that it is quite natural to use this Lie-theoretic description.

Theorem 2.5. ([17], cf. [23] 6.3) *Let* p *be an odd prime, and let* G *be a group of exponent* p *such that* G' *is contained in the center* $Z := \mathrm{Z}(G)$. *Then* G *is isomorphic to a Heisenberg group* $\mathrm{GH}(G/Z,Z,\beta)$, *where* $\beta : G/Z \times G/Z \to Z$ *maps* (Zg,Zh) *to the commutator* $g^{-1}h^{-1}gh$. □

This may be interpreted as a generalization of [7] 3.1. A standard trick of linear algebra (e.g., see [14] Ch. V, §2) allows to replace any alternating map $\beta : V \times V \to$

Z with the linear map $\hat{\beta} : V \wedge V \to Z$ such that $(v \wedge w)^{\hat{\beta}} = (v, w)^{\beta}$. Our frequent assumption that $\{0\} \times Z$ is generated by commutators in $\mathrm{GH}(V, Z, \beta)$ just means that $\hat{\beta}$ is surjective. In that case, the inequality $\dim_{\mathbb{F}} Z \le \dim_{\mathbb{F}}(V \wedge V) = \binom{\dim_{\mathbb{F}} V}{2}$ is obtained. By 2.5, this generalizes the observation made in [7] 2.4: for any special p-group G of order p^{m+s} with $|G'| = p^s$, one has $s \le \binom{m}{2}$.

Definition 2.6. *A Heisenberg group $H = \mathrm{GH}(V, Z, \beta)$ is called reduced if its center $\mathrm{Z}(H)$ coincides with its commutator subgroup H'. Thus the last assertion of* 2.4 *says that every Heisenberg group is the cartesian product of a reduced Heisenberg group and a vector space.*

Corollary 2.7. *Let p be an odd prime. A group of exponent p is a special p-group if, and only if, it is isomorphic to a reduced Heisenberg group.* □

3. Automorphisms of Heisenberg groups

For abelian groups V, Z, let $\mathrm{Hom}(V, Z)$ denote the abelian group of additive maps from V to Z. Simple computations suffice to verify:

Lemma 3.1. *Let $\mathrm{GH}(V, Z, \beta)$ be a Heisenberg group, let $\mu \in \mathrm{Aut}(V)$ and $\tau \in \mathrm{Hom}(V, Z)$, and assume that there exists $\mu' \in \mathrm{Aut}(Z)$ such that $\langle v^{\mu}, w^{\mu} \rangle = \langle v, w \rangle^{\mu'}$ holds for all $v, w \in V$. Then*

$$\varphi_{\mu,\tau,\mu'} : \mathrm{GH}(V, Z, \beta) \to \mathrm{GH}(V, Z, \beta) : (v, x) \mapsto (v^{\mu}, x^{\mu'} + v^{\tau})$$

is an automorphism of $\mathrm{GH}(V, Z, \beta)$*, and of* $\mathfrak{gh}(V, Z, \beta)$ *(considered as a Lie algebra over the prime field), as well. In particular, the set*

$$\mathrm{K} := \{(v, z) \mapsto (v, z + v^{\tau}) \mid \tau \in \mathrm{Hom}(V, Z)\}$$

is a subgroup of $\mathrm{Aut}(\mathrm{GH}(V, Z, \beta))$. □

In many cases, these are in fact *all* the automorphisms:

Theorem 3.2. ([23] 4.4, cf. [1] 5.1) *Let V and Z be vector spaces of characteristic different from* 2*. Assume that $\beta \colon V \times V \to Z$ is an alternating map such that Z is additively generated by the image $(V \times V)^{\beta}$. Then the automorphisms of* $\mathrm{GH}(V, Z, \beta)$ *are exactly the maps $\varphi_{\mu,\tau,\mu'}$ introduced in* 3.1. □

Consequently, the automorphisms of the group $\mathrm{GH}(V, Z, \beta)$ are the same as the automorphisms of the Lie algebra $\mathfrak{gh}(V, Z, \beta)$, considered as an algebra over the prime field – another reason for the Lie-theoretic point of view!

While quite different bi-additive maps may describe the same isomorphism type of groups, the alternating map is as unique[1] as it can be, and allows simple solutions for the isomorphism problem (cf. [1] 6.2):

[1] In fact, it is nothing but the commutator map, see 2.4.2.

Corollary 3.3. *Let S, Y and V, Z be vector spaces over commutative fields $\mathbb{E}$ and $\mathbb{F}$, respectively. Assume that $\gamma : S \times S \to Y$ and $\beta : V \times V \to Z$ are bi-additive maps with the additional property that Y and Z are generated by the image of γ and of β, respectively. Then $\mathrm{B}(S, Y, \gamma)$ and $\mathrm{B}(V, Z, \beta)$ are isomorphic if, and only if, the alternating maps $\check{\gamma}$ and $\check{\beta}$ are equivalent (that is, there are additive bijections $\mu : S \to V$ and $\mu' : Y \to Z$ such that $(s^\mu, t^\mu)^{\check{\beta}} = (s,t)^{\check{\gamma}\mu'}$ holds for all $s, t \in S$).* $\square$

Remark 3.4. Let $H := \mathrm{GH}(V, Z, \beta)$ be a reduced Heisenberg group. Mapping $\psi = \varphi_{\mu,\tau,\mu'} \in \mathrm{Aut}(H)$ to μ is a group homomorphism σ from $\mathrm{Aut}(H)$ onto a subgroup Σ of $\mathrm{Aut}(V)$. The kernel of σ is the group $\mathrm{K} = \{(v, z) \mapsto (v, z + v^\tau) | \tau \in \mathrm{Hom}(V, ,)Z)\}$ *central automorphisms*, which contains the group of inner automorphisms of H.

Note also that μ' is determined by $\mu = \psi^\sigma$ (and our assumption that H is reduced), and we obtain a group homomorphism $\delta : \Sigma \to \mathrm{Aut}(Z)$ mapping μ to $\mu^\delta := \mu'$. The kernel of δ is the "symplectic group" $\mathrm{Sp}\,(\beta) := \{\mu \in \mathrm{Aut}(V) | \forall v, w \in V : \langle v^\mu, w^\mu \rangle = \langle v, w \rangle\}$.

This discussion shows:

Theorem 3.5. *Let $\mathrm{GH}(V, Z, \beta)$ be a reduced Heisenberg group. Then $\mathrm{Aut}(\mathrm{GH}\,(V, Z, \beta))$ is isomorphic to a semidirect product $\Sigma \ltimes \mathrm{Hom}(V, Z)$, where Σ is defined as in 3.4, and $\mu \in \Sigma$ acts on the additive group $\mathrm{Hom}(V, Z)$ as multiplication from the left by μ^{-1} and, at the same time, multiplication from the right by the image of μ under δ.* $\square$

Together with the observation that $\Sigma / \mathrm{Sp}\,(\beta)$ is a subgroup of $\mathrm{Aut}(Z)$, this result imposes severe restrictions on the size (and structure) of the automorphism group of a reduced Heisenberg group. For instance, only in rare instances it will happen that Σ coincides with $\mathrm{Aut}(V)$, contrary to the claims made in [26] 2.3, 2.5. See 5.3, 7.6, and 9.12 below. It is even possible that Σ consists of scalar multiples of the identity; see [33].

Frequently, it is easier to understand $\mathbb{F}$-linear maps instead of arbitrary additive maps. Additive maps between vector spaces over $\mathbb{F}$ are linear over the prime field of $\mathbb{F}$. For dimension arguments, it is usually sufficient to assume that $\mathbb{F}$ has finite dimension over its prime field. This condition is fulfilled for every finite field. In a topological context, it is remarkable that every non-discrete locally compact field of characteristic 0 has finite dimension over the closure $\bar{\mathbb{Q}}$ of its prime field, and every continuous additive map is $\bar{\mathbb{Q}}$-linear.

We introduce a useful invariant to distinguish orbits under the automorphism group. In [15] and in [30], this invariant is also used to show that injective homomorphisms do not exist between certain Heisenberg groups. For the groups $\mathrm{V}_{\mathbb{F}_p[G]}$ that are introduced in 4.2 below, the non-central elements with maximal values of this invariant are discussed in Section 3 of [34].

Lemma 3.6. *Let $H = \mathrm{GH}(V, Z, \beta)$ be a generalized Heisenberg group, where V and Z are modules over a commutative ring A such that 2 is invertible. For each $v \in V$, let C_v denote the centralizer of $(v, 0)$ in H. Then the following hold.*

1. $\mathrm{C}_v = \{w \in V \mid \langle v, w\rangle = 0\} \times Z$.
2. *The orbit of $(v, 0)$ under $\mathrm{Aut}(H)$ contains $\{v\} \times \{v^\tau \mid \tau \in \mathrm{Hom}(V, Z)\} \subseteq \{v\} \times Z$.*
3. *If $v \neq 0$ generates a free direct summand of the A-module V (in particular, if A is a field), the orbit of $(v, 0)$ contains $\{v\} \times Z$.*
4. *If every element of V generates a free direct summand of V, then every orbit has a representative of the form $(v, 0)$ or $(0, x)$, where $v \in V$ and $x \in Z$.*
5. *If A is a field of finite dimension over its prime field and Z is generated by the image of β then the cardinal number $c_v := \dim_A \{w \in V \mid \langle v, w\rangle = 0\}$ is invariant under $\mathrm{Aut}(H)$.*

Proof. The first assertion is obvious. The set $\{v\} \times \{v^\tau \mid \tau \in \mathrm{Hom}(V, Z)\}$ is the orbit of $(v, 0)$ under the subgroup K of $\mathrm{Aut}(H)$. If v generates a free direct summand S of V, there exists a homomorphism from V onto A, mapping v to 1, and we find $\{v^\tau \mid \tau \in \mathrm{Hom}(V, Z)\} = \{1^\varphi \mid \varphi \in \mathrm{Hom}(R, Z)\} = Z$.

Since H' is characteristic in H, every automorphism α of H induces an isomorphism from C_v/H' onto C_{v^α}/H'. This isomorphism is A-semilinear, and the last assertion follows. □

The following invariants will also be useful:

Definition 3.7. *For $v \in V$, let $\mathrm{CC}_v := \{u \in V \mid \forall (w, 0) \in \mathrm{C}_v : \langle u, w\rangle = 0\} = \bigcap_{(w,x)\in \mathrm{C}_v} \mathrm{C}_w$, and put $\mathrm{D}_v := \{\langle v, w\rangle \mid w \in V\}$.*

Let x be any element of Z. Then $\{0\} \times \mathrm{D}_v$ consists of all commutators of elements of $\mathrm{GH}(V, Z, \beta)$ with (v, x), and this set of commutators does not depend on x.

4. Verardi's construction

In [34], L. Verardi constructs and discusses a class of finite special p-groups, as follows.

Examples 4.1. Let G be a finite group, let p be an odd prime, and let $\mathbb{F}_p$ be the field with p elements. Using the multiplication in the group algebra $\mathbb{F}_p[G]$, we define a bi-additive map

$$\alpha : \mathbb{F}_p[G]^2 \to \mathbb{F}_p[G] : \big((a, s), (b, t)\big) \mapsto -bs\,,$$

and put $P_G := \mathrm{B}(\mathbb{F}_p[G]^2, \mathbb{F}_p[G], \alpha)$.

Verardi shows that P_G is a special group of exponent p; this is also an easy consequence of 2.4 and 2.3. We generalize Verardi's construction, replacing $\mathbb{F}_p[G]$ by the group ring $\mathbb{F}[G]$ over a larger ground field $\mathbb{F}$, or even by an arbitrary ring R. For reasons as stated above, we prefer the description as Heisenberg groups.

Definition 4.2. *Let R be a ring. Then the map*

$$\beta : R^2 \times R^2 \to R : \big((a,s),(b,t)\big) \mapsto \big\langle (a,s),(b,t)\big\rangle := at - bs$$

is alternating. We write $\mathrm{V}_R := \mathrm{GH}(R^2, R, \beta)$*, and call this a Verardi group.*

Example 4.3. Let G be any group, and assume $\operatorname{char}\mathbb{F} \neq 2$. Then 2 is a unit in $\mathbb{F}[G]$, and 2.4.1 yields that $P_G = \mathrm{B}(\mathbb{F}_p[G]^2, \mathbb{F}_p[G], \alpha)$ is isomorphic to $\mathrm{V}_{\mathbb{F}_p[G]}$.

Theorem 4.4.
1. *The set of commutators in* V_R *is* $C := \{(0,0)\} \times R$.
2. *The center of* V_R *is* C.
3. *The Frattini subgroup of* V_R *is* C.
4. *If the characteristic of the ring R is an odd prime p (in particular, if R is a group ring over a commutative field $\mathbb{F}$ with* $\operatorname{char}\mathbb{F} = p > 2$*) then* V_R *has exponent p, and is a special p-group.*

Proof. For any $a \in R$, we put $v := (a,0)$ and $w := (0,1)$ and find that $\big((0,0),a\big) = \big((0,0),\langle v,w\rangle\big)$ is a commutator in V_R; cf. 2.4. Thus $C = \{(0,0)\} \times R$.
For $\big((a,s),z\big)$ in $R^2 \times R$, we compute commutators with $\big((0,1),0\big)$ and $\big((1,0),0\big)$ in V_R as $\big((0,0),a\big)$ and $\big((0,0),-s\big)$, respectively. This shows that C is the center of V_R. The last assertions repeat general properties of (reduced) Heisenberg groups, see 2.4 and 2.3. ☐

If R is a commutative ring, we have

$$\big\langle (a,s),(b,t)\big\rangle = \det_R \begin{pmatrix} a & s \\ b & t \end{pmatrix} .$$

For matrices $A, B \in R^{2\times 2}$, multiplicativity $\det_R(AB) = \det_R A \det_R B$ of the determinant implies

$$\forall A \in \mathrm{GL}(2,R)\ \forall \alpha \in \mathrm{Aut}(R)\ \forall v,w \in V : \langle v^\alpha A, w^\alpha A\rangle = \langle v,w\rangle^\alpha \det_R A\,,$$

and we obtain an embedding of $\Gamma\mathrm{L}(2,R) := \mathrm{Aut}(R) \ltimes \mathrm{GL}(2,R)$ into Σ:

Theorem 4.5. *If R is a commutative ring then* $\mathrm{Aut}(\mathrm{V}_R)$ *contains subgroups* $\Lambda \cong \mathrm{GL}(2,R)$ *and* $\Gamma \cong \Gamma\mathrm{L}(2,R)$*. The group Γ is mapped injectively into Σ. Restricting the homomorphism δ introduced in* 3.4 *to Λ, we obtain the determinant map over the ring R. The intersection of Γ with the group of inner automorphisms is trivial.* ☐

We shall show in Section 7 that Σ and $\Gamma\mathrm{L}(2,R)$ coincide for every commutative ring R.

5. Automorphisms of Verardi groups

Proposition 5.1. *If the ring R contains divisors of zero then* $\mathrm{Aut}(\mathrm{V}_R)$ *has more than three orbits on* V_R*, and more than two orbits on* $\mathrm{V}_R/(\mathrm{V}_R)'$.

Proof. Assume that a, t are nonzero elements of R with $at = 0$. Then t belongs to the annihilator $\mathrm{N}_a := \{x \in R \mid ax = 0\}$, and $\mathrm{C}_{(a,0)} = (R \times \mathrm{N}_a) \times R$ is different from $\mathrm{CC}_{(a,0)}$ because $((1,0),0) \in \mathrm{C}_{(a,0)}$ is not contained in $\mathrm{CC}_{(a,0)} \leq \mathrm{C}_{(0,s)}$. Thus $((1,0),0)$ and $((a,0),0)$ represent different orbits in V_R, as well as in the quotient $\mathrm{V}_R/(\mathrm{V}_R)'$. The neutral element forms a third orbit in $\mathrm{V}_R/(\mathrm{V}_R)'$. □

Corollary 5.2. *Assume* $\mathrm{char}\,\mathbb{F} \neq 2$*. If G is a group with more than one element then* $\mathrm{Aut}(\mathrm{V}_{\mathbb{F}[G]})$ *has more than two orbits on* $\mathrm{V}_{\mathbb{F}[G]}/\mathrm{V}'_{\mathbb{F}[G]}$.

Proof. For any $g \in G \setminus \{1\}$, the elements $a := 1 - g$ and $t := \sum_{g \in G} g$ in $\mathbb{F}[G] \setminus \{0\}$ satisfy $at = 0$. □

This observation yields information about the group Σ introduced in 3.4:

Corollary 5.3. *If $n := |G| > 1$ then Σ is a proper subgroup of the group of additive automorphisms of $\mathbb{F}[G]^2$; it is not even transitive on $\mathbb{F}[G]^2 \setminus \{(0,0)\}$. In the case where $\mathbb{F} = \mathbb{F}_p$, we have that $|\Sigma|$ is a proper divisor of* $|\mathrm{GL}(2n,p)| = p^{2n^2-n}(p^{2n}-1)\cdots(p-1) = p^{2n^2-n}\prod_{k=1}^{2n}(p^k-1)$. □

Remarks 5.4. Corollary 5.3 shows that the claims made in [26] 2.3, 2.4(d), and 2.5 are false for all cases except the trivial one. In [26] 2.5, it is claimed that every automorphism of the subgroup $A := (\mathbb{F}_p[G] \times \{0\}) \times \mathbb{F}_p[G]$ of P_G extends to an automorphism of P_G. As $\mathrm{Aut}(A)$ acts transitively on the nontrivial elements of the vector space A, while A contains the characteristic commutator subgroup of P_G, this is a sheer impossibility. The claim in [26] 2.4(b), stating that $\mathrm{Aut}(P_G)$ contains a subgroup of order $p^{2|G|}|\mathrm{Aut}(P_G)|$, appears to be misprinted. The claim [26] 2.4(a), stating that the Sylow p-subgroups of $\mathrm{Aut}(P_G)$ have order $p^{4|G|^2-|G|}$ is false for $|G| = 2$, see 7.6 and 9.12 below.

Straightforward computations suffice to check the following.

Lemma 5.5. *Let R be any ring such that 2 is a unit, and let $R^\times$ be its group of units.*

1. *For each $h \in R^\times$, mapping $\big((a,s),x\big)$ to $\big((ah, h^{-1}s),x\big)$ is an automorphism ζ_h of V_R. Mapping h to ζ_h is an injective group homomorphism ζ from $R^\times$ to* $\mathrm{Aut}(\mathrm{V}_R)$.
2. *For each $c \in R^\times$, automorphisms λ_c and ρ_c of V_R are defined by $\big((a,s),x\big)^{\lambda_c} := \big((ca,s),cx\big)$ and $\big((a,s),x\big)^{\rho_c} := \big((a,sc),xc\big)$. Mapping (c,d) to $\lambda_{c^{-1}}\rho_d$ is an injective group homomorphism from $(R^\times)^2$ to* $\mathrm{Aut}(\mathrm{V}_R)$.
3. *Mapping (c,h,d) to $\lambda_{c^{-1}}\zeta_h\rho_d$ is a homomorphism from $(R^\times)^3$ onto a subgroup Δ of* $\mathrm{Aut}(\mathrm{V}_R)$*, with kernel* $\{(c,c,c) \mid c \in \mathrm{Z}(R^\times)\}$.

4. *Every ring automorphism* α *of* R *gives an automorphism* $\tilde\alpha$ *of* V_R, *by* $\big((a,s),x\big)^{\tilde\alpha} := \big((a^\alpha,s^\alpha),x^\alpha\big)$. *Mapping* α *to* $\tilde\alpha$ *is an injective homomorphism from* $\mathrm{Aut}(R)$ *onto the subgroup* $\mathrm{A} := \{\tilde\alpha \mid \alpha \in \mathrm{Aut}(R)\}$ *of* $\mathrm{Aut}(\mathrm{V}_R)$.
5. *If* R *is commutative then every semilinear bijection of the free module* R^2 *belongs to* Σ, *and we obtain an embedding of* $\Gamma\mathrm{L}(2,R)$ *into* Σ, *cf.* 4.5. □

In general, the group $\mathrm{GL}(2,R)$ is not contained in Σ, but certain elementary transvections can be found in Σ, see 5.11.

For any group G, linear extension of $g \mapsto g^{-1}$ yields an *anti-automorphism* of $\mathbb{F}[G]$: that is, an additive bijection $x \mapsto \bar x$ with $\overline{xy} = \bar y \bar x$.

Lemma 5.6. *For every anti-automorphism* α *of the ring* R, *we obtain an automorphism* $\hat\alpha$ *of* V_R *by putting* $\big((a,s),x\big)^{\hat\alpha} := \big((s^\alpha,a^\alpha),-x^\alpha\big)$. □

In particular, mapping $\big((a,s),x\big)$ to $\big((\bar s,\bar a),-\bar x\big)$ is an automorphism of $\mathrm{V}_{\mathbb{F}[G]}$.

Theorem 5.7. *The stabilizer of* $(1,0)$ *and* $(0,1)$ *in* Σ *equals the set* $\mathrm{A}^\sigma = \{\tilde\alpha^\sigma \mid \alpha \in \mathrm{Aut}(R)\}$. *Every element* $\mu \in \Sigma$ *that interchanges* $(1,0)$ *with* $(0,1)$ *is induced by an anti-automorphism of* R.

Proof. Let μ be an element of the stabilizer, and let $\delta : \Sigma \to \mathrm{Aut}(R,+)$ be as in 3.4. As $\mathrm{C}_{(1,0)}/(\mathrm{V}_R)' = R \times \{0\}$ and $\mathrm{C}_{(0,1)}/(\mathrm{V}_R)' = \{0\} \times R$ are invariant under μ, we may define maps $\alpha_i : R \to R$ by $(r,0)^\mu = (r^{\alpha_1},0)$ and $(0,r)^\mu = (0,r^{\alpha_2})$, respectively. Clearly, these are additive maps. We claim that they are multiplicative, as well. Indeed, evaluating the functional equation $\langle v^\mu, w^\mu\rangle = \langle v,w\rangle^{\mu^\delta}$ first at $v \in \{(1,0),(0,1)\}$ we find $\alpha_1 = \mu^\delta = \alpha_2$, and then the general case $v = (a,0)$ and $w = (0,b)$ yields that μ^δ is multiplicative. Thus $\alpha := \mu^\delta$ is an automorphism of R with $\mu = \tilde\alpha^\sigma$, and the proof of the first assertion is complete.

The second assertion follows analogously, we just note that μ extends to an automorphism of V_R that interchanges $\mathrm{C}_{(1,0)} = (R \times \{0\}) \times R$ with $\mathrm{C}_{(0,1)} = (\{0\} \times R) \times R$. □

Definition 5.8. *For each ring* R, *let* R' *denote the additive subgroup generated by the set* $\{xy - yx \mid x,y \in R\}$.

Lemma 5.9. *For* $a,s \in R$, *with* $a \in R^\times$ *we have:*
1. $\mathrm{C}_{(a,s)}$ *is commutative if, and only if,* $R's = \{0\}$.
2. $\mathrm{C}_{(s,a)}$ *is commutative if, and only if,* $sR' = \{0\}$.
3. *If* R' *contains invertible elements then commutativity of* $\mathrm{C}_{(a,s)}$ *or* $\mathrm{C}_{(s,a)}$ *is equivalent to* $s = 0$.

Proof. Without loss, we may assume $a = 1$, cf. 5.5. We have $\mathrm{C}_{(s,1)} = \{\big((sx,x),z\big) \mid x,z \in R\}$, and $\mathrm{C}_{(1,s)} = \{\big((x,xs),z\big) \mid x,z \in R\}$. The commutator subgroups $\mathrm{C}'_{(s,1)}$ and $\mathrm{C}'_{(1,s)}$ are generated by the sets $\{\big((0,0),s(xy-yx)\big) \mid x,y \in R\}$, and $\{\big((0,0),(xy-yx)s\big) \mid x,y \in R\}$ of commutators, respectively. □

Example 5.10. Let $\mathbb{K}$ be a (not necessarily commutative) field with center $\mathrm{Z}(\mathbb{K})$, and let $n \geq 2$ be an integer. Then the subset $\{xy - yx \mid x, y \in \mathrm{Z}(\mathbb{K})^{n\times n}\} \subseteq \{xy - yx \mid x, y \in \mathbb{K}^{n\times n}\}$ additively generates the $\mathrm{Z}(\mathbb{K})$-subspace $\mathfrak{sl}(n, \mathrm{Z}(\mathbb{K}))$ containing all elements of $\mathrm{Z}(\mathbb{K})^{n\times n}$ with vanishing trace. In particular, $\mathfrak{sl}(n, \mathrm{Z}(\mathbb{K}))$ contains invertible elements.

Lemma 5.11. *Let $z \in R$.*

1. *If $R't = \{0\}$ then the transvection $\tau_t : \big((x,y),z\big) \mapsto \big((x, y + xt), z\big)$ belongs to* $\mathrm{Aut}(\mathrm{V}_R)$.
2. *If $sR' = \{0\}$ then the transvection ${}_s\tau : \big((x,y),z\big) \mapsto \big((x + sy, y), z\big)$ belongs to* $\mathrm{Aut}(\mathrm{V}_R)$. □

Of course, these elements of $\mathrm{Aut}(\mathrm{V}_R)$ are new only if the ring R is not commutative; they induce elements of $\mathrm{SL}(2, R)$ on R^2 if R is commutative (and the annihilator conditions on s, t are superfluous).

Definition 5.12. *The subgroups of* $\mathrm{Aut}(\mathrm{V}_R)$ *generated by the sets* $\{\tau_t | t \in R,\ R't = \{0\}\}$ *and* $\{{}_s\tau \mid s \in R, sR' = \{0\}\}$ *are denoted by* T_R *and* ${}_R\mathrm{T}$*, respectively. The group generated by* T_R *and* ${}_R\mathrm{T}$ *will be called* T.

Theorem 5.13. *Let R be a ring such that 2 is invertible. Then the following hold:*

1. *The stabilizer $\Sigma_{(1,0)}$ equals $(\mathrm{A}\Delta\, {}_R\mathrm{T})^\sigma$.*
2. *If $(0,1)$ belongs to the orbit $(1,0)^\Sigma$ then the ring R admits an anti-automorphism $*$, and we find $\{\mu \in \Sigma \mid (1,0)^\mu = (0,1)\} = (\mathrm{A}\Delta\, {}_R\mathrm{T}\langle\hat{*}\rangle)^\sigma = (\langle\hat{*}\rangle\mathrm{A}\Delta\mathrm{T}_R)^\sigma$.*
3. *If Φ is a subgroup of $\mathrm{Aut}(\mathrm{V}_R)$ such that the orbits $(1,0)^\Sigma$ and $(1,0)^{\Phi^\sigma}$ coincide, then $\Sigma = \Sigma_{(1,0)}\Phi^\sigma = (\mathrm{A}\Delta\, {}_R\mathrm{T}\Phi)^\sigma$, and $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\, {}_R\mathrm{T}\Phi\mathrm{K}$.*

Proof. Let $\mu \in \Sigma_{(1,0)}$, and put $(s,a) := (0,1)^\mu$. For any $x \in R$, the set of commutators $[\mathrm{C}_{(1,0)}, \big((s,a),x\big)] = \{(0,0)\} \times Ra$ equals $[\mathrm{C}_{(1,0)}, \big((0,1),0\big)]^\mu = \{(0,0)\} \times R^{\mu^\delta} = \{(0,0)\} \times R$, and there exists $x \in R$ with $xa = 1$. Now $\big((ax,1),0\big)$ belongs to $\mathrm{C}_{(s,a)}$, and commutativity of that group implies that it is contained in $\{(axt,t) \mid t \in R\} \times R$. Because the commutator $[\big((1,0),0\big), \mathrm{C}_{(s,a)}]$ also equals $[\big((1,0),0\big), \mathrm{C}_{(0,1)}] = \{(0,0)\} \times R$, we conclude $\mathrm{C}_{(s,a)} = \{(axt,t) \mid t \in R\} \times R$. Using commutativity of $\mathrm{C}_{(s,a)}$ again, we infer $axR' = \{0\}$. Applying a suitable transvection, we see that $(0,a)$ also belongs to the orbit of $(0,1)$ under $\Sigma_{(1,0)}$.

Now commutativity of $\mathrm{C}_{(0,a)}$ yields that $r \mapsto ra$ is an injective endomorphism of $(R,+)$, and we have proved that a is invertible. Now 5.9 applies, yielding $sR' = \{0\}$. Thus $\psi := ({}_{-s}\tau)^\sigma$ belongs to $({}_R\mathrm{T})^\sigma$, and $\mu\rho^\sigma_{a^{-1}}\psi$ fixes both $(1,0)$ and $(0,1)$. This means $\mu \in (\mathrm{A}\, {}_R\mathrm{T}\Delta)^\sigma = (\mathrm{A}\Delta\, {}_R\mathrm{T})^\sigma$, as claimed.

Now assume that there exists $\xi \in \Sigma$ such that $(1,0)^\xi = (0,1)$, and put $(0,1)^\xi := (a,s)$. Proceeding as before, we find that a is invertible, and $R's = \{0\}$. Thus we find an element in Σ that interchanges $(1,0)$ with $(0,1)$. According to 5.7, there exists an anti-automorphism $*$ of R, and every element of Σ that maps $(1,0)$ to $(0,1)$ belongs to the coset $\Sigma_{(1,0)}\mu = \Sigma_{(1,0)}\hat{*}^\sigma = (\mathrm{A}\Delta\, {}_R\mathrm{T}\langle\hat{*}\rangle)^\sigma$. The rest of assertion 2 follows from the observations that $\hat{*}$ normalizes A and Δ, but interchanges ${}_R\mathrm{T}$ with T_R.

A Frattini argument yields $\Sigma = \Sigma_{(1,0)}\Phi^\sigma$, and assertion 1 implies $\Sigma_{(1,0)}\Phi^\sigma = (\mathrm{A}\Delta\,{}_R\mathrm{T}\Phi)^\sigma$. The rest of assertion 3 follows from the fact that K is the kernel of the natural surjection from $\mathrm{Aut}(\mathrm{V}_R)$ onto Σ. □

Remark 5.14. The first part of the proof of 5.13 may be simplified if the ring R is *inverse symmetric*[2], that is, if $xa = 1$ implies $ax = 1$ in R.

Every commutative ring, every matrix ring $A^{n\times n}$ over a commutative ring A, every matrix ring $\mathbb{K}^{n\times n}$ over a (not necessarily commutative) field $\mathbb{K}$, every local ring (see Section 9) and every finite ring is inverse symmetric.

6. Unipotent subgroups of classical groups

Verardi groups play their role in important branches of group theory and geometry. For the following remarks, let R be a ring in which 2 is a unit (for instance, a group algebra $\mathbb{F}[G]$ over a commutative field with $\mathrm{char}\,\mathbb{F} \neq 2$). Straightforward calculations show:

Theorem 6.1. *The assignment*

$$\big((a,s),x\big) \mapsto \begin{pmatrix} 1 & a & \frac{1}{2}(x+as) \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} : \mathrm{V}_R \to \mathrm{UT}(3,R) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a,b,c \in R \right\}$$

is an isomorphism from V_R *onto the subgroup* $\mathrm{UT}(3,R)$ *of strict upper triangular matrices in* $\mathrm{GL}(3,R)$. □

Note that the group $\mathrm{UT}(3,R)$ is the unipotent radical of a Borel subgroup of $\mathrm{GL}(3,R)$.

Corollary 6.2. *If* $\mathbb{F}$ *is a finite field of characteristic* $p > 2$ *and* G *is a finite commutative group such that the order of* G *is not divisible by* p*, then* $\mathbb{F}[G]$ *is a cartesian product of finite fields of characteristic* p*, and* $\mathrm{V}_{\mathbb{F}[G]}$ *is isomorphic to a Sylow* p*-subgroup of* $\mathrm{GL}(3,\mathbb{F}[G])$. □

Remark 6.3. The group Δ (consisting of the automorphisms $\lambda_{c^{-1}}\zeta_h\rho_d$, cf. 5.5) is induced by the group of diagonal matrices in $\mathrm{GL}(3,R)$, which is contained in the normalizer of $\mathrm{UT}(3,R)$.

Theorem 6.4. *Assume that* R *is commutative. Then the assignment*

$$\eta : \big((a,s),x\big) \mapsto \begin{pmatrix} 1 & a & s & x \\ 0 & 1 & 0 & s \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

gives an isomorphism η *from* V_R *onto a subgroup* E_R *of* $\mathrm{Sp}(4,R)$. □

[2]Inverse symmetric rings are also called weakly 1-finite, or von Neumann finite. See [6] p. 20 for a generalization.

The group E_R is a proper subgroup of the unipotent radical of a Borel subgroup of $\mathrm{Sp}(4,R)$. However, it has geometric significance, being the elation group for the (Hjelmslev) symplectic generalized quadrangle over the ring R.

The embedding η constructed in 6.4 may also be regarded as an embedding into the semidirect product $\mathrm{Aut}(R) \ltimes \mathrm{GSp}(4,R)$. A large part (if not all) of the automorphism group $\mathrm{Aut}(\mathrm{V}_R)$ is then induced by the normalizer of E_R.

7. Verardi groups over commutative rings

Let R be a commutative ring such that 2 is invertible in R, and consider the group Σ induced on $\mathrm{V}_R/(\mathrm{V}_R)' \cong R^2$ by $\mathrm{Aut}(\mathrm{V}_R)$, as in 3.4. Recall from 4.5 that Σ contains the group $\Gamma\mathrm{L}(2,R)$ of all semilinear bijections of R^2. Our aim in the present section is to show that Σ coincides with $\Gamma\mathrm{L}(2,R)$.

Lemma 7.1. *The orbit of* $(1,0)$ *under* Σ *coincides with the orbit under* $\mathrm{SL}(2,R) \leq \Sigma$.

Proof. It suffices to show that $(1,0)^\Sigma$ is contained in the orbit under $\mathrm{SL}(2,R)$. For $(a,s) \in (1,0)^\Sigma$, we have $\mathrm{D}_{(a,s)} = R$. Therefore, we find $b,t \in R$ such that $at - bs = 1$. Now $(1,0)^\mu := (a,s)$ and $(0,1)^\mu := (b,t)$ defines $\mu \in \mathrm{SL}(2,R)$, as required. □

After 7.1, an application of 5.13 yields:

Theorem 7.2. *Let R be a commutative ring such that 2 is invertible. Then* $\Sigma = \Gamma\mathrm{L}(2,R)$, *and* $\mathrm{Aut}(\mathrm{V}_R) = \Gamma\mathrm{L}(2,R) \ltimes \mathrm{Hom}(R^2,R)$. □

Remark 7.3. Because V_R is isomorphic to $\mathrm{UT}(3,R)$ whenever R is a commutative ring with $2 \in R^\times$, our result 7.2 is a special case of a general result in [22], where the automorphisms of $\mathrm{UT}(n,R)$ are determined for each commutative ring R. We include the (simple) proof for the sake of completeness.

Example 7.4. Let G be the trivial group, and assume $\operatorname{char}\mathbb{F} \neq 2$. Then $\mathrm{V}_{\mathbb{F}[G]}$ is isomorphic to the (classical) Heisenberg group $\mathrm{GH}(\mathbb{F}^2,\mathbb{F},\det)$ obtained from the alternating map

$$\det : \mathbb{F}^2 \times \mathbb{F}^2 : \big((a,s),(b,t)\big) \mapsto \det \begin{pmatrix} a & s \\ b & t \end{pmatrix} .$$

It is well known (and follows easily from either 4.5 or 7.2) that the automorphism group $\mathrm{Aut}(\mathrm{GH}(\mathbb{F}^2,\mathbb{F},\det)) = \mathrm{Aut}(\mathfrak{gh}(\mathbb{F}^2,\mathbb{F},\det)) \cong \Gamma\mathrm{L}(2,\mathbb{F}) \ltimes \mathrm{Hom}(\mathbb{F}^2,\mathbb{F})$ acts with exactly 3 orbits:

$$\{(0,0)\}, \quad \{(0,z) \mid z \in \mathbb{F} \smallsetminus \{0\}\}, \quad \text{and} \quad \{(v,z) \mid v \in \mathbb{F}^2 \smallsetminus \{0\}, z \in \mathbb{F}\} .$$

Recall that $\mathrm{Hom}(\mathbb{F}^2,\mathbb{F})$ denotes the set of *all* additive maps from $\mathbb{F}^2$ to $\mathbb{F}$, and not only the $\mathbb{F}$-linear ones.

We discuss another application in detail. Let $C_2 = \{1, g\}$ be a group with 2 elements, and assume $\operatorname{char}\mathbb{F} \neq 2$. We have $\mathbb{F}[C_2] \cong \mathbb{F} \times \mathbb{F}$ in this case.

Proposition 7.5. *The automorphism group* $\operatorname{Aut}(\mathrm{V}_{\mathbb{F}[C_2]})$ *has* 5 *orbits on* $\mathrm{V}_{\mathbb{F}[C_2]}$. *More precisely, it acts with* 3 *orbits on the commutator subgroup, and* 2 *orbits outside.*

Proof. After 7.2, it remains to note that the non-trivial orbits of Σ correspond to the orbits outside the commutator group because of the action of the group K; cf. 3.4. □

Example 7.6. Let p be an odd prime, and write $R := \mathbb{F}_p[C_2]$. We define $\Sigma \leq \operatorname{Aut}(V, +)$ as in 3.4, and define $\iota : R \to R : a + bg \mapsto a - bg$. Then $\Sigma = \langle\iota\rangle \ltimes \mathrm{GL}(2, R)$, and $\operatorname{Aut}(\mathrm{V}_R) \cong \Gamma\mathrm{L}(2, R) \ltimes \operatorname{Hom}(R^2, R) = (\langle\iota\rangle \ltimes \mathrm{GL}(2, R)) \ltimes \operatorname{Hom}(R^2, R)$. The group $\mathrm{Sp}\,(\beta)$ coincides with $\mathrm{SL}(2, R)$, and we have

$$\begin{array}{rrcl} & |\Sigma| & = & 2(p-1)^4 p^2 (p+1)^2 \\ \text{and} & |\operatorname{Aut}(\mathrm{V}_R)| = |\Sigma|\, p^8 & = & 2(p-1)^4 p^{10} (p+1)^2 \,. \end{array}$$

In particular, the Sylow p-subgroups of Σ are strictly smaller than those of $\mathrm{GL}(2, \mathbb{F}_p)$.

Remark 7.7. The map $s + tg \mapsto (s + t, s - t)$ is an isomorphism from $\mathbb{F}[C_2]$ onto $\mathbb{F} \times \mathbb{F}$. According to a general principle (see 12.2 below), this induces an isomorphism

$$\big((a_1 + a_g g, s_1 + s_g g), x_1 + x_g g\big) \mapsto \\ \Big(\big((a_1 + a_g, s_1 + s_g), (a_1 - a_g, s_1 - s_g)\big), (x_1 + x_g, x_1 - x_g)\Big)$$

from $\mathrm{V}_{\mathbb{F}[C_2]}$ onto the group $\mathrm{V}_{\mathbb{F}\times\mathbb{F}} = \mathrm{GH}((\mathbb{F}^2)^2, \mathbb{F}^2, \gamma)$, where

$$\begin{array}{rccc} \gamma : & (\mathbb{F}^2)^2 \times (\mathbb{F}^2)^2 & \to & \mathbb{F}^2 \\ & \Big(\big((a, s), (a', s')\big), \big((b, t), (b', t')\big)\Big) & \mapsto & \left(\det\begin{pmatrix} a & s \\ b & t \end{pmatrix}, \det\begin{pmatrix} a' & s' \\ b' & t' \end{pmatrix}\right) . \end{array}$$

Thus there is an isomorphism from $\mathrm{V}_{\mathbb{F}[C_2]}$ onto $\mathrm{V}_\mathbb{F} \times \mathrm{V}_\mathbb{F} = \mathrm{GH}(\mathbb{F}^2, \mathbb{F}, \det) \times \mathrm{GH}(\mathbb{F}^2, \mathbb{F}, \det)$, and the result about the number of orbits under $\operatorname{Aut}(\mathrm{V}_{\mathbb{F}[C_2]})$ could also be taken from [31] 2.16.

8. Matrix rings

Full matrix rings occur as direct factors of certain group rings (see 12.1 below), but are also of independent interest, of course.

Let $\mathbb{K}$ be a (not necessarily commutative) field with $\operatorname{char}\mathbb{K} \neq 2$, and let $n \geq 2$ be an integer. In this section, we study V_R for the matrix ring $R := \mathbb{K}^{n\times n}$. We interpret R as the ring of endomorphisms of $\mathbb{K}^n$, acting by multiplication from the right on row vectors: in particular, we have $\ker x = \{v \in \mathbb{K}^n \mid vx = 0\}$ and $\operatorname{im} x = \{vx \mid v \in \mathbb{K}^n\}$. We write $\operatorname{rk} x := \dim_\mathbb{K}(\operatorname{im} x) = n - \dim_\mathbb{K}(\ker x)$ for the *rank* of x. The group of units in $\mathbb{K}^{n\times n}$ is $\mathrm{GL}(n, \mathbb{K}) := \{g \in \mathbb{K}^{n\times n} \mid \operatorname{rk} g = n\}$.

Lemma 8.1. *Let $a, s \in \mathbb{K}^{n\times n}$, and consider $\Delta \le \mathrm{Aut}(\mathrm{V}_{\mathbb{K}^{n\times n}})$ and $\Sigma = \mathrm{Aut}(\mathrm{V}_{\mathbb{K}^{n\times n}})^\sigma$, as in* 5.5 *and* 3.44.

1. *The orbit of $(a,0)$ under Σ contains an element of the form $(\pi_k, 0)$, where*
$$\pi_j := \begin{pmatrix} \underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{j} & \\ & \overbrace{\begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix}}^{n-j} \end{pmatrix}$$
is the standard projection of rank j, and $k = \operatorname{rk} a$.
2. *The orbit of $(0,s)$ under Δ^σ contains $(0, \pi_{\operatorname{rk} s})$.*
3. *More generally, the orbit of (a,s) contains (π_k, t) and (b, π_m) for suitable elements $b, t \in \mathbb{K}^{n\times n}$ with $k = \operatorname{rk} a = \operatorname{rk} b$ and $m = \operatorname{rk} s = \operatorname{rk} t$.*
4. *The orbit of $\big((0,0), x\big)$ under Δ^σ contains $\big((0,0), \pi_{\operatorname{rk} x}\big)$.*
5. *If the field $\mathbb{K}$ possesses an anti-automorphism (in particular, if $\mathbb{K}$ is commutative) then $\mathbb{K}^{n\times n}$ admits an anti-automorphism $*$. In this case, the elements $(\pi_k, 0)$ and $(0, \pi_k)$ belong to the same orbit under $(\langle \hat{*} \rangle \Delta)^\sigma$, and every orbit has a representative of the form (π_k, t) with $k \ge \operatorname{rk} t$.*

Proof. Apply $\lambda_g \rho_h$ for suitable $g, h \in \mathrm{GL}(n, \mathbb{K})$, cf. 5.5. The last assertion follows from 5.6: note that transposition of the matrices and application of an anti-automorphism of $\mathbb{K}$ to the entries yields an anti-automorphism $*$ of the matrix ring $\mathbb{K}^{n\times n}$. □

Theorem 8.2. *Let $\mathbb{K}$ be a field, and let n be a positive integer. Then the set*
$$\mathcal{R}_n := \{\big((\pi_k, \pi_m + 1 - \pi_\ell), 0\big) \mid 0 \le m \le k \le \ell \le n\} \cup \{\big((0,0), \pi_k\big) \mid 0 \le k \le n\}$$
contains a set of representatives for the orbits under $\Delta \le \mathrm{Aut}(\mathrm{V}_{\mathbb{K}^{n\times n}})$. If $\mathbb{K}$ admits an anti-automorphism then $\mathbb{K}^{n\times n}$ admits an anti-automorphism $*$, and
$$\begin{aligned}\mathcal{R}_n^{>} := \{\big((\pi_k, \pi_m + 1 - \pi_\ell), 0\big) \mid 0 \le m + n - \ell \le k \le \ell \le n\} \cup \\ \{\big((0,0), \pi_k\big) \mid 0 \le k \le n\}\end{aligned}$$
contains a set of representatives for the orbits under $(\langle \hat{*} \rangle \Delta)^\sigma$.

Proof. According to 8.1 and 3.6, it suffices to consider the orbits of elements of the form $\big((\pi_k, s), 0\big)$ or $\big((0,0), \pi_k\big)$, where $s \in R$ and $0 \le k \le n$.

Let $K := \ker s \cap \operatorname{im} \pi_k$, and let C be a vector space complement for K in $\ker s$. Using suitable $c, h \in \mathrm{GL}(n, \mathbb{K})$, we achieve $c\pi_k h = \pi_k$ (an obvious condition on the block structure for c, h), $K_k(h^{-1}s) = \ker(1 - \pi_m)$ for $m := \dim K$, and $Ch = \ker(\pi_\ell - \pi_k)$ for $\ell := k + \operatorname{rk} s - m$. The latter condition means that Ch is a complement for $K_k(h^{-1}s)$ in $\ker h^{-1}s$, and $\ker h^{-1}s = \ker(\pi_\ell - \pi_m)$. Thus $h^{-1}s$ is a matrix of rank $\operatorname{rk} s = m + n - \ell$ where the $m + n - \ell$ rows below the mth are zero, and the first m together with the last $n - \ell$ rows form a basis for $\operatorname{im} h^{-1}s$. A suitable element $d \in \mathrm{GL}(n, \mathbb{K})$ now leads to $h^{-1}sd = \pi_m + (1 - \pi_\ell)$, as claimed.

The refinement in the case where $\mathbb{K}$ admits an anti-automorphism follows from 8.1.5. $\square$

Theorem 8.3. *The set $\mathcal{R}_n^{>}$ introduced in 8.2 has cardinality $n + \sum_{\ell=\lceil n/2 \rceil}^{n} \binom{2\ell-n+2}{2}$. In other terms, we have*

$$|\mathcal{R}_n^{>}| = \begin{cases} \frac{1}{24}(2\,n^3 + 15\,n^2 + 58\,n + 24) & \text{if } n \text{ is even,} \\ \frac{1}{24}(2\,n^3 + 15\,n^2 + 58\,n + 21) & \text{if } n \text{ is odd.} \end{cases}$$

Proof. For fixed n, we will count the triplets (ℓ, k, m) with $n \geq \ell \geq k \geq m + (n - \ell) \geq 0$. Clearly, this gives the number of elements in $\mathcal{R}_n^{>} \smallsetminus \{((0,0), \pi_k) \mid 1 \leq k \leq n\}$. First of all, we note $\lceil n/2 \rceil \leq \ell \leq n$. We count the possibilities for each ℓ separately: for any k with $n - \ell \leq k \leq \ell$ we may choose m such that $0 \leq m \leq k - (n - \ell)$. Thus k yields $k - (n - \ell) + 1$ triplets, and we have $\sum_{k=n-\ell}^{\ell}(k - (n - \ell) + 1) = \sum_{j=1}^{2\ell-n+1} j = \binom{2\ell-n+2}{2}$ possibilities for each ℓ.

In order to prove that $|\mathcal{R}_n^{>}|$ can be described by polynomial expressions as stated, we consider $f : \mathbb{N} \to \mathbb{N} : n \mapsto |\mathcal{R}_n^{>}|$. For $k \in \mathbb{N}$, one computes $f(2k+2) - f(2k) = 2\,k^2 + 7\,k + 8$ and $f(2k+3) - f(2k+1) = 2\,k^2 + 9\,k + 12$. This means $f(x+2) - f(x) = p(x) := \frac{1}{2}x^2 + \frac{7}{2}x + 8$, for each positive integer x. Searching for two polynomials q_{odd} and q_{even} that coincide with f on the sets of odd and even positive integers, respectively, we consider a general polynomial q of degree at most 3. Then $q(x+2) - q(x)$ is a polynomial of degree at most 2, independent of the constant term in q. Comparing coefficients in $q(x+2) - q(x) = p(x)$, one obtains $q(x) = \frac{1}{24}(2\,n^3 + 15\,n^2 + 58\,n + C)$, where C is a constant. For odd and even values of x, we determine the value C from the conditions $q_{\text{odd}}(1) = f(1) = 4$ and $q_{\text{even}}(2) = f(2) = 9$, respectively. $\square$

Lemma 8.4. *Let $\mathbb{K}$ be a field, let n be a positive integer, and put $R := \mathbb{K}^{n \times n}$. Then the following are equivalent for $v \in R^2$:*

1. *C_v is commutative.*
2. *$(v, 0)$ belongs to the orbit of $((1,0),0)$ or $((0,1),0)$ under $\mathrm{Aut}(\mathrm{V}_R)$.*
3. *v belongs to the set $(R^\times \times \{0\}) \cup (\{0\} \times R^\times)$.*

Proof. It is clear that assertion 2 implies assertion 1, and that assertion 3 implies assertion 2. Thus it remains to prove that C_v is commutative only if $v \in (R^\times \times \{0\}) \cup (\{0\} \times R^\times)$.

Write $v = (a, s)$, and assume that $\mathrm{C}_v = \{(b, y) \mid b, y \in R, ay = bs\} \times R$ is commutative. Using 8.2, we may assume that there are integers $0 \leq m \leq k \leq \ell \leq n$ such that $(a, s) = (\pi_k, \pi_m + 1 - \pi_\ell)$. Then $((1 - s), 0)$ and $((0, 1 - a), 0)$ belong to C_v, and our assumption yields $0 = \langle (1 - s, 0), (0, 1 - a) \rangle = (\pi_\ell - \pi_m)(1 - \pi_k) = \pi_\ell - \pi_k$. This implies $k = \ell$.

Aiming at a contradiction, we assume $0 < \ell < n$. Then it is possible to pick $c \in \mathbb{K}^{m \times (n-\ell)}$, $d \in \mathbb{K}^{(\ell-m) \times (n-\ell)}$, and $e \in \mathbb{K}^{(n-\ell) \times (\ell-m)}$ such that $ce \in \mathbb{K}^{m \times (\ell-m)}$

and $de \in \mathbb{K}^{(\ell-m)\times(\ell-m)}$ are not both zero. We form block matrices of size $\big(m + (\ell-m) + (n-\ell)\big) \times \big(m + (\ell-m) + (n-\ell)\big)$, as follows:

$$b := \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix}, \ y := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & e & 0 \end{pmatrix}, \text{ then } ab = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} = b,$$

$$bs = \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = b\,, \quad \text{and} \quad by := \begin{pmatrix} 0 & ce & 0 \\ 0 & de & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Computing $\langle (a,s),(b,b)\rangle = b - b = 0$ and $\langle (a,s),(0,y)\rangle = ay = 0$, we check that $\big((b,b),0\big)$ and $\big((0,y),0\big)$ both belong to C_v. Now $\langle (b,b),(0,y)\rangle = by \neq 0$ implies that C_v is not commutative, contradicting our hypothesis.

It remains to treat the case where $\ell \in \{0,n\}$. For $\ell = 0$, we have $a = 0$, and $\mathrm{C}_v = \big(R \times (1-s)R\big) \times R$ is commutative only if $1 - s = 0$. In the case $\ell = n$, we have $a = 1$, and 5.9 yields $s = 0$. □

Theorem 8.5. *Let* $\mathbb{K}$ *be a (not necessarily commutative) field, let* n *be a positive integer, and put* $R := \mathbb{K}^{n\times n}$. *Let* $\Delta = \{\lambda_{c^{-1}}\zeta_h\rho_d \mid c,h,d \in \mathrm{GL}(n,\mathbb{K})\}$, $\mathrm{A} = \{\tilde\alpha \mid \alpha \in \mathrm{Aut}(R)\}$ *and* K *be the subgroups of* $\mathrm{Aut}(\mathrm{V}_R)$ *introduced in* 5.5 *and* 3.1, *respectively.*

1. *If* $\mathbb{K}$ *does not admit any anti-automorphisms, then* $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{K}$.
2. *If* $\mathbb{K}$ *admits an anti-automorphism* $*$, *then* $\mathrm{Aut}(\mathrm{V}_R) = \langle \hat{*}\rangle\mathrm{A}\Delta\mathrm{K}$. *(See* 5.6 *for a definition of* $\hat{*}$*).*

Proof. Our result 8.4 allows to reduce every element $\varphi \in \mathrm{Aut}(\mathrm{V}_R)$ to a product of an element of $\Delta\mathrm{K}$ with an element φ' that either fixes $\big((1,0),0\big)$, or maps it to $\big((0,1),0\big)$. Now 5.13 gives the assertion. □

Any deeper understanding of the automorphisms of $\mathrm{V}_{\mathbb{K}^{n\times n}}$ requires information about $\mathrm{Aut}(\mathbb{K}^{n\times n})$.

Theorem 8.6. ([2] V.4, p. 183, [2] V.5) *Every automorphism of* $\mathbb{K}^{n\times n}$ *is induced (via conjugation) by a semilinear bijection. The ring* $\mathbb{K}^{n\times n}$ *admits an anti-automorphism if, and only if, the field* $\mathbb{K}$ *admits an anti-automorphism.* □

Automorphisms of the ring $\mathbb{K}^{n\times n}$ can be understood in a much wider context, in fact, one has:

Theorem 8.7. [28] *Let* V *and* W *be right vector spaces over fields* $\mathbb{K}$ *and* $\mathbb{L}$, *and let* $S \subseteq \mathrm{End}_{\mathbb{K}}(V)$ *and* $T \subseteq \mathrm{End}_{\mathbb{L}}(W)$ *be subsemigroups containing all rank one operators.*

1. *If* $\dim_{\mathbb{K}} V \geq 2$, *then every isomorphism from* S *onto* T *is induced by a semilinear bijection from* V *onto* W. *In particular, every isomorphism preserves ranks.*

2. *The semigroups* $\mathrm{End}_{\mathbb{K}}(V)$ *and* $\mathrm{End}_{\mathbb{L}}(W)$ *are anti-isomorphic if, and only if, the field* $\mathbb{L}$ *is anti-isomorphic to* $\mathbb{K}$*, and* $\dim_{\mathbb{K}} V = \dim_{\mathbb{L}} W$ *is finite.* □

The proofs in [28] use the fact that the projective spaces are encoded in the sub-semigroups containing all rank one operators. For the special case of commutative ground fields, the information we need can also be obtained using [10] Theorem 3, where the semi-linear bijections of $\mathbb{F}^{n\times n}$ leaving $\mathrm{GL}(n,\mathbb{F})$ invariant are determined. Dieudonné's result [10] generalizes an early observation by Frobenius [12], cf. [21]. See [11] for a generalization to products $\mathbb{F}^{n_1\times n_1} \times \cdots \times \mathbb{F}^{n_\ell\times n_\ell}$. Automorphisms of linear groups over suitable commutative rings are discussed in [4].

According to 8.6, each automorphism of the ring $\mathbb{K}^{n\times n}$ preserves ranks. Thus we obtain:

Corollary 8.8. *Assume* $n \geq 2$*. If* $\mathbb{K}$ *admits an anti-automorphism (in particular, if* $\mathbb{K}$ *is commutative) then* $\mathcal{R}_n^{>}$ *forms a set of representatives for the orbits under* $\mathrm{Aut}(\mathrm{V}_{\mathbb{K}^{n\times n}})$*. If* $\mathbb{K}$ *does not admit any anti-automorphisms then* $\mathcal{R}_n$ *forms a set of representatives.* □

We discuss some special cases in detail, and give alternative arguments to distinguish the orbits. These may be of independent interest.

Example 8.9. Let $\mathbb{F}$ be a commutative field with $\operatorname{char}\mathbb{F} \neq 2$. Then the set

$$\mathcal{R}_2^{>} = \left\{ \begin{array}{ccc} \big((1,\pi_1),0\big), & \big((1,0),0\big), & \big((1,1),0\big), \\ \big((\pi_1,\pi_1),0\big), & \big((\pi_1,0),0\big), & \big((\pi_1,1-\pi_1),0\big), \\ \big((0,0),1\big), & \big((0,0),\pi_1\big), & \big((0,0),0\big) \end{array} \right\}$$

forms a set of representatives for the orbits in $\mathrm{V}_{\mathbb{F}^{2\times 2}}$.

Remarks 8.10. From 8.8 we know that $\mathcal{R}_2^{>}$ forms a set of representatives. The centralizer of the element $\big((\pi_k, \pi_m + 1 - \pi_\ell), 0\big)$ will be denoted by $Z_{\ell k m}$. As usual in Lie theory, we write $\mathfrak{sl}(2,\mathbb{F})$ for the subspace of $\mathbb{F}^{2\times 2}$ consisting of all matrices with vanishing trace. One knows that $\mathfrak{sl}(2,\mathbb{F})$ is additively generated by $\{ab - ba \mid a, b \in \mathbb{F}^{2\times 2}\}$. Different elements of $\mathcal{R}_2^{>}$ outside the center of $\mathrm{V}_{\mathbb{F}^{2\times 2}}$ can be distinguished by a look at the centralizers, as follows.

The centralizer of $\big((1,0),0\big)$ is $Z_{220} := (\mathbb{F}^{2\times 2} \times \{0\}) \times \mathbb{F}^{2\times 2}$, and abelian. The centralizer of $\big((1,\pi_1),0\big)$ is $Z_{221} := \{\big((b, b\pi_1), x\big) \mid b, x \in \mathbb{F}^{2\times 2}\}$, and not abelian: the set of commutators equals $\{(0,0)\} \times \{(ab - ba)\pi_1 \mid a, b \in \mathbb{F}^{2\times 2}\}$, and $Z'_{221} = \{(0,0)\} \times (\mathfrak{sl}(2,\mathbb{F}))\pi_1$. The centralizer of $\big((1,1),0\big)$ is $Z_{222} := \{\big((b,b),x\big) \mid b, x \in \mathbb{F}^{2\times 2}\}$ and $Z'_{222} = \{(0,0)\} \times \mathfrak{sl}(2,\mathbb{F})$.

The centralizer of $\big((\pi_1,0),0\big)$ is $Z_{210} := \{\big((b,t),x\big) \mid b, t, x \in \mathbb{F}^{2\times 2}, t\pi_1 = 0\}$, and its commutator $Z'_{210} = \{(0,0)\} \times \{t \mid t\pi_1 = 0\}$. For the element $\big((\pi_1,\pi_1),0\big)$, we find $Z_{211} := \{\big((b,t),x\big) \mid b, t, x \in \mathbb{F}^{2\times 2}, \pi_1 t = b\pi_1\}$ as centralizer, with commutator $Z'_{211} = \{(0,0)\} \times \mathbb{F}^{2\times 2}$.

Finally, $\big((\pi_1, 1-\pi_1),0\big)$ gives $Z_{110} := \{\big((b,t),x\big) \mid b, t, x \in \mathbb{F}^{2\times 2}, \pi_1 t = b(1-\pi_1)\}$, with commutator $Z'_{110} = \{(0,0)\} \times \{\big((0,0),x\big) \mid x \in \mathbb{F}^{2\times 2}, (1-\pi_1)x\pi_1 = 0\}$.

In any case, the elements $\big((1,0),0\big)$ and $\big((\pi_1,\pi_1),0\big)$ belong to orbits Ω_{220} and Ω_{211} of their own. Every automorphism leaves invariant the pairs $d_{\ell km} := (\dim Z_{\ell km}, \dim Z'_{\ell km})$. (If one is only interested in finite groups, and does not want to use our result 8.8, one might also assume and use the fact that $\mathbb{F}$ has finite dimension over its prime field.) In the present case, these pairs separate the orbits outside the center: we have $d_{220} = (8,0)$, $d_{221} = (8,2)$, $d_{222} = (8,3)$, $d_{210} = (6,2)$, $d_{211} = (6,4)$, and $d_{110} = (6,3)$.

Since the element $\big((0,0),1\big)$ is not obtained as the commutator of any pair of elements in the orbit of $\big((1,\pi_1),0\big)$, it belongs to a separate orbit.

For $n > 2$, the structure of the group $\mathrm{V}_{\mathbb{F}^{n\times n}}$ is more complicated: the *dimensions* of the centralizers and their commutators no longer suffice to distinguish the elements of $\mathcal{R}_n^{>}$.

Example 8.11. *Let $\mathbb{F}$ be a commutative field with* $\operatorname{char}\mathbb{F} \neq 2$. *In $\mathrm{V}_{\mathbb{F}^{3\times 3}}$, the elements $\big((\pi_1,\pi_1),0\big)$ and $\big((\pi_1,1-\pi_2),0\big)$ (that is, the elements of $\mathcal{R}_3^{>}$ corresponding to the triplets $(\ell,k,m) = (3,1,1)$, and $(2,1,0)$, respectively) have centralizers of the same dimension, with commutators of the same dimension. However, if $\mathbb{F}$ has finite dimension over its prime field, then the centralizers are not isomorphic.*

Proof. The centralizer of $\big((\pi_1,\pi_1),0\big)$ equals $Z_{311} = \{\big((a,s),x\big) \mid a,s,x \in \mathbb{F}^{3\times 3}, \pi_1 s = a\pi_1\}$. We use block matrices to write this as

$$Z_{311} = \left\{ \left(\left(\begin{pmatrix} a & B \\ 0 & C \end{pmatrix}, \begin{pmatrix} a & 0 \\ D & E \end{pmatrix} \right), X \right) \,\middle|\, \begin{array}{ll} a \in \mathbb{F}, \ B \in \mathbb{F}^{1\times 2}, & C, E \in \mathbb{F}^{2\times 2}, \\ D \in \mathbb{F}^{2\times 1}, & X \in \mathbb{F}^{3\times 3} \end{array} \right\},$$

and find $\dim Z_{311} = 22$. The set of commutators is

$$\{(0,0)\} \times \left\{ \begin{pmatrix} BX - VD & BY \\ CX - WD & CY - WE \end{pmatrix} \,\middle|\, \begin{array}{ll} B, V \in \mathbb{F}^{1\times 2}, & C, W, E, Y \in \mathbb{F}^{2\times 2}, \\ D, X \in \mathbb{F}^{2\times 1} & \end{array} \right\}.$$

It is easy to see that this set additively generates $\{(0,0)\} \times \mathbb{F}^{3\times 3}$, and $\dim Z'_{311} = 9$.

The centralizer of $\big((\pi_1, 1-\pi_2),0\big)$ is $Z_{210} = \{\big((a,s),x\big) \mid a,s,x \in \mathbb{F}^{3\times 3}, \pi_1 s = a(1-\pi-2)\}$, more explicitly, the conditions on $a = (a_{ij})_{1\le i,j\le 3}$ and $s = (s_{ij})_{1\le i,j\le 3}$ are $s_{11} = s_{12} = 0 = a_{23} = a_{33}$ and $s_{13} = a_{13}$. Thus $\dim Z_{210} = 22$. Since $\big((1,0),0\big)$ and $\big((0,1),0\big)$ belong to Z_{210}, the commutator group Z'_{210} equals $\{(0,0)\} \times \mathbb{F}^{3\times 3}$.

In order to show that the groups Z_{311} and Z_{210} are not isomorphic, we study centralizers of elements in these groups. Let $\big((a,s),x\big) \in Z_{311}$, where

$$a = \begin{pmatrix} f & B \\ 0 & C \end{pmatrix}, \quad s = \begin{pmatrix} f & 0 \\ D & E \end{pmatrix}.$$

We claim that the subspace $J := \{\langle (a,s),(b,t)\rangle \mid (b,t,0) \in Z_{311}\}$ of $\mathbb{F}^{3\times 3}$ satisfies $\dim J \ge 2$ if $(a,s) \notin \mathbb{F}(\pi_1,\pi_1)$. In fact, from $B \neq 0$ or $V \neq 0$ we infer $\dim J \ge 4$, and $C \neq 0$ or $D \neq 0$ at least imply $\dim J \ge 2$. This means that each element in Z_{311} is either central or has a centralizer of dimension at most 11. However, the element $\big((\pi_1,0),0\big) \in Z_{210}$ has 12-dimensional centralizer in Z_{210}. Thus the groups Z_{311} and Z_{210} are not isomorphic, and the elements $\big((\pi_1,\pi_1),0\big)$ and $\big((\pi_1,1-\pi_2),0\big)$ belong to different orbits under $\operatorname{Aut}(\mathrm{V}_{\mathbb{F}^{3\times 3}})$. $\square$

Example 8.12. Table 1 shows, for elements $(v,0) \in \mathcal{R}_3^{>} \smallsetminus \{(0,\pi_k) \mid 1 \le k \le 3\}$, the conditions that determine $\mathrm{C}_v := \{w \in (\mathbb{F}^{3\times 3})^2 \mid \langle v,w\rangle = 0\}$ and the subgroup C'_v of $\mathbb{F}^{3\times 3}$ that is additively generated by $\{\langle u,w\rangle \mid u,w \in \mathrm{C}_v\}$. An asterisk $*$ indicates that no condition is imposed. The last columns give $c_v := \dim \mathrm{C}_v$ and $d_v := \dim \mathrm{C}'_v$. Note that $(\ell,k,m) \in \{(3,1,1),(2,1,0)\}$ gives the only cases where the pair (c_v,d_v) does not suffice to distinguish the orbits.

The computational details have been done in private, their verification is left to the reader. For $n > 3$, even the determination of centralizers and commutators for elements of $\mathcal{R}_n^{>}$ becomes tedious.

(ℓ,k,m)	v	C_v	C'_v	c_v	d_v
$(3,3,3)$	$(1,1)$	$s=a$	$x_{11}+x_{22}+x_{33}=0$	9	8
$(3,3,2)$	$(1,\pi_2)$	$s=a\pi_2$	$x_{13}=x_{23}=x_{33}=0$	9	6
$(3,3,1)$	$(1,\pi_1)$	$s=a\pi_1$	$x_{12}=x_{22}=x_{32}=$ $x_{13}=x_{23}=x_{33}=0$	9	3
$(3,3,0)$	$(1,0)$	$s=0$	$x=0$	9	0
$(3,2,2)$	(π_2,π_2)	$\pi_2 s=a\pi_2$	$*$	10	9
$(3,2,1)$	(π_2,π_1)	$\pi_2 s=a\pi_1$	$*$	11	9
$(3,2,0)$	$(\pi_2,0)$	$\pi_2 s=0$	$*$	12	9
$(3,1,1)$	(π_1,π_1)	$\pi_1 s=a\pi_1$	$*$	13	9
$(3,1,0)$	$(\pi_1,0)$	$\pi_1 s=0$	$*$	15	9
$(3,0,0)$	$(0,0)$	$*$	$*$	18	9
$(2,2,1)$	$(\pi_2,\pi_1+1-\pi_2)$	$\pi_2 s=a(\pi_1+1-\pi_2)$	$x_{32}=0$	10	8
$(2,2,0)$	$(\pi_2,1-\pi_2)$	$\pi_2 s=a(1-\pi_2)$	$x_{31}=0=x_{32}$	11	7
$(2,1,0)$	$(\pi_1,1-\pi_2)$	$\pi_1 s=a(1-\pi_2)$	$*$	13	9

Table 1. Invariants separating the orbits in the Verardi group over $\mathbb{F}^{3\times 3}$

9. Local rings

A ring R is called a *local ring* if the set N of non-invertible elements forms an ideal (that is, if N is additively closed). Clearly, the set N is then the unique maximal ideal, and every one-sided ideal is contained in N.

We know from 5.5 and 5.12 that $\mathrm{Aut}(\mathrm{V}_R)$ contains $\Delta = \{\lambda_{c^{-1}}\zeta_h\rho_d \mid c,h,d \in R^\times\}$, the group $\mathrm{A} \cong \mathrm{Aut}(R)$ induced by automorphisms of the ring R, and the group $\mathrm{K} \cong \mathrm{Hom}(R^2,R)$ of central automorphisms. Our aim in this section is to prove $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{TK}$, whenever R is a local ring.

Lemma 9.1. *Let R be a local ring such that 2 is invertible. Then the orbits of $(1,0)$ and $(0,1)$ under Σ are contained in the union of orbits $(1,0)^{(\mathrm{T}_R\Delta)^\sigma} \cup (0,1)^{({}_R\mathrm{T}\Delta)^\sigma}$, and thus in the set $(R^\times \times N) \cup (N \times R^\times)$.*

Proof. For $(a,s) \in (1,0)^\Sigma$ we first compare $\mathrm{D}_{(1,0)} = R$ with the subgroup $\mathrm{D}_{(a,s)}$ generated by $\{at - bs \mid b,t \in R\}$, see 3.7. As R is a local ring, the set $\mathrm{D}_{(a,s)}$ contains invertible elements only if at least one of the elements a, s is invertible.

If a is invertible, we use $\lambda_a \in \Delta$ to obtain that $(a,s) \in (1,s)^{\Delta^\sigma}$. We compare the centralizers $\mathrm{C}_{(1,s)} = \{(b,bs) \mid b \in R\} \times R$ and $\mathrm{C}_{(1,0)} = (R \times \{0\}) \times R$. Regarding commutators in $\mathrm{C}_v \times R$ for $v \in \{(1,0),(1,s)\}$, we find that the additive subgroup $\mathrm{C}'_{(1,s)}$ generated by $\{\langle u,v\rangle \mid (u,0),(v,0) \in \mathrm{C}_{(1,s)}\} = \{bcs - cbs \mid b,c \in R\}$ equals $R's$. Comparing with $\mathrm{C}'_{(1,0)} = \{0\}$, we find $R's = \{0\}$. Thus the transvection τ_s exists, and $(a,s) = (1,s)^{\lambda_a{}^\sigma} = (1,0)^{\tau_s{}^\sigma \lambda_a{}^\sigma}$ belongs to the orbit $(1,0)^{(\mathrm{T}_R\,\Delta)^\sigma} \subseteq R^\times \times N$.

If s is invertible, we proceed analogously, using $\rho_s \in \Delta$ to derive $aR' = \mathrm{C}'_{(a,1)} = \{0\}$, and then ${}_a\tau \in {}_R\mathrm{T}$ to obtain $(a,s) \in (0,1)^{({}_R\mathrm{T}\Delta)^\sigma} \subseteq N \times R^\times$.

The arguments for the orbit of $(0,1)$ run along the same lines. □

Applying 5.13, we obtain:

Theorem 9.2. *Let R be a local ring such that 2 is invertible.*

1. *If R admits an anti-automorphism $*$, then* $\mathrm{Aut}(\mathrm{V}_R) = \langle \hat{*} \rangle \mathrm{A}\Delta\mathrm{TK}$. *(See* 5.6 *for a definition of $\hat{*}$).*
2. *If R does not admit any anti-automorphisms, then* $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{TK}$. □

Remarks 9.3. For every commutative local ring R, and also for every commutative euclidean ring (in particular, for the rings $\mathbb{Z}$ and $\mathbb{F}[X]$), the group $\mathrm{SL}(2,R)$ is generated by the elementary transvections (see [19], [20] for the case of arbitrary local rings, and [3] 2.8, cf. also [24] pp. 50–56). Thus $\mathrm{A}\Delta\mathrm{TK} = \Gamma\mathrm{L}(2,R) \ltimes \mathrm{Hom}(R^2,R)$ in this case, and the result of 9.2 coincides with that of 7.2.

For commutative rings in general, the group generated by all transvections may be strictly smaller than $\mathrm{SL}(2,R)$. E.g., this happens for the polynomial rings in more than one indeterminate over a commutative field (see [5] §5), and for the ring of algebraic integers in $\mathbb{Q}(\sqrt{-19})$, which is a principal ideal domain, see [5] Theorem 6.1. Thus different proofs for the commutative and the local case seem necessary.

Let $\mathbb{K}$ be a (not necessarily commutative) field with discrete valuation $\nu : \mathbb{K} \to \mathbb{Z} \cup \{\infty\}$. We define $B_n := \{x \in \mathbb{K} \mid \nu(x) \geq n\}$. Then B_0 is a subring of $\mathbb{K}$ (the valuation ring), and B_n is an ideal in B_0, for each $n > 0$. Pick $n \in (\mathbb{N} \smallsetminus \{0\}) \cup \{\infty\}$, and put $R := B_0/B_n$. Then R is a local ring, with maximal ideal $R \smallsetminus R^\times = B_1/B_n$.

Lemma 9.4. *Every ideal of R is of the form B_k/B_n, for some $k \leq n$. Each of these ideals is a principal ideal, of the form $B_0 j/B_n = B_k/B_n = jB_0/B_n$ with $\nu(j) = k$.*

Proof. Passing to full pre-images of ideals, one sees that it suffices to show the assertion for the case $n = \infty$. Then $R = B_0$. Let J be an ideal in B_0, put $m := \min\{\nu(x) \mid x \in J\}$, and pick $j \in J$ with $\nu(j) = m$. For each $x \in J$, we have $\nu(j^{-1}x) = \nu(xj^{-1}) = \nu(x) - \nu(j) \geq 0$. This shows that both $j^{-1}x$ and xj^{-1} belong to B_0, and we find $B_0 j \leq J \leq B_0 j$. This shows $B_0 j = J = jB_0$. □

Theorem 9.5. *Assume that* $\mathbb{F}$ *admits a discrete valuation* $\nu : \mathbb{F} \to \mathbb{Z} \cup \{\infty\}$*. For* $n \in (\mathbb{N} \smallsetminus \{0\}) \cup \{\infty\}$*, consider the quotient* $R := B_0/B_n$ *of the valuation ring. Let* X *be any element of* $B_1 \smallsetminus B_2$*, and put* $Y := B_n + X$*. Then the orbits of* $\mathrm{Aut}(\mathrm{V}_R)$ *on* V_R *are represented by the elements of the set*

$$\mathcal{R} := \big\{ \big((Y^k, 0), 0\big) \bigm| k < n \big\} \cup \big\{ \big((0,0), Y^k\big) \bigm| k \le n \big\} .$$

In particular, the automorphism group has $2n+1$ *orbits on* V_R*.*

Proof. One verifies immediately that the orbits of elements of $\{(Y^k, 0) \mid k \le q\}$ under the group $\mathrm{SL}(2,R) \le \mathrm{Sp}\,(\beta)$ cover R^2: note that every element of R^2 is of the form $Y^k(a,b)$ where at least one of the elements a, b is invertible. Extending the row (a,b) to an element of $\mathrm{SL}(2,R)$ is easy. Mapping $\big((a,b),z\big)$ to $\big((ra,b),rz\big)$ with $r \in R^\times$ gives an automorphism of $\mathrm{V}_{\mathbb{F}[G]}$, and using 3.6 we see that $\mathcal{R}$ contains a set of representatives for the orbits. Different elements of $\mathcal{R}$ do not belong to the same orbit under AΔTK because automorphisms of R preserve the chain of ideals, and thus the valuation (see 9.4).

The invariant $c_{(Y^k,0)} = 2n+k$ shows that every element $\big((Y^k,0),0\big)$ represents an orbit $\mathcal{O}_k$ of its own. Finally, we remark that $\big((0,0),Y^k\big)$ is obtained as the commutator of pairs in $\mathcal{O}_k \times \mathcal{O}_0$ but not of pairs in $\mathcal{O}_{k+1} \times \mathcal{O}_0$, and we see that different elements of $\mathcal{R} \cap (\{(0,0)\} \times R)$ represent different orbits. □

Example 9.6. Let $\mathbb{F}$ be any commutative field, and let $\mathbb{K} := \mathbb{F}(X)$ be the field of quotients for the polynomial ring $\mathbb{F}[X]$. Then $\nu(p/q) := \deg p - \deg q$ gives a valuation on $\mathbb{K}$ such that the valuation ring is $B_0 = \{p/q \mid p, q \in \mathbb{F}[X], q \ne 0, \deg q \le p\}$, and the maximal ideal is $B_1 = B_0(X)$. Note that the valuation ring B_0 is larger than $\mathbb{F}[X]$, for instance, it contains $X/(X+1)$.

Lemma 9.7. *Let* n *be a positive integer, and consider the valuation on* $\mathbb{F}(X)$ *as in* 9.6*. Then every element of* B_0/B_n *has a representative in* $\mathbb{F}[X]$*. In other words: we have* $B_0/B_n \cong \mathbb{F}[X]/\mathbb{F}[X](X^n)$*.*

Proof. For $p, q \in \mathbb{F}[X] \smallsetminus \{0\}$ with $\deg p = \deg q$, we find $f \in \mathbb{F}[X]$ such that $\deg(p - fq) < \deg q$. Thus $p/q - f$ belongs to B_1, and we have proved $B_0 = B_1 + \mathbb{F}[X]$. Multiplying with X^m, we obtain $B_m = B_{m+1} + \mathbb{F}[X](X^m)$ for each positive integer m. Proceeding by induction on m, we may assume $B_0 = B_m + \mathbb{F}[X]$, and infer $B_0 = B_{m+1} + \mathbb{F}[X](X^m) + \mathbb{F}[X] = B_{m+1} + \mathbb{F}[X]$. □

If $\mathrm{char}\,\mathbb{F} =: p$ is positive and G is a cyclic group of order p^n, the structure of $\mathrm{Aut}(\mathrm{V}_{\mathbb{F}[G]})$ is also easy to understand, because the ring $R := \mathbb{F}[G]$ is a local ring of very special type:

Lemma 9.8. *Assume* $\mathrm{char}\,\mathbb{F} = p > 0$*, and let* G *be a cyclic group of order* $q := p^n$*. Then the group algebra* $\mathbb{F}[G]$ *is isomorphic to* $R := \mathbb{F}[X]/(X^q)$*. Every ideal of* R *is a principal ideal of the form* $R_k := R(X^k)$ *for some* $k < q$*.*

Proof. Quite obviously, we have $\mathbb{F}[G] \cong \mathbb{F}[Y]/(Y^q - 1)$. Since $\mathbb{F}$ has characteristic p, we have $Y^q - 1 = (Y-1)^q$. Now $Y \mapsto X := Y + 1$ extends to an automorphism of $\mathbb{F}[Y] = \mathbb{F}[X]$, inducing an isomorphism from $\mathbb{F}[Y]/(Y^q - 1)$ onto R. The rest follows from 9.7 and 9.4. □

Remark 9.9. Lemma 9.8 is a special (and quite explicit) case of the following: If G is a finite p-group and $\operatorname{char}\mathbb{F} = p$ then $\mathbb{F}[G]$ is a local ring, where the powers of the maximal ideal are well understood; cf. [16].

Corollary 9.10. *Assume* $\operatorname{char}\mathbb{F} = p > 0$*, let* $G = \langle g\rangle$ *be a cyclic group of order* $q := p^n$*, and put* $R := \mathbb{F}[G]$*. Then* $\operatorname{Aut}(\mathrm{V}_R)$ *is isomorphic to a semidirect product* $\Gamma\mathrm{L}(2,R) \ltimes \operatorname{Hom}(R^2,R)$*. Note that* $\operatorname{Hom}(R^2,R)$ *is isomorphic to* $\operatorname{Hom}((\mathbb{F}^q)^2,\mathbb{F}^q) = \operatorname{Hom}(\mathbb{F}^{2p^n},\mathbb{F}^{p^n}) \cong \operatorname{Hom}(\mathbb{F},\mathbb{F})^{2p^{2n}}$*. In particular, if* $\mathbb{F}$ *is a finite field of order* p^k*, we have* $\operatorname{Hom}(R^2,R) \cong \mathbb{F}_p^{2k^2p^{2n}}$*.* □

Lemma 9.11. *Assume* $\operatorname{char}\mathbb{F} = p > 0$*, let* G *be a cyclic group of order* $q := p^n$*, let* $R := \mathbb{F}[G]$ *be the group ring, and let* X *be any element of the radical* $N = R \setminus R^\times$ *which does not belong to* N^2*. For every* $a \in R^\times$*, there is a unique algebra automorphism* α_a *of* R *mapping* X *to* aX*. Conversely, every algebra automorphism of* R *is of this form.*

Proof. We identify R with $\mathbb{F}[X]/(X^q)$, as in 9.8, where it already has been noted that $N \setminus N^2 = R_1 \setminus R_2$ is an orbit under $R^\times$. For $a \in R^\times$, a linear bijection α_a is determined by the assignment $X^k \mapsto a^kX^k$, and it is easy to see that this is a ring homomorphism. Since $R_1 \setminus R_2$ is a characteristic subset of R, each automorphism has this form. □

Remark 9.12. Let $R{=}\mathbb{F}_p[X]/(X^{p^n})$ with an odd prime p. For $n\geq 1$, Lemma 9.11 yields $|\operatorname{Aut}(R)| = (p-1)p^{p^n-2}$, while $\operatorname{Aut}(R)$ is trivial for $n = 0$. We count

$$\begin{aligned}
|\operatorname{Hom}(R^2,R)| &= p^{2p^{2n}} \quad\text{and}\\
|\mathrm{GL}(2,R)| &= (p+1)(p-1)^2p^{4p^n-3},\\
\text{leading to}\quad \left|\operatorname{Aut}(\mathrm{V}_{\mathbb{F}_p[\mathbb{Z}/p^n\mathbb{Z}]})\right| &= (p+1)(p-1)^3p^{2p^{2n}+5p^n-5} \quad \text{if } n\geq 1,\\
\text{and}\quad \left|\operatorname{Aut}(\mathrm{V}_{\mathbb{F}_p[\{0\}]})\right| &= (p+1)(p-1)^2p^3.\\
\text{If } n\geq 1 \text{ then the orders}\quad |\mathrm{GL}(2p^n,\mathbb{F}_p)| &= p^{2p^{2n}-p^n}\textstyle\prod_{k=1}^{2p^n}(p^k-1)\\
\text{and}\quad |\mathrm{GL}(2p^n,\mathbb{F}_p) \ltimes \operatorname{Hom}(R^2,R)| &= p^{4p^{2n}-p^n}\textstyle\prod_{k=1}^{2p^n}(p^k-1)
\end{aligned}$$

have larger p-parts than $|\Sigma| = |\Gamma\mathrm{L}(2,R)|$ and $\left|\operatorname{Aut}(\mathrm{V}_{\mathbb{F}_p[\mathbb{Z}/p^n\mathbb{Z}]})\right|$, respectively, and the Sylow p-subgroups of Σ are strictly smaller than those of $\mathrm{GL}(2p^n,\mathbb{F}_p)$.

10. Rings of upper triangular matrices

Example 10.1. Let $\mathrm{T}(n,\mathbb{F})$ denote the ring of upper triangular $n\times n$ matrices with entries in $\mathbb{F}$. Then $\mathrm{NT}(n,\mathbb{F}) = \mathrm{T}(n,\mathbb{F})'$ consists of the strict triangular matrices (i.e., those with zero entries along the diagonal).

Lemma 10.2. *The ring* $\mathrm{T}(n,\mathbb{F})$ *admits anti-automorphisms, for instance the map* $*$ *given by matrix transposition, and conjugation by the permutation matrix reversing the order of the standard basis.*

Remark 10.3. For $n > 1$, the ring $\mathrm{T}(n, \mathbb{F})$ is neither commutative, nor a local ring, nor simple (and thus surely not isomorphic to a full matrix ring).

For the rest of this section, we consider the ring $\mathrm{T}(2, \mathbb{F})$. We use the special elements

$$P := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad N := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Note the relations $P^2 = P$, $PN = N$, $NP = 0$, and $N^2 = 0$. The action of the $\mathbb{F}$-linear anti-automorphism $*$ defined in 10.2 is described by $P^* = 1 - P$, $(1 - P)^* = P$, and $N^* = N$. For the construction of transvections, we note the equalities $\mathrm{NT}(2, \mathbb{F})(\mathbb{F}N + \mathbb{F}P) = \{0\}$ and $(\mathbb{F}N + \mathbb{F}(1 - P))\mathrm{NT}(2, \mathbb{F}) = \{0\}$.

Lemma 10.4. *The set*

$$\mathcal{T}_2 := \{(1, 0), (1, 1 - P), (P, 0), (1 - P, P), (1 - P, N), \\ (1 - P, 0), (N, N), (N, 0), (0, 0)\}$$

contains a set of representatives for the orbits under $(\langle\hat{*}\rangle\Delta\mathrm{T})^\sigma \le \Sigma = \mathrm{Aut}(\mathrm{V}_{\mathrm{T}(2,\mathbb{F})})^\sigma$.

Proof. Let $(a, s) \in (\mathrm{T}(2, \mathbb{F}))^2$, and let Ω denote the orbit of (a, s) under Σ. As usual, we write

$$a := \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \qquad s := \begin{pmatrix} s_{11} & s_{12} \\ 0 & s_{22} \end{pmatrix}.$$

(a) If a is invertible, we apply an element of Δ^σ to find $(1, s) \in \Omega$. Using a suitable transvection from $({}_{\mathrm{T}(2,\mathbb{F})}\mathrm{T})^\sigma$ and another element of Δ^σ, we see that Ω contains an element of $\{(1, 0), (1, 1 - P)\}$.

(b) The case where s is invertible may be reduced to case (a), by an application of $\hat{*}$.

(c) Now assume $a_{11} \neq 0 = a_{22}$. An element of Δ^σ yields $(P, s) \in \Omega$, and a transvection from $(\mathrm{T}_{\mathrm{T}(2,\mathbb{F})})^\sigma$ yields that Ω contains an element of $\{(P, 0), (P, 1 - P)\}$. We note that $({}_{1-P}T)^\sigma$ maps $(P, 1 - P)$ to $(1, 1 - P)$.

(d) In the case $a_{11} = 0 \neq a_{22}$, we may use Δ^σ to find $(1 - P, s) \in \Omega$. If $s_{22} \neq 0$, we may use $\hat{*}$ to reduce this case to case (a) or case (c). If $s_{22} = 0$, we use a suitable element ρ_x to find that Ω contains one of $(1 - P, P)$, $(1 - P, N)$, or $(1 - P, 0)$.

(e) There remains the case where $a \in \mathbb{F}N$. Up to reduction to a previous case by an application of $\hat{*}$, we may also assume $s \in \mathbb{F}N$. Then Ω contains one of (N, N), $(N, 0)$, or $(0, 0)$. □

Lemma 10.5. *No element of* $\mathcal{T}_2 \smallsetminus \{(1, 0)\}$ *belongs to the orbit* $(1, 0)^\Sigma$. *Consequently, the orbits of* $(1, 0)$ *under* Σ *and under* $(\langle\hat{*}\rangle\Delta\mathrm{T})^\sigma$ *coincide.*

Proof. Computing the centralizer $\mathrm{C}_{(1,1-P)} = \{(a, a(1-P)) \mid a \in \mathrm{T}(2, \mathbb{F})\} \times \mathrm{T}(2, \mathbb{F})$, we find $\mathrm{C}'_{(1,1-P)} = (\mathrm{T}(2, \mathbb{F}))'(1 - P) \neq \{0\}$, and conclude $(1, 1 - P) \notin (1, 0)^\Sigma$. For every $v \in \mathcal{T}_2 \smallsetminus \{(1, 0), (1, 1 - P)\}$, it is easy to see that D_v, as defined in 3.7 is a proper subset of R. Thus none of these elements belongs to the orbit $(1, 0)^\Sigma$. □

Applying 5.13, we obtain:

Theorem 10.6. $\mathrm{Aut}(\mathrm{V}_{\mathrm{T}(2,\mathbb{F})}) = \langle\hat{*}\rangle\mathrm{A}\Delta\mathrm{TK}$. □

11. Products of fields

Proposition 11.1. *Let $\mathbb{K}$ be a field which is not commutative, with* $\operatorname{char}\mathbb{K} \neq 2$.

1. *If $\mathbb{K}$ admits an anti-automorphism $*$ then $\{(1,0),(1,1),(0,0)\}$ is a set of representatives for the orbits under $\Sigma := \mathrm{Aut}(\mathrm{V}_\mathbb{K})^\sigma$ on $\mathbb{K}^2$, and* $\mathrm{Aut}(\mathrm{V}_\mathbb{K}) = \langle\hat{*}\rangle \mathrm{A}\Delta\mathrm{K}$.
2. *If $\mathbb{K}$ does not admit any anti-automorphisms then $\{(1,0),(0,1),(1,1),(0,0)\}$ is a set of representatives for the orbits under $\Sigma := \mathrm{Aut}(\mathrm{V}_\mathbb{K})^\sigma$ on $\mathbb{K}^2$, and* $\mathrm{Aut}(\mathrm{V}_\mathbb{K}) = \mathrm{A}\Delta\mathrm{K}$.

Proof. In order to show that $(1,0)$ and $(0,1)$ do not belong to the orbit $(1,1)^\Sigma$, we compute $\mathrm{C}_{(1,1)} = \{(a,a) \mid a \in \mathbb{K}\} \times \mathbb{K}$, and $\mathrm{C}'_{(1,1)} = \mathbb{K}' \neq \{0\}$ follows. Now the subgroups $(\langle\hat{*}\rangle\Delta)^\sigma$ and Δ^σ of Σ suffice to prove the claims about sets of representatives. □

Example 11.2. Let $\mathbb{K}$ and $\mathbb{L}$ be two non-commutative fields with $\operatorname{char}\mathbb{K} \neq 2 \neq \operatorname{char}\mathbb{L}$, and put $R := \mathbb{K} \times \mathbb{L}$. We note that $R' = \mathbb{K}' \times \mathbb{L}'$ contains invertible elements, whence T is trivial.

We compute $\mathrm{C}_{\big((1,0),(0,1)\big)} = \big((\mathbb{K} \times \{0\}) \times (\{0\} \times \mathbb{L})\big) \times R = \mathrm{CC}_{\big((1,0),(0,1)\big)}$, and $\mathrm{D}_{\big((1,0),(0,1)\big)} = R$. Thus the orbits of $w := \big((1,0),(0,1)\big)$ and of $v := \big((1,1),(0,0)\big)$ cannot be distinguished by the methods that we have developed so far. However, the two elements belong to different orbits under our standard group $(\mathrm{A}\Delta\mathrm{T})^\sigma = (\mathrm{A}\Delta)^\sigma$.

If $\mathbb{L}$ admits an anti-automorphism $*$, we define an automorphism φ of V_R by putting $\big(\big((a,x),(b,y)\big),(c,z)\big)^\varphi := \big(\big((a,y^*),(b,x^*)\big),(c,-z^*)\big)$. In this case, the elements v and w belong to the same orbit under Σ. In the general case, the map φ is an isomorphism from $\mathrm{V}_{\mathbb{K}\times\mathbb{L}}$ onto $\mathrm{V}_{\mathbb{K}\times\mathbb{M}}$, where $\mathbb{M}$ denotes the opposite field for $\mathbb{L}$.

If neither $\mathbb{L}$ nor $\mathbb{K}$ admits an anti-automorphism, we cannot yet decide whether v and w belong to the same orbit under Σ. The invariants $\dim \mathrm{C}_u$, c_u, $\dim \mathrm{CC}_u$, $\dim \mathrm{C}'_u$ and $\dim \mathrm{D}_u$ coincide for both choices of $u \in \{v,w\}$.

However, it is possible to distinguish the orbits of $e := ((1,0),(0,0))$ and $f = ((0,1),(0,0))$ under Σ. To this end, we use the reduced form of the Heisenberg groups that occur as centralizers:

Consider a Heisenberg group $H = \mathrm{GH}(V,Z,\beta)$ over a commutative ring in which 2 is invertible. The center Z of H contains the commutator subgroup H', and we define an alternating map $\beta^r : H/Z \times H/Z \to H'$ mapping $(Z(v,x), Z(w,y))$ to the (unique) square root $(0,(v,w)^\beta)$ of the commutator $[(v,x),(w,y)] = (0, 2(v,w)^\beta)$. Now the Heisenberg group $H^r = \mathrm{GH}(H/Z, H', \beta^r)$ is reduced (cf. 2.6), and its isomorphism type clearly only depends on the isomorphism type of H. In order to distinguish Heisenberg groups H and G, it therefore suffices to distinguishe the reduced forms H^r and G^r.

Lemma 11.3. *The reduced forms of the centralizers of* $(e,(0,0))$ *and of* $(f,(0,0))$ *are isomorphic to* $\mathrm{V}_{\mathbb{K}}$ *and* $\mathrm{V}_{\mathbb{L}}$*, respectively. Therefore, the elements* e *and* f *belong to the same orbit under* Σ *only if* $\mathrm{V}_{\mathbb{K}}$ *and* $\mathrm{V}_{\mathbb{L}}$ *are isomorphic; that is, only if the fields* $\mathbb{K}$ *and* $\mathbb{L}$ *are isomorphic or anti-isomorphic to each other.*

Proof. A direct computation gives $\mathrm{C}_e = \{\big((a,c),(0,u)\big) \mid a \in \mathbb{K}, c,u \in \mathbb{L}\}$, and, analogously, $\mathrm{C}_f = \{\big((a,c),(s,0)\big) \mid a,s \in \mathbb{K}, c \in \mathbb{L}\}$. The centralizer $H := \mathrm{C}_e \times (\mathbb{K}\times\mathbb{L})$ of $(e,(0,0))$ is a Heisenberg group with center $Z := \{\big((0,c),(0,0)\big) | c \in \mathbb{L}\} \times (\mathbb{K}\times\mathbb{L})$ and commutator subgroup $H' = \{(0,0)\}^2 \times (\mathbb{K}\times\{0\})$, and β^r maps $\big(Z\big(((a,0),(s,0)),(0,0)\big), Z\big(((b,0),(t,0)),(0,0)\big)$ to $\big(((0,0),(0,0)),(at-bs,0)\big)$. This shows $H^r \cong \mathrm{V}_{\mathbb{K}}$. The centralizer of $(f,(0,0))$ is treated analogously. The existence of an isomorphism between $\mathrm{V}_{\mathbb{K}}$ and $\mathrm{V}_{\mathbb{L}}$ implies that $\mathbb{K}$ and $\mathbb{L}$ are isomorphic or isomorphic to each other, see 13.2. □

12. Functorial properties

Remark 12.1. ([8] 15.6, 25.8, 25.15, 26.4) Let G be a finite group, and assume that $\operatorname{char}\mathbb{F}$ does not divide $|G|$. Then $\mathbb{F}[G]$ is a semisimple ring, and isomorphic to a direct product of finitely many rings $R_i \cong \mathbb{K}_i^{n_i\times n_i}$, where each $\mathbb{K}_i$ is a finite (skew-)field extension of $\mathbb{F}$.

See [25] Chapter 7 for a discussion of more general situations where $\mathbb{F}[G]$ is semisimple.

If $\mathbb{F}[G]$ is semisimple, repeated application of the following observation reduces $\mathrm{V}_{\mathbb{F}[G]}$ to groups that are manageable – at least in principle:

Proposition 12.2. *Assume that* R *and* S *are rings. Then the groups* $\mathrm{V}_R \times \mathrm{V}_S$ *and* $\mathrm{V}_{R\times S}$ *are isomorphic.*

Proof. The map $\big(((a,s),x\big),\big((a',s'),x')\big) \mapsto \big(((a,a'),(s,s')\big),(x,x')\big)$ is an isomorphism. □

Let G,H be groups, and let $\mathbb{E},\mathbb{F}$ be commutative fields. Clearly, every ring homomorphism $\varphi : \mathbb{E}[G] \to \mathbb{F}[H]$ yields a group homomorphism

$$\tilde{\varphi} : \mathrm{V}_{\mathbb{E}[G]} \to \mathrm{V}_{\mathbb{F}[H]} : \big((a,s),x\big) \mapsto \big((a^\varphi,s^\varphi),x^\varphi\big)\,.$$

In particular, isomorphic group rings lead to isomorphic Verardi groups, and every automorphism of the group ring induces an automorphism of the corresponding Verardi group.

Remarks 12.3. Non-isomorphic groups may have isomorphic group rings: Dade [9] gives an example of two non-isomorphic groups G_1, G_2 (metabelian of order p^3q^6 for primes p,q with $q \equiv 1 \bmod p^2$) such that the group rings $\mathbb{F}[G_1]$ and $\mathbb{F}[G_2]$ are isomorphic, for every commutative field $\mathbb{F}$; see also [25] 14.2.2. In fact, even the group rings $\hat{\mathbb{Z}}_r[G_1]$ and $\hat{\mathbb{Z}}_r[G_2]$ over the ring $\hat{\mathbb{Z}}_r$ of r-adic integers are always isomorphic, see [27] p. 74. Moreover, Roggenkamp [27] VIII constructs pairs of nonisomorphic groups G, H of order $3 \cdot 7 \cdot 13$ such that for each prime r the group rings $R[G]$ and $R[H]$ are isomorphic for suitable extensions R of $\hat{\mathbb{Z}}_r$, but the group rings $\mathbb{Q}_7[G]$ and $\mathbb{Q}_7[H]$ are not isomorphic.

Proposition 12.4. 1. *The isomorphism type of a Verardi group* $\mathrm{V}_{\mathbb{F}[G]}$ *does not determine the isomorphism type of* G.

2. *The isomorphism type of a Verardi group* V_R *does not determine the ring* R, *up to isomorphism or anti-isomorphism, cf.* 11.2. □

The only examples that we presently have in 12.4.2 are rings that are decomposable as direct products. Thus the first part of 12.4 is still interesting.

Fix a commutative field $\mathbb{F}$. Each group homomorphism $\varphi : G \to H$ extends to an algebra homomorphism $\mathbb{F}[\varphi] : \mathbb{F}[G] \to \mathbb{F}[H]$, yielding a homomorphism $\mathrm{V}_{\mathbb{F}[\varphi]} : \mathrm{V}_{\mathbb{F}[G]} \to \mathrm{V}_{\mathbb{F}[H]}$.

Theorem 12.5. *We have a faithful functor* V *from the category of rings in which* 2 *is a unit to the category of nilpotent groups of class* 2.

For fixed $\mathbb{F}$ *with* $\operatorname{char}\mathbb{F} = p > 2$, *we have a faithful functor* $\mathrm{V}_{\mathbb{F}[\cdot]}$ *from the category of all groups to the category of all special p-groups.* □

Note, however, that there are commutative fields such that $\mathrm{V}_{\mathbb{F}[\cdot]}$ is not injective on (isomorphism types of) objects; cf. 12.4. The functors V and $\mathrm{V}_{\mathbb{F}[\cdot]}$ are not full: non-trivial central automorphisms (i.e., elements of K) never occur as images.

13. Recognition of the ring

Remark 13.1. The proofs in the previous sections use the fact that the union $(1,0)^\Sigma \cup (0,1)^\Sigma$ of orbits is characterized by the following two properties:

(C) C_v is commutative.

(D) $\mathrm{D}_v = R$.

Clearly, each $v \in (1,0)^\Sigma \cup (0,1)^\Sigma$ has both properties. Conversely, we have shown that these properties imply that v belongs to an orbit under a well-understood subgroup of Σ, at least in the following cases:

- Over each commutative ring, every element satisfying (D) belongs to $(1,0)^{\mathrm{SL}(2,R)}$, cf. 7.1.
- Over each full matrix ring, every element that satisfies (C) belongs to the union of orbits $\{(1,0),(0,1)\}^{\Delta^\sigma}$, see 8.4.
- Over each local ring, every element that satisfies both (C) and (D) belongs to the union of orbits $\{(1,0),(0,1)\}^{(\Delta\mathrm{T})^\sigma}$, see 9.1.

Thus, in each of these three cases, the union $\{(1,0),(0,1)\}^\Sigma$ of orbits is characterized by properties that are invariant under each isomorphism between Verardi groups.

Theorem 13.2. *Let $\mathcal{N}$ denote the class of all rings such that 2 is invertible and that $\{(1,0),(0,1)\}^\Sigma$ is characterized by the properties* (C) *and* (D).

For rings R and S with $S \in \mathcal{R}$, the groups V_R and V_S are isomorphic if, and only if, there exists an isomorphism or an anti-isomorphism from R onto S.

Proof. Let $\varphi : \mathrm{V}_R \to \mathrm{V}_S$ be an isomorphism, and let $(v,x) \in S^2 \times S$ be the image of $((1,0),0)$ under φ. Then v has the properties (C) and (D), and our assumption about S implies that we may assume $v \in \{(1,0),(0,1)\}$. Adapting φ further by automorphisms of V_S, we may also achieve that $((0,1),0)$ is mapped to (w,y), where $\{v,w\} = \{(1,0),(0,1)\}$. The proof of 5.7 now shows that our isomorphism is induced by an isomorphism or an anti-isomorphism of rings. □

Let us repeat again that $\mathcal{N}$ contains all commutative rings, all local rings, and all full matrix rings over fields, such that 2 is invertible.

14. Open problems

Let R be a ring such that 2 is a unit in R. We have seen in 5.5 that $\mathrm{Aut}(\mathrm{V}_R)$ contains the group $\Delta = \{\lambda_{c^{-1}}\zeta_h\rho_d \mid c,h,d \in R^\times\}$, the group $\mathrm{A} \cong \mathrm{Aut}(R)$ induced by automorphisms of the ring R, and the group $\mathrm{K} \cong \mathrm{Hom}(R^2,R)$ of central automorphisms. Moreover, if one-sided annihilators of R' are not trivial, the group T may be useful (see 5.12).

We have proved $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{TK}$ or $\mathrm{Aut}(\mathrm{V}_R) = \langle\hat{*}\rangle\mathrm{A}\Delta\mathrm{TK}$ (where $*$ is some anti-automorphism of R) in each of the following cases:

1. If R is a commutative ring such that $\mathrm{SL}(2,R)$ is generated by elementary transvections, see 7.2. (For a general commutative ring, we have $\Gamma\mathrm{L}(2,R) = \Sigma$.)
2. If R is a local ring, see 9.2.
3. If $R = \mathbb{K}^{n\times n}$ is a full matrix ring over a field, see 8.5 and 11.1.
4. If $R = \mathrm{T}(2,\mathbb{F})$ is the ring of all upper triangular 2×2 matrices over a commutative field $\mathbb{F}$, see 10.6.

The situation for commutative rings (where $\Sigma = \Gamma\mathrm{L}(2,R)$ may be strictly larger than $(\mathrm{A}\Delta\mathrm{T})^\sigma$) and the example 11.2 are indications that a general proof for a large class of rings (including all group rings of finite groups, say) is not possible.

Problem 14.1. *Find conditions that ensure that* $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{K}$, *or* $\mathrm{Aut}(\mathrm{V}_R) = \langle\hat{*}\rangle\mathrm{A}\Delta\mathrm{K}$, *where $*$ is an anti-automorphism of R.*

Problem 14.2. *Find conditions that ensure that either* $\mathrm{Aut}(\mathrm{V}_R) = \mathrm{A}\Delta\mathrm{TK}$, *or* $\mathrm{Aut}(\mathrm{V}_R) = \langle\hat{*}\rangle\mathrm{A}\Delta\mathrm{TK}$, *where $*$ is an anti-automorphism of R.*

Clearly, a necessary condition will be that the ring R is not commutative, since $\Phi\Delta$ does not induce all of $\mathrm{GL}(2,R)$ on $\mathrm{V}_R/(\mathrm{V}_R)'$, cf. 5.5.

Problem 14.3. *Find conditions on rings R, S such that the existence of an isomorphism between the Verardi groups V_R and V_S implies that R and S are (anti-) isomorphic.*

See 13.2 for examples of such criteria.

Problem 14.4. *Find conditions on the Verardi groups such that the existence of an isomorphism between the Verardi groups V_R and V_S implies that R and S are (anti-)isomorphic.*

An example of such a criterion is that $\{(1,0),(0,1)\}^\Sigma$ can be characterized by group theoretic properties, see 13.1. A problematic case appears to be V_R, where $R = \mathbb{K} \times \mathbb{L}$ for fields $\mathbb{K}, \mathbb{L}$ admitting no anti-automorphism, see 11.2.

References

[1] Baer, R.: *Groups with abelian central quotient group.* Trans. Amer. Math. Soc. **44**(3) (1938), 357–386. Zbl 0020.00802

[2] Baer, R.: *Linear algebra and projective geometry.* Academic Press, New York 1952. Zbl 0049.38103

[3] Bass, H.: *Introduction to some methods of algebraic K-theory.* Conference Board of the Mathematical Sciences. Regional Conference Series n Mathematics **20**, Am. Math. Soc., Providence, RI, 1974. Zbl 0323.18007

[4] Bloshchitsyn, V. Ya.: *Automorphisms of the general linear group over a commutative ring not generated by zero-divisors.* (Russian), Algebra i Logika **17**(6) (1978), 639–642. English translation: Algebra Logic **17** (1979), 415–417. Zbl 0432.20040

[5] Cohn, P. M.: *On the structure of the* GL_2 *of a ring.* Publ. Math., Inst. Hautes Étud. Sci. **30** (1966), 5–53, cf. pp. 365–413. Zbl 0144.26301

[6] Cohn, P. M.: *Skew fields. Theory of general division rings.* Encyclopedia of Mathematics and Its Applications **57**, University Press, Cambridge 1995. Zbl 0840.16001

[7] Cortini, R.: *On special p-groups.* Boll. Unione Mat. Ital. Sez. B, Artic. Ric. Mat. (8) **1**(3) (1998), 677–689. Zbl 0912.20016

[8] Curtis, C. W.; Reiner, I.: *Representation Theory of finite groups and associative algebras.* Pure and Applied Mathematics **11**, Wiley-Interscience, New York-London 1962. Zbl 0131.25601

[9] Dade, E. C.: *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps.* Math. Z. **119** (1971), 345–348. Zbl 0201.03303

[10] Dieudonné, J.: *Sur une généralisation du groupe orthogonal à quatre variables.* Arch. Math., Oberwolfach **1** (1949), 282–287. Zbl 0032.10601

[11] Formanek, E.; Sibley, D.: *The group determinant determines the group.* Proc. Am. Math. Soc. **112**(3) (1991), 649–656. Zbl 0742.20008

[12] Frobenius, G.: *Über die Darstellung der endlichen Gruppen durch lineare Substitutionen*. Berl. Ber. (1897), 994–1015. JFM 28.0130.01

[13] Gorenstein, D.: *Finite groups*. Harper's Series in Modern Mathematics, Harper & Row, New York etc. 1968. Zbl 0185.05701

[14] Greub, W. H.: *Multilinear algebra*. Springer-Verlag, Berlin-Heidelberg-New York 1967. Zbl 0169.35302

[15] Hoheisel, J.; Stroppel, M.: *More about Embeddings of Almost Homogeneous Heisenberg Groups*. J. Lie Theory **13** (2003), 443–455. Zbl 1030.22002

[16] Jennings, S. A.: *The structure of the group ring of a p-group over a modular field*. Trans. Amer. Math. Soc. **50** (1941), 175–185. Zbl 0025.24401 and JFM 67.0072.03

[17] Kaloujnine, L.: *Zum Problem der Klassifikation der endlichen metabelschen p-Gruppen*. Wiss. Z. Humboldt-Univer. Berlin, Math.-Naturw. Reihe **4** (1954/1955), 1–7. Zbl 0068.25502

[18] Khukhro, E. I.: *p-automorphisms of finite p-groups*. London Mathematical Society Lecture Note Series **246**. Cambridge University Press, Cambridge 1998. Zbl 0897.20018

[19] Klingenberg, W.: *Lineare Gruppen über lokalen Ringen*. Am. J. Math. **83** (1961), 137–153. Zbl 0098.02303

[20] Klingenberg, W.: *Die Struktur der linearen Gruppe über einem nichtkommutativen lokalen Ring*. Arch. Math. **13** (1962), 73–81. Zbl 0106.25203

[21] Lautemann, C.: *Linear transformations on matrices: rank preservers and determinant preservers*. Linear Multilinear Algebra **10**(4) (1981), 343–345. Zbl 0484.15004

[22] Levchuk, V.M.: *Connections between the unitriangular group and certain rings. II. Groups of automorphisms*. Sibirsk. Mat. Zh. **24** (1983), 64–80. English translation: Siberian Math. J. **24** (1983), 543–557. Zbl 0525.20031

[23] Mäurer, H.; Stroppel, M.: *Groups that are almost homogeneous*. Geom. Dedicata **68** (1997), 229–243. Zbl 0890.20025

[24] McDonald, B. R.: *Linear algebra over commutative rings*. Pure and Applied Mathematics **87**, Marcel Dekker, New York-Basel 1984. Zbl 0556.13003

[25] Passman, D. S.: *The algebraic structure of group rings*. Wiley-Interscience, New York-London-Sydney 1977. Zbl 0368.16003

[26] Rahnamai Barghi, A.; Ahmedy, M. Mofidy: *On automorphisms of a class of special p-groups*. Arch. Math. **77** (2001), 289–293. Zbl 0997.20029

[27] Roggenkamp, K. W.: *Group rings: Units and the isomorphism problem*. In: Roggenkamp, K. W., and M. Taylor: *Group rings and class groups*. DMV Seminar **18**, Birkhäuser Verlag, Basel 1992. Zbl 0769.20004

[28] Schwachhöfer, M.; Stroppel, M.: *Isomorphisms of linear semigroups*. Geom. Dedicata **65** (1997), 355–366. Zbl 0878.20041

[29] Stroppel, M.: *Homogeneous symplectic maps and almost homogeneous Heisenberg groups*. Forum Math. **11** (1999), 659–672. Zbl 0928.22008

[30] Stroppel, M.: *Embeddings of almost homogeneous Heisenberg groups.* J. Lie Theory **10** (2000), 443–453. Zbl 0955.22009

[31] Stroppel, M.: *Locally compact groups with many automorphisms.* J. Group Theory **4** (2001), 427–455. Zbl 0999.22006

[32] Stroppel, M.: *Locally compact groups with few orbits under automorphisms.* Topol. Proc. **26** (2001–2002), 819–842. Zbl 1081.22004

[33] Verardi, L.: *Una classe di gruppi finiti di esponente p in cui ogni sottogruppo normale è caratteristico.* (English summary) Boll. Unione Mat. Ital. VI. Ser., **4-B** (1985), 307–317. Zbl 0562.20010

[34] Verardi, L.: *A class of special p-groups.* Arch. Math. **68** (1997), 7–16. Zbl 0866.20012

[35] Zassenhaus, H.: *Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit Charakteristik p zuzuordnen.* Abh. Math. Sem. Hansische Univ. **13** (1939), 200–207. Zbl 0021.20001 and JFM 65.0091.01

Received December 22, 2004