Glasgow Math. J. **60** (2018) 435–445. © Glasgow Mathematical Journal Trust 2017.
doi:10.1017/S0017089517000192.

THREE-DIMENSIONAL ISOLATED QUOTIENT SINGULARITIES IN EVEN CHARACTERISTIC

VLADIMIR SHCHIGOLEV
Financial University under the Government of the Russian Federation,
49 Leningradsky Prospekt, Moscow, Russia
e-mail: shchigolev_vladimir@yahoo.com

and DMITRY STEPANOV
The Department of Mathematical Modelling Bauman Moscow State Technical University
2-ya Baumanskaya ul. 5, Moscow 105005, Russia
e-mail: dstepanov@bmstu.ru

(Received 8 February 2017; revised 26 June 2017; accepted 16 June 2017;
first published online 30 October 2017)

Abstract. This paper is a complement to the work of the second author on modular quotient singularities in odd characteristic. Here, we prove that if V is a three-dimensional vector space over a field of characteristic 2 and $G < \mathrm{GL}(V)$ is a finite subgroup generated by pseudoreflections and possessing a two-dimensional invariant subspace W such that the restriction of G to W is isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$, then the quotient V/G is non-singular. This, together with earlier known results on modular quotient singularities, implies first that a theorem of Kemper and Malle on irreducible groups generated by pseudoreflections generalizes to reducible groups in dimension three, and, second, that the classification of three-dimensional isolated singularities that are quotients of a vector space by a linear finite group reduces to Vincent's classification of non-modular isolated quotient singularities.

2010 *Mathematics Subject Classification.* Primary 13A50, Secondary 14L30.

1. Introduction. Let k be a field of characteristic p and V a finite dimensional vector space over k. A linear map $\varphi\colon V \to V$ is called a *pseudoreflection* if the set of points fixed by φ is a hyperplane in V. A pseudoreflection φ is called a *transvection* if 1 is the only eigenvalue of φ. Denote by V^* the dual space and by $S(V^*)$ its symmetric algebra. In [**6**], Kemper and Malle proved the following theorem.

THEOREM 1.1. *Let G be a finite irreducible subgroup of* $\mathrm{GL}(V)$. *Then, its ring of invariants $S(V^*)^G$ is polynomial if and only if G is generated by pseudoreflections and the pointwise stabilizer in G of any non-trivial subspace of V has a polynomial ring of invariants.*

Kemper and Malle also asked if the condition "irreducible" could be eliminated from the statement of their theorem. They showed that to obtain such a generalization it is sufficient to investigate the general reducible but non-decomposable case and pointed out that the generalized theorem holds in dimension 2. Note that the direct statement of Theorem 1.1 (if the ring $S(V^*)$ is polynomial, then . . .) is correct without the condition of irreducibility; it follows from the Chevalley–Shephard–Todd Theorem if p does not divide the order of G, and in the modular case $p \mid |G|$ it was proven by Serre.

From the perspective of singularity theory, Stepanov in [**7**] showed that if the generalized (to reducible groups G) theorem of Kemper and Malle is correct, it can be interpreted as saying that each isolated singularity which is a quotient of a vector space by a finite modular linear group is in fact isomorphic to a quotient by a non-modular group. Thus, the classification of such singularities reduces to the known Vincet's classification of isolated quotient singularities in the non-modular case; for details, see [**7**] and references therein. Stepanov also started studying three-dimensional case and obtained the following result.

THEOREM 1.2 [**7**, Theorem 4.1]. *Let V be a three-dimensional vector space over an algebraically closed field of characteristic p. Let G be a finite subgroup of $GL(V)$ generated by pseudoreflections. Denote by G_p the normal subgroup of G generated by all elements of order p^r, $r \geq 1$. Assume that G_p is either*

(1) *irreducible on V, or*
(2) *has a one-dimensional invariant subspace U, or*
(3) *has a two-dimensional invariant subspace W and the restriction of G_p to W is generated by two non-commuting transvections (and thus is irreducible).*

Then, the generalized Kemper–Malle Theorem holds for G. Moreover, if G satisfies condition (3) or condition (2) plus the induced action of G_p on V/U is generated by two non-commuting transvections, then V/G is non-singular.

Note that if a map $\varphi \in \mathrm{GL}(W)$, $\dim W = 2$, has order p^r, $r \geq 1$, then it has order p and is a transvection. In view of the classification of two-dimensional groups generated by transvections, Theorem 1.2 applies to all modular groups in odd characteristic. In characteristic 2 it remains to consider only the case when G has a two-dimensional invariant subspace W and the restriction H of G_2 to W is isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ (the group of all 2×2 matrices of determinant 1 with entries in the Galois field with 2^n elements), $n > 1$, in its natural representation.

In the present paper, we fill this gap and show, moreover, that no singularities arise in the remaining case $H = \mathrm{SL}_2(\mathbb{F}_{2^n})$, $n > 1$. Our main result is Theorem 1.3. As was shown in [**7**], we can assume from the beginning that $G = G_2$ and the base field k is algebraically closed.

THEOREM 1.3. *Let V be a three-dimensional vector space over an algebraically closed field k of characteristic 2. Let G be a finite subgroup of $\mathrm{GL}(V)$ generated by pseudoreflections of order 2^r, $r \geq 1$, and hence by transvections. Assume that G has a two-dimensional invariant subspace W and the restriction of G to W is isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$, $n > 1$, in its natural representation. Then, the ring of invariants $S(V^*)^G$ is polynomial.*

REMARK 1.4. It follows from our results that if $G < \mathrm{GL}(V)$, $\dim V = 3$, characteristic is arbitrary, is any finite subgroup generated by pseudoreflections and possessing a two-dimensional invariant subspace or a one-dimensional invariant subspace satisfying the additional condition of Theorem 1.2, then the quotient V/G is non-singular. However, it is not true that Chevalley–Shephard–Todd Theorem holds for modular groups in dimension 3. In [**6**], Kemper and Malle give examples of *irreducible* groups G generated by pseudoreflections for which the ring $S(V^*)^G$ is not polynomial. In dimension 4, there are examples (see [**5**, Example 11.0.3]) of reducible groups generated by pseudoreflections with singular quotients. For general reducible three-dimensional groups G generated by pseudoreflections, we do not know if the quotient V/G can be singular.

As we explained above, our results and Theorem 1.1 of Kemper and Malle imply the following corollaries.

COROLLARY 1.5. *The generalized Kemper–Malle Theorem holds in dimension* 3*, i.e., if V is a three-dimensional vector space and $G < \mathrm{GL}(V)$ is* any *finite subgroup, then the ring of invariants $S(V^*)^G$ is polynomial if and only if G is generated by pseudoreflections and the pointwise stabilizer in G of any non-trivial subspace of V has a polynomial ring of invariants.*

COROLLARY 1.6. *If V is a three-dimensional vector space over an arbitrary field k, and G a finite subgroup of* $\mathrm{GL}(V)$ *such that the variety V/G has isolated singularity, then V/G is isomorphic to one of the non-modular isolated quotient singularities from Vincent's classification.*

We prove our Theorem 1.3 by a more or less direct computation of the ring of invariants of the group G. The proof is contained in Sections 2 and 3.

2. Proof of Theorem 1.3: the group G as an extension of $\mathrm{SL}_2(\mathbb{F}_{2^n})$. Assume that a group G satisfies the conditions of Theorem 1.3, i.e., G is generated by transvections, acts on a three-dimensional vector space V with a two-dimensional invariant subspace W, and the restriction of G to W is isomorphic to the natural action of the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ on the space k^2 of column vectors. We shall fix a basis (e_1, e_2, e_3) of V such that e_1 and e_2 span W and each element of the group G is represented in this basis by a matrix

$$\begin{pmatrix} a & b & \alpha \\ c & d & \beta \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c, d \in \mathbb{F}_{2^n} \subset k$, $ad + bc = 1$, $\alpha, \beta \in k$. We have an exact sequence of groups

$$0 \to N \to G \to \mathrm{SL}_2(\mathbb{F}_{2^n}) \to 1, \tag{1}$$

where N is the kernel of the natural restriction map. In our basis, N consists of the matrices

$$\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix},$$

where the column $(\alpha, \beta)^T$ varies in some finite subset Λ of k^2. Denote by Λ_1 the projection of Λ to the first coordinate.

LEMMA 2.1. *The sets Λ and Λ_1 have natural structures of vector spaces over the Galois field $\mathbb{F}_{2^n}$. Moreover, $\Lambda = (\Lambda_1, \Lambda_1)^T$ and* $\dim_{\mathbb{F}_{2^n}} \Lambda = 2 \dim_{\mathbb{F}_{2^n}} \Lambda_1$.

Proof. Obviously, N is an abelian group, and thus Λ is a subgroup of k^2. It remains to show that Λ is preserved by multiplication by an element $e \in \mathbb{F}_{2^n}$. Note that, as always in extensions with abelian N, the quotient group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ acts on N via conjugation.

https://doi.org/10.1017/S0017089517000192 Published online by Cambridge University Press

In our case, this action is nothing else but the left multiplication of a column $(\alpha, \beta)^T$ by a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{2^n}).$$

So, we have

$$\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{2^n}), \ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \Lambda \Rightarrow$$

$$\begin{pmatrix} \alpha + e\beta \\ \beta \end{pmatrix}, \begin{pmatrix} \alpha \\ e\alpha + \beta \end{pmatrix} \in \Lambda \Rightarrow e \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \in \Lambda.$$

But

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{2^n}) \Rightarrow e \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \Lambda.$$

Multiplying a column $(\alpha, \beta)^T \in \Lambda$ by matrices from the subgroup $\mathrm{SL}_2(\mathbb{F}_2) < \mathrm{SL}_2(\mathbb{F}_{2^n})$, one readily checks that the set Λ also contains $(\alpha, 0)^T$, $(0, \beta)^T$, $(0, \alpha)^T$, and $(\beta, 0)^T$. The remaining statements follow directly from this fact. □

The following proposition describes a convenient set of generators of the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$.

PROPOSITION 2.2. *The group* $\mathrm{SL}_2(\mathbb{F}_{2^n})$ *is generated by the matrices*

$$R = \begin{pmatrix} e^{-1} & 0 \\ 0 & e \end{pmatrix}, \ S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

where e is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$ *of the field* $\mathbb{F}_{2^n}$.

Proof. It is well known (see, e.g., [**2**, Chapter 1]) that $\mathrm{SL}_2(\mathbb{F}_{2^n})$ is generated by its subgroup of diagonal matrices, the subgroup of upper triangular unipotent matrices, and the element

$$STS = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If we are given the elements R, S, T, we can get any matrix

$$\begin{pmatrix} 1 & e^r \\ 0 & 1 \end{pmatrix}$$

as $R^{-r/2}SR^{r/2}$, where

$$R^{r/2} = \begin{pmatrix} e^{-r/2} & 0 \\ 0 & e^{r/2} \end{pmatrix}$$

(recall that each element of $\mathbb{F}_{2^n}$ has a unique square root in $\mathbb{F}_{2^n}$). □

REMARK 2.3. Note that the matrices S and T generate the group $\mathrm{SL}_2(\mathbb{F}_2)$.

In our next step, we show that sequence (1) splits.

LEMMA 2.4. *After a change of the basis vector e_3, if necessary, we can assume that the group G contains matrices*

$$\tilde{S} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \tilde{T} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and one of the matrices

$$\tilde{R} = \begin{pmatrix} e^{-1} & 0 & 1 \\ 0 & e & e \\ 0 & 0 & 1 \end{pmatrix} \text{ or } \tilde{R}' = \begin{pmatrix} e^{-1} & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Proof. As was shown in [**7**, Lemma 4.4], the group G contains transvections $\tilde{S}$ and $\tilde{T}$ that restrict to the elements S and T of $\mathrm{SL}_2(\mathbb{F}_{2^n})$, respectively. Each of the transvections $\tilde{S}$ and $\tilde{T}$ fixes a plane, and these planes intersect along a line not contained in the invariant subspace W. If we take e_3 to be any non-zero vector from this line, then, in the basis e_1, e_2, e_3, $\tilde{S}$ and $\tilde{T}$ have the desired matrices.

Now consider any element

$$\begin{pmatrix} e^{-1} & 0 & \alpha \\ 0 & e & \beta \\ 0 & 0 & 1 \end{pmatrix} \in G$$

that restricts to $R \in \mathrm{SL}_2(\mathbb{F}_{2^n})$. Using the matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \tilde{S}\tilde{T}\tilde{S},$$

we get one more matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e^{-1} & 0 & \alpha \\ 0 & e & \beta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} e & 0 & \beta \\ 0 & e^{-1} & \alpha \\ 0 & 0 & 1 \end{pmatrix} \in G,$$

thus

$$\begin{pmatrix} e^{-1} & 0 & \alpha \\ 0 & e & \beta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e & 0 & \beta \\ 0 & e^{-1} & \alpha \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & e^{-1}\beta + \alpha \\ 0 & 1 & e\alpha + \beta \\ 0 & 0 & 1 \end{pmatrix} \in N.$$

Further,

$$\begin{pmatrix} 1 & 0 & e^{-1}\beta + \alpha \\ 0 & 1 & e\alpha + \beta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e^{-1} & 0 & \alpha \\ 0 & e & \beta \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} e^{-2} & 0 & e^{-1}(\alpha + \beta) \\ 0 & e^2 & e(\alpha + \beta) \\ 0 & 0 & 1 \end{pmatrix} \in G.$$

The 2^{n-1}-th power of the last matrix equals

$$\begin{pmatrix} e^{-1} & 0 & (e^{1-2^n}+e^{3-2^n}+\cdots+e^{-1})(\alpha+\beta) \\ 0 & e & (e^{2^n-1}+e^{2^n-3}+\cdots+e)(\alpha+\beta) \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} e^{-1} & 0 & (e+1)^{-1}(\alpha+\beta) \\ 0 & e & e(e+1)^{-1}(\alpha+\beta) \\ 0 & 0 & 1 \end{pmatrix}.$$

If $\alpha+\beta=0$, then we have found the matrix $\tilde{R}' \in G$. If $\alpha+\beta \neq 0$, then, rescaling the basis vector e_3, we come to the matrix $\tilde{R} \in G$. □

LEMMA 2.5. *Let $f\colon \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}$ be a function defined by the formula*

$$f(x,y) = 1 + x + y + x^{2^{n-1}} y^{2^{n-1}}.$$

Then, for all $a,b,c,d,p,q \in \mathbb{F}_{2^n}$ such that $ad+bc=1$, the following identity holds:

$$pf(a,b) + qf(c,d) + f(p,q) = f(pa+qc, pb+qd).$$

Proof. The lemma is proven by a straightforward substitution, bearing in mind that for any $x \in \mathbb{F}_{2^n}$ one has $x^{2^n} = x$. □

COROLLARY 2.6. *For all $\gamma \in k$, the set of matrices*

$$H_\gamma = \left\{ \begin{pmatrix} a & b & \gamma f(a,b) \\ c & d & \gamma f(c,d) \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{2^n}) \right\}$$

is a subgroup of $\mathrm{GL}(V)$ *isomorphic to* $\mathrm{SL}_2(\mathbb{F}_{2^n})$.

REMARK 2.7. For any $\gamma \in k$, the map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} \gamma f(a,b) \\ \gamma f(c,d) \end{pmatrix}$$

is a skew homomorphism from the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ to the additive group k^2, generating the cohomology group $H^1(\mathrm{SL}_2(\mathbb{F}_{2^n}), k^2)$, where $\mathrm{SL}_2(\mathbb{F}_{2^n})$ acts on the space k^2 of column vectors by left multiplication, see [**4**].

PROPOSITION 2.8. *The group G contains one of the groups H_0 or H_1 defined in Corollary 2.6. It follows, in particular, that G is a semidirect product of the subgroups N and H_0 (H_1), that is, sequence* (1) *splits.*

Proof. Indeed, it can be directly checked that $\tilde{R}$, $\tilde{S}$, $\tilde{T} \in H_1$, whereas $\tilde{R}'$, $\tilde{S}$, $\tilde{T} \in H_0$. □

REMARK 2.9. It is known that the second cohomology group $H^2(\mathrm{SL}_2(\mathbb{F}_{2^n}))$ with coefficients in the natural module is non-zero for $n > 2$ ([**3**, Proposition 4.4]), i.e., there exist non-split extensions of $\mathrm{SL}_2(\mathbb{F}_{2^n})$ by $\mathbb{F}_{2^n}^2$. Our results mean that those non-split extensions do not have representations of the type that we study in this section.

REMARK 2.10. Note that the groups H_0 and H_1 are defined over the field $\mathbb{F}_{2^n}$, i.e., the entries of all the matrices of H_0 and H_1 belong to $\mathbb{F}_{2^n}$.

3. Proof of Theorem 1.3: invariants. In this section, we compute the invariants of the action of the group G on the space $V \simeq k^3$. We do this in two steps: first, we compute the invariants of the kernel N and show that V/N is again isomorphic to k^3; then, we compute the action of the quotient group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ ($\simeq H_0$ or H_1, see Proposition 2.8) on the invariants of N and show that also

$$V/G \simeq \frac{V/N}{H_0(H_1)} \simeq k^3.$$

To show that a ring of invariants $S(V^*)^G$ is polynomial, we shall use the following criterion that is a direct consequence of [**5**, Corollary 3.1.6].

PROPOSITION 3.1. *Let V be a vector space of dimension n and $G < \mathrm{GL}(V)$ a finite group. Then, $S(V^*)^G$ is polynomial if and only if there exist homogeneous invariants $f_1, \ldots, f_n \in S(V^*)^G$ of degrees $d_1, \ldots, d_n$ such that $\prod_{i=1}^n d_i = |G|$ and the ideal $(f_1, \ldots, f_n) \subset S(V^*)$ is zero-dimensional. If such $f_1, \ldots, f_n$ exist, then they generate freely the ring $S(V^*)^G$.*

Recall that N acts on V by matrices

$$\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix},$$

where the column $(\alpha, \beta)^T$ runs over a finite dimensional $\mathbb{F}_{2^n}$-vector space $\Lambda \subset k^2$. Let x ,y, z be a basis of V^* dual to the basis e_1, e_2, e_3 of V chosen in Section 2. Obviously, the polynomials

$$f_x = \prod_{\alpha \in \Lambda_1} (x + \alpha z),$$
$$f_y = \prod_{\alpha \in \Lambda_1} (y + \alpha z),$$
$$f_z = z$$

are invariant under the action of N.

LEMMA 3.2. *The polynomial f_x (f_y) can involve x (y) only in degrees 2^{mn}, where $0 \le m \le d = \dim_{\mathbb{F}_{2^n}} \Lambda_1$.*

Proof. Let $q = 2^n$ and

$$f'_x = \prod_{\alpha \in \Lambda_1} (x + \alpha).$$

By the definition of the *Dickson invariants* $c_m \in k$ (see, e.g., [**1**, Section 8.1]), we have

$$f'_x = x^{q^d} + \sum_{m=0}^{d-1} c_m x^{q^m}.$$

https://doi.org/10.1017/S0017089517000192 Published online by Cambridge University Press

To conclude the proof, it remains to note that f_x is obtained from f'_x by "homogenization" with the help of z: a monomial x^k with $k \leq q^d$ is replaced by $x^k z^{q^d - k}$. $\square$

PROPOSITION 3.3. *The ring of invariants $S(V^*)^N$ is a polynomial ring generated by f_x, f_y, f_z.*

Proof. We have $|N| = |\Lambda| = 2^{2dn} = \deg f_x \cdot \deg f_y \cdot \deg f_z$. Also, the system of equations

$$\begin{cases} f_x = 0 \\ f_y = 0 \\ f_z = 0 \end{cases}$$

obviously has the only solution $x = y = z = 0$, so the ideal (f_x, f_y, f_z) is zero-dimensional and Proposition 3.1 applies. $\square$

Recall that since N is normal in G, the quotient group G/N acts on $S(V^*)^N$. Thus, next we have to determine the action of the groups H_0 and H_1 on f_x, f_y and f_z. Let us begin with H_0. The generators of this group leave invariant the variable z and are defined over the field $\mathbb{F}_{2^n}$ (see Remark 2.10). From this and from Lemma 3.2, it follows that the action of H_0 on f_x, f_y, f_z is linear, that is, if $h \in H_0$, then it acts on the tuple (f_x, f_y, f_z) by right matrix multiplication:

$$(f_x, f_y, f_z) \mapsto (f_x, f_y, f_z) \cdot h.$$

Therefore, in this case we can simply ignore the kernel N. Furthermore, since (the representation of) the group H_0 is decomposable, the polynomiality of its ring of invariants has been already established by Kemper and Malle [**6**, Section 8].

Now, consider the indecomposable group H_1. For the sake of clearness and simplicity, let us start with the case when there is no kernel, i.e., $N = \{0\}$ and $H_1 = G$. We shall need the invariants of the action of $\mathrm{SL}_2(\mathbb{F}_{2^n})$ on its natural module. Let $W = k^2$ be a two-dimensional space of column vectors over a field k containing $\mathbb{F}_{2^n}$, and let the group $\mathrm{SL}_2(\mathbb{F}_{2^n})$ act on W by left matrix multiplication. Denote by W^* the dual space. The Dickson invariants (see, e.g., [**1**, Proposition 8.1.3]) are

$$c_0 = \prod_{\substack{l \in W^* \\ l \neq 0}} l,$$

and

$$c_1 = \sum_{\substack{U \subseteq W \\ \dim U = 1}} \prod_{\substack{l \in W^* \\ l|_U \neq 0}} l$$

(for c_1 the sum is taken over all one-dimensional subspaces of W, and the product over all linear forms that restrict to a non-zero form on U). It is not hard to see that there exists a root of degree $2^n - 1$ of the polynomial c_0, that is, $\exists u \in S(W^*)$: $u^{2^n - 1} = c_0$, and that u and c_1 are $\mathrm{SL}_2(\mathbb{F}_{2^n})$-invariant.

THEOREM 3.4 ([**1**, Theorem 8.2.1]). *The ring of invariants of $\mathrm{SL}_2(\mathbb{F}_{2^n})$ on W is polynomial and generated by u and c_1.*

Let us come back to our group $G = H_1$ and space V. Since we have a G-invariant subspace W, the restriction to W of each invariant of G is an $\mathrm{SL}_2(\mathbb{F}_{2^n})$-invariant. Thus, we have a homomorphism $S(V^*)^G \to S(W^*)^{\mathrm{SL}_2(\mathbb{F}_{2^n})}$ of invariant rings. In a general modular case, there is no reason for such a homomorphism to be surjective. However, we shall see that we do have a surjection in our case and this will be a crucial step in computing the invariants of G.

LEMMA 3.5. *Let G, V and W be as defined above. Then, the restriction homomorphism $S(V^*)^G \to S(W^*)^{\mathrm{SL}_2(\mathbb{F}_{2^n})}$ is surjective.*

Proof. It is sufficient to lift to the ring $S(V^*)^G$ the invariants $u, c_1 \in S(W^*)^{\mathrm{SL}_2(\mathbb{F}_{2^n})}$. We shall work in the explicit coordinates x, y, z defined after Proposition 3.1, so that any linear form $l \in V^*$ can be written as $l = ax + by + cz$, $a, b, c \in k$. Together with the function f (see Lemma 2.5), consider also a function $g \colon \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}$:

$$g(x, y) = f(x, y) + 1 = x + y + x^{2^{n-1}} y^{2^{n-1}}.$$

It follows from Lemma 2.5 that g has the following property: for all $a, b, c, d, p, q \in \mathbb{F}_{2^n}$, if $ad + bc = 1$, then

$$pf(a, b) + qf(c, d) + g(p, q) = g(pa + qc, pb + qd). \tag{2}$$

Note also that g is a homogeneous function of degree 1 on $\mathbb{F}_{2^n}^2$, i.e.,

$$\forall a, b, t \in \mathbb{F}_{2^n} \quad g(ta, tb) = tg(a, b). \tag{3}$$

Now, let us lift each linear form $l = ax + by \in W^*$ to V^* by the formula $\tilde{l} = ax + by + g(a, b)z$ and define

$$\tilde{c}_0 = \prod_{\substack{l \in W^* \\ l \neq 0}} \tilde{l},$$

$$\tilde{c}_1 = \sum_{\substack{U \subseteq W \\ \dim U = 1}} \prod_{\substack{l \in W^* \\ l|_U \neq 0}} \tilde{l}.$$

Property (2) implies that both $\tilde{c}_0$ and $\tilde{c}_1$ are G-invariant. Obviously, $\tilde{c}_0|_W = c_0$, $\tilde{c}_1|_W = c_1$. But, using property (3), one readily shows that $\tilde{c}_0$ admits a root of degree $2^n - 1$, i.e., there exists $\tilde{u} \in S(V^*)$ such that $\tilde{u}^{2^n-1} = \tilde{c}_0$. Moreover, this $\tilde{u}$ is G-invariant and restricts to $u \in S(W^*)^{\mathrm{SL}_2(\mathbb{F}_{2^n})}$. □

PROPOSITION 3.6. *The ring of invariants $S(V^*)^G$ (for $G = H_1$) is polynomial and generated by (algebraically independent) invariants $\tilde{u}$, $\tilde{c}_1$, z, where $\tilde{u}$ and $\tilde{c}_1$ are defined in the proof of Lemma 3.5.*

Proof. Let $\tilde{c} \in S(V^*)^G$ be an arbitrary homogeneous invariant. Let $c = \tilde{c}|_W$. Write c as a polynomial of u and c_1:

$$c = h(u, c_1).$$

The G-invariant $\tilde{c} - h(\tilde{u}, \tilde{c}_1)$ vanishes on W, thus it is divisible by z. But since z is also a G-invariant, so is the polynomial

$$\tilde{c}' = (\tilde{c} - h(\tilde{u}, \tilde{c}_1))/z.$$

The degree of $\tilde{c}'$ is strictly less than that of $\tilde{c}$, so, proceeding by induction, we express $\tilde{c}$ through $\tilde{u}$, $\tilde{c}_1$ and z.

As an alternative method of proof, note that $\deg \tilde{u} = \deg u = 2^n + 1$, $\deg \tilde{c}_1 = \deg c_1 = 2^{2n} - 2^n$, so that $\deg \tilde{u} \cdot \deg \tilde{c}_1 \cdot \deg z = 2^{3n} - 2^n$, which is the order of $\mathrm{SL}_2(\mathbb{F}_{2^n})$. To apply Proposition 3.1, we have to show that the ideal generated by the invariants $\tilde{u}$, $\tilde{c}_1$, z is zero-dimensional. But this question reduces to a similar question about the ideal $(u, c_1) \subset S(W^*)$, which is zero-dimensional because u and c_1 generate the invariant ring of $\mathrm{SL}_2(\mathbb{F}_{2^n})$. □

Now we return to the general case of a non-zero kernel N. A direct calculation with a use of Lemma 3.2 shows that the two generators $\tilde{S}$, $\tilde{T}$ (see Lemma 2.4) of the group H_1 act on the basis invariants f_x, f_y, f_z of N by the formulae

$$f_x \cdot \tilde{S} = f_x + f_y, \quad f_y \cdot \tilde{S} = f_y, \quad f_z \cdot \tilde{S} = f_z,$$
$$f_x \cdot \tilde{T} = f_x, \quad f_y \cdot \tilde{T} = f_x + f_y, \quad f_z \cdot \tilde{T} = f_z,$$

i.e., their action is linear. It follows from Lemma 3.2 that the third generator $\tilde{R}$ acts by the formulae

$$f_x \cdot \tilde{R} = e^{-1} f_x + \alpha z^{2^{dn}}, \quad f_y \cdot \tilde{R} = e f_x + e\alpha z^{2^{dn}}, \quad f_z \cdot \tilde{R} = f_z,$$

where $\alpha \in k$. It can happen that $\alpha = 0$, so that the action of H_1 on V/N is linear (in coordinates f_x, f_y, f_z) and decomposable. But then again by the results of Kemper and Malle the ring of invariants $S((V/N)^*)^{H_1} = S(V^*)^G$ is polynomial. In general, the coefficient α does not vanish and the action of $\tilde{R}$ becomes non-linear. Still, it is possible to adapt the argument of Lemma 3.5 and Proposition 3.6.

Note that the equation $f_z = z = 0$ defines an invariant subspace W/N of the quotient V/N (which we consider as a vector space isomorphic to k^3, the isomorphism being defined by the functions f_x, f_y, f_z). The action of H_1 on W/N is the natural action of $\mathrm{SL}_2(\mathbb{F}_{2^n})$. So, let u and c_1 be the basis invariants of $\mathrm{SL}_2(\mathbb{F}_{2^n})$, but now considered as functions of f_x, f_y, f_z. Repeating the proof of Lemma 3.5 with f_x in place of x, f_y in place of y, and $\alpha z^{2^{dn}}$ in place of z, we find some liftings $\bar{u}$ and $\bar{c}_1$ of u and c_1 to the ring of invariants $S(V^*)^G$.

The following proposition finishes the proof of Theorem 1.3.

PROPOSITION 3.7. *The ring of invariants* $S(V^*)^G = S((V/N)^*)^{H_1}$ *is polynomial and generated by (algebraically independent) invariants* $\bar{u}$, $\bar{c}_1$, z.

Proof. This proposition is proven by argument similar to any of the two proofs of Proposition 3.6. For example, for the second proof note that the degrees of $\bar{u}$ and $\bar{c}_1$ will multiply by $2^{dn} = \deg f_x = \deg f_y$ when compared to the degrees of $\tilde{u}$ and $\tilde{c}_1$. It follows that $\deg \bar{u} \cdot \deg \bar{c}_1 \cdot \deg z = 2^{2dn} \cdot |\mathrm{SL}_2(\mathbb{F}_{2^n})| = |N| \cdot |\mathrm{SL}_2(\mathbb{F}_{2^n})| = |G|$. □

ACKNOWLEDGEMENTS. Vladimir Shchigolev was supported by RFBR grant no. 16-01-00756. Dmitry Stepanov was supported by RFBR grants no. 14-01-00160 and no. 15-01-02164.

REFERENCES

1. D. J. Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series, vol. 190 (Cambridge University Press, Cambridge, UK, 1993).

2. C. Bonnafé, *Representations of* $\mathrm{SL}_2(\mathbb{F}_q)$, *Algebra and Applications*, vol. 13 (Springer Verlag, London, 2011).

3. C.-H. Sah, Cohomology of split group extensions, II, *J. Algebra* **45** (1977), 17–68.

4. E. Cline, B. Parshall and L. Scott, Cohomology of finite groups of Lie type, I, *Publ. Math. l'IHES* **45** (1975), 169–191.

5. H. E. A. E. Campbell and D. L. Wehlau, *Modular invariant theory*, *Encyclopaedia of Mathematical Sciences*, vol. 139, Invariant Theory and Algebraic Transformation Groups VIII (subseries Gamkrelidze, R. V. and Popov V. L., Editors) (Springer, 2011), XIV, 234 p.

6. G. Kemper and G. Malle, The finite irreducible linear groups with polynomial ring of invariants, *Transformation Groups* **2**(1) (1997), 57–89.

7. D. A. Stepanov, Three-dimensional isolated quotient singularities in odd characteristic, *Sbornik: Mathematics* **207**(6) (2016), 873–887.