ISRAEL JOURNAL OF MATHEMATICS 77 (1992), 65–81

RESIDUAL PROPERTIES OF FREE GROUPS, III

BY

T. S. WEIGEL*

Mathematisches Institut der Universität Freiberg
Alberstr. 23b, D-7800 Freiberg, Germany

ABSTRACT

In this paper we want to prove the following theorem: Let χ be an infinite set of non-abelian finite simple groups. Then the free group F_2 on 2 generators is residually χ. This answers a question first posed by W. Magnus and later by A. Lubotzky [9], Yu. Gorchakov and V. Levchuk [4].

1. Introduction

A group G is called residually $\mathcal{X}$ if the intersection of all normal subgroups $N \trianglelefteq G$ such that $G/N \in \mathcal{X}$ is the trivial group. In this paper we consider a certain residual property of free groups F_n on n generators ($n \geq 2$). We consider the case in which every group in $\mathcal{X}$ is a non-abelian finite simple group and $\mathcal{X}$ is infinite. For these classes we prove the following theorem:

THEOREM 1: *Let $\mathcal{X}$ be any infinite set of non-abelian finite simple groups. Then the free group F_2 on 2 generators is residually $\mathcal{X}$.*

This answers a question first posed by W. Magnus and later by A. Lubotzky [9], Yu. Gorchakov and V. Levchuk [4]. As every non-abelian free group F_n is residually $\{F_2\}$ [14], the transitivity implies that F_n is also residually $\mathcal{X}$. So the theorem still holds for any free group F_n, where n is a cardinal number greater than 1.

To prove Theorem 1 we show the following:

* The author gratefully acknowledges financial support by the Deutsche Forschungsgemeinschaft.
Received December 2, 1990 and in revised form May 9, 1991

THEOREM 2: *Let $\mathcal{Z}$ be an infinite set of exceptional groups of Lie type such that all groups are of the same type. Then the free group F_2 of rank 2 is residually $\mathcal{Z}$.*

Then the proof of Theorem 1 can be carried out as follows:

Proof of Theorem 1: Let $\mathcal{X}$ be any infinite set of non-abelian finite simple groups. Then the pidgeon-hole principle and the classification of finite simple groups imply that one of the following has to hold:

(a) $\mathcal{X}$ contains an infinite set of alternating groups.

(b) $\mathcal{X}$ contains an infinite set of classical groups of Lie type

(c) $\mathcal{X}$ contains an infinite set of exceptional groups of Lie type.

In case (a) the assertion was proved by R. Katz and W. Magnus [6]. In [18] and [19] the assertion was proved for classes of groups $\mathcal{X}$ satisfying (b). So the only case we have to consider is (c). The pidgeon-hole principle implies that it is sufficient to consider infinite classes of groups $\mathcal{Z}$ consisting of exceptional groups such that each group is of the same type. Then Theorem 2 implies the assertion. ∎

For some certain classes of finite simple groups it has already been known for some time that the desired assertion holds. These classes are of the form $\{X(S) \mid S \in \mathcal{M}\}$ where X is some scheme of twisted or untwisted Chevalley groups, $\mathcal{M}$ is a set of finite fields and there exists a ring R such that each element of $\mathcal{M}$ is a homomorphic image of R and the intersection of all the kernels of the homomorphisms of R onto an element of $\mathcal{M}$ is trivial. Now this ring R should have the following property: X is defined over R, one can find a subgroup $F \leq X(R)$ which is isomorphic to the free group on 2 generators and $\Psi_S^* : F \mapsto X(S)$, where Ψ_S^* is induced by $\Psi_S : R \mapsto S$, is onto for all but finitely many $S \in \mathcal{M}$. Under this assumption it is an obvious consequence that the free group F_2 on 2 generators is residually $\{X(S) | S \in \mathcal{M}\}$.

For certain classes $\{X(S) | S \in \mathcal{M}\}$ and some polynomial ring R an explicit subgroup $F \leq X(R)$ has been constructed, such that $\Psi_S^* : F \mapsto X(S)$ is onto for all but finitely many $S \in \mathcal{M}$ ([7],[8],[15],[22]).

In [9] A. Lubotzky considers the case where X and R can be chosen, such that $X(R)$ has the "strong approximation property" for every Zarisky dense subgroup [12],[21]. By a theorem of J. Tits it is known that $X(R)$ contains a Zarisky dense subgroup of F isomorphic to the free group of rank 2 and so the desired result follows.

Now in the cases we are considering we cannot take a ring R for which a "strong approximation theorem" is known. For a scheme of exceptional type it is difficult to find a subgroup $F \in X(R)$ isomorphic to the free group on 2 generators, such that Ψ_S^*: $F \mapsto X(S)$ is onto for all but finitely many S. The only cases in which this attempt has been successful so far are if X is of type $^2B_2$, $^2G_2$ or A_n.

We choose a different approach which was already used to obtain the desired result for classes satisfying the condition (b) ([17],[18],[19]). The background of the following theorems is to obtain a lower bound for $C(G_F)$, where $C : \mathcal{G}_2 \mapsto \mathbb{N} \cup \{\infty\}$ is the function defined on any 2-generated group introduced in [18]. We recall the definition. Let G be a group generated by two elements. Let $M_G \subseteq F_2$ be the set of all words in x and y vanishing on all pairs of elements s and t of G, for which $< s,t >= G$ is satisfied. Then we define

$$C(G) = \min\left\{ \ell(w) \mid w \in M_G \backslash \{1\} \right\}, \text{where } \min\{\quad\} = \infty.$$

We see easily that the definition is independent of the generators $x, y \in F_2$. The following theorem gives the connection between the set of values of this function on a class of 2-generated groups $\mathcal{X}$ and residual properties for the free group F_2 on 2 generators ([18], theorem 2).

THEOREM 3: *F_2 is residually $\mathcal{X}$ $\Longleftrightarrow$ $\{C(G) \mid G \in \mathcal{X}\}$ is an unbounded set.*

All notations used in the following are standard and can be found in [1], [2] and [3]. For each finite simple group of Lie type we look at the corresponding covering (central extension) G_F which is the fixed point set of some Frobenius map defined on an algebraic simple simply connected group G. For each of these groups G_F we choose an element $c \in G_F$ which generates a certain cyclic maximal torus T_F. The type and the order are listed in Table 1. The case that $\mathcal{Z}$ is a class consisting of groups of type $^2B_2$ or $^2G_2$ is not considered in the following, as in this case Theorem 2 is already proved in [7] and [8].

The proof of theorem 2 will be found in section 4.

2. The Verbal Topology and Zariski Topology for Affine Algebraic Groups

Let G be an affine algebraic group. Then it carries the well known Zariski topology. Here the closed sets are exactly the affine subvarieties of G. On any group G there can be defined the verbal topology as follows: Consider a reduced word $w \in F_n$ in the free group F_n on n generators. Now we can interpret

Table 1

G_F	Type of $T_F[2]$	$\lvert T_F \rvert$	Remark
$G_2(q)$	G_2	$q^2 - q + 1$	
${}^3D_4(q)$	–	$q^4 - q^2 + 1$	
$F_4(q)$	F_4	$q^4 - q^2 + 1$	
$E_6(q)$	$E_6(a_1)$	$q^6 + q^3 + 1$	
${}^2E_6(q)$	–	$q^6 - q^3 + 1$	
$E_7(q)$	E_7	$(q+1)(q^6 - q^3 + 1)$	$q \equiv 0, 1 \bmod 3$
	$E_6(a_1)$	$(q-1)(q^6 + q^3 + 1)$	$q \equiv 2 \bmod 3$
$E_8(q)$	E_8	$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$	
${}^2F_4(2^{2k+1})$	–	$q_0^4 + \sqrt{2}\, q_0^3 + q_0^2 + \sqrt{2}\, q_0 + 1$	$q_0 = 2^k\sqrt{2}$

$n-1$ of the generators as constants (elements in the group G) and one as an indeterminate, e.g. for $c_1, \dots, c_r \in < g_1, \dots, g_{n-1} > \leq G$ consider $w_{g_1,\dots,g_{n-1}}(x) = x^{\alpha_1} c_1 \dots x^{\alpha_r} c_r$. The vanishing set of $w_{g_1,\dots,g_{n-1}}$ is now defined by

$$\mathrm{Van}_{w_{g_1,\dots,g_{n-1}}}(G) = \{x \in G \mid w(x) = 1\}.$$

The vanishing sets for all reduced words and any set of constants form a subbase of the closed sets of the verbal topology. We also see that if G is an affine algebraic group then every set which is closed in the verbal topology is also closed in the Zariski topology. Next we prove that if G is a simple algebraic group of the type listed in Table 1 the group G cannot be equal to a certain vanishing set. Therefore we need a theorem concerning certain free products of groups in $\mathrm{PGL}(2, \boldsymbol{F}_q(x))$.

THEOREM 4: *Let c be a non-trivial semisimple element contained in a split torus of $\mathrm{PGL}(2, \boldsymbol{F}_q)$. Then there exists an element $t \in \mathrm{PGL}(2, \boldsymbol{F}_q(x))$ (already in $\mathrm{PSL}(2, \boldsymbol{F}_q(x))$) such that $< c, t > \cong < c > \coprod \mathbb{Z}$, the free product of a cyclic subgroup of order $\mathrm{ord}(c)$ and the free cyclic group $\mathbb{Z}$.*

Proof: For $\mathrm{PGL}(2, \boldsymbol{F}_q(x))$ we have the natural action on the projective line $\boldsymbol{F}_q(x) \cup \{\infty\}$. Without loss of generality we may assume that c is fixing ∞ and

0. Furthermore we may assume that c is acting on $\boldsymbol{F}_q(x)$ by $p \cdot c = p \cdot \xi$, where $\xi \in \boldsymbol{F}_q^*$ is an element of order $\mathrm{ord}(c)$.

On $\boldsymbol{F}_q[x]$ there is defined the degree function ∂ which can be extended to $\boldsymbol{F}_q(x)$ by:

$$\partial\left(\frac{f}{g}\right) = \partial(f) - \partial(g), \quad \text{for } f, g \in \boldsymbol{F}_q[x].$$

Here $\partial(0)$ is defined to be $-\infty$. This function can be made into a valuation on $\boldsymbol{F}_q(x)$ if we define $|p| = \exp(\partial(p))$. Then we obtain the usual equality and inequality, for $a, b \in \boldsymbol{F}_q(x)$:

$$|a+b| \leq |a| + |b|,$$
$$|a \cdot b| = |a| \cdot |b|.$$

We define open balls and circles as usual:

$$B_r(z) = \{\theta \in \boldsymbol{F}_q(x) \big| |z-\theta| < r\} \quad \text{and } k_r(z) = \{\theta \in \boldsymbol{F}_q(x) \big| |z-\theta| = r\}.$$

By definition c leaves the valuation $|.|$ invariant, that means $|p.c| = |p|$, for all $p \in \boldsymbol{F}_q(x)$.

For all $n \in \boldsymbol{N}$, $n \geq 2$, we have: $|x^n - x^n.c^k| = e^n$, where k ranges over the set $\{1, \ldots, \mathrm{ord}(c) - 1\}$. Therefore for two points z, z_0 where $z \in B_1(x^n)$, $z_0 \in B_1(x^n).c^k$, we get the following inequality:

$$\begin{aligned} |z - z_0| &= |z - x^n - z_0 + x^n.c^k + x^n - x^n.c^k| \\ &\geq |x^n - x^n.c^k| - (|z - x^n| + |z_0 - x^n.c^k|) \\ &\geq e^n - 2. \end{aligned}$$

So the two points z and z_0 always have positive distance, and this implies that c is an element all of whose non-trivial powers c^k are sending $B_1(x^n)$ into the complement $\overline{B_1(x^n)}^c$. To apply the ping-pong lemma of Lyndon and Ullman [10], we have to look for an element t all of whose non-trivial powers t^k send $\overline{B_1(x^n)}^c$ into $B_1(x^n)$. Therefore we look for an element $s \in \mathrm{PSL}(2, \boldsymbol{F}_q(x))$ for which $\overline{B_1(0)}^c.s^k \subseteq B_1(0)$ holds for every $k \neq 0$. Take s to be represented by the matrix

$$\begin{pmatrix} x & 0 \\ x^n & x^{-1} \end{pmatrix}.$$

Then the powers s^k, $|k| \geq 2$ have the form

$$s^k = \begin{pmatrix} x^k & 0 \\ p_k(x) & x^{-k} \end{pmatrix},$$

where

$$p_k(x) = \operatorname{sgn}(k)(x^{n-(|k|-1)} + x^{n-(|k|-3)} + \ldots + x^{n+(|k|-3)} + x^{n+(|k|-1)}).$$

Therefore we have

$$f.s^k = \frac{f \cdot x^k}{p_k(x) f + x^{-k}} = \frac{x^k}{p_k(x) + \frac{1}{x^k f}}$$

and this implies for $|f| \geq 1$

$$\begin{aligned} |f.s^k| &= |x^k|\, |p_k(x) + \frac{1}{x^k f}|^{-1} \\ &\leq e^{|k|}(e^{n+(|k|-1)})^{-1} = e^{-n+1}. \end{aligned}$$

So for $n \geq 2$, s is an element that has the property that $\overline{B_1(0)}^c.s^k \subseteq B_1(0)$ for $k \neq 0$ and s has infinite order. Let us define

$$t = \begin{pmatrix} 1 & -x^n \\ 0 & 1 \end{pmatrix} s \begin{pmatrix} 1 & x^n \\ 0 & 1 \end{pmatrix}.$$

Then t has infinite order and $\overline{B_1(x^n)}^c.t^k \subseteq B_1(x^n)$ for $k \neq 0$. Now we can apply the ping-pong lemma ([10], lemma A) to the group $< c, t >$ and this completes the proof. ∎

The next point we have to consider are reduced words in two generators and their vanishing set in algebraic groups. Let $w = x^{\alpha_1} y^{\beta_1} \cdots x^{\alpha_r} y^{\beta_r} \in F_2$. Then for $c \in G$ we define $w_c(x) = x^{\alpha_1} c^{\beta_1} \cdots x^{\alpha_r} c^{\beta_r}$. The next theorem considers algebraic groups on which the functions w_c do not vanish, if the element c is semisimple and one further condition is satisfied.

THEOREM 5: *Let c be a non-central semisimple element of the algebraic group G defined over $\overline{\boldsymbol{F}_q}$. Assume further that there exists a reductive subgroup H such that $c \in H$ and $[H,H] \cong$ (P)SL$(2, \overline{\boldsymbol{F}_q})$. Let T be a maximal torus containing c. For the root $\alpha \in \Phi(H) \subset X(T)$ assume that $\alpha(< c >) \cong < c > Z(G)/Z(G)$. Then for any non-trivial reduced word w_c in two generators with constants in*

$< c > \backslash Z(G)$, *i.e.* $x^{\alpha_1}c^{\beta_1}\cdots x^{\alpha_r}c^{\beta_r}$, *with* $\beta_i \in \{1,\ldots,\mathrm{ord}(cZ(G))\}$, *the vanishing set* $\mathrm{Van}_{w_c}(G)$ *is not equal to the whole group* G.

Proof: Assume that $G = \mathrm{Van}_{w_c}(G)$. Then we also have $H = \mathrm{Van}_{w_c}(H)$. Let us define

$$\rho : H \longmapsto H/Z(H) \cong [H,H]/[H,H] \cap Z(H) \cong \mathrm{PGL}(2,\overline{\boldsymbol{F}_q}).$$

Then we also have $\rho(H) = \mathrm{Van}_{w_{\rho(c)}}(\rho(H))$. Furthermore $w_{\rho(c)}(x)$ is a non-trivial word of positive length ℓ. This follows easily because we assumed that

$$\alpha(< c >) \cong < c > Z(G)/Z(G).$$

Let $Z_1 \cong \mathrm{PGL}(2,\boldsymbol{F}_{q^m})$ be a subgroup of $\rho(H)$ containing $\rho(c)$ such that $\rho(c)$ is even contained in a maximally split torus of Z_1. Then we find a series of subgroups $Z_k \cong \mathrm{PGL}(2,\boldsymbol{F}_{q^{mk}})$, $Z_k \leq Z_{k+1}$ and $\rho(c)$ lies in a maximally split torus of Z_k for all k's. By Theorem 4 we can find a subgroup K of $\mathrm{PGL}(2,\boldsymbol{F}_{q^m}(x))$ isomorphic to $< \rho(c) > \coprod \mathbb{Z}$ containing $\rho(c)$. So for each k we have the following:

$$\begin{array}{ccccc} Z_1 \cong \mathrm{PGL}(2,F_{q^m}) & \longleftarrow & < \rho(c) > & & \\ \downarrow & & \downarrow & & \\ \mathrm{PGL}(2,\boldsymbol{F}_{q^m}(x)) & \longleftarrow & K \cong < \rho(c) > \coprod \mathbb{Z} & \xrightarrow{\phi_k} & Z_k \cong \mathrm{PGL}(2,\boldsymbol{F}_{q^{mk}}) \\ & & & \longrightarrow & \mathrm{PGL}(2,\overline{\boldsymbol{F}_q}) \end{array}$$

where each arrow means inclusion except the map $\phi_k : K \mapsto Z_k$, which is a morphism of the finitely generated subgroup K of $\mathrm{PGL}(2,\boldsymbol{F}_{q^m}(x))$ in $\mathrm{PGL}(2,\boldsymbol{F}_{q^{mk}})$ by sending x to a primitive element in $\boldsymbol{F}_{q^{mk}}$. Let t be a generator of $\mathbb{Z} < K$. Then for each k we get: $\phi_k(t) \in \mathrm{Van}_{w_{\rho(c)}}(Z_k)$. As K is residually $\{\phi_k(K) \mid k \geq k_0\}$, $w_{\rho(c)}(t) \in K$ has to be the trivial element in K. So $w_a(b) \in < a,b > \cong F_2$ has to be contained in $< (a^\kappa)^z \mid z \in F_2 >$ where $\kappa = \mathrm{ord}(\rho(c))$. But this is impossible by the choice of w and the proof is complete. ∎

For our purpose we have to apply Theorem 5 to the generating element of the cyclic torus T_F. The following proposition shows that this is possible.

PROPOSITION 6: *Let* G *be a simple algebraic group and* F: $G \mapsto G$ *a Frobenius map such that* G_F *is one of the groups listed in Table 1. Let* T *be an* F*-stable maximal torus for* G *such that* T_F *is of the types listed in Table 1. Let* $w \in W$ *be an element such that* T *is obtained from the maximally split torus* T_0 *by twisting with the element* w. *Then there exists a root* $\alpha \in \Phi(T_0)$ *such that the following holds:*

(a) *If G_F is of type G_2 for any root $\alpha \in \Phi(G_2)$ we obtain*

$$\left\langle w_\alpha^x \mid x \in < F.w > \right\rangle \cong S_3;$$

if G_F is of type F_4 and $\alpha \in \Phi$ is a long root then

$$\left\langle w_\alpha^x \mid x \in < F.w > \right\rangle = W(D_4).3 < W(F_4).$$

If G_F is of type ${}^3D_4$, ${}^2F_4$, ${}^2E_6$, E_6, E_7 or E_8, then there exists a root $\alpha \in \Phi$ such that $W = \left\langle w_\alpha^x \mid x \in < F.w > \right\rangle$.

(b) *Let $g \in G$ be such that $\pi\big(F(g)g^{-1}\big) = w$ and $T = T_0^g$, where $\pi : N_G(T_0) \mapsto W$ is the canonical epimorphism on the Weyl group. Then $\ker_{T_0}(\alpha) \cap (T_F)^{g^{-1}} \leq Z(G)$.*

Proof: (a) If G_F is not of type ${}^2F_4$ this is an immediate consequence of the propositions 6, 7, 8, 10 and 11 of [20]. So only the case that G_F is of type ${}^2F_4$ has to be considered. Let $\alpha \in \Phi$ be any root and assume that

$$W_0 = \left\langle w_\alpha^x \mid x \in < F.w > \right\rangle$$

is a proper subgroup of $W(F_4)$. As W_0 is generated by reflections W_0 has to be a Weyl subgroup of W with corresponding root system $\Psi = \{\gamma \in \Phi \mid w_\gamma \in W_0\}$. Then Ψ is invariant under $F.w$. By theorem 5 of [20] there is a proper F-stable reductive subgroup H of G containing T. So we conclude that $T_F < H_F < G_F$. But this is a contradiction to the main result of [11] and our assertion holds.

(b) Here we use the fact that $(T_F)^{g^{-1}} = \mathrm{Fix}_{T_0}(F.w)$ (cf. Prop. 3.3.6 of [3]) and $\ker_{T_0}(\alpha) \leq \mathrm{Fix}_{T_0}(w_\alpha)$. Therefore if G_F is not of type G_2 or F_4 we have:

$$\ker_{T_0}(\alpha) \cap (T_F)^{g^{-1}} \leq \mathrm{Fix}_{T_0}(w_\alpha) \cap \mathrm{Fix}_{T_0}(F.w) = \mathrm{Fix}_{T_0}(W. < F >).$$

So we have to look at $S = \mathrm{Fix}_{T_0}(W. < F >) \leq (T_F)^{g^{-1}}$. Let $t \in S$. Then for all $\gamma \in \Phi(T_0)$ the following holds:

$$\gamma(t) = \gamma(t^{w_\gamma}) = \gamma^{w_\gamma}(t) = \gamma(t)^{-1}.$$

So $S/Z(G_F)$ has to be 2-group. But in all the cases except the case that G_F is of type E_7, T_F is of odd order and this already implies the assertion. If G_F is of type E_7 we can use the fact that $|S|$ has to divide the order of any maximal torus of G_F and so we obtain

$$|S| \mid \gcd\big((q+1)(q^6 - q^3 + 1), (q-1)(q^6 + q^3 + 1)\big) = \gcd(q-1, 2)$$

and this leads to our assertion in this case. If G_F is of type F_4 then similar arguments lead to the case that $\mathrm{Fix}_{T_0}\big(W(D_4).3. < F > \big)$ equals the center of ${}^3D_4(q)$ which is trivial and so the proposition holds in this case as well. If G_F is of type G_2 the argumentation is a little bit different: Let S be 3-Sylow subgroup of $(T_F)^{g^{-1}}$. Then $|S| = 3$ or $|S| = 1$. If S is non-trivial, S is also non-central and so there exists a root α such that $S \not\leq \ker_{T_0}(\alpha)$. Let $W_0 = \langle w_\alpha^x \mid x \in< F.w > \rangle$ and $\Psi = \{\gamma \in \Phi \mid w_\gamma \in W_0\}$. Then Ψ is a root system of type A_2 and so $\ker_{T_0}(W_0)$ is isomorphic to $\mathbb{Z}_3$ or trivial. But in both cases we obtain $\ker_{T_0}(W_0) \cap (T_F)^{g^{-1}} = 1$. ∎

The statement we need in one of the following sections is the following:

COROLLARY: *Let G be a simple algebraic group and F a Frobenius map on G such that G_F is one of the groups of Table 1. Let c be a non-central element that generates a maximal torus T_F of the type listed in Table 1. Then for any word $v = x^{\alpha_1} y^{\beta_1} \cdots x^{\alpha_r} y^{\beta_r}$ in two generators with $\beta_i \in \{1, \dots, \mathrm{ord}(cZ(G))\}$ the vanishing set $\mathrm{Van}_{w_c}(G)$ is a proper subset of G.*

Proof: For each group G let $\alpha \in \Phi$ be a root that satisfies the assertion of Proposition 6(b) and define $H =< U_\alpha, U_{-\alpha}, T_0 >^g$. Then $\ker_{T_0}(\alpha) \cap (T_F)^{g^{-1}} \leq Z(G)$ and this implies that $\alpha(T_F) \cong T_F Z(G)/Z(G)$. Then Theorem 5 implies the assertion. ∎

3. The Number of Rational Points on an Affine Variety

Let $\boldsymbol{K}$ be a locally finite algebraically closed field of positive characteristic and F a Frobenius automorphism of $\boldsymbol{K}$ with q fixed points on $\boldsymbol{K}$. We denote the induced map $\boldsymbol{K}^n \mapsto \boldsymbol{K}^n$ also by F. In the following we want to consider an irreducible affine variety $X \subseteq \boldsymbol{K}^n$. We want to obtain an upper bound for $|X_F|$, the number of F-rational points on X. Therefore we define the degree for affine varieties in the following way: Let us consider the embedding $\sigma : \boldsymbol{K}^n \mapsto \boldsymbol{P}^n$ of $\boldsymbol{K}^n$ in the n-dimensional projective space $\boldsymbol{P}^n$ such that $\sigma(\boldsymbol{K}^n)$ is a dense open subset of $\boldsymbol{P}^n$ (see [13], p.22). Let us define $\overline{\sigma}(X) = \overline{\sigma(X)}$, where $\overline{\sigma(X)}$ is the Zariski closure of the image of X in $\boldsymbol{P}^n$. Then for any irreducible affine variety $X \subseteq \boldsymbol{K}^n$ we define: $\deg(X) = \deg\big(\overline{\sigma}(X)\big)$. This is a well-defined function on the set of irreducible affine varieties ([13], chapter 5). Furthermore let H be an irreducible hypersurface in $\boldsymbol{K}^n$. Then $\overline{\sigma}(H)$ is an irreducible hypersurface in $\boldsymbol{P}^n$. If $X \not\subseteq H$ then the intersection $\overline{\sigma}(X) \cap \overline{\sigma}(H) = Z_1 \cup \cdots \cup Z_r$ is a variety all of whose irreducible components Z_i have the same dimension. In this case we obtain the following:

$$\deg\left(\overline{\sigma}(X)\right)\cdot\deg\left(\overline{\sigma}(H)\right)=\sum_{1\leq k\leq r} i\left(\overline{\sigma}(X),\overline{\sigma}(H);Z_k\right)\cdot\deg(Z_k)$$

where $i\left(\overline{\sigma}(X),\overline{\sigma}(H);Z_k\right)\in \boldsymbol{N}$ are the intersection multiplicities (see [5], p. 53, theorem 7.7). In the affine case this implies the following: Let $H\subset \boldsymbol{K}^n$ be an affine hyperplane of $\boldsymbol{K}^n$. Let $X\cap H = Y_1\cup\cdots\cup Y_r$, where the Y_i's are the non-trivial irreducible components of $X\cap H$. Then

$$\begin{aligned} r &\leq \deg(X)\cdot\deg(H) \quad \text{and} \\ \deg(Y_i) &\leq \deg(X)\cdot\deg(H) \quad \text{for all} \quad i=1,\ldots,r. \end{aligned} \tag{3.1}$$

This leads to the following

THEOREM 7: *Let X be an irreducible affine variety over $\boldsymbol{K}$ of dimension k and degree d. Then $|X_F|\leq d^k\cdot q^k$.*

Proof: We will prove the assertion by induction. If the dimension of X equals zero X is a point and there is nothing to prove. So let us assume that the inequality holds for every irreducible affine variety of dimension less than k. We may also assume that $X\subseteq \boldsymbol{K}^n$, but that X is not contained in any F-stable hyperplane of $\boldsymbol{K}^n$. Then there exist q disjoint F-stable hyperplanes $H_1,\ldots,H_q$ such that

$$(\boldsymbol{K}^n)_F\subseteq H_1\cup\cdots\cup H_q.$$

So we conclude

$$\begin{aligned} X_F\subseteq X\cap(\boldsymbol{K}^n)_F &\subseteq (X\cap H_1)\cup\ldots\cup(X\cap H_q)\\ &\subseteq \bigcup_{1\leq\alpha\leq q}\ \bigcup_{1\leq\beta\leq\ell_\alpha} Z_{\alpha\beta}. \end{aligned}$$

Here $X\cap H_\alpha = Z_{\alpha 1}\cup\cdots\cup Z_{\alpha\ell_\alpha}$ and all $Z_{\alpha\beta}$ are non-trivial irreducible affine varieties of dimension $k-1$. By (3.1) we conclude that $\ell_\alpha\leq\deg(X)$ and $\deg(Z_{\alpha\beta})\leq\deg(X)$. So we obtain

$$\begin{aligned} |X_F| &\leq \Big|\bigcup_{1\leq\alpha\leq q}\ \bigcup_{1\leq\beta\leq\ell_\alpha}(Z_{\alpha\beta})_F\Big|\leq q\cdot d\cdot\max\left\{|(Z_{\alpha\beta})_F|\,\big|\,1\leq\alpha\leq q, 1\leq\beta\leq\ell_\alpha\right\}\\ &\leq d^k\cdot q^k \end{aligned}$$

and the theorem is proved. ∎

Now let $\mathrm{char}(\boldsymbol{K}) = 2$ and consider an affine space of even dimension. We also have to consider another type of surjective endomorphisms $F : \boldsymbol{K}^{2n} \mapsto \boldsymbol{K}^{2n}$. As we will see later $F_4(\boldsymbol{K})$ is an affine subvariety of $\boldsymbol{K}^{2\cdot 26^2}$ which is stable under such an endomorphism F.

We say that $F : \boldsymbol{K}^{2n} \mapsto \boldsymbol{K}^{2n}$ is a twisted Frobenius morphism on $\boldsymbol{K}^{2n}$ if the following holds:

- Let $\boldsymbol{K}^{2n} = U \oplus U$ be a decomposition of $\boldsymbol{K}^{2n}$ in two affine subspaces of dimension n. Let $\sigma\colon U \mapsto U$, be the standard Frobenius morphism induced by $x \mapsto x^{2^f}$ and $\tau\colon U \mapsto U$ be the standard Frobenius morphism induced by $x \mapsto x^{2^{f+1}}$. Then for $(u,v) \in \boldsymbol{K}^{2n}$ we have $(u,v)^F = (v^\sigma, u^\tau)$.

We will write σ, τ for $\sigma, \tau\colon \boldsymbol{K} \mapsto \boldsymbol{K}$ and also $\sigma, \tau\colon \boldsymbol{K}^{2n} \mapsto \boldsymbol{K}^{2n}$. Let us define $q = 2^{2f+1}$ and $q_0 = \sqrt{q}$. The aim of the following is to obtain a similar upper bound as in Theorem 7. First we want to study some properties of twisted Frobenius morphisms.

PROPOSITION 8: *Let F be a twisted Frobenius morphism on the affine variety $\boldsymbol{K}^{2n}$, i.e. $(u,v)^F = (v^\sigma, u^\tau)$. Let us denote by U_q the set of fixed points of F^2 on U. Then*

(a) *F is a homomorphism of additive groups.*

(b) *$(\boldsymbol{K}^{2n})_F = \{(u,v) \mid (u,v) = (\xi, \xi^\tau),\ \xi \in U_q\}$.*

Proof: Both facts are straightforward. ∎

Now we prove the analogue of Theorem 7 for irreducible subvarieties of $\boldsymbol{K}^{2n}$.

THEOREM 9: *Let $X \subseteq \boldsymbol{K}^{2n}$ be an irreducible affine variety of dimension k and degree d. Then $|X_F| \leq d \cdot (\sqrt{2} \cdot q_0)^k$, where $q_0 = \sqrt{q}$.*

Proof: We will prove the assertion by induction. If X is an irreducible variety of dimension 0 there is nothing to prove. So let us assume that the assertion holds for irreducible varieties of dimension less than k. Now we choose a basis for $\boldsymbol{K}^{2n}$ such that for the coordinates the following holds:

$$(u_1, \ldots, u_n, v_1, \ldots, v_n)^F = (v_1^\sigma, \ldots, v_n^\sigma, u_1^\tau, \ldots, u_n^\tau).$$

Define

$$H_i = \{(u_1, \ldots, u_n, v_1, \ldots, v_n) \mid u_i^\tau + v_i = 0\}$$

and

$$H_i' = \{(u_1, \ldots, u_n, v_1, \ldots, v_n) \mid u_i + v_i^\sigma = 0\}.$$

Then $(\boldsymbol{K}^{2n})_F \subseteq H_i$ and $(\boldsymbol{K}^{2n})_F \subseteq H_i^!$, for all $i = 1, \ldots, n$. Obviously

$$\deg(H_i) = \sqrt{2} \cdot q_0 \quad \text{and} \quad \deg(H_i^!) = \sqrt{1/2} \cdot q_0.$$

First let us assume that there is an i such that $X \not\subseteq H_i$. Then

$$X \cap H_i = \bigcup_{j=1}^{r} Z_j,$$

where each irreducible component Z_j is of dimension $k-1$. So as before the following holds:

$$\deg(H_i) \cdot \deg(X) \geq \sum_{j=1}^{r} i(H_i, X; Z_j) \cdot \deg(Z_j). \tag{3.2}$$

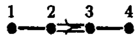
As $X_F \subseteq (X \cap H_i)_F \subseteq \bigcup_{j=1}^{r} (Z_j)_F$ we obtain the following:

$$\begin{aligned} |X_F| = |(X \cap H_i)_F| \; &\leq \; \sum_{j=1}^{r} |(Z_j)_F| \quad \text{and so by induction} \\ &\leq \left(\sqrt{2} \cdot q_0\right)^{k-1} \sum_{j=1}^{r} \deg(Z_j) \quad \text{then (3.2) implies} \\ &\leq \deg(X) \cdot \left(\sqrt{2} \cdot q_0\right)^{k} \end{aligned}$$

and the assertion is proved in this case. If there exists an i such that $X \not\subseteq H_i^!$ then the same arguments as before lead to our assertion. So the case we still have to consider is $X \subseteq \bigcap_{i=1}^{n} (H_i \cap H_i^!)$. But a straightforward calculation shows that $\bigcap_{i=1}^{n} (H_i \cap H_i^!) = (\boldsymbol{K}^{2n})_F$. The irreducible components of this affine variety are points and so this case only occurs for $k = 0$. This completes the proof. ∎

It is remarkable that for twisted Frobenius morphisms the bound depends linearly on the degree of X, while for standard Frobenius morphisms the bound depends on $\deg(X)^{\dim(X)}$.

The last statement we have to show in this section is that the Frobenius map F on the affine algebraic group G of type F_4 such that $G_F = {}^2F_4(q_0^2)$ is induced by such a twisted Frobenius morphism. Therefore we consider the Lie algebra $\mathcal{L}$ of type F_4 defined over $\overline{\boldsymbol{F}_2}$, the locally finite algebraic closed field of characteristic 2. The corresponding Dynkin diagram is the following:



Let Φ be the corresponding root system and $\Pi = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ be a basis of Φ. We will denote the non-trivial graph automorphism by γ. Furthermore we define Φ_s to be the set of all short roots and Φ_l to be the set of all long roots. Similarly we define $\Pi_s = \{\alpha_3, \alpha_4\}$ and $\Pi_l = \{\alpha_1, \alpha_2\}$.

Let $\{e_\alpha, h_\beta \mid \alpha \in \Phi, \beta \in \Pi\}$ be a Chevalley basis of $\mathcal{L}$. Then

$$I = [e_\alpha, h_\beta \mid \alpha \in \Phi_s, \beta \in \Pi_l]$$

is an ideal of the Lie algebra $\mathcal{L}$. Let us denote by $\tilde{} : \mathcal{L} \mapsto \mathcal{L}/I$ the canonical Lie algebra epimorphism.

There is also a map $\bar{} : \Phi \mapsto \Phi$ defined by the following: for $r \in \Phi$ with $r = \Sigma_{i=1}^4 n_i \cdot \alpha_i$ we define

$$\bar{r} = \sum_{i=1}^{4} n_i \cdot \frac{(\alpha_i, \alpha_i)}{(r, r)} \cdot \alpha_i^\gamma.$$

Then $\overline{\Phi_s} = \Phi_l$ and $\overline{\Phi_l} = \Phi_s$ ([1], p. 64). The same holds for Π_s and Π_l. By [16], 10.1 there is an isomorphism of Lie algebras $\theta : \mathcal{L}/I \mapsto I$ defined through

$$\tilde{e}_r^\theta = e_{\bar{r}},$$
$$\tilde{h}_r^\theta = h_{\bar{r}}.$$

G is acting on $\mathcal{L}$ and $\mathcal{L}/I$ and the action is well known ([1], p. 64). Let us consider the Frobenius map F such that $G_F = {}^2F_4(q_0^2)$. Then for rootelements we have the following ([1], prop. 12.3.3):

$$x_r(t)^F = \begin{cases} x_{\bar{r}}(t^\sigma) & \text{if } r \text{ is a long root,} \\ x_{\bar{r}}(t^\tau) & \text{if } r \text{ is a short root.} \end{cases}$$

Let $\mathcal{B}_1 = \{e_r, h_{\alpha_4}, h_{\alpha_3} \mid r \in \Phi_s\}$ be a basis of I and $\mathcal{B}_2 = \{\tilde{e}_r, \tilde{h}_{\alpha_1}, \tilde{h}_{\alpha_2} \mid r \in \Phi_l\}$ be a basis of $\mathcal{L}/I$, where the ordering is chosen to be compatible with the map $\bar{} : \Phi_s \mapsto \Phi_l$. We define an additive function F^*: $I \oplus \mathcal{L}/I \mapsto I \oplus \mathcal{L}/I$ by the following: if we write an element $w \in I \oplus \mathcal{L}/I$ in coordinates of the basis $\mathcal{B}_1 \cup \mathcal{B}_2$, i.e. $w = (\lambda_1, \ldots, \lambda_{26}, \mu_1, \ldots, \mu_{26})$, then

$$w^{F^*} = (\lambda_1, \ldots, \lambda_{26}, \mu_1, \ldots, \mu_{26})^{F^*} = (\mu_1^\sigma, \ldots, \mu_{26}^\sigma, \lambda_1^\tau, \ldots, \lambda_{26}^\tau).$$

With the equations of [1], p. 64 we easily verify that for all $\ell \in I \oplus {}^{\mathcal{L}}/_{I}$ and for all $g \in G$,

$$(\ell.g)^{F^*} = \ell^{F^*}.g^F. \tag{3.3}$$

G is acting as a group of linear transformations on $I \oplus {}^{\mathcal{L}}/_{I}$, so there is an embedding $G \hookrightarrow GL(I \oplus {}^{\mathcal{L}}/_{I})$. With respect to the basis $\mathcal{B}_1 \cup \mathcal{B}_2$ an element $g \in G$ is represented by a matrix of the form

$$g = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Then (3.3) implies that

$$g^F = \begin{pmatrix} B^\sigma & 0 \\ 0 & A^\tau \end{pmatrix}$$

and so we see that G is embedded in $K^{2\cdot 26^2}$ such that the Frobenius map $F\colon G \mapsto G$ with fixed point set ${}^2F_4(q_0^2)$ is induced by a twisted Frobenius morphism.

4. Proof of Theorem 2

Now we come to a theorem which is the keypoint of the proof of the main theorem.

THEOREM 10: *Let G be a simple simply connected algebraic group and F a Frobenius map on G such that G_F is one of the groups listed in Table 1. Let X denote the type of G_F, such that $G_F \cong X(q)$. Furthermore let c be a semisimple element such that $T_F =< c >$ where T_F is a maximal torus for G_F of the type listed in Table 1. Then there exists a constant $q(X)$ which depends only on the type of G_F such that, for $q \geq q(X)$, for any reduced word $w(x,y) = x^{\alpha_1}y^{\beta_1}\cdots x^{\alpha_r}y^{\beta_r}$ of length $\ell \leq \log(q)$, $\mathrm{Gen}_{G_F}(c) \not\subseteq \mathrm{Van}_{w_c}(G_F)$, where $\mathrm{Gen}_{G_F}(c) = \{g \in G_F \mid < c, g >= G_F\}$.*

Before we prove this theorem we want to mention that Theorem 10 implies Theorem 2 at once. This can be seen as follows: Then for all but finitely many exceptional groups of Lie-type $X(q)$ not of type ${}^2B_2$ or ${}^2G_2$, we obtain that $C(X(q)) \geq \log(q)$, where $C : \mathcal{G}_2 \mapsto \mathbb{N} \cup \{\infty\}$ is the function introduced in [18], and so the application of Theorem 3 will lead to our assertion.

Proof: Let $w = x^{\alpha_1}y^{\beta_1}\cdots x^{\alpha_r}y^{\beta_r}$ be a reduced word of length less than $\log(q)$ and let us assume that for a fixed type X and infinitely many values for q we have that

$$\mathrm{Gen}_{G_F}(c) \subseteq \mathrm{Van}_{w_c}(G_F) \quad \text{where } G_F = X(q). \tag{4.1}$$

Theorem A of [20] implies that, for $q \geq q(X)$,

$$|\mathrm{Gen}_{G_F}(c)| \geq |G_F| - |G_F|^{\varepsilon} \tag{4.2}$$

where $0 < \varepsilon < 1$ is a fixed real number depending only on the type X of G_F.

Now we want to bound the number of points in $\mathrm{Van}_{w_c}(G_F)$ using Theorems 7 and 9. Let us consider a rational representation ρ: $G \mapsto \mathrm{SL}(s, \boldsymbol{K})$ such that the Frobenius map is induced by a standard Frobenius morphism or twisted Frobenius morphism $F^* : \boldsymbol{K}^{s^2} \mapsto \boldsymbol{K}^{s^2}$. The degrees s of these representations are listed in Table 2.

Table 2

G_F	G	Representation ρ	Degree of ρ
G_2	G_2	standard	7
${}^3D_4$	D_4	$D_4 \mapsto F_4 \mapsto A_{25}$	26
F_4	F_4	standard	26
E_6	E_6	standard	27
${}^2E_6$	E_6	$E_6 \mapsto E_7 \mapsto A_{55}$	56
E_7	E_7	standard	56
E_8	E_8	standard	248
${}^2F_4$	F_4	$F_4 \mapsto A_{25} \times A_{25} \mapsto A_{51}$	52

For these embeddings we have the following:

$$\begin{array}{ccccccc} & & \mathrm{Van}_{w_c}(G) & \longrightarrow & G & & \\ & & \big\downarrow \rho & & \big\downarrow \rho & & \\ H_{ij} & \longleftarrow & \mathrm{Van}_{w_{\rho(c)}}\big(\mathrm{SL}(s,\boldsymbol{K})\big) & \longrightarrow & \mathrm{SL}(s,\boldsymbol{K}) & \longrightarrow & \boldsymbol{K}^{s^2} \end{array}$$

Each arrow of this diagram denotes an injective morphism of varieties. We define H_{ij} to be the affine variety vanishing on the (i,j)th entry of the function $X \mapsto w_{\rho(c)}(X) - 1$ defined on $\mathrm{SL}(s, \boldsymbol{K})$. By the Corollary of Theorem 5 we know that $\rho(G)$ cannot vanish on $w_{\rho(c)}$ and so there exists (α, β) such that $\rho(G) \not\subseteq H_{\alpha\beta}$. Let us set $H = H_{\alpha\beta}$. Each entry of the matrix $w_{\rho(c)}(X) - 1$ is a polynomial of total degree at most $s \cdot \ell$ in X_{ij} and so the degree of H is also bounded by $s \cdot \ell$. Let us consider $H \cap \rho(G) = \bigcup_{j=1}^{R} Z_j$, where each variety Z_j is a non-trivial irreducible affine variety. We will write $d_G = \deg\big(\rho(G)\big)$. The degree is independent of the characteristic and depends only on the corresponding Dynkin diagram of G.

Then (3.1) implies that the number of irreducible components R is bounded by $d_G \cdot s \cdot \ell$. The dimension of all irreducible components is equal to $k-1$, where $k = \dim\big(\rho(G)\big)$. So if G_F is not of type ${}^2F_4$, Theorem 7 implies that

$$\begin{aligned} |\mathrm{Van}_{w_c}(G_F)| &= |\mathrm{Van}_{w_{\rho(c)}}\big(\rho(G)\big)_F| \\ &\le |\big(H \cap \rho(G)\big)_F| \\ &\le \sum_{j=1}^{R} |(Z_j)_F| \\ &\le \ell^k \cdot (d_G \cdot s)^k \cdot q^{k-1}. \end{aligned}$$

So we see that $|\mathrm{Van}_{w_c}(G_F)| = \mathcal{O}\big(\log(q)^k q^{k-1}\big)$ and, by (4.2), $|\mathrm{Gen}_{G_F}(c)| = q^k - o(q^k)$. So we conclude that (4.1) cannot hold for infinitely many q's and this leads to a contradiction in this case. If G_F is of type ${}^2F_4$ then we obtain the inequality

$$|\mathrm{Van}_{w_c}(G_F)| \le (\sqrt{2})^{k-1} \cdot \ell^2 \cdot (d_G \cdot s)^2 \cdot q_0^{k-1}$$

where $q_0 = \sqrt{q}$. In this case we obtain $|\mathrm{Van}_{w_c}(G_F)| = \mathcal{O}\big(\log(q_0)^2 q_0^{k-1}\big)$ and $|\mathrm{Gen}_{G_F}(c)| = q_0^k - o(q_0^k)$. This leads to a contradiction as well and the proof is complete. ∎

References

1. R. W. Carter, *Simple Groups of Lie-type*, Wiley, New York, 1972.
2. R. W. Carter, *Conjugacy classes in the Weyl group*, Comp. Math. **25** (1972), 1–59.
3. R. W. Carter, *Finite Groups of Lie-Type: Conjugacy Classes and Complex Characters*, Wiley, New York, 1985.
4. Yu. M. Gorchakov and V. M. Levchuk, *On approximation of free groups*, Alg. i Log. **9**, No. 4 (1970), 415–421.
5. R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.
6. R. Katz and W. Magnus, *Residual properties of free groups*, Comm. Pure Appl. Math. **22** (1969), 1–13.
7. V. M. Levchuk, *A property of Suzuki groups*, Alg. i Log. **9**, No. 4 (1970), 551–557.
8. V. M. Levchuk and Y. N. Nuzhin, *Structure of Ree groups*, Alg. i. Log. **24** No. 1 (1985), 26–41.
9. A. Lubotzky, *On a Problem of Magnus*, Proc. Am. Math. Soc. **98**, No. 4 (1986), 583–585.

10. R. C. Lyndon and J. L. Ullman, *Pairs of real 2 by 2 matrices that generate free products*, Mich. Math. J. **15** (1968), 161–166.
11. G. Malle, *The maximal subgroups of* ${}^2F_4(q^2)$, J. Algebra, to appear.
12. C. R. Matthews, L. N. Vaserstein and B.Weisfeiler, *Congruence properties of Zariski-dense subgroups*, Proc. London Math. Soc. **48** (1984), 514–532.
13. D. Mumford, *Algebraic Geometry, 1. Complex Projective Varieties*, Springer, Berlin, 1976.
14. A. Peluso, *A residual property of free groups*, Comm. Pure Appl. Math. **19** (1967), 435–437.
15. S. Pride, *Residual properties of free groups*, Pacific J. Math. **43** (1972), 725–733.
16. R. Steinberg, *Representations of algebraic groups*, Nagoya Math.J. **22** (1963), 33–56.
17. Th. Weigel, *Residual Properties of Free Groups*, Ph.D. Thesis, Freiburg, 1989.
18. Th. Weigel, *Residual properties of free groups*, J. Algebra, to appear.
19. Th. Weigel, *Residual properties of free groups, II*, Commun. Algebra, to appear.
20. Th. Weigel, *Generation of exceptional groups*, Geom. Dedicata **41** (1992), 63–87.
21. B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. Math. (2) **120** (1984), 271–315.
22. J. S. Wilson, *A residual property of free groups*, J. Algebra **138** (1991), 36–47.