Arch. Math. 108 (2017), 441–451

0003-889X/17/050441-11
published online February 23, 2017
DOI 10.1007/s00013-016-1008-x

Archiv der Mathematik

Strange divisibility in groups and rings

Anton A. Klyachko and Anna A. Mkrtchyan

Abstract. We prove a general divisibility theorem that implies, e.g., that, in any group, the number of generating pairs (as well as triples, etc.) is a multiple of the order of the commutator subgroup. Another corollary says that, in any associative ring, the number of Pythagorean triples (as well as four-tuples, etc.) of invertible elements is a multiple of the order of the multiplicative group.

Mathematics Subject Classification. Primary 20D60; Secondary 20D60, 20F05, 20F70, 16P10, 16U60.

Keywords. Equations in groups, Equations in rings, Generators of groups.

1. Introduction. The starting point of our investigation is the following fact generalising an old theorem of Solomon [8].

Gordon–Rodriguez–Villegas Theorem [5]. *Let F be a finitely generated group whose commutator subgroup is of infinite index and let G be an arbitrary group. Then the number of homomorphisms $F \to G$ is divisible by the order of G.*

This theorem is essentially about the number of solutions to systems of coefficient-free equations in a group. In [6], this result was extended to equations with coefficients and even to arbitrary first-order formulae in group language (with constants).

The main theorem of this paper has a claim to the title of "the maximal" generalisation of the Gordon–Rodriguez–Villegas Theorem (although such a maximality can never be proven). The statement of the Main Theorem can be found in the Section 2; a (quite elementary) proof is in the last section. Roughly speaking, the Main Theorem asserts that the divisibility is retained when we take into account only some set of homomorphisms provided the set

The work of A. A. Klyachko was supported by the Russian Foundation for Basic Research, Project No. 15-01-05823.

is invariant with respect to some natural operations on homomorphisms. One of the corollaries of the Main Theorem is the unexpected fact mentioned in the abstract:

in any group G, the number of generating tuples
$$(g_1, \ldots, g_{2017}) \in G^{2017}$$
($i.e.$ such tuples that $G = \langle g_1, \ldots, g_{2017} \rangle$) is a multiple of the order of the commutator subgroup of G.

(Here, the number 2017 can be replaced by any integer; see Section 3 for a more general fact and other group-theoretic applications.) Surprisingly, this result seems to be new, although many related facts on the divisibility of the Möbius function (which is related to the number of generating tuples via the Hall formula [3]) are known, see, e.g., [1,4,7], and references therein. We refer to [2] for yet other not widely known but beautiful results about generating tuples.

The Main Theorem is an assertion about groups, but it has nontrivial ring-theoretic corollaries. In Section 4, we derive a ring-theoretic analogue of the Gordon–Rodriguez-Villegas theorem (to be more precise, an analogue of the generalisation of this theorem from [6], which is about equations with coefficients). A particular case of this theorem on equations over rings is the fact mentioned in the abstract, or, e.g., the following higher-order assertion:

in any associative ring R with unity, the number of tuples of invertible elements $(a, b, \ldots, z) \in (R^*)^{26}$ such that $a^{2017} + b^{2017} + \cdots + z^{2017} = 0$ is divisible by the order of the multiplicative group of this ring, i.e. by $|R^*|$.

(Here, the number 2017 can be replaced by any integer; see Section 4 for a more general fact.)

Our notation is mainly standard. Note only that if $k \in \mathbb{Z}$ and x and y are elements of a group, then x^y, x^{ky}, and x^{-y} denote $y^{-1}xy$, $y^{-1}x^k y1$, and $y^{-1}x^{-1}y$, respectively. The commutator subgroup of a group G is denoted by G'. If X is a subset of a group, then $|X|$, $\langle X \rangle$, $\langle\langle X \rangle\rangle$, and $C(X)$ are the cardinality of X, the subgroup generated by X, the normal closure of X, and the centraliser of X, respectively. The index of a subgroup H of a group G is denoted by $|G : H|$. The symbol $N(H)$ denotes the normaliser of a subgroup H (in a group G). The free product of groups A and B is denoted by $A * B$ and $F(x_1, \ldots, x_n)$ is the free group with basis $x_1, \ldots, x_n$. If R is an associative ring with unity, then R^* denotes the group of invertible elements of this ring.

Note also that, in almost all assertions about the divisibility (e.g., in the Gordon–Rodriguez-Villegas Theorem), one need not assume that the corresponding group is finite. The divisibility can be understood in the sense of cardinal arithmetics: an infinite cardinal is divisible by all nonzero smaller (and equal) cardinals. We really need finiteness assumptions only in the Theorem on Monomorphisms and Subgroups in Section 3 (see the corresponding remark there).

2. Main theorem. A group F equipped with an epimorphism $F \to \mathbb{Z}$ is called *indexed*. This epimorphism $F \to \mathbb{Z}$ is called *degree* and denoted by deg; thus, an integer $\deg f$ is assigned to each element f of an indexed group F in such a way that F contains elements of all integer degrees and

$$\deg(fg) = \deg f + \deg g \quad \text{for any } f, g \in F.$$

Suppose that $\varphi\colon F \to G$ is a homomorphism from an indexed group F to a group G and H is a subgroup of G. We say that the subgroup

$$H_\varphi = \bigcap_{f \in F} H^{\varphi(f)} \cap C(\{\varphi(f) \mid \deg f = 0\})$$

is the φ-*core* of H. In other words, the φ-core H_φ of H consists of such elements h that $h^{\varphi(f)} \in H$ for all f and, moreover, $h^{\varphi(f)} = h$ if $\deg f = 0$.

Main Theorem. *Let H be a subgroup of a group G and let Φ be a set of homomorphisms from an indexed group F to G with the following two properties.*

I. Φ *is invariant with respect to conjugation by elements of H:*

if $h \in H$ and $\varphi \in \Phi$, then the homomorphism $\psi\colon f \mapsto \varphi(f)^h$ lies in Φ.

II. *For any $\varphi \in \Phi$ and any h from the φ-core H_φ of H, the homomorphism ψ defined by*

$$\psi(f) = \begin{cases} \varphi(f) & \text{for all } f \in F \text{ of degree zero;} \\ \varphi(f)h & \text{for some element } f \in F \text{ of degree one} \\ & (\text{and, hence, for all degree-one elements}) \end{cases}$$

belongs to Φ too.

Then $|\Phi|$ is divisible by $|H|$.

Note that the mapping ψ from Condition I is a homomorphism for any $h \in G$; and the formula for ψ from Condition II defines a homomorphism for any $h \in C(\varphi(\ker \deg))$ (see Lemma 0). Conditions I and II only require these homomorphisms to belong to Φ (under some additional restrictions on h).

Lemma 0. *Suppose that $\varphi\colon F \to G$ is a homomorphism from an indexed group F to a group G, f_1 is a degree-one element of F, and $g \in G$. Then*

(1) *if (and only if) $g \in C(\varphi(\ker \deg))$, then there exists a (unique) homomorphism $\psi\colon F \to G$ such that $\psi(f) = \varphi(f)$ for all f of degree zero and $\psi(f_1) = \varphi(f_1)g$;*

(2) *if H is a subgroup of G and $g \in H_\varphi$, then $\psi(f)H = \varphi(f)H$ for all $f \in F$.*

Proof. Note that F is a semidirect product $F = \langle f_1 \rangle_\infty \rightthreetimes \ker \deg$. This means that a mapping $\alpha\colon \ker \deg \cup \{f_1\} \to G$ extends to a homomorphism if and only if its restriction to $\ker \deg$ is a homomorphism and $\alpha(f^{f_1}) = \alpha(f)^{\alpha(f_1)}$ for all $f \in \ker \deg$.

For all $f \in \ker \deg$, we have

$$\psi(f^{f_1}) = \varphi(f^{f_1}) = \varphi(f)^{\varphi(f_1)} \quad \text{and} \quad \psi(f)^{\psi(f_1)} = \varphi(f)^{\varphi(f_1)g}.$$

This implies that

$$\psi(f^{f_1}) = \psi(f)^{\psi(f_1)} \quad \text{for all} \quad f \in \ker \deg$$

if and only if

$$\varphi(x)^g = \varphi(x) \quad \text{for all } x \in \ker \deg.$$

This proves the first assertion.

To prove (2) note that any $f \in F$ has the form $f = f_1^k x$, where $x \in \ker \deg$ and $k \in \mathbb{Z}$. So,

$$\psi(f)H = \psi(f_1)^k \psi(x)H = \psi(f_1)^k \varphi(x)H = \\ (\varphi(f_1)g)^k \varphi(x)H = \!= \varphi(f_1)^k \varphi(x)H = \varphi(f_1^k x)H = \varphi(f)H,$$

where the equality $=\!=$ is valid because

$$\varphi(F) \textit{ normalises } H_\varphi \quad \textit{and} \quad g \in H_\varphi \subseteq H.$$

This proves assertion (2). □

3. Applications: groups. First, note that the conditions of the Main Theorem are obviously satisfied if Φ is the set of all homomorphisms $F \to G$ (and H is any subgroup of G, e.g., the entire group G). Therefore, the Gordon–Rodriguez–Villegas theorem is the simplest special case of the Main Theorem.

Theorem on equations over groups [6]. *The number of solutions to a system of equations $\{v_i(x_1, \ldots, x_n) = 1\}$ over a group G (where $v_i(x_1, \ldots, x_n) \in G * F(x_1, \ldots, x_n)$) is divisible by the order of the centraliser of the set of coefficients if the rank of the matrix consisting of the exponent-sums of the i-th unknown in the j-th equation is less than the number of unknowns.*

Proof. Let $A \subseteq G$ be the subgroup generated by all coefficients of the equations. Let F be the quotient group $F = (A * F(x_1, \ldots, x_n))/\langle\langle\{v_i\}\rangle\rangle$ of the free product $A * F(x_1, \ldots, x_n)$ of A and the free group by the normal subgroup $\langle\langle\{v_i\}\rangle\rangle$ generated by the left-hand sides of the equations. Let Φ be the set of homomorphisms $F \to G$ that are identity on A. (We assume that A embeds into F via the natural map $A \to F$, because if this map is not injective, then there are no solutions and we have nothing to prove.) Clearly, solutions to the system of equations are in a natural one-to-one correspondence with the elements of Φ.

The condition on the rank means that F admits an epimorphism onto $\mathbb{Z}$ whose kernel contains A. Let H be the centraliser of A in G. Clearly, the conditions of the Main Theorem are satisfied. Indeed, Condition I holds, because h centralises $A \subseteq G$ and, hence, ψ coincides with φ on $A \subset F$; Condition II holds, because elements of $A \subset F$ are of degree zero and, hence, ψ coincides with φ on $A \subset F$ again. □

Theorem on roots of subgroups [KM14]. *The number of elements g of a group G such that $g^n \in H$ is divisible by $|H|$ for any subgroup H of G and any integer n.*

The Theorem on Roots of Subgroups is the simplest special case of the following fact.

Theorem on homomorphisms and subgroups. [KM14]. *Let H be a subgroup of a group G and let W be a subgroup (or subset) of a finitely generated group F whose commutator subgroup F' is of infinite index. Then the number of homomorphisms $\varphi\colon F \to G$ such that $\varphi(W) \subseteq H$ is divisible by $|H|$.*

We shall prove a yet more general fact.

Theorem on homomorphisms and double cosets. *Let H be a subgroup of a group G, let W be a subset of a finitely generated group F whose commutator subgroup F' is of infinite index, and let $W \ni w \mapsto g_w \in G$ be an arbitrary map $W \to G$. Then the number of homomorphisms $\varphi\colon F \to G$ such that $\varphi(w) \in Hg_wH$ for all $w \in W$ is divisible by $|H|$.*

Proof. Take some epimorphism $\deg\colon F \to \mathbb{Z}$ (which exists because F/F' is an infinite finitely generated abelian group) and let Φ be the set of all homomorphisms $\varphi\colon F \to G$ such that $\varphi(w) \in Hg_wH$ for all $w \in W$. The conditions of the Main Theorem hold. For Condition I, this is quite obvious. As for Condition II, it suffices to note that the formula for ψ implies the equality $\psi(f)H = \varphi(f)H$ for all $f \in F$ by Lemma 0. □

The following theorem is an "epimorphism analogue" of the Gordon–Rodriguez-Villegas theorem.

Theorem on epimorphisms. *Let F be a finitely generated group whose commutator subgroup is of infinite index and let G be an arbitrary group. Then the number of surjective homomorphisms $F \to G$ is divisible by the order of the commutator subgroup of G.*

Proof. Take some epimorphism $\deg\colon F \to \mathbb{Z}$, let Φ be the set of all epimorphisms $F \to G$, and put $H = G'$. Let us verify that the conditions of the Main Theorem are satisfied. For Condition I, this is obvious.

To verify Condition II, we have to show that, for any epimorphism $\varphi\colon F \to G$ and any element $h \in G'$ centralising the subgroup $\varphi(\ker \deg)$, the homomorphism ψ from Condition II is surjective. Clearly, it is surjective modulo G' (i.e. $\psi(F)G' = G$), because ψ equals φ modulo G'. It remains to show that each element $g \in G'$ lies in $\psi(F)$. By the surjectivity of φ, we can find $f \in F$ such that $\varphi(f) = g$; moreover, the element f can be found in the commutator subgroup of F (because, for an epimorphism, the image of the commutator subgroup equals the commutator subgroup of the image). But then $f \in \ker \deg$ and, therefore, $\psi(f) = \varphi(f) = g$ as required. □

Remark 0.1. The number of surjective homomorphisms $F \to G$ is a multiple of $|\mathrm{Aut}\, G|$, because $\mathrm{Aut}\, G$ acts faithfully on the set of epimorphisms $F \to G$. However, the Theorem on Epimorphisms does not follow immediately from this observation, because, as was noted by A. V. Vasil'ev,

there exists a group G such that $|\mathrm{Aut}\, G|$ is not divisible by $|G'|$.

Examples of such groups are the groups $3 \cdot A_6$ and $3 \cdot A_7$ (see, e.g., [9]) of orders $\frac{3}{2} \cdot 6! = 1080$ and $\frac{3}{2} \cdot 7! = 7560$; they coincide with their commutator subgroups and have centres of order three; the central quotients are the alternating group

A_6 and A_7 while $|\mathrm{Aut}(3 \cdot A_6)| = 2 \cdot 6!$ and $\mathrm{Aut}(3 \cdot A_7)$ is the symmetric group of order 7!. Actually, Savelii Skresanov, and Dmitrii Churikov showed (using `GAP`) that the smallest group G such that $|G'| \not| \, |\mathrm{Aut}\, G|$ is of order 108.

Corollary on generating tuples in groups. *For each group G and each positive integer n, the number of tuples $(g_1, \ldots, g_n) \in G^n$ of elements of G generating G (i.e. such that $\langle g_1, \ldots, g_n \rangle = G$) is divisible by $|G'|$.*

Proof. The generating n-tuples of elements of G are in a natural one-to-one correspondence with the epimorphisms from the free group of rank n to G. Therefore, the assertion follows immediately from the Theorem on Epimorphisms. $\square$

Clearly, in the Theorem on Epimorphisms and even in the above corollary, the divisibility by $|G'|$ cannot be strengthened to the divisibility by $|G|$, because, in a prime-order group, the number of generating n-tuples is $|G|^n - 1$.

The following theorem generalises the Theorem on Epimorphisms and is an analogue of the Theorem on Homomorphisms and Subgroups.

Theorem on epimorphisms and subgroups. *Let A be a subgroup of a group G and let W be a subgroup of a finitely generated group F whose commutator subgroup F' is of infinite index. Then the number of homomorphisms $\varphi\colon F \to G$ such that $\varphi(W) = A$ is divisible by $|A'|$.*

Proof. Take some epimorphism $\deg\colon F \to \mathbb{Z}$ and put

$$\Phi = \{\textit{homomorphisms } \varphi\colon F \to G \textit{ such that } \varphi(W) = A\} \quad \text{and} \quad H = A'.$$

Let us verify that the conditions of the Main Theorem are satisfied. For Condition I, it is obvious.

To verify Condition II, we have to show that, for any homomorphism $\varphi\colon F \to G$ such that $\varphi(W) = A$ and any element $h \in A'$ centralising the subgroup $\varphi(\ker \deg)$, we have $\psi(W) = A$ for the homomorphism ψ from Condition II. The inclusion $\psi(W) \subseteq A$ certainly holds. To prove the inverse inclusion, note that $\psi(W)A' = A$. It remains to show that each element $a \in A'$ lies in $\psi(W)$. Since $\varphi(W) = A$, we can find $w \in W$ such that $\varphi(w) = a$; clearly, such an element w can be found in the commutator subgroup of W. But then $w \in \ker \deg$ and, therefore, $\psi(w) = \varphi(w) = a$ as required. $\square$

A similar statement on injective homomorphisms also holds (for finite groups G); moreover, the divisibility is much better in this case.

Theorem on monomorphisms and subgroups. *Let A be a subgroup of a group G and let W be a subgroup of a finitely generated group F such that WF' is of infinite index in F. Then $|N(A)|$ divides the following numbers:*

(a) *the number of homomorphisms $\varphi\colon F \to G$ such that the restriction of φ to W is injective and $\varphi(W) \subseteq A$;*
(b) *the number of homomorphisms $\varphi\colon F \to G$ such that the restriction of φ to W is injective and $\varphi(W) = A$.*

Proof. Let us prove a) (the proof of b) is quite similar). Take an epimorphism $\deg\colon F \to \mathbb{Z}$ such that $W \subseteq \ker\deg$ and put

$$\Phi = \{\text{homomorphisms } \varphi\colon F \to G \text{ such that } \varphi(W) \subseteq A \text{ and } \varphi|_W \text{ is injective}\} \text{ and}$$
$$H = N(A).$$

Condition I of the main theorem is obviously satisfied. Condition II is also satisfied, because $W \subseteq \ker\deg$ and, hence, ψ and φ (from Condition II) coincide on W. □

Remark 3.2. The condition $|F : F'W| = \infty$ cannot be replaced by $|F : F'| = \infty$ in the last theorem (even though we understand divisibility in the sense of cardinal arithmetics). Indeed,

(a) if $F = W = A = \mathbb{Z}$ and $G = \mathbb{R}$, then the number of injective homomorphisms $F = W \to A$ is $\aleph_0$ which is not a multiple of $|N(A)| = |\mathbb{R}| = 2^{\aleph_0}$;
(b) if $F = W = G = A = \mathbb{Z}$, then the number of bijective homomorphisms is two which is not a multiple of $|N(A)| = |\mathbb{Z}| = \aleph_0$.

4. Applications: rings. A *generalised homogeneous* equation over an associative ring R with the set of unknowns X is a finite equation of the form

$$\sum_i \prod_j c_{ij} x_{ij}^{k_{ij}} = 0,$$

where *coefficients* $c_{ij} \in R$, *unknowns* $x_{ij} \in X$, and *exponents* $k_{ij} \in \mathbb{Z}$, such that for some nonzero mapping $\deg\colon X \to \mathbb{Z}$ the value $\sum_j k_{ij} \deg(x_{ij})$ does not depend on i (i.e. the "polynomial" in the left-hand side of the equation is homogeneous with respect to some nonzero assignment of degrees to variables[1]). A system of equations is called generalised homogeneous if all its equations are generalised homogeneous (possibly of different degrees) with respect to the same function $\deg\colon X \to \mathbb{Z}$.

To test generalised homogeneity, one can use the following simple algorithm.

Algorithm for testing generalized homogeneity of a system

1. For each equation $v = 0$, construct the matrix A_v with integer entries a_{ij} that are the degree of i-th monomial with respect to j-th unknown (i.e. a_{ij} is the exponent-sum of j-th unknown in i-th monomial of v).
2. Subtract the first row of this matrix A_v from each row of A_v. Do it for all matrices A_v.
3. Combine the matrices A'_v thus obtained (with zero first rows) into one matrix: $A' = \begin{pmatrix} A'_v \\ A'_w \\ \vdots \end{pmatrix}$.
4. The system is generalised homogeneous if and only if the rank of A' is less than the number of unknowns.

[1] A variable may have zero degree, but at least one variable must have a nonzero degree.

For example, for the system of equations $\begin{cases}(xdy)^2 - yx^2 + xy^2cy^{-100}x = 0\\ xy - yx = 0\end{cases}$
(where $c, d \in R$ are coefficients and x, y are unknowns), we obtain:

$$A_u = \begin{pmatrix}2 & 2\\ 2 & 1\\ 2 & -98\end{pmatrix}, \quad A_v = \begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \quad A'_u = \begin{pmatrix}0 & 0\\ 0 & -1\\ 0 & -100\end{pmatrix}, \quad A'_v = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},$$

$$A' = \begin{pmatrix}0 & 0\\ 0 & -1\\ 0 & -100\\ 0 & 0\\ 0 & 0\end{pmatrix}, \quad \text{rank}\, A' = 1 \text{ and the system is generalised homogeneous.}$$

Proposition. *Any system of equations such that*

$$\sum_i \Big(\textit{(the number of monomials in } i\text{th } \textit{equation)} - 1\Big) < \textit{(the number of unknowns)}$$

is generalised homogeneous.

Proof. The assertion follows immediately from the above algorithm, but we leave the proof of correctness of this algorithm to readers as an exercise. (We shall use neither this proposition nor this algorithm in this paper.) □

The notion of a *solution* to a system of equations is defined naturally (if some exponents k_{ij} are negative, then the corresponding components of the solution must be invertible elements of the ring).

Theorem on equations over rings. *Let R be an associative ring with unity and let G be a subgroup of the multiplicative group of this ring. Then, for each generalised homogeneous system of equations over R with n unknowns, the number of solutions lying in G^n is divisible by the order of the intersection of G and the centraliser of the set of coefficients of the system.*

Proof. Let us apply the Main Theorem by letting F be the free group $F(x_1, \ldots, x_n)$ and extending the mapping $\deg\colon \{x_1, \ldots, x_n\} \to \mathbb{Z}$ (from the definition of generalised homogeneous systems) to a homomorphism $F \to \mathbb{Z}$, which can be assumed to be surjective, because it is nonzero. Let Φ be the set of homomorphisms $\varphi\colon F \to G$ such that $(\varphi(x_1), \ldots, \varphi(x_n))$ is a solution to the system of equations, and let H be the intersection of G and the centraliser of the set of coefficients of the system.

Let us verify the conditions of the Main Theorem. Condition I holds obviously. To verify Condition II, choose an element $t \in F$ of degree one and write each variable x_i in the form $x_i = t^{\deg x_i} y_i$, where $y_i = t^{-\deg x_i} x_i$ has zero degree.

Consider an equation $w(x_1, \ldots, x_n) = 0$ of the system and let us rewrite it in the form $v(t, y_1, \ldots, y_n) = 0$. By virtue of homogeneity, all monomials in $v(t, y_1, \ldots, y_n)$ have the same degree k with respect to t.

We have to show that if $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_n)) = 0$ and $h \in H_\varphi$, then $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_n)) = 0$.

And this is indeed so, because $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_n))$ is a multiple of $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_n))$ by the following lemma (which should be applied to each monomial of v). $\square$

Lemma 1. *Suppose that M is a monoid, $b_i, a, h \in M$, elements a and h are invertible, and $a^{-s}ha^s$, where $s \in \mathbb{Z}$, commute with all b_i. Then, for any expression of the form $u(t) = b_0 t^{n_1} b_1 \ldots t^{n_l} b_l$, where $n_i \in \mathbb{Z}$, we have*

$$u(ah) = \begin{cases} h^{a^{-1}} h^{a^{-2}} \ldots h^{a^{-k}} u(a) & \text{if } k = \sum n_i > 0 \\ h^{-1} h^{-a} \ldots h^{-a^{-1-k}} u(a) & \text{if } k = \sum n_i < 0 \\ u(a) & \text{if } k = \sum n_i = 0. \end{cases}$$

Proof. Using the commuting rules $a^i h^{a^j} = h^{a^{j-i}} a^i$ and $b_i h^{a^j} = h^{a^j} b_i$, we bring all letters h (and h^{a^j}) to the left end of the word $u(ah)$ and obtain the required form. This completes the proofs of Lemma 1 and the Theorem on Equations over Rings. $\square$

Example 1. *The number of* Pythagorean triples *of invertible elements of an associative ring with unity, i.e. the number of invertible solutions to the equation $x^2 + y^2 = z^2$ is always divisible by the order of the multiplicative group of the ring.*
Indeed, the equation is homogeneous and we can take $G = R^*$. Moreover, *the number of invertible solutions to the equation $ax^k + by^l + cz^m + dt^n + \cdots = 0$ is divisible by $|R^*|$ for any $a, b, c, d, \ldots, k, l, m, \cdots \in \mathbb{Z}$,* because this equation is generalised homogeneous.

5. Proof of the main theorem. The argument is to some extent similar to that near the end of Section 3 of [6]. To emphasise the similarity we use the same terms as in [6] (albeit their meaning is different).

The *tail* of a homomorphism $\varphi \in \Phi$ is the pair (φ_0, φ_H), where φ_0 is the restriction of φ to the subgroup $\ker \deg \subset F$ and $\varphi_H : F \to \{gH \ ; \ g \in G\}$ is the mapping from F to the set of left cosets of H in G that sends an element $f \in F$ to the coset $\varphi(f)H$.

We say that two homomorphisms $\varphi, \psi \in \Phi$ are *similar* and write $\varphi \sim \psi$ if their tails are conjugate by an element of H, i.e.

$$\begin{aligned} \varphi \sim \psi \quad \Longleftrightarrow \quad & \text{there exists } h \in H \text{ such that} \\ & \psi(f) = h\varphi(f)h^{-1} \quad \text{for all } f \in F \text{ of degree zero and} \\ & \psi(f)H = h\varphi(f)H \quad \text{for all } f \in F. \end{aligned}$$

Clearly, similarity is an equivalence relation on Φ. The Main Theorem is an immediate corollary of the following proposition.

Proposition. *In Φ, each class of similar homomorphisms consists of exactly $|H|$ elements. More precisely, for each $\varphi \in \Phi$,*

(1) *the number of different tails of elements of Φ similar to φ is $|H : H_\varphi|$;*
(2) *for each homomorphism ψ similar to φ, the number of elements of Φ with the same tail as ψ is $|H_\varphi|$.*

Proof. To prove (1), note that the group H acts by conjugation on the set of tails of elements of Φ. Indeed, if we conjugate the tail of a homomorphism $\psi \in \Phi$ by an element $h \in H$, then we obtain the tail of the homomorphism $f \mapsto \psi(f)^h$. This homomorphism lies in Φ by Condition I of the Main Theorem. The tails of homomorphisms similar to φ form the orbit of the tail of φ under this action. The cardinality of an orbit equals to the index of the stabiliser. It remains to note that the subgroup H_φ is the stabiliser of the tail of φ.

Let us prove the second assertion. Choose an element $x \in F$ of degree one. A homomorphism $\alpha\colon F \to G$ is uniquely determined by its tail and the value $\alpha(x)$. Moreover, for two homomorphisms α and β with the same tail, the quotient $h = (\alpha(x))^{-1}\beta(x)$ must stabilise this tail, i.e. h must lie in H_α. Indeed, for all $f \in F$ of degree zero, we have

$$\alpha(f^x)^h = \alpha(f)^{\alpha(x)h} = \alpha(f)^{\beta(x)} = \beta(f)^{\beta(x)} = \beta(f^x) = \alpha(f^x),$$

i.e. h centralises the subgroup $\alpha(\ker \deg)$; and, for any element $f \in F$, we have

$$\begin{aligned}\alpha(x)\alpha(f)H =& \alpha(xf)H = \\ & \beta(xf)H = \beta(x)\beta(f)H = \alpha(x)h\beta(f)H = \alpha(x)h\alpha(f)H,\end{aligned}$$

i.e. $h \in \alpha(f)H\alpha(f)^{-1}$. Thus, $h = (\alpha(x))^{-1}\beta(x) \in H_\alpha$.

On the other hand, if h is an arbitrary element of H_α, then the formula

$$f \mapsto \begin{cases} \alpha(f) & \text{if } \deg f = 0 \\ \alpha(x)h & \text{if } f = x \end{cases}$$

defines a homomorphism with the same tail as α (by Lemma 0). This homomorphism lies in Φ by Condition II of the Main Theorem.

Thus, for any $\alpha \in \Phi$, the set Φ contains precisely $|H_\alpha|$ homomorphisms with the same tail as α. It remains to note that, for similar homomorphisms ψ and φ, the subgroups H_φ and H_ψ have the same order, because they are conjugate. This completes the proofs of assertion 2) and the Main Theorem. □

Acknowledgements. The authors thank E. B. Vinberg for a question that brought us to writing this paper, Andrey V. Vasil'ev for a valuable remark (see Section 3), and the anonymous referee for a lot of comments allowing us to improve the text.

References

[1] K. S. Brown, The coset poset and probabilistic zeta function of a finite group, J. Algebra **225** (2000), 989–1012.

[2] D. J. Collins, Generating sequences of finite group, Senior Thesis, Cornell University Mathematics Department, 2010. http://www.math.cornell.edu/m/sites/default/files/imported/Research/SeniorTheses/2010/collinsThesis.pdf. (accessed January 1 2017).

[3] P. Hall, The Eulerian functions of a group, Quart. J. Math. Oxford Ser. **7** (1936), 134–151.

[4] T. Hawkes, I. M. Isaacs, and M. Özaydin, On the Möbius function of a finite group, Rocky Mountain J. Math. **19** (1984), 1003–1034.

[5] C. Gordon and F. Rodriguez-Villegas, On the divisibility of $\#\mathrm{Hom}(\Gamma, G)$ by $|G|$, J. Algebra **350** (2012), 300–307.

[6] A. A. Klyachko and A. A. Mkrtchyan, How many tuples of group elements have a given property? With an appendix by Dmitrii V. Trushin, Int. J. Algebra Comp. **24** (2014), 413–428.

[7] C. Kratzer and J. Thévenaz, Fonction de Möbius d'un groupe fini et anneau de Burnside, Comment. Math. Helv. **59** (1984), 425–438.

[8] L. Solomon, The solutions of equations in groups, Arch. Math. **20** (1969), 241–247.

[9] R. A. Wilson, The finite simple groups. graduate texts in mathematics, Springer, 251, London, 2009.

Anton A. Klyachko
Faculty of Mechanics and Mathematics,
Moscow State University (MSU),
Leninskie Gory,
Moscow 119991,
Russia
e-mail: klyachko@mech.math.msu.su

Anna A. Mkrtchyan
School of Mathematics,
University of Edinburgh,
Room 5402, James Clerk Maxwell Building, King's Buildings,
Edinburgh EH9 3JZ,
UK
e-mail: anna.mkr@gmail.com

Received: 20 July 2016