On the number of epi-, mono- and homomorphisms of groups

E. K. Brusyanskaya and Ant. A. Klyachko

Abstract. It is well known that the number of homomorphisms from a group $F$ to a group $G$ is divisible by the greatest common divisor of the order of $G$ and the exponent of $F/[F,F]$. We study the question of what can be said about the number of homomorphisms satisfying certain natural conditions like injectivity or surjectivity. A simple non-trivial consequence of our results is the fact that in any finite group the number of generating pairs $(x,y)$ such that $x^3 = 1 = y^5$ is divisible by the greatest common divisor of fifteen and the order of the group $[G,G] \cdot \{g^{15} \mid g \in G\}$.

Keywords: number of homomorphisms, equations in groups, Frobenius’ theorem, Solomon’s theorem.

Introduction

This paper is based on three classical results about divisibility in groups: the theorems of Frobenius (1895), Solomon (1969) and Iwasaki (1985).

Frobenius’ Theorem ([1], see also [2]). The number of solutions of the equation $x^n = 1$ in a finite group $G$ is divisible by GCD$(|G|, n)$ for any positive integer $n$.

Solomon’s Theorem ([3]). In any group $G$, the number of solutions of a finite system of equations without coefficients is divisible by the order of this group if there are fewer equations than unknowns. In other words, the number of homomorphisms $\langle x_1, \ldots, x_m \mid w_1 = \cdots = w_n = 1 \rangle \to G$ is divisible by $|G|$ if $m > n$.

Iwasaki’s Theorem ([4]). For any integer $n$, the number of elements of a finite group $G$ whose the $n$th powers belong to a given subgroup $A \subseteq G$ is divisible by $|A|$.

These theorems have been generalized many times in various directions (see [5]–[21] and the literature cited therein). For example, the following generalization of Solomon’s theorem was proved in [16].

Gordon–Rodriguez-Villegas Theorem ([16]). The number of homomorphisms $F \to G$ is divisible by the order of $G$ if $F$ is a finitely generated group whose derived subgroup has infinite index.

This research was supported by the Russian Foundation for Basic Research (grant no. 19-01-00591).

AMS 2020 Mathematics Subject Classification. 20F70, 20D60, 20F05.

© 2022 Russian Academy of Sciences (DoM) and London Mathematical Society
It later became clear that there is a connection between these three classical results:

- in [19] a certain general fact was proved, called here the KM theorem, which includes as special cases Solomon’s theorem and Iwasaki’s theorem (and generalizations of them);

- in [20] it was shown that all three classical theorems (and generalizations of them, including the KM theorem) are special cases of one very general theorem, which is called here the BKV theorem (see §1).

The authors of [19] derived from the KM theorem the following fact about the divisibility of the number of homomorphisms satisfying conditions like injectivity or surjectivity. Let $F \supseteq W$ and $G \supseteq A$ be groups and let

\[ \text{Hom}(F, W; G, A) = \{ \phi: F \to G \mid \phi(W) \subseteq A \}, \]
\[ \text{Epi}(F, W; G, A) = \{ \phi: F \to G \mid \phi(W) = A \}, \]
\[ \text{Mono}(F, W; G, A) = \{ \phi: F \to G \mid \phi(W) \subseteq A \text{ and the restriction of } \phi \text{ to } W \text{ is injective} \}. \]

**Theorem** (on epi-, mono- and homomorphisms; see [19]). Let $W$ be a subgroup of a finitely generated group $F$ whose derived subgroup $F'$ has infinite index, and let $A$ be a subgroup of a group $G$. Then

a) each of the numbers $|\text{Hom}(F, W; G, A)|$, $|\text{Epi}(F, W; G, A)|$ and $|\text{Mono}(F, W; G, A)|$ is divisible by the order of the normalizer $N(A)$ of $A$ if the index $|F : F'W|$ is infinite;

b) $|\text{Hom}(F, W; G, A)|$ is divisible by $|A|$;

c) $|\text{Epi}(F, W; G, A)|$ is divisible by $|A'|$.

The purpose of this paper is to add ‘Frobeniusness’ to this theorem, that is, to get rid of the conditions $|F : F'| = \infty$ and $|F : F'W| = \infty$. The result turned out to be as expected for parts a) and b), much less obvious in the case of c) and, furthermore, a new part d) appears.

**‘Frobenius’ Theorem** (on epi-, mono- and homomorphisms). Let $A$ be a subgroup of a group $G$ and $W$ a subgroup of a finitely generated group $F$. Then

a) each of the numbers $|\text{Hom}(F, W; G, A)|$, $|\text{Epi}(F, W; G, A)|$ and $|\text{Mono}(F, W; G, A)|$ is divisible by $\text{GCD}(N(A), \exp(F/(F'W)))$;

b) $|\text{Hom}(F, W; G, A)|$ is divisible by $\text{GCD}(A, \exp(F/F'))$;

c) $|\text{Epi}(F, W; G, A)|$ is divisible by $\text{GCD}(A', \exp(F/F'), \exp(F/F'))$;

d) $|\text{Mono}(F, W; G, A)|$ is divisible by $\text{GCD}(A, \exp(F/(F'Z(W))))$.

This is a greatly simplified statement of Theorem 1 below, or rather corollary of it (see §3). Not all that is claimed here about the number $|\text{Hom}(F, W; G, A)|$ is new: some facts established in [20] are included simply for completeness.

We point out that in this theorem $G$ is not assumed to be finite. We adhere to the notation in [20]: the greatest common divisor $\text{GCD}(G, n)$ of a group $G$ and an integer $n$ is defined to be the least common multiple of the orders of the subgroups of $G$ dividing $n$, and divisibility is always understood in the sense of cardinal arithmetic: every infinite cardinal is divisible by all smaller non-zero cardinals (and of course zero is divisible by all cardinals, while only zero is divisible by zero). This means
that $\text{GCD}(G, 0) = |G|$ for any group $G$ while, for example, $\text{GCD}(\text{SL}_2(\mathbb{Z}), 2020) = 2$. We assume without loss of generality that all groups in this paper are finite, and in this case, $\text{GCD}(G, n) = \text{GCD}(|G|, n)$ by Sylow’s theorem (and because a finite $p$-group contains subgroups of all possible orders).

Part b) of this theorem, of course, contains the classical theorems

- of Frobenius (it is sufficient to take as $F = W$ a cyclic group and put $A = G$);
- of Solomon, and even of Gordon–Rodriguez-Villegas (it is sufficient to take as $F = W$ a finitely generated group whose derived subgroup has infinite index and put $A = G$);
- of Iwasaki (it is sufficient to put $F = \mathbb{Z} \supseteq n\mathbb{Z} = W$).

Furthermore, if, for example, we take as $F = W$ a free product of cyclic groups and put $A = G$ in part c) of the theorem, then we obtain the following fact.

**Corollary** (on systems of generators). For any group $G$ and any $k_i \in \mathbb{Z}$, the number of tuples $(g_1, \ldots, g_n)$ of elements of $G$ such that $\langle g_1, \ldots, g_n \rangle = G$ and $g_i^{k_i} = 1$ is divisible by $\text{GCD}(G', G^{\text{LCM}(k_1, \ldots, k_n)}, \text{LCM}(k_1, \ldots, k_n))$. (Here and below, $G^m := \langle g^m \mid g \in G \rangle$.)

We point out that crucial to our generalization of the theorem on epi-, mono- and homomorphisms is using, instead of the KM theorem, its ‘Frobenius analogue’, that is, the BKV theorem. But in fact we generalize both the BKV theorem itself (see Main Theorem in §1) and its proof (in §2).

The notation and conventions that we use are on the whole standard. We only point out that if $k \in \mathbb{Z}$ while $x$ and $y$ are elements of some group, then $x^y$, $x^{ky}$ and $x^{-y}$ denote $y^{-1}xy$, $y^{-1}x^ky$ and $y^{-1}x^{-1}y$, respectively. The derived subgroup of a group $G$ is denoted by $G'$ or $[G, G]$, and the centre of $G$ by $Z(G)$. The subgroup of $G$ generated by the $n$th powers of all the elements is denoted by $G^n$. The cardinality of a set $X$ is denoted by $|X|$. If $X$ is a subset of some group, then $\langle X \rangle$, $C(X)$ and $N(X)$ mean the subgroup generated by $X$, the centralizer of $X$ and the normalizer of $X$, respectively. The index of a subgroup $H$ of a group $G$ is denoted by $|G : H|$. The symbol $\mathbb{Z}$ denotes the set of integers. GCD and LCM mean the greatest common divisor and the least common multiple. The symbol $\exp(G)$ denotes the exponent of a group $G$ if this exponent is finite, and we assume that $\exp(G) = 0$ if the exponent is infinite. Furthermore, we point out once again that the finiteness of groups is not assumed by default anywhere, divisibility is always understood in the sense of cardinal arithmetic (an infinite cardinal is divisible by all non-zero cardinals that are not greater than it), and $\text{GCD}(G, n) := \text{LCM}(|H| \mid H$ is a subgroup of $G$ and $|H|$ divides $n$).

§1. Main Theorem

A group $F$ with a fixed epimorphism $F \to \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ (where $n \in \mathbb{Z}$) is called an $n$-indexed group [20]. This epimorphism $F \to \mathbb{Z}_n$ is called the degree and denoted by $\deg$. Thus, for any element $f$ of $F$, an element $\deg f \in \mathbb{Z}_n$ is defined, $F$ contains elements of all degrees, and $\deg(fg) = \deg f + \deg g$ for any $f, g \in F$. 
Suppose that $\phi: F \to G$ is a homomorphism from an $n$-indexed group $F$ to some group $G$ and let $H$ be a subgroup of $G$. The subgroup

$$H_\phi = \bigcap_{f \in F} H^{\phi(f)} \cap C(\phi(\ker \deg))$$

is called the $\phi$-core of $H$ (see [19]). In other words, the $\phi$-core $H_\phi$ of $H$ consists of elements $h$ such that $h^{\phi(f)} \in H$ for all $f$, and $h^{\phi(f)} = h$ if $\deg f = 0$.

**BKV Theorem** (see [20]). Suppose that an integer $n$ is divisible by the order of a subgroup $H$ of some group $G$, and $\Phi$ is some set of homomorphisms from an $n$-indexed group $F$ into $G$ satisfying the following conditions.

I. $\Phi$ is invariant under conjugation by elements of $H$: if $h \in H$ and $\phi \in \Phi$, then the homomorphism $\psi: f \mapsto \phi(f)^h$ also belongs to $\Phi$.

II. For any $\phi \in \Phi$ and any element $h$ of the $\phi$-core $H_\phi$ of $H$, the homomorphism $\psi$ defined by the rule

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

is also contained in $\Phi$.

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

We make the following observations.

The map $\psi$ in condition I is a homomorphism for any $h \in G$; the formula for $\psi$ in condition II defines a homomorphism for any $h \in H_\phi$ (as explained in [20]). The meaning of conditions I and II is that these homomorphisms belong to $\Phi$.

By Lemma 3 in [20], in condition II of the BKV theorem we have $\psi(f) \in \phi(f)H_\phi$ for all $f \in F$.

The condition “$n$ is divisible by the order of the subgroup $H$” can be dropped, but then the conclusion of the theorem must be “$|\Phi|$ is divisible by $\gcd(H,n)$” (instead of “$|\Phi|$ is divisible by $|H|$”). This follows immediately from the definition of the greatest common divisor of a group and an integer (see the introduction) and the fact that if conditions I and II hold for $H$, then they also hold for any subgroup of $H$.

The KM theorem is precisely the BKV theorem with $n = 0$.

**Main Theorem.** Suppose that $F$ is an $n$-indexed group, $H$ a subgroup of a group $G$, $k$ a positive integer, and $\Phi$ some set of homomorphisms from $F$ to $G$ satisfying the following conditions.

(i) For all $\phi \in \Phi$ and $h \in H$, the homomorphism $\psi: f \mapsto \phi(f)^h$ belongs to $\Phi$.

(ii) For every $\phi \in \Phi$, the $\phi$-core $H_\phi$ of $H$ contains a subgroup $H_{\phi,k}$ such that

- $H_\phi \supseteq H_{\phi,k} \supseteq \langle H_\phi \cup \phi(F) \rangle$,
- $|H_\phi / H_{\phi,k}|$ divides $k$,
- if $\phi \in \Phi$ and $\psi: F \to G$ is a homomorphism coinciding with $\phi$ on the elements of degree zero and such that $\psi(w) \in \phi(w)H_{\phi,k}$ for all elements $w \in F$ whose degrees are divisible by $k$ (that is, $\deg w \in k\mathbb{Z}_n$), then $\psi \in \Phi$.

Then $|\Phi|$ is divisible by $\gcd(H,n)$. 


This fact generalizes the BKV theorem and essentially (that is, in view of the comments after the BKV theorem) turns into it if we put \( k = 1 \) and \( H_{\phi,k} = H_{\phi} \).

§ 2. Proof of Main Theorem

We can assume that \( |H| \) divides \( n \) (by the definition of the greatest common divisor of a group and an integer and because conditions (i) and (ii) are preserved when \( H \) is replaced by a subgroup). It is further sufficient to show that conditions I and II of the BKV theorem hold for these \( F, G, H \) and \( \Phi \). Condition I obviously holds by condition (i).

We now verify condition II. Suppose that \( \phi \in \Phi \), an element \( f_1 \in F \) has degree 1, \( \phi(f_1) = g \) and \( h \in H_{\phi} \). We need to show that a homomorphism \( \psi : F \to G \) coinciding with \( \phi \) on elements of degree zero and taking \( f_1 \) to \( gh \) belongs to \( \Phi \). Every element \( w \in F \) whose degree is divisible by \( k \) can be written in the form \( w = f_0 f_1^k i \) for some \( i \in \mathbb{Z} \) and \( f_0 \in \ker \deg \).

\[
\psi(w) = \psi(f_0 f_1^k) = \psi(f_0)(gh)^k = \phi(f_0)(gh)^k
\]

(since \( \phi \) and \( \psi \) coincide on \( \ker \deg \)). The subgroup \( H_{\phi} \) is normal in \( \langle H_{\phi}, g \rangle \) by the definition of the \( \phi \)-core \( H_{\phi} \).

Brauer’s Lemma (see [22], also [20]). If \( U \) is a finite normal subgroup of a group \( V \), then for all \( v \in V \) and \( u \in U \) the elements \( v^{[U]} \) and \( (vu)^{[U]} \) are conjugate by an element of \( U \).

By applying Brauer’s Lemma to the normal subgroup \( H_{\phi}/H_{\phi,k} \) of \( \langle g, H_{\phi} \rangle / H_{\phi,k} \) we obtain the inclusion \( (gh)^k \in g^{k h'} H_{\phi,k} \) for some \( h' \in H_{\phi} \) that does not depend on \( i \) or \( w \) but is determined only by the homomorphisms \( \phi \) and \( \psi \). Therefore,

\[
\psi(w) = \phi(f_0)(gh)^k = \phi(f_0)g^{k h'} H_{\phi,k} \overset{\text{(1)}}{=} (\phi(f_0)g^{k i})^{h'} H_{\phi,k} \overset{\text{(2)}}{=} (\phi(f_0 f_1^k))^{h'} H_{\phi,k} \overset{\text{(3)}}{=} (\phi(w))^{h'} H_{\phi,k}.
\]

where the equality \( \overset{\text{(1)}}{=} \) follows from the fact that the element \( h' \in H_{\phi} \) commutes with the image \( \phi(f_0) \) of the element \( f_0 \) of degree zero by the definition of the \( \phi \)-core \( H_{\phi} \), the equality \( \overset{\text{(2)}}{=} \) follows from the definition of the element \( g \), and the equality \( \overset{\text{(3)}}{=} \) follows from the definition of \( w \).

The homomorphism \( f \mapsto (\phi(f))^{h'} \) belongs to \( \Phi \) by condition (i), and, consequently, \( \psi \in \Phi \) by condition (ii). The proof of Main Theorem is complete.

§ 3. By what the number of epi-, mono- and homomorphisms is divisible

Let \( \Phi \) be a set of homomorphisms from an \( n \)-indexed group \( F \) to a group \( G \) and let \( B \) and \( H \) be subgroups of \( G \). A subgroup \( H \) is said to be \((B,k,\Phi)\)-\textit{smooth} if for every \( \phi \in \Phi \) the group \( H_{\phi} \cap B \) contains a subgroup \( \hat{B} \) (depending on \( \phi \)) that is normal in \( \langle H_{\phi}, \phi(F) \rangle \) such that \( |H_{\phi}/\hat{B}| \) divides \( k \).

The following lemma contains some fairly obvious examples of smooth subgroups.
Lemma (on smooth subgroups). The following subgroups of $G$ are $(B, k, \Phi)$-smooth:

1) any subgroup contained in $B$;
2) any subgroup of order dividing $k$;
3) any subgroup $H$ such that $|H : H \cap B|$ divides $k$ if $B \triangleleft G$.

Proof. It is sufficient to take the following subgroups as $\hat{B}$: 1) $H_\phi$, 2) $\{1\}$, 3) $H \cap B$.

Theorem 1. Suppose that $A$ is a subgroup of a group $G$, and $W$ is a subgroup of an $n$-indexed group $F$ such that $\deg(W) = k\mathbb{Z}_n$. Let

$$
\text{Hom}(F, W; G, A) = \{\phi : F \to G \mid \phi(W) \subseteq A\},
$$

$$
\text{Epi}(F, W; G, A) = \{\phi : F \to G \mid \phi(W) = A\},
$$

$$
\text{Mono}(F, W; G, A) = \{\phi : F \to G \mid \phi(W) \subseteq A \text{ and the restriction of } \phi \text{ to } W \text{ is injective}\}.
$$

Then $\text{GCD}(H, n)$ divides $|\text{Hom}(F, W; G, A)|$ for any $(A, k, \text{Hom}(F, W; G, A))$-smooth subgroup $H \subseteq N(A)$ of $G$;

b) $|\text{Epi}(F, W; G, A)|$ for any $(A'A^n, k, \text{Epi}(F, W; G, A))$-smooth subgroup $H \subseteq N(A)$ of $G$, where $A^n := \langle a^n \mid a \in A \rangle$;

c) $|\text{Mono}(F, W; G, A)|$ for any $(A, k, \text{Mono}(F, W; G, A))$-smooth subgroup $H \subseteq N(A)$ of $G$ if the indexing of the group $F$ is chosen in such a way that $\deg(w) = 0$ for every central (in $W$) element $w \in W$ such that $w^n = 1$.

Note that the subgroup $A'A^n$ in part b) and the subgroup $\{w \in Z(W) \mid w^n = 1\}$ in part c) are none other than the verbal subgroup of $A$ and the marginal subgroup of $W$ corresponding to the variety of Abelian groups of exponent $n$.

Proof of Theorem 1. It is sufficient to verify that conditions (i) and (ii) of the Main Theorem hold for the given $F$, $G$, $H$, $k$, $\Phi$, and $H_\phi,k = \hat{B}$ (where $\hat{B}$ is from the definition of a smooth subgroup $B$, which is chosen to be $A$ in parts a) and c), and $A'A^n$ in part b)). The first two parts of (ii) hold automatically by the definition of smoothness, so we only need to verify the last part of condition (ii).

a) $B = A$ and $\Phi = \text{Hom}(F, W; G, A)$. Condition (i) obviously holds since $H \subseteq N(A)$. Condition (ii) also holds, since $\psi(w) \in \phi(w)\hat{B} \subseteq \phi(w)A = A$ for all $w \in W$, that is, $\psi \in \Phi$, as required.

b) $B = A'A^n$ and $\Phi = \text{Epi}(F, W; G, A)$. Condition (i) obviously holds for the same reason, $H \subseteq N(A)$. Condition (ii) also holds:

$$
A \equiv (1) \phi(W) \subseteq (2) \psi(W)A'A^n \equiv (3) \psi(W)\phi(W'W^n) \equiv (4) \psi(W)\psi(W'W^n) = \psi(W),
$$

where $^{(1)}$ holds by the definition of $\Phi \ni \phi$, $^{(2)}$ holds by the definition of $\psi$ in condition (ii) for $B = A'A^n \supseteq \hat{B} = H_\phi,k$, $^{(3)}$ follows from $^{(1)}$, and $^{(4)}$ follows from the fact that $\deg(W'W^n) = \{0\}$, while $\psi$ and $\phi$ in condition (ii) coincide on elements of degree zero.

As a result we have obtained that $A = \psi(W)$, that is, $\psi \in \Phi$, as required.
c) $B = A$ and $\Phi = \text{Mono}(F, W; G, A)$. Condition (i) obviously holds for the same reason, $H \subseteq N(A)$. We now show that (ii) also holds. First, $\psi(W) \subseteq \phi(W)A = A$. It remains to show that $\ker \psi \cap W = \{1\}$. Let $w \in \ker \psi \cap W$. Then
- for every $w' \in W$ we have $1 = \psi([w, w']) = \phi([w, w'])$ (since commutators have degree zero, while $\phi$ and $\psi$ coincide on elements of degree zero), so that $[w, w'] = 1$ (since $\phi$ is injective on $W$), that is, $w \in Z(W)$;
- we similarly obtain $1 = \psi(w) = \phi(w)$ (since $\deg(w) = n \deg(w) = 0$, while $\phi$ and $\psi$ coincide on elements of degree zero), so that $w^n = 1$ (since $\phi$ is injective on $W$).

We have obtained that $w$ is a central element of $W$ and $w^n = 1$, and such elements have degree zero by hypothesis. Therefore, $\phi(w) = \psi(w) = 1$, that is, $w = 1$ since $\phi \in \text{Mono}(F, W : G, A)$. Therefore, $\ker \psi \cap W = \{1\}$, as required. Theorem 1 is proved.

Corollary. Under the hypotheses of Theorem 1, each of the integers $|\text{Hom}(F, W; G, A)|$, $|\text{Epi}(F, W; G, A)|$ and $|\text{Mono}(F, W; G, A)|$ is divisible by $\text{GCD}(k, N(A))$. Furthermore,

a) $|\text{Hom}(F, W; G, A)|$ is divisible
- by $\text{GCD}(n, A)$,
- by $\text{GCD}(n, |A| \cdot \text{GCD}(k, |G/A|)) = \text{GCD}(n, |G|, k \cdot |A|)$ if $A \vartriangleleft G$ and $G$ is finite;

b) $|\text{Epi}(F, W; G, A)|$ is divisible
- by $\text{GCD}(n, A'A^n)$, and even by $\text{GCD}(n, H)$, where $H$ is any subgroup of $N(A)$ such that $|(C(A'A^n) \cap H : Z(A'A^n) \cap H)|$ divides $k$,
- by

$$\text{GCD}(n, |A'A^n| \cdot \text{GCD}(k, |G/(A'A^n)|)) = \text{GCD}(n, |G|, k \cdot |A'A^n|)$$

if $A \vartriangleleft G$ and $G$ is finite;

c) if $\deg\{|w \in Z(W) \mid w^n = 1\} = \{0\}$, then $|\text{Mono}(F, W; G, A)|$ is divisible
- by $\text{GCD}(n, A)$,
- by

$$\text{GCD}(n, |A| \cdot \text{GCD}(k, |G/A|)) = \text{GCD}(n, |G|, k \cdot |A|)$$

if $A \vartriangleleft G$ and $G$ is finite.

Proof. The first part (about divisibility by $\text{GCD}(k, N(A))$) follows directly from Theorem 1 and part 2) of Lemma on smooth subgroups.

The other parts also follow from Theorem 1 and a suitable assertion about smooth subgroups.

a) The divisibility by $\text{GCD}(n, A)$ follows immediately from part 1) of the lemma on smooth subgroups. The divisibility by $\text{GCD}(n, |G|, k \cdot |A|)$ follows from part 3) of the lemma on smooth subgroups. Indeed, it is sufficient to apply Theorem 1 taking as $H$ a $p$-subgroup of $G$ whose order is the maximum power $p^i$ of $p$ dividing $\text{GCD}(n, k|A|, |G|)$, and choosing this $H$
- within $A$ if $p^i$ divides $|A|$, and
- containing a Sylow $p$-subgroup of $A$ otherwise.
This subgroup is \((A,k,\text{Hom}(F,W;G,A))\)-smooth by the lemma on smooth subgroup. Therefore \(|H|\) divides \(\text{Hom}(F,W;G,A)\) by Theorem 1. By performing this procedure for all primes \(p\), we obtain the required divisibility.

b) The second assertion of part b) is proved in exactly the same fashion as the second assertion of part a). To prove the first assertion of part b), by Theorem 1 it is sufficient to verify that \(H\) is \((A'\tilde{A}^n,k,\text{Epi}(F,W;G,A))\)-smooth, that is, for all \(\phi \in \text{Epi}(F,W;G,A)\) the group \(H_\phi \cap (A'\tilde{A}^n)\) contains a subgroup \(\tilde{B}\) that is normal in \(\langle H_\phi, \phi(F) \rangle\) and such that \(|H_\phi/\tilde{B}|\) divides \(k\). As such a subgroup \(\tilde{B}\) it is sufficient to take \(Z(A'\tilde{A}^n) \cap H_\phi\). Indeed,

\[
H_\phi \quad \subseteq \quad C(\phi(ker \deg)) \quad \subseteq \quad C(\phi(W'W^n)) \quad \equiv \quad C(A'\tilde{A}^n),
\]

where \((1)\) follows from the definition of the \(\phi\)-core \(H_\phi\), \((2)\) follows from the fact that \(\text{deg}(W'W^n) = \{0\}\), and \((3)\) follows from the equation \(\phi(W) = A\).

Therefore \(|H_\phi/(Z(A'\tilde{A}^n) \cap H_\phi)|\) divides

\[
|\left(C(A'\tilde{A}^n) \cap H\right) / (Z(A'\tilde{A}^n) \cap H)|
\]

by Lagrange’s theorem, and this number divides \(k\) by hypothesis.

c) The proof is similar to that of part a).

The corollary is proved.

**Bibliography**

[1] G. Frobenius, “Verallgemeinerung des Sylow’schen Satzes”, *Sitzungsber. Preuß. Akad. Wiss. Berlin* 1895 (1895), 981–993.

[2] R. Andreev, A translation of “Verallgemeinerung des Sylow’schen Satzes” by F. G. Frobenius, arXiv:1608.08813.

[3] L. Solomon, “The solution of equations in groups”, *Arch. Math. (Basel)* 20:3 (1969), 241–247.

[4] S. Iwasaki, “A note on the \(n\)th roots ratio of a subgroup of a finite group”, *J. Algebra* 78:2 (1982), 460–474.

[5] G. Frobenius, “Über einen Fundamentalsatz der Gruppentheorie”, *Sitzungsber. Preuß. Akad. Wiss. Berlin* 1903 (1903), 987–991.

[6] P. Hall, “On a theorem of Frobenius”, *Proc. London Math. Soc.* 40 (1936), 468–501.

[7] A. Kulakoff, “Einige Bemerkungen zur Arbeit: “On a theorem of Frobenius” von P. Hall”, *Mat. Sb. 3*:2 (1938), 403–405.

[8] S. K. Sehgal, “On P. Hall’s generalisation of a theorem of Frobenius”, *Proc. Glasgow Math. Assoc.* 5:3 (1962), 97–100.

[9] I. M. Isaacs, “Systems of equations and generalized characters in groups”, *Canadian J. Math.* 22:5 (1970), 1040–1046.

[10] K. S. Brown and J. Thévenaz, “A generalization of Sylow’s third theorem”, *J. Algebra* 115:2 (1988), 414–430.

[11] T. Yoshida, “[|\text{Hom}(A,G)|]”, *J. Algebra* 156:1 (1993), 125–156.

[12] S. P. Strunkov, “On the theory of equations in finite groups”, *Izv. Ross. Akad. Nauk Ser. Mat.* 59:6 (1995), 171–180; English transl., *Izv. Math.* 59:6 (1995), 1273–1282.
On the number of epi-, mono- and homomorphisms of groups

[13] T. Asai and Yu. Takegahara, “|\text{Hom}(A,G)|. IV”, J. Algebra 246:2 (2001), 543–563.
[14] J. Sato and T. Asai, “On the n-th roots of a double coset of a finite group”, J. Sch. Sci. Eng. Kinki Univ. 43 (2007), 1–4.
[15] A. Amit and U. Vishne, “Characters and solutions to equations in finite groups”, J. Algebra Appl. 10:4 (2011), 675–686.
[16] C. Gordon and F. Rodriguez-Villegas, “On the divisibility of \# \text{Hom}(\Gamma, G) by |G|”, J. Algebra 350:1 (2012), 300–307.
[17] T. Asai, N. Chigira, T. Niwasaki, and Yu. Takegahara, “On a theorem of P. Hall”, J. Group Theory 16:1 (2013), 69–80.
[18] A. A. Klyachko and A. A. Mkrtchyan, “How many tuples of group elements have a given property?”, with an appendix by Dmitrii V. Trushin, Internat. J. Algebra Comput. 24:4 (2014), 413–428.
[19] A. A. Klyachko and A. A. Mkrtchyan, “Strange divisibility in groups and rings”, Arch. Math. 108:5 (2017), 441–451.
[20] E. K. Brusyanskaya, A. A. Klyachko, and A. V. Vasil’ev, “What do Frobenius’s, Solomon’s, and Iwasaki’s theorems on divisibility in groups have in common?”, Pacific J. Math. 302:2 (2019), 437–452.
[21] A. A. Klyachko and M. A. Ryabtseva, “The dimension of solution sets to systems of equations in algebraic groups”, Israel J. Math. 237:1 (2020), 141–154.
[22] R. Brauer, “On a theorem of Frobenius”, Amer. Math. Monthly 76:1 (1969), 12–15.

Elena K. Brusyanskaya
Moscow State University;
Moscow Centre for Fundamental and Applied
Mathematics
E-mail: ebrusianskaia@gmail.com

Anton A. Klyachko
Moscow State University;
Moscow Centre for Fundamental and Applied
Mathematics
E-mail: klyachko@mech.math.msu.su