УДК 512.542 + 512.543.72 MSC: 20D60, 20F70

ЧТО ОБЩЕГО МЕЖДУ ТЕОРЕМАМИ ФРОБЕНИУСА, СОЛОМОНА И ИВАСАКИ О ДЕЛИМОСТИ В ГРУППАХ?

Елена К. Брусянская[♯] Андрей В. Васильев[♭♮] Антон А. Клячко[♯]

[♯] *Механико-математический факультет Московского государственного университета Москва 119991, Ленинские горы, МГУ*

[♭] *Институт математики им. С. Л. Соболева СО РАН, Новосибирск 630090, проспект ак. Коптюга, 4*

[♮] *Новосибирский государственный университет, Новосибирск 630090, ул. Пирогова, 1*

ebrusianskaia@gmail.com vasand@math.nsc.ru klyachko@mech.math.msu.su

Наш результат включает в себя естественным образом теорему Фробениуса (1895) о числе решений уравнения $x^n = 1$ в группе, теорему Соломона (1969) о числе решений в группе системы уравнений, в которой уравнений меньше, чем неизвестных, и теорему Ивасаки (1985) о корнях из подгрупп. Имеются и другие любопытные следствия о группах и кольцах.

0. Введение

Следующий результат доказан ещё в XIX веке.

Теорема Фробениуса [Frob95] (см. также [And16]). *Число решений уравнения $x^n = 1$ в конечной группе G делится на $\text{НОД}(|G|, n)$ для любого натурального n.*

Эта теорема много раз обобщалась в разных направлениях, смотрите, например, [Hall36], [Kula38], [Sehg62], [BrTh88], [Yosh93], [AsTa01], [ACNT13] и литературу там цитируемую. Например, сам Фробениус в 1903 году [Frob03] доказал следующее обобщение:

> *для любого натурального n и любого элемента g любой конечной группы G число решений уравнения $x^n = g$ в G делится на наибольший общий делитель числа n и порядка централизатора элемента g;*

а Ф. Холл ([Hall36], теорема II) показал, что

> *в любой конечной группе число решений системы уравнений с одним неизвестным делится на $\text{НОД}(|C|, n_1, n_2, \ldots)$, где C — это централизатор множества всех коэффициентов, а n_i — сумма показателей степеней при неизвестном в i-м уравнении.*

Здесь, как обычно, под уравнением над группой G понимается формальная запись вида $v(x_1, \ldots, x_m) = 1$, где v является словом, в котором каждая буква — это либо неизвестный, либо обратный к неизвестному, либо элемент группы G (называемый *коэффициентом*). Другими словами, левая часть уравнения — это элемент свободного произведения $G * F(x_1, \ldots, x_m)$ группы G и свободной группы $F(x_1, \ldots, x_m)$ ранга m (где m — число неизвестных).

Теорема Соломона, о которой дальше пойдёт речь, тоже про уравнения в группах и тоже про делимость, но, на первый взгляд, не очень похожа на теорему Фробениуса и её обобщения.

Теорема Соломона [Solo69]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*

Эта теорема также обобщалась в разных направлениях, смотрите [Isaa70], [Стру95], [AmV11], [GRV12], [KM14], [KM17] и литературу, там цитируемую. Например, в [KM14] показано, что

> *в любой группе число решений системы уравнений с коэффициентами из этой группы делится на порядок пересечения централизаторов всех коэффициентов, если ранг матрицы, составленной из сумм показателей степеней при j-м неизвестном в i-м уравнении, меньше числа неизвестных.*

Сам Соломон написал в [Solo69]:

> *“There seems to be no connection between this theorem and the Frobenius theorem on solutions of $x^k = 1$.”*

Тем не менее, связь между теоремами Фробениуса и Соломона есть.

Работа первого и третьего авторов выполнена при поддержке Российского фонда фундаментальных исследований, грант № 19-01-00591.

Работа второго автора выполнена при поддержке программы фундаментальных научных исследований СО РАН № I.1.1., проект № 0314-2016-0001.

Теорема 1*). *В любой (необязательно конечной) группе число решений (необязательно конечной) системы уравнений с m неизвестными делится на наибольший общий делитель централизатора множества всех коэффициентов и числа $\frac{\Delta_m}{\Delta_{m-1}}$, где Δ_i — это наибольший общий делитель всех миноров порядка i матрицы системы. При этом подразумеваются следующие соглашения: $\Delta_i = 0$, если i больше, чем число уравнений; $\Delta_0 = 1$; $\frac{0}{0} = 0$.*

Наибольшим общим делителем НОД(G, n) группы G и целого числа n мы называем наименьшее общее кратное порядков подгрупп группы G, делящих n. Делимость всегда понимается в смысле кардинальной арифметики: каждый бесконечный кардинал делится на все меньшие ненулевые кардиналы (и, разумеется, ноль делится на все кардиналы, а на ноль делится только ноль). Это означает, что НОД$(G, 0) = |G|$ для любой группы G; а, например, НОД$(\mathbf{SL}_2(\mathbb{Z}), 2018) = 2$. Впрочем, читатель не очень много потеряет, если будет считать все группы в этой статье конечными, а в этом случае НОД$(G, n) =$ НОД$(|G|, n)$ по теореме Силова (и поскольку конечная p-группа содержит подгруппы всех возможных порядков).

Под *матрицей системы уравнений над группой* понимается целочисленная матрица $A = (a_{ij})$, где a_{ij} — это сумма показателей степеней при j-м неизвестном в i-м уравнении. Например, матрица системы уравнений

$$\begin{cases} xay^2[x,y]^{2019}(xby)^3 = 1 \\ bx^3y[x,y]^{100}(xby)^4 = 1 \\ [x,y^5]x^{-2} = 1 \end{cases}$$

(где x и y — неизвестные, а a и b — коэффициенты, то есть фиксированные элементы группы) имеет вид

$$\begin{pmatrix} 4 & 5 \\ 7 & 5 \\ -2 & 0 \end{pmatrix}.$$

Под *минорами порядка i* мы понимаем, как обычно, определители подматриц, составленных из элементов стоящих на пересечении каких-то i строк и i столбцов. В описанном выше примере миноров порядка m три (с точностью до знаков):

$$\det\begin{pmatrix} 4 & 5 \\ 7 & 5 \end{pmatrix} = -15, \quad \det\begin{pmatrix} 4 & 5 \\ -2 & 0 \end{pmatrix} = 10, \quad \det\begin{pmatrix} 7 & 5 \\ -2 & 0 \end{pmatrix} = 10,$$

а миноров порядка $m-1$ — шесть: 4, 5, 7, 5, −2, 0. Таким образом, теорема утверждает, что в этом примере число решений делится на

$$\text{НОД}\left(\frac{\text{НОД}(-15, 10, 10)}{\text{НОД}(4, 5, 7, 5, -2, 0)}, |C(a) \cap C(b)|\right) = \text{НОД}(5, |C(a) \cap C(b)|).$$

Отметим, что соглашения по поводу пограничных случаев, указанные в теореме, вполне естественны. Действительно, мы всегда можем добавить фиктивные уравнения 1=1 и добиться того, что число уравнений станет больше чем m. Мы можем также добавить новую переменную z и уравнение $z = 1$ (это не повлияет на число решений и сделает $m > 1$). Что касается философского вопроса об интерпретации частного $\frac{0}{0}$, то его можно понимать как угодно, например, читатель вправе считать, что $\frac{0}{0} = 2019$ — в любом случае наша теорема окажется верным утверждением (но более слабым, чем при нашей интерпретации).

Смысл величины $\frac{\Delta_m}{\Delta_{m-1}}$ состоит в следующем. Хорошо известно (смотрите, например, [Вин99]), что всякую целочисленную матрицу A обратимыми целочисленными элементарными преобразованиями строк и столбцов можно превратить в диагональную матрицу, причём диагональные элементы будут делить друг друга (каждый диагональный элемент будет делить следующий). Полученная диагональная матрица определяется однозначно с точностью до знаков диагональных элементов (и называется иногда *формой Смита* матрицы A); диагональные элементы формы Смита называют иногда *инвариантными множителями* матрицы A; они представляют собой частные $\frac{\Delta_i}{\Delta_{i-1}}$. Таким образом, в этой терминологии величина $\frac{\Delta_m}{\Delta_{m-1}}$ есть m-й инвариантный множитель матрицы системы уравнений. Можно ещё сказать так:

абсолютная величина частного $\frac{\Delta_m}{\Delta_{m-1}}$ есть период (экспонента) факторгруппы свободной абелевой группы $\mathbb{Z}^m$ по подгруппе, порождённой строками матрицы системы уравнений

(с той оговоркой, что это частное равно нулю тогда и только тогда, когда период бесконечен).

В качестве частных случаев теоремы 1 мы немедленно получаем теоремы Фробениуса и Соломона, а также их усиления, сформулированные выше.

Следующая теорема, на первый взгляд, не похожа ни на теорему Фробениуса, ни на теорему Соломона.

---

*) **Theorem 0** в журнальной версии.

Теорема Ивасаки [Iwa82]. *Для любого целого n число элементов конечной группы G, n-е степени которых лежат в данной подгруппе $H \subseteq G$, делится на $|H|$.*

Эта красивая теорема остаётся не очень широко известной (почему-то). В [SaAs07] было замечено, что делимость на $|H|$ имеет место и для числа решений «уравнения» $x^n \in HgH$, где HgH — любой двойной смежный класс по подгруппе H. Разумеется, в теореме Ивасаки и её обобщениях речь идёт уже не об уравнениях в обычном смысле. *Обобщённым уравнением* над группой G мы будем называть произвольную запись вида $w(x_1, \ldots, x_n) \in HgH$, где H — подгруппа группы $G \ni g$, а $w(x_1, \ldots, x_m)$ — элемент свободного произведения $G * F(x_1, \ldots, x_m)$ группы G и свободной группы; другими словами, w представляет собой слово в алфавите $G \sqcup \{x_1^{\pm 1}, \ldots, x_m^{\pm 1}\}$. Элементы группы G, встречающиеся в этом слове, мы называем *коэффициентами* обобщённого уравнения. Система обобщённых уравнений и решение этой системы определяются естественным образом. Матрица системы обобщённых уравнений определяется аналогично.

В [KM17] было получено следующее обобщение теоремы Ивасаки:

> *число решений любой системы обобщённых уравнений без коэффициентов, в правой части которой стоят двойные смежные классы по одной и той же подгруппе H* (например, $\{x^{100}y^{2019}[x,y]^4 \in Hg_1H, \quad [x^5, y^6]^7(xy)^8 \in Hg_2H, \ldots\}$) *делится на $|H|$.*

Теорема, которая включает в себя все сформулированные выше утверждения, звучит так.

Теорема 2 *). *Пусть S — (необязательно конечная) система обобщённых уравнений от конечного числа переменных $x_1, \ldots, x_m$ над группой G а P — её подсистема:*

$$S = \{u_i(x_1, \ldots, x_m) \in H_i g_i H_i \mid i \in I\} \supseteq P = \{u_j(x_1, \ldots, x_m) \in H_j g_j H_j \mid j \in J\},$$

(где $J \subseteq I, \quad u_i \in G * F(x_1, \ldots, x_m), \quad g_i \in G$, а H_i — *подгруппы группы G*). *Тогда число решений системы S в группе G делится на наибольший общий делитель подгруппы*

$$\widetilde{H} = \left(\bigcap_{j \in J} N(H_j g_j H_j) \right) \cap \left(\bigcap_{i \in I \setminus J} H_i \right) \cap (\text{централизатор множества всех коэффициентов системы } S)$$

и числа $\frac{\Delta_m}{\Delta_{m-1}}$, где Δ_k — это наибольший общий делитель всех миноров порядка k матрицы подсистемы P. Здесь и далее $N(A) \overset{\text{опр}}{=} \{g \in G \mid g^{-1}Ag = A\}$ — это нормализатор подмножества A группы G.

Чтобы получить из теоремы 2 теорему 1, достаточно переписать систему уравнений в «обобщённом» виде, то есть положить $S = P = \Big\{u_1(x_1, \ldots, x_m) \in \{1\}1\{1\}, \quad u_2(x_1, \ldots, x_m) \in \{1\}1\{1\}, \ldots\Big\}$ и заметить, что нормализатор тривиальной подгруппы — это вся группа.

С другой стороны, полагая

$$S = \Big\{u_1(x_1, \ldots, x_m) \in Hg_1H, \quad u_2(x_1, \ldots, x_m) \in Hg_2H, \ldots\Big\} \quad \text{и} \quad P = \varnothing \quad (\text{где } u_i \in F(x_1, \ldots, x_m)),$$

мы получаем упомянутое выше обобщение из [KM17] теоремы Ивасаки.

На самом деле, связь между теоремами Соломона и Ивасаки была установлена в [KM14] и [KM17], наше достижение состоит лишь в добавлении «фробениусовости». Основная теорема работы [KM17] говорит, что если имеется группа F с фиксированным эпиморфизмом на $\mathbb{Z}$ и некоторое множество гомоморфизмов из F в другую группу G, причём это множество инвариантно относительно некоторых естественных преобразований (зависящих от эпиморфизма $F \to \mathbb{Z}$ и подгруппы H группы G), то число рассматриваемых гомоморфизмов $F \to G$ делится на $|H|$. При подходящем выборе множества гомоморфизмов авторы [KM17] получают из своей основной теоремы и теорему Соломона, и теорему Ивасаки.

Наша основная теорема (смотрите параграф 1) представляет собой модулярный аналог основной теоремы из [KM17]: вместо фиксированного эпиморфизма $F \to \mathbb{Z}$ мы фиксируем эпиморфизм $F \to \mathbb{Z}/n\mathbb{Z}$. Можно сказать, что основная теорема этой статьи относится к основной теореме из [KM17] так же, как теорема 1 относится к упомянутому в начале статьи обобщению теоремы Соломона из [KM14]. Важную роль в доказательстве (а точнее, даже в корректности формулировки) основной теоремы играет одно элементарное, но не тривиальное, утверждение, принадлежащее Р. Брауэру [Bra69]. В последнем параграфе мы приводим доказательство леммы Брауэра, а в параграфе 5 доказываем основную теорему.

---

*) **Theorem 1** в журнальной версии.

Одним из следствий нашей основной теоремы является теорема 2 (которую мы доказываем в параграфе 2). В качестве другого следствия мы получаем некоторую теорему об уравнениях в кольцах (теорема 3 в параграфе 3), из которой вытекает, например, следующий факт, который можно рассматривать как обобщение теоремы Фробениуса в несколько ином направлении:
для любого представления $\rho: G \to \mathbf{GL}(V)$ группы G и любых слов $u_i(x_1,\dots,x_m) \in F(x_1,\dots,x_m)$

$$\text{число решений уравнения } \sum_{i=1}^{k}\Big(\rho\big(u_i(x_1,\dots,x_m)\big)\Big)^{l_i} = \mathrm{id} \quad \text{делится на } \begin{cases} \text{НОД}(G, \text{НОД}(\{l_i\})) & \text{всегда;} \\ \text{НОД}(G, \text{НОК}(\{l_i\})), & \text{если } k \leqslant m; \\ |G|, & \text{если } k < m. \end{cases}$$

В параграфе 4 мы выводим из основной теоремы некоторый факт о числе скрещенных гомоморфизмов, усиливающий ранее известные результаты. В предпоследнем параграфе мы обсуждаем открытые вопросы.

Авторы благодарят Савелия Скресанова за ценные замечания.

Обозначения и соглашения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем символом G' или $[G,G]$. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$, $\langle\langle X\rangle\rangle$, $C(X)$ и $N(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, нормальное замыкание множества X, централизатор множества X и нормализатор множества X. Индекс подгруппы H группы G обозначается $|G:H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. Если R — ассоциативное кольцо с единицей, то R^* обозначает группу обратимых элементов этого кольца. НОД и НОК — это наибольший общий делитель и наименьшее общее кратное. Символом $\exp(G)$ мы обозначаем период (экспоненту) группы G, если этот период конечен; и считаем $\exp(G) = 0$, если период бесконечен. Символ $\langle g\rangle_n$ обозначает циклическую группу порядка n, порождённую элементом g. Свободную группу ранга n мы обозначаем символом $F(x_1,\dots,x_n)$ или F_n. Символ $A * B$ обозначает свободное произведение групп A и B.

Кроме того, отметим ещё раз, что конечность групп нигде не предполагается по умолчанию, делимость всегда понимается в смысле кардинальной арифметики (бесконечный кардинал делится на все ненулевые кардиналы, не превосходящие его), а $\text{НОД}(G,n) \overset{\text{опр}}{=} \text{НОК}\left(\{|H| \;\mid\; H \text{ — подгруппа в } G \text{ и } |H| \text{ делит } n\}\right)$.

1. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}/n\mathbb{Z}$ (где $n \in \mathbb{Z}$) мы называем *n-индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}/n\mathbb{Z}$ мы называем *степенью* и обозначаем deg. Таким образом, для любого элемента f индексированной группы F определён элемент $\deg f \in \mathbb{Z}/n\mathbb{Z}$, причём группа F содержит элементы всех степеней и $\deg(fg) = \deg f + \deg g$ для любых $f, g \in F$.

Пусть имеется гомоморфизм $\varphi: F \to G$ из n-индексированной группы F в какую-то группу G и подгруппа H группы G. Подгруппу

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

называют *φ-сердцевиной* подгруппы H [KM17]. Другими словами, φ-сердцевина H_φ подгруппы H состоит из таких её элементов h, что $h^{\varphi(f)} \in H$ для всех f, причём $h^{\varphi(f)} = h$, если $\deg f = 0$.

Основная теорема. *Пусть целое число n делится на порядок подгруппы H некоторой группы G, и некоторое множество Φ гомоморфизмов из n-индексированной группы F в G удовлетворяет следующим условиям.*

I. *Φ инвариантно относительно сопряжения элементами из H:*

$$\text{если } h \in H \text{ и } \varphi \in \Phi, \text{ то гомоморфизм } \psi: f \mapsto \varphi(f)^h \text{ тоже лежит в } \Phi.$$

II. *Для любого $\varphi \in \Phi$ и любого элемента h из φ-сердцевины H_φ подгруппы H гомоморфизм ψ, определённый правилом*

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F \text{ степени ноль;} \\ \varphi(f)h & \text{для некоторого элемента } f \in F \text{ степени один (а, значит, и для всех элементов степени один),} \end{cases}$$

также содержится в Φ.

Тогда $|\Phi|$ делится на $|H|$.

Отметим, что отображение ψ из условия I является гомоморфизмом при любом $h \in G$. А формула для ψ из условия II определяет гомоморфизм при любых $h \in H_\varphi$ (как объясняется ниже). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ.

Лемма 0*⁾. *Пусть $\varphi: F \to G$ — гомоморфизм из n-индексированной группы F в группу G, $f_1 \in F$ — элемент степени один и $g \in G$. Тогда гомоморфизм $\psi: F \to G$ такой, что $\psi(f) = \varphi(f)$ для всех $f \in F$ степени ноль и $\psi(f_1) = \varphi(f_1)g$, существует тогда и только тогда, когда $g \in C(\varphi(\ker\deg))$ и $\bigl(\varphi(f_1)g\bigr)^n = \bigl(\varphi(f_1)\bigr)^n$.*

Доказательство. Группу F можно представить в виде

$$F \simeq \bigl(F_0 * \langle x\rangle_\infty\bigr) / \left\langle\!\left\langle \{u^x u^{-f_1} \mid u \in F_0\} \cup \{x^n f_1^{-n}\} \right\rangle\!\right\rangle, \quad \text{где } F_0 = \ker\deg .$$

Значит, отображение $\psi: F_0 \cup \{x\} \to G$ продолжается до гомоморфизма тогда и только тогда, когда его ограничение на F_0 есть гомоморфизм, а соотношения $u^x = u^{f_1}$ (при $u \in F_0$) и $x^n = f_1^n$ превращаются в истинные равенства в группе G:

$$\psi(u)^{\psi(x)} = \psi(u^{f_1}) \quad \text{и} \quad \psi(x)^n = \psi(f_1^n). \tag{$*$}$$

Если ограничение ψ на F_0 совпадает с ограничением гомоморфизма φ на F_0, а $\psi(x) = \varphi(f_1)g$, то первое из равенств $(*)$ эквивалентно тому, что g коммутирует с $\varphi(u)$ (при всех $u \in F_0$), а второе из равенств $(*)$ принимает вид $\bigl(\varphi(f_1)g\bigr)^n = \bigl(\varphi(f_1)\bigr)^n$. Лемма доказана.

Напомним ещё следующий красивый (но не очень широко известный) факт.

Лемма Брауэра [Bra69]. *Если U — конечная нормальная подгруппа группы V, то для всех $v \in V$ и $u \in U$ элементы $v^{|U|}$ и $(vu)^{|U|}$ сопряжены при помощи элемента из U.*

Из этих двух лемм немедленно вытекает, что отображение ψ из условия II основной теоремы является гомоморфизмом при всех $h \in H_\varphi$, поскольку $(\varphi(f)h)^n = (\varphi(f))^n$ по лемме Брауэра, применённой к

$$U = H_\varphi \subset V = H_\varphi \cdot \langle\varphi(f_1)\rangle \ni \varphi(f_1) = v.$$

Действительно, мы получаем равенство $\bigl(\varphi(f_1)h\bigr)^{|H_\varphi|} = \bigl(\varphi(f_1)\bigr)^{|H_\varphi|u}$ при некотором $u \in H_\varphi$ и, следовательно, $\bigl(\varphi(f_1)h\bigr)^n = \bigl(\varphi(f_1)\bigr)^{nu} = \bigl(\varphi(f_1^n)\bigr)^u$ (поскольку $|H_\varphi|$ делит n). Остаётся заметить, что $u \in H_\varphi$ коммутирует с $\varphi(f_1^n)$, поскольку $\deg f_1^n = n = 0 \in \mathbb{Z}/n\mathbb{Z}$. Таким образом, мы получаем равенство $\bigl(\varphi(f_1)h\bigr)^n = \bigl(\varphi(f_1)\bigr)^n$ и остаётся сослаться на лемму 0.

Отметим, что в случае $n = 0$ основная теорема была доказана в [KM17], поэтому наша теорема представляет собой «модулярный аналог» основного результата работы [KM17]. С другой стороны, нашу основную теорему мы выводим (в параграфе 5) из этого частного случая $n = 0$.

Лемма 1⁾.** *В условии II основной теоремы $\psi(f) \in \varphi(f)H_\varphi$ при всех $f \in F$.*

Доказательство. Действительно, если $\deg f = d$, то $f = f_1^d f_0$, где f_1 — (фиксированный) элемент степени один (о котором идёт речь в условии II), а f_0 — некоторый элемент степени ноль. Тогда

$$\psi(f) = \psi(f_1)^d \psi(f_0) = (\varphi(f_1)h)^d \varphi(f_0) \Longrightarrow \varphi(f_1)^d \varphi(f_0)h' = \varphi(f_1^d f_0)h' = \varphi(f)h',$$

где равенство $\Longrightarrow$ имеет место для некоторого $h' \in H_\varphi$, поскольку $h \in H_\varphi$ и $\varphi(F)$ нормализует H_φ.

2. Доказательство теоремы 2

Пусть $L \subseteq G$ — подгруппа, порождённая всеми коэффициентами системы S. Возьмём в качестве H произвольную подгруппу группы $\widetilde{H}$, порядок которой делит $n \overset{\text{опр}}{=} \frac{\Delta_m}{\Delta_{m-1}}$, и положим

$$F = L * F(x_1, \ldots, x_m) \quad \text{и} \quad \Phi = \Bigl\{\varphi: F \to G \;\Big|\; \varphi(f) = f \text{ при } f \in L \quad \text{и} \quad \varphi(u_i) \in H_i g_i H_i \text{ при } i \in I\Bigr\}.$$

В качестве индексации $\deg: F \to \mathbb{Z}/n\mathbb{Z}$ возьмём эпиморфизм, содержащий в своём ядре подгруппу L и все u_j, где $j \in J$. Такой эпиморфизм существует, поскольку число n есть период конечно порождённой абелевой группы $F/\bigl([F,F] \cdot L \cdot \langle\{u_j \mid j \in J\}\rangle\bigr)$.

Проверим, что условия основной теоремы выполнены. Условие I очевидно выполняется при всех $h \in H$ (и даже при всех $h \in \widetilde{H}$), поскольку подгруппа $\widetilde{H}$ по определению централизует подгруппу L и нормализует двойные смежные классы $H_i g_i H_i$.

Условие II тоже выполняется при всех $h \in H_\varphi$, так как

- на подгруппе L гомоморфизм ψ действует так же, как φ, поскольку L состоит из элементов степени ноль;
- $\psi(u_j) = \varphi(u_j)$ при $j \in J$, поскольку опять же $\deg u_j = 0$;
- а при $i \in I \setminus J$ мы имеем $\psi(u_i) \in \varphi(u_i)H_\varphi \subseteq \varphi(u_i)H_i$ (где включение $\in$ имеет место по лемме 1).

Таким образом, по основной теореме $|\Phi|$ делится на порядок любой подгруппы $H \subseteq \widetilde{H}$, порядок которой делит n, то есть $|\Phi|$ делится на НОД$(\widetilde{H}, n)$. Осталось заметить, что $|\Phi|$ есть число решений системы S.

---

*⁾ **Lemma 2** в журнальной версии.

⁾ **Lemma 3 в журнальной версии.

3. Кольца и представления

Под *обобщённо однородным по модулю* n уравнением с множеством неизвестных X над ассоциативным кольцом R с единицей мы понимаем конечную запись вида

$$\sum_i \prod_j c_{ij} x_{ij}^{k_{ij}} = 0, \quad \text{где } \textit{коэффициенты } c_{ij} \in R, \ \textit{неизвестные } x_{ij} \in X \text{ и } \textit{показатели } k_{ij} \in \mathbb{Z},$$

такую, что для некоторого отображения $\deg\colon X \to \mathbb{Z}/n\mathbb{Z}$ величина $\sum\limits_j k_{ij} \deg(x_{ij})$ (называемая *степенью уравнения*) не зависит от i (то есть «многочлен» в левой части уравнения является однородным относительно некоторого приписывания степеней переменным), причём $\langle\{\deg x \mid x \in X\}\rangle = \mathbb{Z}/n\mathbb{Z}$. Систему уравнений мы называем обобщённо однородной по модулю n, если все уравнения этой системы являются обобщённо однородными по модулю n (возможно разных степеней) относительно одной и той же функции $\deg\colon X \to \mathbb{Z}/n\mathbb{Z}$.

Ниже мы объясним, что множество $M = \{n \in \mathbb{Z} \mid \text{данная система обобщённо однородна по модулю } n\}$ состоит из всевозможных делителей некоторого числа n_0, которое мы будем называть *модулем однородности* данной системы. Другими словами, модуль однородности представляет собой наибольшее число из M или ноль, если множество M бесконечно.

Для поиска модуля однородности составим систему линейных однородных уравнений, где неизвестными будут степени переменных, а также степени уравнений (взятые со знаком минус); уравнения говорят, что степень монома равна степени соответствующего уравнения. Матрица этой системы линейных уравнений (которую мы будем называть *матрицей однородности* исходной системы уравнений) устроена следующим образом. Пусть $X = \{x_1, \dots, x_m\}$. *Матрица однородности* p*-го уравнения* — это целочисленная матрица $A_p = (a_{kl})$ размера

$$(\text{общее число мономов в системе}) \times \bigl(m + (\text{число уравнений})\bigr),$$

где при $l \leqslant m$ на (k,l)-м месте стоит сумма показателей степеней при l-м неизвестном в k-м мономе, $(m+p)$-й столбец состоит из единиц, а остальные столбцы нулевые при $l > m$. Тогда матрица однородности системы уравнений будет составлена из таких матриц A_p, записанных друг под другом: $A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \end{pmatrix}$. Например, для системы уравнений

$$\left\{ax^3y^2 + y^7bx - 1 = 0, \quad xy^2x + y^7x^5 = 0\right\} \quad (\text{где } a, b \in R \text{ — коэффициенты, а } x \text{ и } y \text{ — неизвестные}),$$

получаем следующую матрицу однородности:

$$A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 5 & 7 & 0 & 1 \end{pmatrix}, \quad \text{составленную из матриц} \quad A_1 = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ и } A_2 = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 5 & 7 & 0 & 1 \end{pmatrix}.$$

Лемма о модуле однородности. *Модуль однородности системы из s уравнений с m неизвестными над ассоциативным кольцом с единицей равен $\frac{\Delta_{m+s}}{\Delta_{m+s-1}}$, где Δ_i — это наибольший общий делитель всех миноров порядка i матрицы однородности данной системы уравнений. При этом подразумеваются следующие соглашения: $\Delta_i = 0$, если суммарное число мономов всех уравнений меньше, чем i; $\Delta_0 = 1$; $\frac{0}{0} = 0$.*

Доказательство. Пусть A — матрица однородности системы. Нас интересует максимальное число n такое, что система линейных однородных уравнений $AX = 0$ (от $m+s$ переменных) имеет решение в $\mathbb{Z}/n\mathbb{Z}$, компоненты которого порождают $\mathbb{Z}/n\mathbb{Z}$ как аддитивную группу (это эквивалентно тому, что первые m компонент решения порождают $\mathbb{Z}/n\mathbb{Z}$, поскольку последние s компонент решения выражаются через первые m компонент). Другими словами, n — это максимальный порядок циклической факторгруппы конечно порождённой абелевой группы $\mathbb{Z}^{m+s}/N$, где N — подгруппа, порождённая строками матрицы A. Как уже отмечалось, максимальный порядок n циклической факторгруппы группы $\mathbb{Z}^{m+s}/N$ равен $\frac{\Delta_{m+s}}{\Delta_{m+s-1}}$, что и требовалось.

Теорема 3*). *Пусть R — ассоциативное кольцо с единицей, а G — подгруппа мультипликативной группы этого кольца. Тогда для каждой системы уравнений над R от m неизвестных число её решений, лежащих в G^m, делится на наибольший общий делитель модуля однородности системы и пересечения группы G с централизатором множества всех коэффициентов системы.*

Доказательство. Пусть G_0 — пересечение группы G с централизатором множества всех коэффициентов системы и n — модуль однородности. Рассмотрим свободную группу $F(X)$ (где X — множество всех неизвестных нашей системы) и эпиморфизм $\deg\colon F(X) \to \mathbb{Z}/n\mathbb{Z}$.

---

*) **Theorem 4** в журнальной версии.

Применим основную теорему, взяв в качестве Φ множество всех гомоморфизмов $\varphi\colon F(X) \to G$ таких, что набор $(\varphi(x_1), \ldots, \varphi(x_m))$ является решением нашей системы уравнений (и, таким образом, число решений данной системы уравнений равно $|\Phi|$). В качестве H возьмём произвольную подгруппу группы G_0, порядок которой делит n. Условие I основной теоремы очевидно выполнено. Для проверки условия II выберем элемент $t \in F$ степени один и запишем каждую переменную x_i в виде $x_i = t^{\deg x_i} y_i$, где $y_i = t^{-\deg x_i} x_i$ имеет степень ноль. В новых обозначениях каждое уравнение $w(x_1, \ldots, x_m) = 0$ нашей системы примет вид $v(t, y_1, \ldots, y_m) = 0$, при этом каждое слагаемое в этом уравнении будет иметь одну и ту же сумму (по модулю n) показателей степеней у переменной t. Далее заметим, что если $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_m)) = 0$ и $h \in H_\varphi$, то $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_m)) = 0$. Это вытекает из делимости $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_m))$ (справа) на $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_m))$ в силу следующего факта.

Факт ([KM17], лемма 1). *Пусть M — моноид, $b_i, a, h \in M$, причём a и h обратимы, а элементы $a^{-s}ha^s$, где $s \in \mathbb{Z}$, коммутируют со всеми b_i. Тогда для выражения вида $u(t) = b_0 t^{m_1} b_1 \ldots t^{m_l} b_l$, где $m_i \in \mathbb{Z}$, имеет место равенство* $u(ah) = \begin{cases} h^{a^{-1}} h^{a^{-2}} \ldots h^{a^{-k}} u(a), & \text{если } k = \sum m_i > 0; \\ h^{-1} h^{-a} \ldots h^{-a^{-1-k}} u(a), & \text{если } k = \sum m_i < 0; \\ u(a), & \text{если } k = \sum m_i = 0. \end{cases}$

Этот факт следует применить к каждому моному выражения v. При ненулевом n нужно дополнительно воспользоваться тем, что t^n — элемент степени ноль, и $(\varphi(t)h)^n = (\varphi(t))^n$ согласно лемме 0.

Таким, образом, по основной теореме $|\Phi|$ (то есть число решений нашей системы уравнений) делится на $|H|$, что и требовалось (поскольку H — произвольная подгруппа централизатора множества всех коэффициентов, порядок которой делит модуль однородности).

Пример. *Если $\rho\colon G \to R^*$ — гомоморфизм из конечной группы G в мультипликативную группу ассоциативного кольца R с единицей* (например, $\rho\colon G \to \mathbf{GL}(V)$ — линейное представление группы G), *то для любых слов $u_i(x_1, \ldots, x_m) \in F(x_1, \ldots, x_m)$*

$$\textit{число решений уравнения } \sum_{i=1}^{k} \Big(\rho\big(u_i(x_1, \ldots, x_m)\big)\Big)^{l_i} = 1 \quad \textit{делится на } \begin{cases} \text{НОД}\big(G, \text{НОД}(\{l_i\})\big) & \textit{всегда;} \\ \text{НОД}\big(G, \text{НОК}(\{l_i\})\big), & \textit{если } k \leqslant m; \\ |G|, & \textit{если } k < m. \end{cases}$$

Чтобы в этом убедиться, достаточно применить теорему 3 к подгруппе $\rho(G) \subseteq R^*$. Матрица однородности этого уравнения имеет вид $B = \begin{pmatrix} & A & & 1 \\ & & & \vdots \\ 0 & \ldots & 0 & 1 \end{pmatrix}$, где последняя строка соответствует единице в правой части уравнения, а i-я строка матрицы A соответствует i-му слагаемому в левой части уравнения, и, стало быть, все элементы этой строки делятся на l_i. Осталось заметить, что j-й инвариантный множитель матрицы B совпадает с $(j-1)$-м инвариантным множителем матрицы A, и воспользоваться следующим фактом, который мы оставляем читателям в качестве несложного упражнения:

если i-я строка целочисленной матрицы $k \times m$ делится на l_i,

$$\textit{то } n\textit{-й инвариантный множитель этой матрицы} \begin{cases} \textit{делится на } \text{НОД}(\{l_i\}) & \textit{всегда;} \\ \textit{делится на } \text{НОК}(\{l_i\}) & \textit{при } k = m; \\ \textit{равен нулю} & \textit{при } k < m. \end{cases}$$

Отметим, что теорема 1 может быть получена, как следствие теоремы 3. Действительно, достаточно взять в качестве кольца R групповое кольцо $\mathbb{Z}G$ (которое очевидно содержит G в качестве подгруппы мультипликативной группы). Систему уравнений над G надо переписать в «кольцевом» виде: $\{w_i(x_1, \ldots) - 1 = 0\}$ и заметить, что величина $\frac{\Delta_m}{\Delta_{m-1}}$ из теоремы 1 превратится в точности в модуль однородности из леммы о модуле однородности.

4. Скрещенные гомоморфизмы

Пусть группа F действует (справа) на группе B автоморфизмами: $(f, b) \mapsto b^f$. Напомним, что *скрещенным гомоморфизмом* из F в B относительно этого действия называется отображение $\alpha\colon F \to B$ такое, что $\alpha(ff') = \alpha(f)^{f'} \alpha(f')$ для всех $f, f' \in F$. Савелий Скресанов заметил, что из основной теоремы легко выводится следующий факт, который был доказан в [ACNT13] (с использованием теории характеров) для случая, когда группы F и B конечны.

Теорема 4*). *Если группа F, допускающая эпиморфизм на $\mathbb{Z}/n\mathbb{Z}$, действует автоморфизмами на группе B, то число скрещенных гомоморфизмов $F \to B$ делится на* НОД(B, n).

Доказательство. Интересующее нас множество скрещенных гомоморфизмов находится во взаимно однозначном соответствии с множеством Φ (обычных) гомоморфизмов из F в полупрямое произведение $G = F \leftthreetimes B$

*) **Theorem 5** в журнальной версии.

(относительно данного действия) таких, что их композиция с проекцией $\pi: F \leftthreetimes B \to F$ есть тождественное отображение $F \to F$. Нам нужно показать, что $|\Phi|$ делится на $|H|$ для любой подгруппы $H \subseteq B$, порядок которой делит n (по определению числа НОД(B, n)).

Группа F по условию является n-индексированной. Поэтому доказываемое утверждение немедленно следует из основной теоремы. Условия основной теоремы выполнены по простым причинам: для условия I всё очевидно, поскольку $\pi(h^{-1}gh) = \pi(g)$; а условие II сразу вытекает из леммы 1, поскольку $\pi(gh) = \pi(g)$ (при $g \in G$ и $h \in H$).

5. Доказательство основной теоремы

Выберем элемент $f_1 \in F$ степени один, подгруппу $\ker\deg \subset F$ обозначим F_0 и рассмотрим полупрямое произведение $\widetilde{F} = \langle a\rangle_\infty \leftthreetimes F_0$, где a действует на F_0 так же, как f_1: $u^a = u^{f_1}$ при $u \in F_0$. Группа $\widetilde{F}$ обладает естественной индексацией (0-индексацией) $\deg: \widetilde{F} \to \mathbb{Z}$ (мы обозначаем её тем же символом deg). Ядро этого отображения есть F_0 и $\deg a = 1$. Кроме того, имеется естественный эпиморфизм $\alpha: \widetilde{F} \to F$, переводящий a в f_1, и тождественный на F_0. Проверим, что условия основной теоремы выполняются для множества $\widetilde{\Phi} = \{\varphi \circ \alpha \mid \varphi \in \Phi\}$ гомоморфизмов из $\widetilde{F}$ в G.

Условие I очевидно выполнено. Для проверки условия II выберем в качестве элемента степени один элемент $a \in \widetilde{F}$ и возьмём какой-то гомоморфизм $\widetilde{\varphi} = \varphi \circ \alpha \in \widetilde{\Phi}$ (где $\varphi \in \Phi$). Тогда гомоморфизм $\widetilde{\psi}$ из условия II имеет вид

$$\widetilde{\psi}(\widetilde{f}) = \begin{cases} \varphi(\widetilde{f}) & \text{для всех элементов } \widetilde{f} \in F_0; \\ \varphi(f_1)h & \text{при } \widetilde{f} = a; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_{\widetilde{\varphi}}. \tag{1}$$

Нам надо показать, что гомоморфизм $\widetilde{\psi}$ содержится в $\widetilde{\Phi}$, то есть имеет вид $\widetilde{\psi} = \varphi' \circ \alpha$, где $\varphi' \in \Phi$. Заметим, что $H_{\widetilde{\varphi}} = H_\varphi$, поскольку образы гомоморфизмов $\widetilde{\varphi} = \varphi \circ \alpha$ и φ совпадают, и образы элементов степени ноль при этих гомоморфизмах совпадают: $\widetilde{\varphi}(\ker\deg) = \widetilde{\varphi}(F_0) = \varphi(F_0)$. Формула (1) приобретает вид

$$\widetilde{\psi}(\widetilde{f}) = \begin{cases} \varphi(\widetilde{f}) & \text{для всех элементов } \widetilde{f} \in F_0; \\ \varphi(f_1)h & \text{при } \widetilde{f} = a; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_\varphi.$$

Это означает, что $\widetilde{\psi} = \psi \circ \alpha$, где

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F_0; \\ \varphi(f_1)h & \text{при } f = f_1; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_\varphi.$$

Гомоморфизм $\psi: F \to G$ лежит в Φ по условию II доказываемой теоремы. Следовательно, $\widetilde{\psi} \in \widetilde{\Phi}$. Таким образом, условия основной теоремы выполнены для множества $\widetilde{\Phi}$ гомоморфизмов из 0-индексированной группы $\widetilde{F}$ в G и, стало быть, $|\widetilde{\Phi}|$ делится на $|H|$ в силу основной теоремы работы [KM17]. Осталось заметить, что $|\Phi| = |\widetilde{\Phi}|$ в силу сюръективности гомоморфизма α. Теорема доказана.

Отметим, что мы не проверяли здесь, что отображение ψ задаёт гомоморфизм; это хоть и неочевидно, но всегда верно, смотрите параграф 1.

6. Открытые вопросы

Теоремы 1,2,3,4 утверждают, что некоторые величины делятся на частные двух целых чисел. Это может показаться удивительным, но мы не знаем, *можно ли заменить эти частные на их числители.*

Вопросы 1 и 2*). *Можно ли в теоремах 1 и 2 заменить частное Δ_m/Δ_{m-1} на его числитель Δ_m ?*

В случае системы уравнений без коэффициентов вопрос 1 превращается в следующий вопрос, который был впервые сформулирован в [AsYo93] (для конечных групп F и G):

верно ли, что число гомоморфизмов из конечно порождённой группы F в группу G всегда делится на НОД$(|F/F'|, G)$ *?*

Задача остаётся нерешённой даже для конечных групп (насколько мы знаем). Обзор некоторых результатов на эту тему можно найти в [AsTa01], например, известно, что ответ положительный, если группа F абелева [Yosh93].

Аналогичный вопрос возникает в связи с теоремой 3.

Вопрос 3)**. *Можно ли в теореме 3 заменить модуль однородности на на его числитель Δ_{m+s}* (смотрите лемму о модуле однородности)?

Что касается теоремы 4, то здесь тоже возникает аналогичный вопрос. Действительно, теорема 4 означает, в частности, что *если конечно порождённая группа F действует автоморфизмами на группе B, то число скрещенных гомоморфизмов $F \to B$ делится на* НОД$(\exp(F/F'), B)$.

---

*) **Questions 6 and 7** в журнальной версии.

) **Question 8 в журнальной версии.

Вопрос 4*⁾. *Можно ли в приведённом выше утверждении заменить период* $\exp(F/F')$ *факторгруппы по коммутанту на порядок этой факторгруппы?*

Этот вопрос был впервые сформулирован в [AsYo93] (для конечных групп F и B). Чтобы убедиться, что вопрос 4 аналогичен вопросу 1 достаточно вспомнить, что абсолютная величина частного Δ_m/Δ_{m-1} в вопросе 1 есть период факторгруппы свободной абелевой группы $\mathbb{Z}^m$ по подгруппе, порождённой строками матрицы системы уравнений, а абсолютная величина числителя Δ_m — это порядок этой факторгруппы.

7. Доказательство леммы Брауэра

Мы следуем оригинальному доказательству из [Bra69], но переводим его на более удобный (на наш взгляд) язык.

Лемма Брауэра [Bra69]. *Если* U *— конечная нормальная подгруппа группы* V*, то для всех* $v \in V$ *и* $u \in U$ *элементы* $v^{|U|}$ *и* $(vu)^{|U|}$ *сопряжены при помощи элемента из* U*.*

Доказательство. Группа $\mathbb{Z}$ действует перестановками на подгруппе U по формуле

$$a \circ i = v^{-i}a(vu)^i, \quad (\text{где } i \in \mathbb{Z} \text{ и } a \in U).$$

Пусть m — минимальная длина орбиты. Другими словами m — это минимальная длина цикла в разложении перестановки $a \mapsto v^{-1}avu$ (на множестве U) на независимые циклы. Тогда множество $X = \{a \in U \mid a \circ m = a\}$ представляет собой объединение всех орбит длины m, поэтому $|X|$ делится на m. С другой стороны, (по определению нашего действия) $X = \{a \in U \mid v^{-m}a(vu)^m = a\} = \{a \in U \mid a^{-1}v^m a = (vu)^m\}$ и, стало быть, $|X|$ есть порядок централизатора элемента v^m в U (поскольку в любой группе непустое множество вида $\{x \mid x^{-1}yx = z\}$ является смежным классом по централизатору элемента y). Значит $|X|$ делит $|U|$ и, следовательно, m делит $|U|$. Таким образом, $a \circ |U| = a = a$ (если a лежит в орбите длины m), что и требовалось.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Вин99] Э. Б. Винберг, Курс алгебры, М. «Факториал», 1999.

[Стру95] С. П. Струнков, К теории уравнений на конечных группах, Изв. РАН., Сер. матем., 59:6 (1995), 171-180.

[AmV11] A. Amit, U. Vishne, Characters and solutions to equations in finite groups, J. Algebra Appl., 10:4 (2011), 675-686.

[And16] R. Andreev, A translation of "Verallgemeinerung des Sylow'schen Satzes" by F. G. Frobenius. arXiv:1608.08813.

[ACNT13] T. Asai, N. Chigira, T. Niwasaki, Yu. Takegahara, On a theorem of P. Hall, Journal of Group Theory, 16:1 (2013), 69-80.

[AsTa01] T. Asai, Yu. Takegahara, $|\mathrm{Hom}(A,G)|$, IV, J. Algebra, 246 (2001), 543-563.

[AsYo93] T. Asai, T. Yoshida, $|\mathrm{Hom}(A,G)|$, II, J. Algebra, 160 (1993), 273-285.

[Bra69] R. Brauer, On A Theorem of Frobenius, The American Mathematical Monthly, 76:1 (1969), 12-15.

[BrTh88] K. Brown, J. Thévenaz, A generalization of Sylow's third theorem, J. Algebra, 115 (1988), 414-430.

[Frob95] F. G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin) (1895), 981-993.

[Frob03] F. G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin) (1903), 987-991.

[GRV12] C. Gordon, F. Rodriguez-Villegas, On the divisibility of $\#\mathrm{Hom}(\Gamma,G)$ by $|G|$, J. Algebra, 350:1 (2012), 300-307. См. также arXiv::1105.6066.

[Hall36] Ph. Hall, On a theorem of Frobenius, Proc. London Math. Soc. 40 (1936), 468-501.

[Isaa70] I. M. Isaacs, Systems of equations and generalized characters in groups, Canad. J. Math., 22 (1970), 1040-1046.

[Iwa82] S. Iwasaki, A note on the nth roots ratio of a subgroup of a finite group, J. Algebra, 78:2 (1982), 460-474.

[KM14] A. A. Klyachko, A. A. Mkrtchyan, How many tuples of group elements have a given property? With an appendix by Dmitrii V. Trushin, Intern. J. of Algebra and Comp. 24:4 (2014), 413-428. См. также arXiv:1205.2824.

[KM17] A. A. Klyachko, A. A. Mkrtchyan, Strange divisibility in groups and rings, Arch. Math. 108:5 (2017), 441-451. См. также arXiv::1506.08967.

[Kula38] A. Kulakoff, Einige Bemerkungen zur Arbeit: "On a theorem of Frobenius" von P. Hall, Матем. сб., 3(45):2 (1938), 403-405.

[SaAs07] J. Sato, T. Asai, On the n-th roots of a double coset of a finite group, J. School Sci. Eng., Kinki Univ., 43 (2007), 1-4.

[Sehg62] S. K. Sehgal, On P. Hall's generalisation of a theorem of Frobenius, Proc. Glasgow Math. Assoc., 5 (1962), 97-100.

[Solo69] L. Solomon, The solution of equations in groups, Arch. Math., 20:3 (1969), 241-247.

[Yosh93] T. Yoshida, $|\mathrm{Hom}(A,G)|$, Journal of Algebra, 156:1 (1993), 125-156.

*⁾ **Question 9** в журнальной версии.