УДК 512.542.1 + 512.543.1 + 512.552.18 MSC: 20D60, 20F05, 20F70, 16P10, 16U60

СТРАННАЯ ДЕЛИМОСТЬ В ГРУППАХ И В КОЛЬЦАХ

Антон А. Клячко$^\sharp$ Анна А. Мкртчян$^\flat$

$^\sharp$*Механико-математический факультет Московского государственного университета*
Москва 119991, Ленинские горы, МГУ
klyachko@mech.math.msu.su
$^\flat$*University of Edinburgh, School of Mathematics, Room 5402, James Clerk Maxwell Building, King's Buildings, Edinburgh, EH9 3JZ*
anna.mkr@gmail.com

Мы доказываем одну общую теорему о делимости, из которой вытекает, например, что в любой группе число порождающих пар (и троек, и четвёрок...) всегда делится на порядок коммутанта этой группы. Другое следствие говорит, что число пифагоровых троек (и четвёрок, и пятёрок...) обратимых элементов в ассоциативном кольце всегда делится на порядок мультипликативной группы этого кольца.

0. Введение

Отправной точкой нашего исследования послужил следующий результат, обобщающий одну старую теорему Соломона [Solo69].

Теорема Гордона–Родригеса-Виллегаса [GRV12]. *Пусть F — конечно порождённая группа с бесконечным индексом коммутанта, а G — произвольная группа. Тогда число гомоморфизмов $F \to G$ делится на порядок группы G.*

Эта теорема говорит, по сути, о числе решений систем бескоэффициентных уравнений в группе. В работе [KM14] этот результат был обобщен на системы уравнений с коэффициентами и даже на произвольные формулы первого порядка в групповом языке (с константами).

Основная теорема настоящей работы претендует на звание «максимального» обобщения результата Гордона–Родригеса-Виллегаса (хотя такую максимальность доказать невозможно). Формулировку основной теоремы читатель может найти в первом параграфе, а её (вполне элементарное) доказательство — в последнем. Грубо говоря, основная теорема утверждает, что делимость сохранится, если рассматривать не все гомоморфизмы, а их подмножество, от которого требуется инвариантность относительно некоторых естественных операциях над гомоморфизмами. Одним из следствий основной теоремы является неожиданный факт, упомянутый в аннотации:

в любой группе G число порождающих наборов $(g_1, \ldots, g_{2017}) \in G^{2017}$ (то есть таких наборов, что $G = \langle g_1, \ldots, g_{2017}\rangle$) всегда делится на порядок коммутанта группы G.

Это и иные теоретико-групповые следствия мы доказываем в параграфе 2. Удивительно, но этот результат кажется новым, хотя известно много близких фактов о делимости функции Мёбиуса (которая связана с числом порождающих наборов формулой Холла [Hall36]), см., например, [Bro00], [HIÖ89], [KT84] и литературу там цитируемую). О других не очень широко известных, но красивых фактах о системах порождающих в группах мы советуем почитать в [Coll10].

Основная теорема является утверждением о группах, но (как это ни парадоксально) имеет нетривиальные теоретико-кольцевые следствия. В параграфе 3 мы выводим из основной теоремы теоретико-кольцевой аналог теоремы Гордона–Родригеса-Виллегаса (точнее говоря, аналог обобщения этой теоремы, полученного в [KM14] и говорящего об уравнениях с коэффициентами). Частным случаем этой теоремы об уравнениях над кольцами является факт, упомянутый в аннотации, или, например, следующее утверждение высшего порядка:

в любом ассоциативном кольце R с единицей число наборов обратимых элементов $(a, b, \ldots, z) \in (R^*)^{26}$ таких, что $a^{2017} + b^{2017} + \ldots + z^{2017} = 0$, делится на порядок мультипликативной группы этого кольца, то есть на $|R^*|$.

Обозначения, 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 G'. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$, $\langle\langle X\rangle\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, нормальное замыкание множества X и централизатор множества X. Индекс подгруппы H группы G обозначается $|G : H|$. Символ $N(H)$ обозначает нормализатор подгруппы H (в группе G). Свободное произведение групп A и B мы обозначаем символом $A * B$, а свободную группу с базисом $x_1, \ldots, x_n$ — символом $F(x_1, \ldots, x_n)$. Если R — ассоциативное кольцо с единицей, то R^* обозначает группу обратимых элементов этого кольца.

Работа первого автора выполнена при поддержке Российского фонда фундаментальных исследований, грант №15-01-05823.

Отметим ещё, что в почти всех утверждениях о делимости в данной работе (например, в вышеупомянутой теореме Гордона–Родригеса-Виллегаса) необязательно предполагать, что соответствующая группа конечна. Делимость можно понимать в смысле кардинальной арифметики: бесконечный кардинал делится на все ненулевые кардиналы, не превосходящие его. Единственное место, где нам действительно нужна конечность — это теорема о мономорфизмах и подгруппах в параграфе 2, смотрите замечание после этой теоремы.

Авторы благодарят Э. Б. Винберга за вопрос, из ответа на который выросла эта статья, а также Андрея В. Васильева за ценное указание (смотрите замечание в параграфе 2) и анонимного рецензента за ряд комментариев, позволивших нам улучшить текст.

1. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}$ мы называем *индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}$ мы называем *степенью* и обозначаем deg; таким образом, для любого элемента f индексированной группы F определено целое число $\deg f$, причём группа F содержит элементы всех целых степеней и $\deg(fg) = \deg f + \deg g$ для любых $f, g \in F$.

Пусть имеется гомоморфизм $\varphi\colon F \to G$ из индексированной группы F в какую-то группу G и подгруппа H группы G. Мы называем подгруппу

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

φ-сердцевиной подгруппы H. 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 H — подгруппа некоторой группы G и Φ — некоторое множество гомоморфизмов из индексированной группы F в G, причём множество Φ обладает следующими двумя свойствами.*

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

если $h \in H$ и $\varphi \in \Phi$, то гомоморфизм $\psi\colon f \mapsto \varphi(f)^h$ тоже лежит в Φ.

II. *Для любого $\varphi \in \Phi$ 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 любом $h \in C(\varphi(\ker \deg))$ (смотрите лемму 0). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ (при некоторых дополнительных предположениях об h).

Лемма 0. *Пусть $\varphi\colon F \to G$ — это гомоморфизм из индексированной группы F в некоторую группу G, f_1 — элемент степени один группы F и $g \in G$. Тогда*

1) *гомоморфизм $\psi\colon F \to G$ такой, что $\psi(f) = \varphi(f)$ для всех f степени ноль и $\psi(f_1) = \varphi(f_1)g$, существует тогда и только тогда, когда $g \in C(\varphi(\ker \deg))$;*
2) *если такой гомоморфизм ψ существует и H — это подгруппа в G, то $\psi(f)H = \varphi(f)H$ для всех $f \in F$ тогда и только тогда, когда $g \in H_\varphi$.*

Доказательство. Заметим, что F раскладывается в полупрямое произведение $F = \langle f_1 \rangle_\infty \leftthreetimes \ker \deg$. Это означает, что отображение $\alpha\colon \ker \deg \cup \{f_1\} \to G$ продолжается до гомоморфизма тогда и только тогда, гкогда его ограничение на $\ker \deg$ является гомоморфизмом и $\alpha(f^{f_1}) = \alpha(f)^{\alpha(f_1)}$ для всех $f \in \ker \deg$. Таким образом, для всех $f \in \ker \deg$ мы имеем $\psi(f^{f_1}) = \varphi(f^{f_1}) = \varphi(f)^{\varphi(f_1)}$ и $\psi(f)^{\psi(f_1)} = \varphi(f)^{\varphi(f_1)g}$. Значит, $\psi(f^{f_1}) = \psi(f)^{\psi(f_1)}$ для всех $f \in \ker \deg$ тогда и только тогда, когда $\varphi(x)^g = \varphi(x)$ для всех $x \in \ker \deg$. Это доказывает первое утверждение.

Чтобы доказать 2), заметим, что каждый $f \in F$ имеет вид $f = f_1^k x$, где $x \in \ker \deg$ и $k \in \mathbb{Z}$. Таким образом,

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

(где равенство $=\!=\!=$ выполняется, поскольку $\varphi(F)$ нормализует H_φ и $g \in H_\varphi \subseteq H$). Это доказывает утверждение 2) в одну сторону. Доказательство в другую сторону мы оставляем читателям в качестве упражнения (поскольку мы не будем это использовать).

2. Применения. Группы

Прежде всего заметим, что условия основной теоремы очевидно выполняются, если в качестве Φ взять множество всех гомоморфизмов $F \to G$ (а в качестве H взять любую подгруппу группы G, например, всю группу G). Поэтому теорема Гордона–Родригеса-Виллегаса является простейшим частным случаем основной теоремы.

Теорема об уравнениях над группами [KM14]. *Число решений системы уравнений $\{v_i(x_1, \dots, x_n) = 1\}$ над группой G (где $v_i(x_1, \dots, x_n) \in G * F(x_1, \dots, x_n)$) делится на порядок централизатора множества всех коэффициентов, если ранг матрицы, состоящей из сумм показателей при i-м неизвестном в j-м уравнении, меньше числа неизвестных.*

Доказательство. Пусть $A \subseteq G$ — подгруппа, порождённая всеми коэффициентами всех уравнений. В качестве группы F мы возьмём факторгруппу $F = (A * F(x_1, \dots, x_n))/\langle\langle\{v_i\}\rangle\rangle$ свободного произведения $A * F(x_1, \dots, x_n)$ группы A и свободной группы по нормальной подгруппе $\langle\langle\{v_i\}\rangle\rangle$, порождённой левыми частями уравнений. В качестве множества Φ мы рассмотрим гомоморфизмы $F \to G$, тождественные на A. (Мы предполагаем, что A вкладывается в F посредством естественного отображения $A \to F$, поскольку если это отображение не инъективно, то решений нет и доказывать нечего.) Ясно, что решения системы уравнений находятся в естественном взаимно однозначном соответствии с элементами множества Φ.

Условие на ранг означает, что группа F обладает эпиморфизмом на $\mathbb{Z}$, ядро которого содержит A. Если теперь в качестве H взять централизатор подгруппы A в G, то условия основной теоремы окажутся очевидным образом выполненными. Действительно, I выполняется, поскольку h централизует $A \subseteq G$ и, следовательно, ψ совпадает с φ на $A \subset F$, а II выполнено, поскольку элементы из $A \subset F$ имеют степень ноль и, значит, опять ψ совпадает с φ на $A \subset F$.

Теорема о корне из подгруппы [KM14]. *Число элементов g произвольной группы G таких, что $g^n \in H$, делится на $|H|$ для любой подгруппы H группы G и любого целого n.*[*)]

Теорема о корне из подгруппы является простейшим частным случаем следующего факта.

Теорема о гомоморфизмах и подгруппах [KM14]. *Пусть H — подгруппа группы G, а W — подгруппа (или подмножество) конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(W) \subseteq H$, делится на $|H|$.*

Мы докажем ещё более общее утверждение.

Теорема о гомоморфизмах и двойных смежных классах. *Пусть H — подгруппа группы G, а W — подмножество конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Пусть $W \ni w \mapsto g_w \in G$ — произвольное отображение $W \to G$. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(w) \in Hg_wH$ для всех $w \in W$, делится на $|H|$.*

Доказательство. Выберем какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ (который существует, поскольку F/F' является бесконечной конечно порождённой абелевой группой) и возьмём в основной теореме в качестве Φ множество всех гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(w) \in Hg_wH$ для всех $w \in W$. Условия основной теоремы выполняются. Для условия I это совсем очевидно. А что касается условия II, то достаточно заметить, что из формулы для ψ вытекает равенство $\psi(f)H = \varphi(f)H$ для всех $f \in F$ по лемме 0.

Следующую теорему можно назвать «эпиморфным аналогом» теоремы Гордона–Родригеса-Виллегаса.

Теорема об эпиморфизмах. *Пусть F — конечно порождённая группа с бесконечным индексом коммутанта, а G — произвольная группа. Тогда число сюръективных гомоморфизмов $F \to G$ делится на порядок коммутанта группы G.*

Доказательство. Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$, возьмём качестве Φ множество всех эпиморфизмов $F \to G$ и положим $H = G'$. Проверим, что условия основной теоремы выполняются. Для условия I это очевидно.

Проверим условие II. Мы должны показать, что для любого эпиморфизма $\varphi\colon F \to G$ и любого элемента $h \in G'$, централизующего подгруппу $\varphi(\ker\deg)$, гомоморфизм ψ, определённый равенствами из условия II основной теоремы является сюръективным. По модулю G' гомоморфизм ψ сюръективен (то есть $\psi(F)G' = G$), поскольку он равен φ по модулю G'. Осталось показать, что каждый элемент $g \in G'$ лежит в образе гомоморфизма ψ. Пользуясь сюръективностью гомоморфизма φ, найдём $f \in F$ такой, что $\varphi(f) = g$; причём элемент f можно найти в коммутанте группы F (поскольку для эпиморфизма образ коммутанта равен коммутанту образа). Но тогда $f \in \ker\deg$ и, следовательно, $\psi(f) = \varphi(f) = g$, что и требовалось.

Замечание. Число сюръективных гомоморфизмов $F \to G$ делится на $|\mathrm{Aut}\,G|$, поскольку $\mathrm{Aut}\,G$ естественным образом точно действует на множестве эпиморфизмов $F \to G$. Однако теорема об эпиморфизмах не вытекает немедленно из этого наблюдения, поскольку, как нам любезно подсказал А. В. Васильев,

существует группа G такая, что $|\mathrm{Aut}\,G|$ не делится на $|G'|$.

[*)] В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

Примерами таких групп могут служить группы $3 \cdot A_6$ и $3 \cdot A_7$ (см., например, [Wils09]) порядков $\frac{3}{2} \cdot 6! = 1080$ и $\frac{3}{2} \cdot 7! = 7560$, совпадающие с коммутантами и имеющие центры порядка три, факторгруппы по которым суть знакопеременные группы A_6 и A_7; при этом $|\mathrm{Aut}(3 \cdot A_6)| = 2 \cdot 6!$, а $\mathrm{Aut}(3 \cdot A_7)$ есть просто симметрическая группа порядка $7!$. На самом деле, как показали Савелий Скресанов и Дмитрий Чуриков (с помощью GAPа), наименьшая группа G такая, что $|G'| \not| \, |\mathrm{Aut}\, G|$ имеет порядок 108.

Следствие о системах порождающих в группах. *Для каждой группы G и для каждого натурального числа n число наборов $(g_1, \ldots, g_n) \in G^n$ элементов группы G, порождающих группу G (то есть таких наборов, что $\langle g_1, \ldots, g_n \rangle = G$), всегда делится на $|G'|$.*

Доказательство. Порождающие наборы длины n находятся в естественном взаимно однозначном соответствии с эпиморфизмами из свободной группы ранга n в G. Поэтому утверждение немедленно вытекает из теоремы об эпиморфизмах.

Разумеется, ни в теореме об эпиморфизмах, ни в её следствии делимость на $|G'|$ нельзя усилить до делимости на $|G|$, как показывает пример группы простого порядка — число порождающих наборов длины n в такой группе очевидно равно $|G|^n - 1$.

Следующая теорема обобщает предыдущую и является аналогом теоремы о гомоморфизмах и подгруппах.

Теорема об эпиморфизмах и подгруппах. *Пусть A — подгруппа группы G и W — подгруппа конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(W) = A$, делится на $|A'|$.*

Доказательство. Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ и положим

$$\Phi = \{\text{гомоморфизмы } \varphi\colon F \to G \text{ такие, что } \varphi(W) = A\} \quad \text{и} \quad H = A'.$$

Проверим, что условия основной теоремы выполняются. Для условия I это очевидно.

Проверим условие II. Мы должны показать, что для любого гомоморфизма $\varphi\colon F \to G$ такого, что $\varphi(W) = A$, и любого элемента $h \in A'$, централизующего подгруппу $\varphi(\ker \deg)$, гомоморфизм ψ, определённый равенствами из условия II, также удовлетворяет равенству $\psi(W) = A$. Включение $\psi(W) \subseteq A$, разумеется, выполняется. Для доказательства обратного включения сперва заметим, что ограничение гомоморфизма $\psi(W)A' = A$. Осталось показать, что каждый элемент $a \in A'$ лежит в $\psi(W)$. Воспользовавшись равенством $\varphi(W) = A$, найдём $w \in W$ такой, что $\varphi(w) = a$; ясно, что такой w можно найти в коммутанте группы W. Но тогда $w \in \ker \deg$ и, следовательно, $\psi(w) = \varphi(w) = a$, что и требовалось.

Аналогичная теорема об инъективных гомоморфизмах тоже верна (для конечных групп G), причём с гораздо более хорошей делимостью.

Теорема о мономорфизмах и подгруппах. *Пусть A — подгруппа группы G, а W — подгруппа конечно порождённой группы F и индекс $|F : F'W|$ бесконечен. Тогда $|N(A)|$ делит следующие числа:*

а) *число гомоморфизмов $\varphi\colon F \to G$ таких, что ограничение φ на W инъективно и $\varphi(W) \subseteq A$;*

б) *число гомоморфизмов $\varphi\colon F \to G$ таких, что ограничение φ на W инъективно и $\varphi(W) = A$;*

Доказательство. Докажем а) (доказательство для б) вполне аналогично). Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ такой, что $W \subseteq \ker \deg$ и положим

$$\Phi = \{\text{гомоморфизмы } \varphi\colon F \to G \text{ такие, что } \varphi(W) \subseteq A \text{ и } \varphi|_W \text{ инъективно}\} \quad \text{и} \quad H = N(A).$$

Проверим, что условия основной теоремы выполняются. Для условия I это очевидно. Условие II также очевидно, поскольку W содержится в ядре гомоморфизма deg и, следовательно, ψ и φ (из условия II) одинаково действуют на элементы подгруппы W.

Замечание. Условие бесконечности индекса $|F : WF'|$ нельзя заменить в последней теореме на бесконечность индекса коммутанта (несмотря на то, что делимость мы понимаем в смысле кардинальной арифметики). Действительно,

а) если $F = W = A = \mathbb{Z}$ and $G = \mathbb{R}$, то число инъективных гомоморфизмов равно $\aleph_0$ и не делится на $|N(A)| = |\mathbb{R}| = 2^{\aleph_0}$;

б) если $F = W = G = A = \mathbb{Z}$, то число инъективных гомоморфизмов равно двум и не делится на $|N(A)| = |\mathbb{Z}| = \aleph_0$.

3. Применения. Кольца

Под *обобщённо однородным* уравнением над ассоциативным кольцом R с множеством неизвестных X 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 ненулевого отображения $\deg\colon X \to \mathbb{Z}$ величина $\sum\limits_j k_{ij} \deg(x_{ij})$ не зависит от i (то есть «многочлен» в левой части уравнения является однородным относительно некоторого ненулевого приписывания степеней переменным*)). Систему уравнений мы называем обобщённо однородной, если все уравнения этой системы являются обобщённо однородными (возможно разных степеней) относительно одной и той же функции $\deg\colon X \to \mathbb{Z}$.

Для проверки обобщённой однородности можно воспользоваться следующим простым алгоритмом.

АЛГОРИТМ ПРОВЕРКИ ОБОБЩЁННОЙ ОДНОРОДНОСТИ СИСТЕМЫ

1. Для каждого уравнения $v = 0$ системы составить матрицу A_v из целых чисел a_{ij}, представляющих собой степени i-го монома относительно j-го неизвестного (то есть a_{ij} есть сумма показателей в i-м мономе выражения v при j-м неизвестном).
2. Вычесть из всех строк матрицы A_v первую строку этой матрицы. Сделать это для всех матриц A_v.
3. Получившиеся матрицы A'_v (с нулевыми первыми строками) написать друг под другом: $A' = \begin{pmatrix} A'_v \\ A'_w \\ \vdots \end{pmatrix}$.
4. Система обобщённо однородна тогда и только тогда, когда $\operatorname{rank} A'$ меньше числа неизвестных.

Например, для системы уравнений $\begin{cases} (xdy)^2 - yx^2 + xy^2cy^{-100}x = 0 \\ xy - yx = 0 \end{cases}$ (где $c, d \in R$ — коэффициенты, а x и y — неизвестные) мы получаем:

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

$\operatorname{rank} A' = 1$ и система является обобщённо однородной.

Утверждение. *Всякая система уравнений, в которой*

$$\sum_i \Big((\textit{число мономов в } i\textit{-м уравнении}) - 1 \Big) < (\textit{число неизвестных}),$$

является обобщённо однородной.

Доказательство. Утверждение немедленно вытекает из приведённого выше алгоритма, но доказательство корректности этого алгоритма мы оставляем читателю в качестве упражнения. (В дальнейшем мы не будем использовать ни это утверждение, ни этот алгоритм.)

Понятие *решения* системы уравнений определяется естественным образом (если среди показателей k_{ij} есть отрицательные числа, то соответствующие компоненты решения обязаны быть обратимыми элементами кольца).

Теорема об уравнениях над кольцами. *Пусть R — ассоциативное кольцо с единицей, и G — подгруппа мультипликативной группы этого кольца. Тогда для каждой обобщённо однородной системы уравнений над R от n неизвестных число её решений, лежащих в G^n, делится на порядок пересечения группы G с централизатором множества всех коэффициентов системы.*

Доказательство. Нужно применить основную теорему, взяв в качестве F свободную группу $F(x_1, \ldots, x_n)$ и продолжить отображение $\deg\colon \{x_1, \ldots, x_n\} \to \mathbb{Z}$ (из определения обобщённо однородной системы) до гомоморфизма $F \to \mathbb{Z}$, который можно считать сюръективным, поскольку он ненулевой. В качестве Φ следует взять множество всех гомоморфизмов $\varphi\colon F \to G$ таких, что набор $(\varphi(x_1), \ldots, \varphi(x_n))$ является решением нашей системы уравнений, а в качестве H следует взять пересечение группы G с централизатором множества всех коэффициентов системы.

---

*) Переменная может иметь степень ноль, но важно, что не все переменные имеют степень ноль.

Проверим, что условия основной теоремы выполнены. Условие I 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.

Рассмотрим уравнение $w(x_1, \ldots, x_n) = 0$ нашей системы. В новых обозначениях оно перепишется в виде $v(t, y_1, \ldots, y_n) = 0$, причём в силу однородности каждое слагаемое в выражении $v(t, y_1, \ldots, y_n)$ будет иметь одну и ту же степень k относительно переменной t.

Нам надо показать, что если $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_n)) = 0$ и $h \in H_\varphi$, то $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_n)) = 0$. Чтобы в этом убедиться достаточно заметить, что $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_n))$ делится (справа) на $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_n))$ в силу следующей леммы (которую следует применить к каждому моному выражения v).

Лемма 1. *Пусть M — моноид, $b_i, a, h \in M$, причём a и h обратимы, а элементы $a^{-s} h a^s$, где $s \in \mathbb{Z}$, коммутируют со всеми b_i. Тогда для выражения вида*

$$u(t) = b_0 t^{n_1} b_1 \ldots t^{n_l} b_l, \quad \text{где } n_i \in \mathbb{Z},$$

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

Доказательство. Пользуясь правилами коммутирования $a^i h^{a^j} = h^{a^{j-i}} a^i$ и $b_i h^{a^j} = h^{a^j} b_i$, будем последовательно передвигать все буквы h (и h^{a^j}) в слове $u(ah)$ влево и получим то, что требуется. Это завершает доказательство леммы 1 и теоремы об уравнениях над кольцами.

Пример. *Число пифагоровых троек обратимых элементов ассоциативного кольца с единицей, то есть число обратимых решений уравнения*

$$x^2 + y^2 = z^2$$

всегда делится на порядок мультипликативной группы этого кольца.
Действительно, уравнение однородно, а в качестве G следует взять мультипликативную группу кольца R. Более того,
число обратимых решений уравнения

$$ax^k + by^l + cz^m + dt^n + \ldots = 0$$

делится на $|R^*|$ при любых фиксированных $a, b, c, d, \ldots, k, l, m, \ldots \in \mathbb{Z}$,
поскольку это уравнение является обобщённо однородным.

4. Доказательство основной теоремы

Наше доказательство в некотором смысле похоже на рассуждение, которое содержится в конце параграфа 3 работы [KM14]. Чтобы подчеркнуть эту аналогию, мы будем использовать те же термины, что в [KM14] (но означать они будут другие понятия, строго говоря).

Хвостом гомоморфизма $\varphi \in \Phi$ мы будем называть пару (φ_0, φ_H), где φ_0 — это ограничение гомоморфизма φ на подгруппу $\ker\deg \subset F$, а $\varphi_H\colon F \to \{gH \ ; \ g \in G\}$ — это отображение из F в множество левых смежных классов группы G по подгруппе H, которое переводит элемент $f \in F$ в класс $\varphi(f)H$.

Мы будем говорить, что два гомоморфизма $\varphi, \psi \in \Phi$ *похожи* и писать $\varphi \sim \psi$, если их хвосты сопряжены при помощи элемента из H, то есть

$$\varphi \sim \psi \iff \text{найдётся } h \in H \text{ такой, что } \begin{array}{ll} \psi(f) = h\varphi(f)h^{-1} & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = h\varphi(f)H & \text{для всех } f \in F. \end{array}$$

Ясно, что похожесть — это отношение эквивалентности на Φ. Основная теорема немедленно вытекает из следующего утверждения.

Утверждение. *В каждом классе похожих гомоморфизмов из Φ содержится ровно $|H|$ элементов. Более точно, для каждого $\varphi \in \Phi$*
1) *число различных хвостов гомоморфизмов из Φ похожих на φ равно $|H : H_\varphi|$;*
2) *для каждого гомоморфизма ψ похожего на φ число гомоморфизмов из Φ с таким же хвостом как у ψ равно $|H_\varphi|$.*

Доказательство. Для доказательства утверждения 1) заметим, что на множестве хвостов гомоморфизмов из Φ группа H действует сопряжением. Действительно, если хвост гомоморфизма $\psi \in \Phi$ сопрячь при помощи элемента $h \in H$ то мы получим хвост гомоморфизма $f \mapsto \psi(f)^h$. Этот гомоморфизм лежит в Φ в силу условия I основной теоремы. Хвосты гомоморфизмов похожих на φ составляют орбиту хвоста гомоморфизма φ

при этом действии. Мощность орбиты равна, как известно, индексу стабилизатора. Осталось заметить, что подгруппа H_φ — это стабилизатор хвоста гомоморфизма φ.

Докажем второе утверждение. Выберем элемент $x \in F$ степени один. Гомоморфизм $\alpha\colon F \to G$ однозначно определяется своим хвостом и значением $\alpha(x)$. При этом для двух гомоморфизмов α и β с одинаковым хвостом частное $h = (\alpha(x))^{-1}\beta(x)$ должно коммутировать с этим хвостом, то есть лежать в H_α; действительно, для всех $f \in F$ степени ноль мы имеем

$$\alpha(f^x)^h = \alpha(f)^{\alpha(x)h} = \alpha(f)^{\beta(x)} = \beta(f)^{\beta(x)} = \beta(f^x) = \alpha(f^x), \quad \text{то есть } h \text{ централизует подгруппу } \alpha(\ker\deg);$$

а для любого элемента $f \in F$ мы имеем

$$\alpha(x)\alpha(f)H = \alpha(xf)H = \beta(xf)H = \beta(x)\beta(f)H = \alpha(x)h\beta(f)H = \alpha(x)h\alpha(f)H, \quad \text{то есть } h \in \alpha(f)H\alpha(f)^{-1}.$$

Таким образом, $h = (\alpha(x))^{-1}\beta(x) \in H_\alpha$.

С другой стороны, если h — произвольный элемент из H_α, то отображение $f \mapsto \begin{cases} \alpha(f), & \text{если } \deg f = 0 \\ \alpha(x)h, & \text{если } f = x \end{cases}$ очевидно продолжается до гомоморфизма с таким же хвостом, как у α (по лемме 0). Этот гомоморфизм лежит в Φ в силу условия II основной теоремы.

Мы показали, что для любого $\alpha \in \Phi$ множество Φ содержит ровно $|H_\alpha|$ гомоморфизмов с таким же хвостом как у α. Осталось заметить, что для похожих гомоморфизмов ψ и φ подгруппы H_φ и H_ψ имеют одинаковый порядок, поскольку эти подгруппы сопряжены. Это завершает доказательство утверждения 2), а вместе с ним и основной теоремы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Bro00] Brown K. S. The coset poset and probabilistic zeta function of a finite group //J. Algebra, 2000. V.225. P.989-1012.

[Coll10] Collins D. J. Generating Sequences of Finite Groups. Senior Thesis. Cornell University Mathematics Department, 2010. (Доступно здесь: `http://www.math.cornell.edu/m/sites/default/files/imported/Research/SeniorTheses/2010/collinsThesis.pdf`)

[Hall36] Hall P. The Eulerian functions of a group // Quart. J. Math. Oxford Ser., 7 (1936), pp. 134-151.

[HIÖ89] Hawkes T., Isaacs I. M., Özaydin M. On the Möbius function of a finite group // Rocky Mountain J. Math. 1989. 19:4, 1003-1034

[GRV12] Gordon C., Rodriguez-Villegas F. On the divisibility of $\#\mathrm{Hom}(\Gamma, G)$ by $|G|$ // J. Algebra. 2012. V.350, no.1, P. 300–307. See also arXiv:1105.6066.

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

[KT84] Kratzer C., Thévenaz J. Fonction de Möbius d'un groupe fini et anneau de Burnside. // Commentarii Mathematici Helvetici. 59:1(1984): 425-438.

[Solo69] Solomon L. The solutions of equations in groups // Arch. Math. 1969. V.20. no.3. P. 241–247.

[Wils09] Wilson R. A. The Finite Simple Groups. Graduate Texts in Mathematics. Springer - 2009.