УДК 512.74 + 512.543.72 MSC: 14L17, 20F70

РАЗМЕРНОСТЬ МНОЖЕСТВА РЕШЕНИЙ СИСТЕМЫ УРАВНЕНИЙ В АЛГЕБРАИЧЕСКОЙ ГРУППЕ

Антон А. Клячко Мария А. Рябцева
Механико-математический факультет Московского государственного университета
Москва 119991, Ленинские горы, МГУ
klyachko@mech.math.msu.su ryabtseva.mariya@gmail.com

Теорема Гордона–Родригеса-Виллегаса утверждает, что в конечной группе число решений системы уравнений (без коэффициентов) делится на порядок этой группы, если ранг матрицы, составленной из сумм показателей при j-м неизвестном в i-м уравнении, меньше, чем число неизвестных. Мы доказываем аналог этого факта (и его известных обобщений) для алгебраических групп. В частности, из наших результатов вытекает, что размерность каждой неприводимой компоненты многообразия гомоморфизмов из конечно порождённой группы с бесконечным индексом коммутанта в алгебраическую группу G не меньше, чем $\dim G$.

1. Введение

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

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

Теорема Соломона обобщалась в разных направлениях, смотрите [Isaa70], [Стру95], [AmV11], [GRV12], [KM14], [KM17], [BKV18] и литературу, там цитируемую. Например, в [KM14] доказано следующее обобщение.

Теорема KM [KM14]. *Число решений системы уравнений над группой делится на порядок централизатора множества всех коэффициентов, если ранг матрицы, составленной из сумм показателей степеней при j-м неизвестном в i-м уравнении, меньше числа неизвестных.*

Для случая уравнений без коэффициентов эта теорема была доказана ранее Гордоном и Родригесом-Виллегасом [GRV12] (и в этом случае имеет место делимость на порядок централизатора пустого множества, то есть на порядок всей группы). Например, число решений системы уравнений $\{x^{100}y^{100}[x,y]^{777}=1,\ (xy)^{2020}=1\}$ всегда делится на порядок группы, поскольку эта система, хотя и не удовлетворяет условиям теоремы Соломона, но удовлетворяет условиям теоремы Гордона–Родригеса-Виллегаса: матрица составленная из сумм показателей степеней (которую мы будем называть *матрицей системы уравнений*) имеет в данном случае вид $\left(\begin{smallmatrix}100&100\\2020&2020\end{smallmatrix}\right)$, и ранг её равен единице (а число неизвестных равно двойке).

Отметим, что в этих теоремах о делимости не предполагается, что группа конечная; делимость всегда понимается в смысле кардинальной арифметики: каждый бесконечный кардинал делится на все меньшие ненулевые кардиналы. Впрочем, наиболее интересные применения упомянутых теорем относятся всё же к конечным группам.

Цель нашей работы — получить аналоги упомянутых теорем для уравнений над алгебраическими группами. Аналогом числа решений системы уравнений является в этом случае размерность многообразия решений. Более точно (но всё равно грубо и «с философской точки зрения») можно сказать, что размерность есть логарифм числа решений. Отметим, что решения (конечной или бесконечной) системы уравнений от m неизвестных над аффинной алгебраической группой G всегда образуют аффинное алгебраическое подмногообразие в G^m. Аналогом теоремы Соломона является следующее простое наблюдение.

Теорема 0. *В любой аффинной алгебраической группе G размерность каждой неприводимой компоненты многообразия решений конечной системы уравнений (возможно с коэффициентами) не меньше, чем*

$$\Big((\textit{число неизвестных})-(\textit{число уравнений})\Big)\cdot\dim G.$$

Доказательство. Левые части уравнений задают морфизм алгебраических многообразий $\gamma\colon G^m\to G^n$, где m — число неизвестных, а n — число уравнений. Многообразие решений представляет собой слой $\gamma^{-1}(1,\dots,1)$. Каждая неприводимая компонента M многообразия G^m изоморфна G_0^m как алгебраическое многообразие (где G_0 — неприводимая компонента единицы группы G) и, следовательно, $\dim M=m\cdot\dim G$. Сужение морфизма γ на M представляет собой доминантный морфизм неприводимых алгебраических многообразий $M\to N$, где N есть замыкание (в топологии Зарисского) множества $\gamma(M)$. Остаётся воспользоваться следующим общим фактом (смотрите, например, [Бо72]).

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

Лемма о слое. *Если $\gamma\colon M \to N$ — доминантный морфизм неприводимых алгебраических многообразий, то для любой точки $s \in f(M)$ размерность слоя $\gamma^{-1}(s)$ не меньше чем $\dim M - \dim N$; причём N содержит непустое открытое подмножество $U \subset f(X)$ такое, что $\dim \gamma^{-1}(u) = \dim M - \dim N$ для любой точки $u \in U$.*

Теорему 0 едва ли можно назвать новым результатом; для уравнений без коэффициентов этот факт был отмечен, например, в [LM11].

Теорема Соломона выглядит лучше теоремы 0 в том смысле, что в теореме Соломона утверждается делимость, а в теореме 0 — лишь неравенство; но здесь ничего нельзя поделать — ни о какой делимости размерностей не может быть речи. Во всех прочих отношениях теорема 0 выглядит лучше; но с этим тоже ничего нельзя сделать, как показывают следующие простые примеры.

Неверная теорема. *В любой группе G число решений совместной системы уравнений, в которой неизвестных больше чем уравнений,*
1) *не меньше порядка этой группы;*
2) *делится на $|G|^{(\textit{число неизвестных})-(\textit{число уравнений})}$, если коэффициентов нет.*

Доказательство.
1) Первое утверждение неверно по простой причине. В симметрической группе из шести элементов уравнение $x^3y^3 = (1\ 2\ 3)$ имеет ровно три решения, так как x и y должны иметь одинаковую чётность, причём чётными эти перестановки быть не могут, поскольку куб чётной перестановки равен единице; произведение двух различных транспозиций всегда равно тройному циклу, причём половина из этих шести произведений даёт один тройной цикл, а половина — другой. (Заметим в скобках, что число решений обязано делиться на три по теореме КМ.)
2) Второе утверждение тоже неверно, как показывает уравнение $x^2y^2z^2 = 1$ в той же симметрической группе из шести элементов. Квадраты перестановок чётные, поэтому эти квадраты должны быть либо одним и тем же тройным циклом, либо один из квадратов есть тождественная перестановка, а два других — разные тройные циклы, либо все три квадрата суть тождественные перестановки. При этом из тождественной перестановки четыре квадратных корня, из циклов по одному. Всего получается $2 + 3 \cdot 2 \cdot 4 + 4 \cdot 4 \cdot 4 = 90$ решений.

Аналогом теоремы КМ служит следующее утверждение.

Теорема 1. *Если ранг матрицы системы уравнений с конечным числом неизвестных над аффинной алгебраической группой меньше числа неизвестных, то размерность каждой компоненты многообразия решений этой системы не меньше, чем размерность централизатора множества всех коэффициентов.*

Пример уравнения $[x, y] = 1$ (с нулевой матрицей и двумя неизвестными) над связной неабелевой группой показывает, что оценку из теоремы 1 (даже при отсутствии коэффициентов) нельзя усилить до неравенства

$$\dim(\textit{многообразие решений}) \geqslant \Big((\textit{число неизвестных}) - (\textit{ранг матрицы системы})\Big) \cdot \dim G,$$

подобного тому, что написано в теоремы 0.

Вопрос (предложенный рецензентом). *Верно ли, что в условиях теоремы 1 класс многообразия решений делится на класс централизатора коэффициентов в кольце Гротендика (многообразий)?*

Если это верно, то это включало бы в себя и теорему 1, и теорему КМ (для конечных групп).

Следствие (а вернее сказать, переформулировка теоремы 1 для случая уравнений без коэффициентов). *Пусть G — аффинная алгебраическая группа, а F — конечно порождённая группа, коммутант которой имеет бесконечный индекс. Тогда размерность каждой неприводимой компоненты многообразия гомоморфизмов $F \to G$ не меньше размерности группы G.*

Многообразию представлений (или *Многообразию гомоморфизмов*) $\mathrm{Hom}(F, G)$ конечно порождённой группы F в алгебраической группе G посвящено очень много работ, смотрите, например, [RBCh96], [MO10], [LM11], [LL13], [LS05], [Ki18], [LT18] и литературу там цитируемую. В частности, исследовался вопрос, когда существуют инъективные или *топологически сюръективные* гомоморфизмы, то есть гомоморфизмы с всюду плотным (в топологии Зарисского) образом, и насколько много таких гомоморфизмов. Например, в [Ki18] показано, что топологически сюръективные гомоморфизмы из фундаментальной группы замкнутой ориентированной поверхности рода больше единицы в вещественную полупростую алгебраическую группу всегда существуют, причём их много в некотором смысле. А в работе [BGGT12] показано, что из свободной группы в почти любую полупростую алгебраическую группу существует гомоморфизм, ограничение которого на любую нециклическую подгруппу топологически сюръективно. Смотрите также недавний обзор [ГКП18].

Вообще говоря, ни инъективные, ни топологически сюръективные гомоморфизмы уже не образуют многообразия, но следующая теорема показывает, что в каком-то смысле все «компоненты» этих (и похожих) немногообразий имеют размерность не меньше, чем размерность коммутанта группы G. Мы рассматриваем следующие свойства гомоморфизма $\varphi\colon F \to G$ из конечно порождённой группы F, содержащей некоторую подгруппу W, в алгебраическую группу G, содержащую замкнутую подгруппу A.

$\mathbf{F}_{W,A}$ (точность): $\varphi(W) \subseteq A$ и ограничение гомоморфизма φ на подгруппу $W \subseteq F$ инъективно;

$\mathbf{S}_{W,A}$ (топологическая сюръективность): замыкание подгруппы $\varphi(W)$ равно A;

$\mathbf{C}_{W,A}$ (связность): $\varphi(W) \subseteq A$ и замыкание подгруппы $\varphi(W)$ неприводимо.

Теорема 2. *Пусть A — подгруппа аффинной алгебраической группы G, а F — конечно порождённая группа, коммутант которой имеет бесконечный индекс. Тогда каждый гомоморфизм $F \to G$, обладающий какой-то (возможно бесконечной) комбинацией (конъюнкцией)*

$$\mathbf{P} = \left(\bigwedge_{W\in\mathcal{F}} \mathbf{F}_{W,A}\right) \wedge \left(\bigwedge_{W\in\mathcal{S}} \mathbf{S}_{W,A}\right) \wedge \left(\bigwedge_{W\in\mathcal{C}} \mathbf{C}_{W,A}\right), \quad \text{где } \mathcal{F},\mathcal{S},\mathcal{C} \text{ — некоторые семейства подгрупп группы } F,$$

перечисленных выше свойств содержится в $(\dim[A,A])$*-мерном неприводимом подмногообразии многообразия* $\mathrm{Hom}(F,G)$*, целиком состоящим гомоморфизмов обладающих той же комбинацией свойств* $\mathbf{P}$*, если индекс подгруппы* $[F,F]\cdot\prod\limits_{W\in\mathcal{F}\cup\mathcal{C}} W$ *в* F *бесконечен* (а на семейство $\mathcal{S}$ никаких условий не накладывается).

Заменить здесь размерность коммутанта на размерность всей группы нельзя, как показывает следующий простейший пример: из бесконечной циклической группы в тор $(\mathbb{C}^*)^{2020}$ есть топологически сюръективные гомоморфизмы, но они одиноки в том смысле, что всякое ненульмерное подмногообразие в $\mathrm{Hom}\left(\mathbb{Z},(\mathbb{C}^*)^{2020}\right)$ содержит не топологически сюръективный гомоморфизм (поскольку всякое бесконечное подмногообразие в $\mathbb{C}^*$ содержит элемент конечного порядка).

Убрать условия на семейства $\mathcal{F}$ и $\mathcal{C}$ тоже нельзя, как показывают простые примеры гомоморфизмов из $\mathbb{Z}$ в $\mathbf{SL}_n(\mathbb{C})$.

Например, теорема 2 говорит, что

> *если гомоморфизм из фундаментальной группы кренделя* $F = \langle x,y,z,t \mid [x,y]=[z,t]\rangle$ (или из любой другой группы, у которой образующих больше, чем соотношений) *в алгебраическую группу G инъективен на подгруппе $\langle x,y,z\rangle$ и переводит всякую неабелеву подгруппу во всюду плотную в G подгруппу, то он содержится в* $(\dim[G,G])$*-мерном подмногообразии многообразия* $\mathrm{Hom}(F,G)$*, состоящем из гомоморфизмов с теми же двумя свойствами.*

Частично теорема 2 также является аналогом известного факта [KM17]:

> *число сюръективных гомоморфизмов из конечно порождённой группы с бесконечным индексом коммутанта в* (конечную, если угодно) *группу G делится на порядок коммутанта группы G.* Например, *число пар элементов, порождающих (2-порождённую) группу всегда делится на порядок коммутанта этой группы.*

Но вообще говоря, в «алгебраической ситуации» возникают некоторые новые эффекты.

Теоремы 1 и 2 являются частными случаями более общей *основной теоремы*, которую мы формулируем в следующем параграфе. Наша основная теорема является прямым «алгебраическим» аналогом основной теоремы работы [KM17] (частными случаями которой являются все сформулированные выше теоремы о делимости и множество других любопытных фактов, смотрите [KM17] и [BKV18]).

Авторы благодарят Д. А. Тимашёва и анонимного рецензента 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 $\langle X\rangle$, $\langle\langle X\rangle\rangle$ и $C(X)$ означают, соответственно, подгруппу, порождённую множеством X, нормальное замыкание множества X и централизатор множества X. Индекс подгруппы H группы G обозначается $|G:H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. Символом $\mathrm{Hom}(A,B)$ мы обозначаем множество гомоморфизмов из группы A в группу B. Свободную группу ранга n мы обозначаем символом $F(x_1,\ldots,x_n)$ или F_n. Символ $A*B$ обозначает свободное произведение групп A и B. Слово *многообразие* всегда означает (не обязательно неприводимое) квазипроективное алгебраическое многообразие над алгебраически замкнутым полем (произвольной характеристики), а слово *подмногообразие* означает локально замкнутое подмножество в многообразии. Все топологические термины относятся к топологии Зарисского.

2. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}$ мы называем *индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}$ мы называем *степенью* или *индексацией* 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 — аффинная алгебраическая подгруппа некоторой алгебраической группы G и Φ — некоторое подмногообразие многообразия гомоморфизмов из конечно порождённой индексированной группы F в G, причём множество Φ обладает следующими двумя свойствами.*

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

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

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 размерность каждой неприводимой компоненты многообразия Φ не меньше, чем размерность группы 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 $h \in C(\varphi(\ker\deg))$ ([KM17], лемма 0). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ (при некоторых дополнительных предположениях об h).

Эта теорема является аналогом основной теоремы из [KM17], которая утверждает, что для любой (абстрактной) группы G и любой её подгруппы H мощность множества Φ гомоморфизмов из индексированной группы F в G делится на $|H|$ при выполнении условий I и II.

3. Доказательство теоремы 1

Пусть $A \subseteq G$ — подгруппа, порождённая всеми коэффициентами всех уравнений. В качестве группы F мы возьмём факторгруппу $F = (A * F(x_1, \ldots, x_n))/\langle\langle\{v_i\}\rangle\rangle$ свободного произведения $A * F(x_1, \ldots, x_n)$ группы A и свободной группы $F(x_1, \ldots, x_n)$ 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 (которое, очевидно, является подмногообразием многообразия всех гомоморфизмов из F в G).

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 $A \subset F$.

4. Доказательство теоремы 2

Если индекс коммутанта конечно порождённой группы бесконечен, то, как известно, существует эпиморфизм из этой группы на $\mathbb{Z}$. Поэтому из условий теоремы вытекает наличие индексации $\deg\colon F \to \mathbb{Z}$, ядро которой содержит все подгруппы из семейств $\mathcal{C}$ и $\mathcal{F}$ (и коммутант F' группы F, разумеется). Возьмём в качестве H коммутант A' группы A, а в качестве Φ — множество гомоморфизмов $F \to G$, совпадающих с данным гомоморфизмом $\alpha\colon F \to G$ по модулю H и совпадающих с α на элементах степени ноль:

$$\Phi = \{\varphi\colon F \to G \mid \quad \varphi(f)H = \alpha(f)H \text{ для всех } f \in F; \quad \varphi(f) = \alpha(f) \text{ для всех } f \in \ker\deg\}.$$

Ясно, что условия основной теоремы выполнены для этих F, $\deg$, Φ и H. Поэтому размерность каждой компоненты многообразия Φ не меньше, чем $\dim H = \dim A'$. Осталось проверить, что если гомоморфизм α обладает свойством $\mathbf{P}$, то все гомоморфизмы из Φ также обладают этим свойством. Пусть $\varphi \in \Phi$, то есть $\varphi(f) = \alpha(f)h_f$ для всех $f \in F$, где $h_f \in H = A'$.

Сперва заметим, что подгруппа $\varphi(W') = \alpha(W')$ плотна в коммутанте $H = A'$ группы A для всех $W \in \mathcal{S}$. Действительно, алгебраическая группа имеет конечную *коммутаторную ширину*, то есть морфизм $\varkappa\colon A^{2n} \to A'$, посылающий набор $(x_1, \dots, x_n, y_1, \dots, y_n)$ в произведение коммутаторов $\prod[x_i, y_i]$ сюръективен при достаточно большом n (смотрите, например, [BO88]). Образ всюду плотного множества при непрерывном сюръективном отображении всюду плотен (и D^{2n} плотно в A^{2n}, если множество D плотно в A). Так что в любом непустом открытом подмножестве коммутанта $A' = H$ группы A найдётся элемент из $\varkappa\left(\left(\alpha(W)\right)^{2n}\right) \subseteq \alpha(W') = \varphi(W')$, что и требовалось.

Пусть $U \subseteq A$ — непустое открытое множество. В силу плотности множества $\alpha(W)$ в A (где $W \in \mathcal{S}$) множество U содержит некоторый элемент $\alpha(w) = \varphi(w)h_w^{-1}$ где $w \in W$. Значит открытое множество $\varphi(w^{-1})U$ содержит $h_w^{-1} \in A' = H$. Следовательно, $\varphi(w^{-1})U \cap A'$ — непустое открытое подмножество в коммутанте $A' = H$ группы A. По доказанному оно содержит некоторый элемент $\varphi(w_1)$, где $w_1 \in W$. Следовательно, $U \ni \varphi(ww_1)$, и это завершает доказательство свойства $\mathbf{S}_{W,A}$ для гомоморфизма φ.

Свойства $\mathbf{F}_{W,A}$ (где $W \in \mathcal{F}$) и $\mathbf{C}_{W,A}$ (где $W \in \mathcal{C}$) выполняются по очевидной причине: все эти подгруппы W состоят из элементов степени ноль (по выбору индексации $\deg$), поэтому гомоморфизмы φ и α совпадают на таких подгруппах W.

5. Доказательство основной теоремы

Наше доказательство проводится по той же схеме, что доказательство основной теоремы работы [KM17]. Некоторая трудность состоит в том, что подгруппа $\ker\deg \subset F$ может оказаться не конечно порождённой, и поэтому множество гомоморфизмов $\ker\deg \to G$ не имеет, вообще говоря, естественной структуры алгебраического многообразия. Побороть эту неприятность позволяет следующее простое наблюдение:

существует такое конечное подмножество $K \subseteq \ker\deg \subset F$, что любые два гомоморфизма из F в G, совпадающие на K, совпадают на $\ker\deg$.

Действительно, пусть $\ker\deg = \{d_1, d_2, \dots\}$ и Π_i — это множество пар гомоморфизмов $F \to G$, совпадающих на $d_1, \dots, d_i$. Ясно, что Π_i образуют убывающую цепочку подмногообразий в $\mathrm{Hom}(F, G) \times \mathrm{Hom}(F, G)$. Такая цепочка обязана стабилизироваться: $\Pi_n = \Pi_{n+1} = \dots$ для некоторого n. Следовательно, можно положить $K = \{d_1, d_2, \dots, d_n\}$.

Нам понадобится ещё аналогичный в некотором смысле факт:

существует такое конечное подмножество $A \subset F$, что если у двух гомоморфизмов α и β из F в G их композиции с естественной отображением $G \to G/H$ (где G/H — множество левых смежных классов G по H) совпадают на A, то они совпадают на всей группе F:

$$\forall \alpha, \beta \in \mathrm{Hom}(F, G) \qquad \Big(\forall a \in A \quad \alpha(a)H = \beta(a)H\Big) \Longrightarrow \Big(\forall f \in F \quad \alpha(f)H = \beta(f)H\Big).$$

Действительно, пусть теперь $F = \{d_1, d_2, \dots\}$ и Π_i — это множество пар гомоморфизмов $\alpha, \beta\colon F \to G$ таких, что $\alpha(d_k)H = \beta(d_k)H$ при $k \leqslant i$. Ясно, что Π_i образуют убывающую цепочку многообразий. Такая цепочка обязана стабилизироваться: $\Pi_n = \Pi_{n+1} = \dots$ для некоторого n. Следовательно, можно положить $A = \{d_1, d_2, \dots, d_n\}$.

Рассмотрим теперь многообразие $X = G^K \times (G/H)^A$, состоящее из всех пар отображений $K \to G$ и $A \to G/H$ (где G/H — это многообразие левых смежных классов группы G по подгруппе H). На многообразии X действует группа H (сопряжениями): $h \circ (\alpha, \beta) = \big(f \mapsto h\alpha(f)h^{-1},\ a \mapsto h\beta(a)\big)$

Хвостом $\chi(\varphi)$ гомоморфизма $\varphi\colon F \to G$ мы будем называть пару (φ_0, φ_H), где φ_0 — это ограничение гомоморфизма φ на множество $K \subseteq \ker\deg \subset F$, а $\varphi_H\colon A \to \{gH\ ;\ g \in G\}$ — это отображение из A в G/H, которое переводит элемент $a \in A$ в класс $\varphi(a)H$. Понятно, что отображение $\chi\colon \mathrm{Hom}(F, G) \to X$ является морфизмом алгебраических многообразий.

Мы будем говорить, что два гомоморфизма $\varphi, \psi \in \Phi$ *похожи*, и писать $\varphi \sim \psi$, если их хвосты лежат в одной орбите относительно описанного выше действия H на X. Отметим, что ни похожесть гомоморфизмов, ни совпадение их хвостов не зависят от выбора множеств A и K (они нам понадобились только для того, чтобы сопоставление гомоморфизму его хвоста оказалось морфизмом алгебраических многообразий, и действие группы H на хвостах оказалось действием алгебраической группы на алгебраическом многообразии):

$$\chi(\varphi) = \chi(\psi) \iff \begin{cases} \psi(f) = \varphi(f) & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = \varphi(f)H & \text{для всех } f \in F. \end{cases} \qquad (*)$$

$$\varphi \sim \psi \iff \text{для некоторого } h \in H \begin{cases} \psi(f) = h\varphi(f)h^{-1} & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = h\varphi(f)H & \text{для всех } f \in F. \end{cases}$$

Не ограничивая общности мы будем считать, что группа H неприводима (поскольку неприводимая компонента единицы группы H является группой той же размерности).

Каждый класс похожих гомоморфизмов является локально замкнутым подмногообразием в многообразии $\mathrm{Hom}(F,G)$, поскольку класс похожих — это прообраз орбиты при морфизме χ, а орбита действия алгебраической группы на алгебраическом многообразии всегда локально замкнута (смотрите, например, [BO88]). Основная теорема немедленно вытекает из следующего утверждения.

Утверждение. *Размерность каждой компоненты каждого класса похожих гомоморфизмов из Φ равна $\dim H$. Более точно, для каждого $\varphi\in\Phi$*

1) *размерность многообразия X_φ хвостов гомоморфизмов из Φ, похожих на φ, равна $\dim H-\dim H_\varphi$;*
2) *для каждого гомоморфизма ψ, похожего на φ, размерность каждой компоненты многообразия гомоморфизмов из Φ с таким же хвостом как у ψ равна $\dim H_\varphi$.*

Доказательство. Для доказательства утверждения 1) заметим, что множество $\chi(\Phi)\subseteq X$ инвариантно относительно действия H на X. Действительно, если на хвост гомоморфизма $\varphi\in\Phi$ подействовать элементом $h\in H$, то мы получим хвост гомоморфизма $f\mapsto h\varphi(f)h^{-1}$. Этот гомоморфизм лежит в Φ в силу условия I основной теоремы. Хвосты гомоморфизмов похожих на φ составляют орбиту хвоста гомоморфизма φ при этом действии. Размерность орбиты равна, как известно, коразмерности стабилизатора (это частный случай леммы о слое). Осталось заметить, что подгруппа H_φ есть стабилизатор хвоста гомоморфизма φ (по формуле $(*)$).

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

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

(здесь и далее равенства $\overset{*}{=}$ имеют место в силу утверждения $(*)$); а для любого элемента $f\in F$ мы имеем

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

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

С другой стороны, если h — произвольный элемент из H_α, то отображение

$$f\mapsto\begin{cases}\alpha(f), & \text{если } \deg f=0\\ \alpha(x)h, & \text{если } f=x\end{cases}\tag{$**$}$$

очевидно продолжается до гомоморфизма с таким же хвостом, как у α (смотрите замечание после формулировки основной теоремы в параграфе 2). Этот гомоморфизм лежит в Φ в силу условия II основной теоремы.

Мы показали, что для любого $\alpha\in\Phi$ отображение $H_\alpha\to\mathrm{Hom}(F,G)$, переводящее элемент $h\in H_\alpha$ в гомоморфизм $(**)$, является инъективным морфизмом алгебраических многообразий, образ которого представляет собой множество элементов из Φ с таким же хвостом как у α. Это означает, что $\dim\chi^{-1}(\chi(\alpha))=\dim H_\alpha$.

Осталось заметить, что для похожих гомоморфизмов ψ и φ подгруппы H_φ и H_ψ изоморфны и даже сопряжены в H, поскольку они являются стабилизаторами точек $\chi(\varphi)$ и $\chi(\psi)$, лежащих в одной орбите при действии H на X. Это завершает доказательство утверждения 2).

Теперь заметим, что многообразие X_φ неприводимо (так как мы считаем группу H неприводимой), а каждая содержащая φ компонента Π_φ многообразия гомоморфизмов, похожих на φ, отображается на X_φ сюръективно, поскольку $\chi\bigl(f\mapsto h\varphi(f)h^{-1}\bigr)=h\circ\chi(\varphi)$, а многообразие $\{f\mapsto h\varphi(f)h^{-1}\mid h\in H\}$ неприводимо, так как является орбитой при действии связной группы H на $\mathrm{Hom}(F,G)$. Поэтому то, что размерность каждой компоненты каждого класса похожих гомоморфизмов из Φ равна $\dim H$, на самом деле вытекает из 1) и 2) в силу следующего общего факта.

Лемма. *Пусть γ — морфизм многообразия P в неприводимое многообразие N такой, что все компоненты всех слоёв $\gamma^{-1}(y)$ (где $y\in N$) имеют одинаковую размерность d, причём образ каждой компоненты многообразия P плотен в N. Тогда размерность каждой компоненты многообразия P равна $\dim N+d$.*

Доказательство. Пусть M — неприводимая компонента многообразия P. Выберем открытое непустое подмножество $U\subseteq\gamma(M)\subseteq N$, о котором идёт речь в лемме о слое. В силу неприводимости многообразия M в $\gamma^{-1}(U)$ найдётся точка x, не содержащаяся ни в какой другой компоненте многообразия P, кроме M. Тогда каждая компонента K слоя $\gamma^{-1}(\gamma(x))$, содержащая x, обязана целиком лежать в M и, следовательно, быть одной из компонент слоя ограничения морфизма γ на M. Понятно, что у остальных компонент этого слоя $M\cap\gamma^{-1}(\gamma(x))$ размерность не больше $d=\dim K$. По лемме о слое мы получаем $\dim M=\dim K+\dim N$, что и требовалось. Это завершает доказательство леммы, а вместе с ней и основной теоремы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Бо72] А. Борель, Линейные алгебраические группы, М.: Мир, (1972).

[ВО88] Э. Б. Винберг, А. Л. Онищик, Семинар по группам Ли и алгебраическим группам, М., Наука 1988.

[ГКП18] Н. Л. Гордеев, Б. Э. Кунявский, Е. Б. Плоткин, Геометрия вербальных уравнений в простых алгебраических группах над специальными полями, УМН, 73:5(443) (2018), 3-52; English translation: Russian Math. Surveys, 73:5 (2018), 753-796. См. также arXiv:1808.02303.

[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 Its Appl., 10:4 (2011), 675-686.

[BGGT12] E. Breuillard, B.Green, R. Guralnick, and T. Tao, Strongly dense free subgroups of semisimple algebraic groups, Israel Journal of Mathematics, 192:1 (2012), 347-379. См. также arXiv:1010.4259.

[BKV18] E. K. Brusyanskaya, A. A. Klyachko, A. V. Vasil'ev, What do Frobenius's, Solomon's, and Iwasaki's theorems on divisibility in groups have in common?, Pacific Journal of Mathematics, 302:2 (2019), 437-452. См. также arXiv:1806.08870.

[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.

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

[Ki18] K. Kishore, Representation variety of surface groups, Proc. Amer. Math. Soc. 146 (2018), 953-959. См. также arXiv:1702.05981.

[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.

[LL13] M. Larsen, A. Lubotzky, Representation varieties of Fuchsian groups, From Fourier analysis and number theory to radon transforms and geometry, 375-397, Dev. Math., 28, Springer, New York, 2013. См. также arXiv:1203.3408.

[LS05] M. Liebeck, A. Shalev, Fuchsian groups, finite simple groups and representation varieties, Inventiones mathematicae 159:2 (2005), 317-367.

[LM11] S. Liriano, S. Majewicz, Algebro-geometric invariants of groups (the dimension sequence of representation variety), Int. J. Algebra Comput., 21:4 (2011), 595-614.

[LT18] D. D. Long, M. B. Thistlethwaite, The dimension of the Hitchin component for triangle groups, Geometriae Dedicata (to appear).

[MO10] J. Martín-Morales, A. M. Oller-Marcén, On the number of irreducible components of the representation variety of a family of one-relator groups, Internat. J. Algebra Comput. 20:1 (2010), 77-87. См. также arXiv:0805.4716.

[RBCh96] A. S. Rapinchuk, V. V. Benyash-Krivetz, V. I. Chernousov, Representation varieties of the fundamental groups of compact orientable surfaces, Israel Journal of Mathematics, 93:1 (1996), 29-71.

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