Сибирский математический журнал
Сентябрь—октябрь, 2000. Том 41, № 5

УДК 512.5

О СВЯЗИ МЕЖДУ НИЛЬПОТЕНТНЫМИ ГРУППАМИ И КОЛЬЦАМИ ЛИ

А. Хайкин Запирайн, Е. И. Хухро

Аннотация: Пусть G — нильпотентная группа ступени c. На основе формулы Бейкера — Хаусдорфа определяется структура кольца Ли M на подгруппе G^n для некоторого $n = n(c)$, зависящего только от c, причем так, что многие важные параметры кольца Ли M такие, как ступени нильпотентности и разрешимости, равны соответствующим параметрам группы G^n. В качестве приложения уточняются сведения теорем о «почти регулярных» p-автоморфизмах конечных p-групп к соответствующим теоремам о кольцах Ли. Кроме того, показывается, что функции Хигмэна и Крекнина из теорем о регулярных (т. е. без нетривиальных неподвижных точек) автоморфизмах алгебр Ли являются наилучшими оценками (если они должны зависеть только от порядка автоморфизма) для ступеней нильпотентности и разрешимости подгрупп ограниченного индекса в теоремах о p-автоморфизмах конечных p-групп. Библиогр. 17.

Введение

Пусть G — нильпотентная группа ступени c. Используя формулу Бейкера — Хаусдорфа, мы определяем структуру кольца ($\mathbb{Z}$-алгебры) Ли M на подгруппе G^n для некоторого $n = n(c)$, зависящего только от c, причем так, что многие важные параметры кольца Ли M такие, как ступени нильпотентности и разрешимости, равны соответствующим параметрам группы G^n.

В качестве приложения мы уточняем сведения теорем о «почти регулярных» p-автоморфизмах конечных p-групп к соответствующим теоремам о кольцах Ли. В частности, доказываем, что m-ограниченная функция в теореме Ю. А. Медведева [1] о p-группах может быть выбрана в точности такой же, как в его теореме о кольцах Ли. Мы также приводим новый вариант части доказательства теоремы Е. И. Хухро [2] (это доказательство послужило одним из источников настоящей работы). Кроме того, мы показываем, что функции Хигмэна и Крекнина из теорем о регулярных (т. е. без нетривиальных неподвижных точек) автоморфизмах алгебр Ли являются наилучшими оценками (если они должны зависеть только от порядка автоморфизма) для ступеней нильпотентности и разрешимости подгрупп ограниченного индекса в теоремах о p-автоморфизмах конечных p-групп. (Мы не улучшаем оценок для функций Хигмэна и Крекнина для алгебр Ли; наша цель — получить неулучшаемые оценки для групп в терминах этих функций.)

Использование экспоненциального отображения и формулы Бейкера — Хаусдорфа $H(x, y) = \log(e^x e^y)$ берет начало в теории групп Ли. Для дискрет-

Работа первого автора поддержана грантом правительства Страны Басков и грантом DGICYT (№ PB97–0604), работа второго автора — Российским фондом фундаментальных исследований (код проекта 99–01–00576).

ных групп формула Бейкера — Хаусдорфа используется в соответствии Мальцева, которое является эквивалентностью категорий (локально) нильпотентных $\mathbb{Q}$-групп (т. е. делимых и без кручения) и (локально) нильпотентных $\mathbb{Q}$-алгебр Ли. Именно, для любой нильпотентной $\mathbb{Q}$-алгебры Ли M то же множество становится нильпотентной $\mathbb{Q}$-группой $G = M$ относительно операций $a \cdot b := H(a, b)$ и $a^r := ra$, $r \in \mathbb{Q}$, где справа — операции в M. Обращения формулы Бейкера — Хаусдорфа выражают операции $\mathbb{Q}$-алгебры Ли M через операции $\mathbb{Q}$-группы G. Это соответствие позволяет доказывать результаты о нильпотентных группах, используя алгебры Ли; конечно, можно утверждать и обратное, но часто легче иметь дело именно с алгебрами Ли как с более линейным объектом. Например, так можно доказать фольклорную теорему о том, что (локально) нильпотентная группа без кручения с регулярным автоморфизмом конечного порядка n разрешима ступени, ограниченной в терминах n. Именно, используя соответствие Мальцева, можно перейти к алгебрам Ли, для которых такой результат доказан В. А. Крекниным [3] (с использованием расширения основного поля и вычислений с корневыми пространствами, которые образуют $(\mathbb{Z}/n\mathbb{Z})$-градуировку).

Однако эту технику нельзя напрямую применить к конечным p-группам, которые не являются ни делимыми, ни группами без кручения. У любой нильпотентной группы есть так называемое присоединенное кольцо Ли, но оно не отражает в полной мере некоторые важные черты группы, например, ее ступень разрешимости. Для применения соответствия Лазара [4] для p-групп, также основанного на формуле Бейкера — Хаусдорфа, требуются весьма сильные ограничения на p-группу, например, чтобы ступень нильпотентности была меньше, чем p. Недавно Вайгель [5] применил соответствие Лазара (в его более общей форме) к p-группам при $p \geq 5$, которые одновременно мощны и p-центральны (этот класс включает униформно мощные p-группы).

Наше соответствие применимо к любой нильпотентной группе, включая конечные p-группы, любой ступени нильпотентности c, но оно основано на подгруппе вида G^n для некоторого $n = n(c)$, зависящего от c. Оно может не быть столь же хорошим, как соответствие Мальцева; например, не каждая подгруппа из G^n соответствует подкольцу Ли, и т. п. Но оно все же сохраняет многие важные параметры подгруппы G^n и соответствующего кольца Ли такие, как ступени разрешимости и нильпотентности. В приложениях к p-автоморфизмам конечных p-групп (секционный) ранг группы часто является ограниченным параметром, так что подгруппа $G^{n(c)}$ тогда имеет ограниченный индекс, конечно, если уже удалось ограничить ступень нильпотентности.

1. Предварительные леммы

Чтобы различать групповые и кольцевые коммутаторы, будем использовать индексы $_G$ и $_L$ соответственно. Например, по формуле Бейкера — Хаусдорфа имеем $[x, y]_G = [x, y]_L + \dots$, где точки обозначают рациональную линейную комбинацию кольцевых коммутаторов веса ≥ 3 от переменных x и y. Аналогично мы будем использовать знак $\triangleleft_G$ для нормальных подгрупп, $\triangleleft_L$ — для идеалов, а $\langle S\rangle_G$ или $\langle S\rangle_L$ — для подгруппы или подкольца Ли, порожденного множеством S. Мы используем стандартные обозначения ${}_{\mathrm{id}}\langle S\rangle$ для идеала, порожденного S, и $\langle S\rangle^T$ для нормального замыкания S в T.

Пусть L — свободное нильпотентное кольцо Ли ($\mathbb{Z}$-алгебра) ступени c на множестве свободных порождающих $x_1, x_2, \dots$ (не обязательно счетном), естественным образом вложенная в свободную нильпотентную $\mathbb{Q}$-алгебру Ли $\mathbb{Q}L$ на том же множестве свободных порождающих. Формула Бейкера — Хаусдорфа

$H(x,y)$ определяет структуру нильпотентной $\mathbb{Q}$-группы $\widehat{F}$ на том же множестве $\mathbb{Q}L$ относительно операций $a\cdot b := H(a,b)$ и $a^r := ra$, $r\in\mathbb{Q}$, где в правых частях — операции в $\mathbb{Q}L$ (см., например, [6]). Как $\mathbb{Q}$-группа $\widehat{F}$ является свободной нильпотентной ступени c на свободных порождающих $x_1, x_2, \dots$. Обращения формулы Бейкера — Хаусдорфа выражают операции $\mathbb{Q}$-алгебры Ли на $\mathbb{Q}L$ через операции $\mathbb{Q}$-группы $\widehat{F}$. Пусть F — абстрактная подгруппа, порожденная в $\widehat{F}$ элементами $x_1, x_2, \dots$; тогда F — свободная нильпотентная группа на свободных порождающих $x_1, x_2, \dots$. Каждый элемент группы F является некоторой степенью элемента из $\widehat{F}$. Каждый элемент $g\in\widehat{F}$ имеет однозначное представление $g=\prod c_i^{r_i}$, где $r_i\in\mathbb{Q}$ и c_i — базисные групповые коммутаторы от элементов x_i в некотором фиксированном порядке, причем $g\in F$ тогда и только тогда, когда $r_i\in\mathbb{Z}$ для всех i. Если не настаивать на единственности, каждый элемент из $\widehat{F}$ может быть записан в виде произведения рациональных степеней простых коммутаторов от элементов x_i.

В доказательствах мы будем часто пользоваться следующим рассуждением, основанным на том, что F, $\widehat{F}$, L и $\mathbb{Q}L$ — свободные объекты в соответствующих категориях. Предположим, что установлено равенство $v(x_1,\dots,x_k) = w(x_1,\dots,x_k)$ для некоторых слов v и w от свободных порождающих x_i. Тогда $v(a_1,\dots,a_k) = w(a_1,\dots,a_k)$ для любых элементов a_i любого объекта в той же категории в силу гомоморфизма, продолжающего отображение $x_i\to a_i$. Если оставаться в рамках $\mathbb{Q}L=\widehat{F}$, то v и w могут быть даже словами в разных категориях: так как операции в $\widehat{F}$ выражены фиксированными формулами через операции в $\mathbb{Q}L$ и наоборот, гомоморфизм одного из этих объектов является также гомоморфизмом другого (оставаясь тем же отображением).

Ввиду связи между групповыми и кольцевыми операциями мы будем использовать любое из обозначений для $ng=g^n$, где $g\in\widehat{F}$, $n\in\mathbb{Z}$, так как это не может вызвать никакой путаницы; например, тогда nF — множество всех n-х степеней элементов из F. Напомним, что F^n обозначает подгруппу, порожденную всеми n-ми степенями, т. е. $F^n=\langle nF\rangle$. Распространяя эти обозначения, мы можем также написать, что $\mathbb{Q}F=\widehat{F}$.

Будем говорить, что величина $(a,b,\dots)$-*ограничена*, если она ограничена в терминах только $a,b,\dots$.

Лемма 1. *Существуют c-ограниченные натуральные числа $n_1=n_1(c)$ и $n_2=n_2(c)$ такие, что $n_1L\subseteq F\subseteq n_2^{-1}L$.*

Доказательство. Докажем сначала, что $F\subseteq n_2^{-1}L$. Для произвольного k произведение $x_1x_2\cdots x_k$, будучи элементом из $\mathbb{Q}L$, является рациональной линейной комбинацией кольцевых коммутаторов от x_i. Любой коммутатор в этой комбинации зависит не более чем от c элементов $x_{i_1},\dots,x_{i_d}$, $d\le c$, так как алгебра нильпотентна ступени c. Он не меняется под действием гомоморфизма, посылающего x_{i_j} в x_{i_j}, $j=1,\dots,d$, а все остальные свободные порождающие в 0. Заметим, что это также гомоморфизм $\mathbb{Q}$-группы $\widehat{F}$ (напомним, что $\mathbb{Q}L\ni 0=1\in\widehat{F}$). Поэтому коэффициент при этом коммутаторе такой же, как в аналогичном разложении произведения $x_{i_1}\cdots x_{i_d}$. Поскольку $d\le c$, последнее, очевидно, принадлежит $n_2^{-1}L$ для некоторого c-ограниченного натурального $n_2=n_2(c)$. Следовательно, $x_1x_2\cdots x_k\in n_2^{-1}\langle x_1,\dots,x_k\rangle_L$ для любого k. Тогда любой элемент из F, имея вид $\prod x_{j_i}^{r_i}$, где $r_i\in\mathbb{Z}$, принадлежит $n_2^{-1}\langle r_1x_{j_1}, r_2x_{j_2},\dots\rangle_L\subseteq n_2^{-1}L$.

Теперь докажем, что $n_1L\subseteq F$. Известно, что $(x_1+\dots+x_c)^{f_1}\in F$ для некоторого натурального $f_1 = f_1(c)$, ибо $x_1 + \dots + x_c \in \mathbb{Q}L = \widehat{F}$. Тем самым и $(x_{i_1} + \dots + x_{i_d})^{f_1} \in F$ для любого $d \le c$. Утверждается, что $(x_1 + \dots + x_k)^{f_1} \in F$ для любого $k \in \mathbb{N}$ для того же показателя f_1. В самом деле, $(x_1 + \dots + x_k)^{f_1} = \prod c_j^{r_j}$ — произведение рациональных степеней базисных (групповых) коммутаторов c_j от x_i в некотором фиксированном порядке. Нам надо показать, что $r_j \in \mathbb{Z}$ для всех j. Любой коммутатор c_t зависит не более чем от c переменных $x_{i_1}, \dots, x_{i_d}$, $d \le c$. Применяя гомоморфизм, посылающий x_{i_k} в x_{i_k} для $k = 1, \dots, d$, а остальные свободные порождающие в 1 (т. е. в $0 \in \mathbb{Q}L$), получаем выражение для $(x_{i_1} + \dots + x_{i_d})^{f_1}$ как образ произведения $\prod c_j^{r_j}$, в котором сомножитель $c_t^{r_t}$ остается неизмененным. Так как это элемент из F по выбору f_1, мы должны иметь $r_t \in \mathbb{Z}$, как и требуется. Далее, существует натуральное $f_2 = f_2(c)$ такое, что $f_2[x_{i_1}, \dots, x_{i_d}]_L \in F$ для любого $d \le c$. Любой элемент из L имеет вид $\sum \alpha_i c_i$, где $\alpha_i \in \mathbb{Z}$ и c_i — (простые) коммутаторы веса $\le c$ от x_j. Применяя гомоморфизм, продолжающий отображение $x_i \to \alpha_i f_2 c_i$, к включению $f_1 \sum x_i \in \langle x_1, x_2, \dots \rangle_G$, получаем, что

$$f_1 f_2 \sum \alpha_i c_i = f_1 \sum f_2 \alpha_i c_i \in \langle f_2 \alpha_1 c_1, f_2 \alpha_2 c_2, \dots \rangle_G.$$

Правая часть содержится в F, так как $f_2 \alpha_i c_i \in F$ для всех i. Таким образом, мы можем положить $n_1 = f_1 f_2$. $\square$

Лемма 2. *Существуют c-ограниченные натуральные числа $n_3 = n_3(c)$ и $n_4 = n_4(c)$ такие, что $nn_3 L \subseteq F^n \subseteq nn_4^{-1} L$ для любого $n \in \mathbb{N}$.*

Доказательство. Так как $F^n \supseteq nF \supseteq nn_1 L$ по лемме 1, первое включение справедливо при $n_3 = n_1$. Докажем второе. Для любого $k \in \mathbb{N}$ имеем $x_1 \cdots x_k \in n_2^{-1} L$ по лемме 1. Для любых $g_i \in F$ гомоморфизм, продолжающий отображение $x_i \to ng_i$ $(= g_i^n)$, дает, что $g_1^n \cdots g_k^n \in n_2^{-1} S$, где $S = \langle ng_1, \dots, ng_k \rangle_L$. Очевидно, что $S \subseteq nS_1$, где $S_1 = \langle g_1, \dots, g_k \rangle_L$. Снова $g_i \in n_2^{-1} L$ по лемме 1; так как ступень нильпотентности равна c, имеем $S_1 \subseteq n_2^{-c} L$. Отсюда $F^n \subseteq nn_2^{-c-1} L$. Таким образом, можно положить $n_4 = n_2^{c+1}$. $\square$

Здесь и далее мы используем то, что аддитивная группа $\mathbb{Q}L$ не имеет кручения и потому в ней извлечение корней однозначно, так что $rS \subseteq T \Leftrightarrow S \subseteq r^{-1} T$ для любого $r \in \mathbb{Q}$ и любых подмножеств $S, T \subseteq \mathbb{Q}L$. Следующая лемма обобщает лемму Блэкберна из [7].

Лемма 3. *Существует c-ограниченное натуральное число $n_5 = n_5(c)$ такое, что для любого n, кратного n_5, в любой нильпотентной группе ступени c любое произведение n-х степеней является nn_5^{-1}-й степенью некоторого элемента.*

Доказательство. Достаточно доказать лемму для F; тогда подходящий гомоморфизм $F \to G$ даст тот же результат для G. По лемме 2 имеем $F^n \subseteq nn_4^{-1} L \subseteq nn_4^{-1} n_3^{-1} F$, так что можно положить $n_5 = n_3 n_4$. $\square$

Лемма 4. *Для n_5 из леммы 3, для любого n, кратного n_5, элемент $[x_1^n, x_2, \dots, x_k]_G$ является nn_5^{-1}-й степенью произведения целых степеней групповых коммутаторов от $x_1, \dots, x_k$, в каждый из которых входят все эти элементы.*

Доказательство. Поскольку $[x_1^n, x_2, \dots, x_k]_G \in F^n$, по лемме 3 уже имеем

$$[x_1^n, x_2, \dots, x_k]_G = \Big(\prod c_i^{r_i}\Big)^{nn_5^{-1}}$$

или, что равносильно,

$$n_5 n^{-1} [x_1^n, x_2, \dots, x_k]_G = \prod c_i^{r_i},$$

где $r_i \in \mathbb{Z}$ для всех i, а c_i — базисные коммутаторы от x_j в некотором фиксированном порядке. Нам нужно показать, что здесь присутствуют (нетривиальным образом) только те коммутаторы, которые зависят от всех элементов $x_1, \ldots, x_k$. Чтобы показать, что все c_i действительно зависят от данного x_t, $t \in \{1, 2, \ldots, k\}$, применим гомоморфизм, продолжающий отображение $x_t \to 1$, $x_j \to x_j$ для $j \neq t$, к вышеуказанному равенству. Левая часть превратится в $1 = 0 \in \mathbb{Q}L$. В правой части все сомножители с x_t исчезнут, а все без x_t останутся неизмененными. В силу единственности представления в виде такого произведения коммутаторы c_i, не зависящие от x_t, должны входить только в тривиальных степенях. $\square$

Лемма 5. *Существует c-ограниченное натуральное число $n_6 = n_6(c)$ такое, что для любого n, кратного n_6,*

$$x_1^n + x_2 = x_1^n \cdot x_2 \cdot A(x_1, x_2), \tag{1}$$

где $A(x_1, x_2) \in \left\langle \left[x_1^{nn_6^{-1}}, x_2\right]_G \right\rangle^F$;

$$\left[x_1^n, x_2\right]_L = \left[x_1^n, x_2\right]_G \cdot B(x_1, x_2), \tag{2}$$

где $B(x_1, x_2) \in \left\langle \left[\left[x_1^{nn_6^{-1}}, x_2\right]_G, \langle x_1^n, x_2\rangle\right]_G \right\rangle^F$;

$$x_1^n \cdot x_2 = x_1^n + x_2 + C(x_1, x_2), \tag{3}$$

где $C(x_1, x_2)$ принадлежит идеалу, порожденному элементом $\left[nn_6^{-1}x_1, x_2\right]_L$ в $\langle x_1, x_2\rangle_L$;

$$\left[x_1^n, x_2\right]_G = \left[x_1^n, x_2\right]_L + D(x_1, x_2), \tag{4}$$

где $D(x_1, x_2)$ принадлежит идеалу, порожденному множеством

$$\left[\left[nn_6^{-1}x_1, x_2\right]_L, \langle nx_1, x_2\rangle_L\right]_L$$

в $\langle x_1, x_2\rangle_L$.

(Конечно, одно и то же число n_6, скажем, наименьшее общее кратное, выбрано здесь просто для экономии обозначений.)

Доказательство. В силу обращений формулы Бейкера — Хаусдорфа $A(x_1, x_2)$ в (1) является произведением некоторых рациональных степеней коммутаторов от x_1^n и x_2. Так как нам не нужна единственность, без ограничения общности можно считать, что здесь участвуют только простые коммутаторы от x_1^n и x_2, каждый из которых начинается с $\left[x_1^n, x_2\right]$. Пусть $f(c)$ — наименьшее общее кратное знаменателей показателей степеней, которое зависит только от c. К каждому сомножителю мы применяем лемму 4, пользуясь первым вхождением элемента x_1^n в коммутатор. Для n_6, кратного $f(c)n_5(c)$, коммутатор будет $f(c)$-й степенью произведения целых степеней коммутаторов от $x_1^{nn_6^{-1}}, x_2$. Значит, каждый сомножитель также является таким произведением, так что $A(x_1, x_2) \in \left\langle \left[x_1^{nn_6^{-1}}, x_2\right]_G \right\rangle^F$.

Аналогично $B(x_1, x_2)$ в (2) является произведением рациональных степеней простых коммутаторов веса ≥ 3 от x_1^n и x_2, начинающихся с $\left[x_1^n, x_2, y\right]_G$, где y — либо x_1^n, либо x_2. Получаем требуемый результат таким же образом, как для (1), применяя лемму 4 к каждому коммутатору, используя первое вхождение элемента x_1^n.

По формуле Бейкера — Хаусдорфа $C(x_1, x_2)$ в (3) является рациональной линейной комбинацией кольцевых коммутаторов от $x_1^n = nx_1$ и x_2. Можно считать их всех простыми и начинающимися с $[nx_1, x_2]_L$. Достаточно взять в качестве n_6 наименьшее общее кратное знаменателей коэффициентов, зависящее только от c.

Аналогично $D(x_1, x_2)$ в (4) является линейной комбинацией простых кольцевых коммутаторов веса ≥ 3 от $x_1^n = nx_1$ и x_2, начинающихся с $[nx_1, x_2, y]_L$, где y либо nx_1, либо x_2. Снова достаточно взять в качестве n_6 наименьшее общее кратное знаменателей коэффициентов, зависящее только от c. $\square$

Лемма 6. *Существуют c-ограниченные натуральные числа $n_7 = n_7(c)$ и $n_8 = n_8(c)$ такие, что для любого n, кратного n_8,*

$$g + nn_7L \subseteq g \cdot F^n \subseteq g + nn_8^{-1}L$$

для любого $g \in F$.

Доказательство. Для любого $l \in L$ согласно (1) имеем $nn_6n_3l + g = nn_6n_3l \cdot g \cdot A$, где $A \in [nn_3l, F]_G \leq F^n$, ибо $nn_3l \in F^n$ по лемме 2. Так как и $nn_6n_3l \in F^n$, имеем $nn_6n_3l + g \in g \cdot F^n$. Значит, можно положить $n_7 = n_6n_3$.

По лемме 2 имеем $F^n \subseteq nn_4^{-1}L$. Следовательно, любой элемент из $g \cdot F^n = F^n \cdot g$ имеет вид $nn_4^{-1}l \cdot g$ для $l \in L$. В силу (3) для n, кратного n_4n_6, имеем $nn_4^{-1}l \cdot g = nn_4^{-1}l + g + C$, где C лежит в идеале, порожденном элементом $\left[nn_4^{-1}n_6^{-1}l, g\right]_L$ в $\langle l, g\rangle_L$. Поскольку $g \in n_2^{-1}L$ по лемме 1 и ступень нильпотентности равна c, имеем $C \in nn_4^{-1}n_6^{-1}n_2^{-c+1}L$, откуда $g \cdot F^n \subseteq g + nn_4^{-1}n_6^{-1}n_2^{-c+1}L$. Значит, можно положить $n_8 = n_4n_6n_2^{c-1}$. $\square$

Лемма 7. *Для любого $n \in \mathbb{N}$ справедливо соотношение $F^{nn_3n_4n_6} \subseteq n_6F^n$.*

Доказательство. По лемме 2 получаем $F^{nn_3n_4n_6} \subseteq n_6nn_3L \subseteq n_6F^n$. $\square$

Замечание. Можно дать явные оценки функций $n_i(c)$ из вышеприведенных лемм (и из теорем в следующем разделе). Например, оценим n_2 из леммы 1. Пусть A — свободное нильпотентное ступени c ассоциативное $\mathbb{Z}$-кольцо с 1 от переменных x_i, естественно вложенное в $\mathbb{Q}$-алгебру $\mathbb{Q}A$. Элементы $e^{x_1}, e^{x_2} \ldots$ свободно порождают свободную нильпотентную группу F ступени c. Свободную нильпотентную алгебру Ли $\mathbb{Q}L$ ступени c можно отождествить с алгеброй Ли, порожденной элементами x_i относительно операции $[a, b] = ab - ba$, а кольцо Ли L — с кольцом Ли, порожденным элементами x_i. Индукция по длине произведения элементов $e^{\pm x_{i_j}}$ показывает, что $F \subseteq \frac{1}{c!}A$. Тогда $\log f \in \frac{1}{(c!)^2}A$. По формуле Бейкера — Хаусдорфа $\log f \in \mathbb{Q}L$. Так как $\mathbb{Q}L \cap \frac{1}{(c!)^2}A = \frac{1}{(c!)^2}L$, получаем, что $\log f \in \frac{1}{(c!)^2}L$. Проследив доказательство леммы 1, мы видим, что можно положить $n_2 = (c!)^2$. Другие функции n_i могут быть оценены на основе этой информации о формуле Бейкера — Хаусдорфа и оценки для n_2. В частности, довольно грубая индукция по c дает, что можно взять $n_1 = n_2^c$. Однако должна существовать гораздо лучшая, «более симметричная» оценка для n_1, возможно, включающая какую-то лучшую оценку для обращений формулы Бейкера — Хаусдорфа. Было бы интересно найти лучшие (или даже наилучшие) оценки для функций n_i. Заметим, что в приложениях к нильпотентным p-группам имеют значение только p-адические оценки.

2. Соответствие между нильпотентными кольцами Ли и нильпотентными группами

Сначала мы построим нашу конструкцию для свободной нильпотентной группы; затем тот же результат будет следовать для произвольной нильпотентной группы.

Теорема 1. *Существует c-ограниченное натуральное число $n_9 = n_9(c)$ такое, что для любого n, кратного n_9, выполняются следующие утверждения.*

(а) *Подгруппа $U = F^n$ является $\mathbb{Z}$-подкольцом Ли кольца L (т. е. U замкнуто относительно операций $\pm$ и $[,]_L$).*

(б) *Любая нормальная подгруппа N группы F, содержащаяся в U, является идеалом кольца Ли U, и $g + N = g \cdot N$ для любого $g \in U$.*

Пусть U_1, N_1 и N_2 — нормальные подгруппы группы F такие, что $U \supseteq U_1 \supseteq N_1 \supseteq N_2$.

(в) *Если фактор-группа N_1/N_2 абелева, то фактор-кольцо Ли N_1/N_2 абелево.*

(г) *Если фактор-группа N_1/N_2 центральна в группе U_1, то фактор-кольцо Ли N_1/N_2 центрально в кольце Ли U_1.*

(д) *Если I — идеал кольца U, содержащийся в $V = F^{nn_3n_4n_6}$, то это же множество I является нормальной подгруппой группы $F^{nn_3n_4n_6}$.*

Пусть V_1, I_1 и I_2 — идеалы кольца U такие, что $V \supseteq V_1 \supseteq I_1 \supseteq I_2$.

(е) *Если фактор-кольцо Ли I_1/I_2 абелево, то фактор-группа I_1/I_2 абелева.*

(ж) *Если фактор-кольцо Ли I_1/I_2 центрально в V_1, то фактор-группа I_1/I_2 центральна в группе V_1.*

Замечание. Части (д)–(ж) теоремы, посвященные переходам от колец Ли к группам, не выглядят вполне двойственными к частям (а)–(г), посвященным переходам от групп к кольцам Ли. На самом деле соответствующие двойственные утверждения имеют место (мы оставляем их читателю в качестве упражнения). Например, для n, кратного некоторому $n_{10}(c)$, если J — идеал кольца L, содержащийся в nL, то это же множество J является нормальной подгруппой группы $nL \leq F$. Но в приложениях к задачам о группах нам потребуются именно утверждения (д)–(ж) теоремы 1; ведь с произвольной нильпотентной группой G заранее не связано никакое кольцо Ли, и, применяя гомоморфизм из F на G, мы должны полагаться на подгруппы.

Доказательство. Далее мы предполагаем, что n кратно $n_4n_6n_5$; тогда $U = F^n \subseteq n_6F \cap L$ по леммам 2 и 3.

(а) Пусть $a, b \in U$. Имеем $a = a_1^{n_6}$ для некоторого $a_1 \in F$. Тогда согласно (1) $a+b = a \cdot b \cdot A$, где $A \in [F, b]_G \leq U$, так как $b \in U \triangleleft_G F$. В силу (2) $[a, b]_L = [a, b]_G \cdot B$, где $B \in [F, b]_G \leq U$ по той же причине.

(b) Пусть $a, b \in N$. Снова $a = a_1^{n_6}$ для некоторого $a_1 \in F$. С учетом (1) имеем $a + b = a \cdot b \cdot A$, где $A \in [F, b]_G \leq N$, ибо $b \in N \triangleleft_G F$. Для любого $g \in U$ будет также $g = g_1^{n_6}$ для некоторого $g_1 \in F$. Тогда согласно (2) имеем $[g, b]_L = [g, b]_G \cdot B$, где $B \in [F, b]_G \leq N$ по той же причине. Далее, согласно (1) $g + b = g \cdot b \cdot A$, где $A \in [F, b]_G \leq N$, так что $g + N \subseteq gN$. Пусть далее n кратно $n_6n_5^2$. Тогда $g = g_1^{n_6}$, где $g_1 \in F^{n_6n_5}$. Ввиду (3) $g \cdot b = g + b + C(g_1, b)$, где $C(g_1, b)$ принадлежит идеалу, порожденному элементом $[g_1, b]_L$ в $\langle g_1, b\rangle_L$. Но, как показано выше, $N \triangleleft_L F^{n_6n_5}$. Поскольку $b \in N$, то $C(g_1, b) \in N$, так что $g \cdot N \subseteq g + N$.

(в) Пусть $a, b \in N_1$. Имеем $a = a_1^{n_6}$ для некоторого $a_1 \in F$. Согласно (2) $[a, b]_L = [a, b]_G \cdot B$, где B лежит в нормальном замыкании в F подгруппы $[[a_1, b]_G, \langle a, b\rangle_G]_G$. Но $[a_1, b]_G \in N_1$, так как $b \in N_1 \triangleleft_G F$; также $\langle a, b\rangle_G \leq N_1$. Значит, $[[a_1, b]_G, \langle a, b\rangle_G]_G \leq [N_1, N_1] \leq N_2 \triangleleft_G F$, откуда $[a, b]_L \in N_2$.

(г) Пусть $g \in U_1$ и $b \in N_1$. Имеем $g = g_1^{n_6}$ для некоторого $g_1 \in F$. Согласно (2) $[g,b]_L = [g,b]_G \cdot B$, где B лежит в нормальном замыкании в F подгруппы $[[g_1,b]_G, \langle g,b\rangle_G]_G$. Но $[g_1,b]_G \in N_1$, ибо $b \in N_1 \lhd_G F$, и $\langle g,b\rangle_G \leq U_1$. Значит, $[[g_1,b]_G, \langle g,b\rangle_G]_G \leq [N_1,U_1] \leq N_2 \lhd_G F$, откуда $[g,b]_L \in N_2$.

(д) Пусть $v,w \in I$. Тогда $v = n_6 v_1$ для некоторого $v_1 \in U$ по лемме 7. Согласно (3) $v \cdot w = v + w + C$, где C лежит в идеале, порожденном элементом $[v_1,w]_L$ в $\langle v_1,w\rangle_L$. Этот идеал содержится в I, так как $w \in I \lhd_L U$ и $v_1 \in U$. Следовательно, $v \cdot w \in I$. Также $v^{-1} = -v \in I$. Значит, I — подгруппа. Для любого $g \in V$ по лемме 7 имеем $g = g_1^{n_6}$ для некоторого $g_1 \in U$. Согласно (4) $[g,w]_G = [g,w]_L + D$, где D лежит в идеале, порожденном множеством $[[g_1,w]_L, \langle g,w\rangle_L]_L$ в $\langle g_1,w\rangle_L$. Этот идеал содержится в I, поскольку $[g_1,w]_L \in I \lhd_L U$ и $\langle g,w\rangle_L \leq U$. Таким образом, I — нормальная подгруппа группы V.

(е) Пусть $v,w \in I_1$. Тогда $v = n_6 v_1$ для некоторого $v_1 \in U$ по лемме 7. Ввиду (4) $[v,w]_G = [v,w]_L + D$, где D лежит в идеале, порожденном множеством $[[v_1,w]_L, \langle v,w\rangle_L]_L$ в $\langle v_1,w\rangle_L$. Этот идеал содержится в $[I_1,I_1]_L \leq I_2$, так как $[v_1,w]_L \in I_1$ и $\langle v,w\rangle_L \leq I_1$; также $[v,w]_L \in [I_1,I_1]_L \leq I_2$. Значит, $[v,w]_G \in I_2$.

(ж) Пусть $w \in I_1$ и $g \in V_1$. Тогда $g = n_6 g_1$ для некоторого $g_1 \in U$ по лемме 7. Согласно (4) $[g,w]_G = [g,w]_L + D$, где D лежит в идеале, порожденном множеством $[[g_1,w]_L, \langle g,w\rangle_L]_L$ в $\langle g_1,w\rangle_L$. Так как $[g_1,w]_L \in I_1$ и $\langle g,w\rangle_L \leq V_1$, этот идеал содержится в $[I_1,V_1] \leq I_2$; также $[g,w]_L \in [V_1,I_1]_L \leq I_2$. Значит, $[g,w]_G \in I_2$. $\square$

Теперь предположим, что P — произвольная нильпотентная группа ступени c. Пусть F — свободная нильпотентная группа ступени c, построенная в рамках $\mathbb{Q}L$, как выше, на достаточно большом множестве свободных порождающих, и пусть $\pi : F \to P$ — эпиморфизм группы F на P. Тогда $\pi(F^n) = P^n$. Для n_9 из теоремы 1 для любого n, кратного n_9, определим следующим образом новые операции на множестве P^n:

$$\pi(a) + \pi(b) = \pi(a+b); \quad [\pi(a), \pi(b)]_L = \pi([a,b]_L) \tag{5}$$

для любых $a,b \in F^{p^n}$. Покажем, что это определение корректно. Положим $N = \operatorname{Ker}\pi \cap F^n \lhd F$; тогда $N \lhd_L F^n$ по теореме 1(б). Предположим, что $a'N = aN$ и $b'N = bN$. Тогда

$$\begin{aligned}(a'+b')N &= (a'+b') + N = (a'+N) + (b'+N) = a'N + b'N \\ &= aN + bN = (a+N) + (b+N) = (a+b) + N = (a+b)N\end{aligned}$$

по теореме 1(б). Далее, по теореме 1(б)

$$\begin{aligned}[a',b']_L N &= [a',b']_L + N = [a'+N, b'+N]_L = [a'N, b'N]_L \\ &= [aN, bN]_L = [a+N, b+N]_L = [a,b]_L + N = [a,b]_L N.\end{aligned}$$

Теорема 2. (а) *Множество $\overline{U} = P^n$ является кольцом Ли относительно операций* (5).

(б) *Любая нормальная подгруппа $\overline{N}$ группы P, содержащаяся в $\overline{U}$, является идеалом кольца Ли $\overline{U}$, причем $g + \overline{N} = g\overline{N}$ для любого $g \in \overline{U}$.*

Пусть $\overline{U}_1$, $\overline{N}_1$ и $\overline{N}_2$ — нормальные подгруппы группы P такие, что $\overline{U} \supseteq \overline{U}_1 \supseteq \overline{N}_1 \supseteq \overline{N}_2$.

(в) *Если фактор-группа $\overline{N}_1/\overline{N}_2$ абелева, то фактор-кольцо Ли $\overline{N}_1/\overline{N}_2$ абелево. Кольцо Ли $\overline{U}$ разрешимо ступени не выше ступени разрешимости группы $\overline{U}$.*

(г) *Если фактор-группа $\overline{N}_1/\overline{N}_2$ центральна в группе $\overline{U}_1$, то фактор-кольцо Ли $\overline{N}_1/\overline{N}_2$ центрально в кольце Ли $\overline{U}_1$. Кольцо Ли $\overline{U}_1$ нильпотентно ступени не выше ступени нильпотентности группы $\overline{U}_1$.*

(д) *Если $\overline{I}$ — идеал кольца $\overline{U}$, содержащийся в $\overline{V} = P^{nn_3n_4n_6}$, то это же множество $\overline{I}$ является нормальной подгруппой группы $P^{nn_3n_4n_6}$.*

Пусть $\overline{V}_1$, $\overline{I}_1$ и $\overline{I}_2$ — идеалы кольца $\overline{U}$ такие, что $\overline{V} \supseteq \overline{V}_1 \supseteq \overline{I}_1 \supseteq \overline{I}_2$.

(е) *Если фактор-кольцо Ли $\overline{I}_1/\overline{I}_2$ абелево, то фактор-группа $\overline{I}_1/\overline{I}_2$ абелева. Ступень разрешимости подгруппы $P^{nn_3n_4n_6}$ равна ступени разрешимости кольца Ли $\overline{V}$.*

(ж) *Если фактор-кольцо Ли $\overline{I}_1/\overline{I}_2$ центрально в $\overline{V}_1$, то фактор-группа $\overline{I}_1/\overline{I}_2$ центральна в группе $\overline{V}_1$. Ступень нильпотентности подгруппы $\overline{V}_1$ равна ступени нильпотентности кольца Ли $\overline{V}_1$.*

(з) *Если φ — автоморфизм группы P, то его ограничение на $\overline{U}$ является автоморфизмом кольца Ли $\overline{U}$.*

Доказательство. Мы можем считать, что $\overline{U} = \pi(U)$, где U — как в теореме 1, $\overline{N} = \pi(N)$, и т. д. Тогда утверждения (а)–(ж) сразу следуют из теоремы 1 в силу определения операций (5), потому что все они выражаются либо формулами, либо включениями. Например, так как $[a,b,c]_L + [b,c,a]_L + [c,a,b]_L = 0$ в U, применяя π, получаем тождество Якоби в $\overline{U}$:

$$[\pi(a),\pi(b),\pi(c)]_L + [\pi(b),\pi(c),\pi(a)]_L + [\pi(c),\pi(a),\pi(b)]_L = 0.$$

Другой пример: если $[\overline{N}_1,\overline{N}_1]_G \le \overline{N}_2$ в $\overline{U}$, то $[N_1,N_1]_G \le N_2$ в U; значит, по теореме 1(в) $[N_1,N_1]_L \le N_2$; применяя π, получаем, что $[\overline{N}_1,\overline{N}_1]_L \le \overline{N}_2$. Чтобы получить дополнительные утверждения о ступенях разрешимости и нильпотентности, достаточно заметить, что члены ряда коммутантов и нижнего центрального ряда подгруппы $\overline{U}_1$ нормальны в P и что такие же члены в кольце Ли $\overline{V}_1$ являются идеалами в $\overline{U}$.

Докажем (з). Для данного c многочлены $A(x_1,x_2)$ и $B(x_1,x_2)$ из леммы 5 можно считать фиксированными; тогда те же формулы выполняются для любых элементов группы F. По лемме 3 для любого $x \in F^n$ имеется $x' \in F$ такой, что $x = {x'}^{n_6}$. Тогда $\pi(x+y) = \pi(xyA(x',y)) = \pi(x)\pi(y)A(\pi(x'),\pi(y))$. Значит, в $\overline{U}$ имеем $u+v = uvA(u',v)$, как только $u = {u'}^{n_6}$, и такой элемент u' всегда существует. Теперь

$$\varphi(u+v) = \varphi(uvA(u',v)) = \varphi(u)\varphi(v)A(\varphi(u'),\varphi(v)) = \varphi(u)+\varphi(v).$$

Аналогично $[u,v]_L = [u,v]_G B(u',v)$ для любого $u,v \in \overline{U}$, если $u = {u'}^{n_6}$; значит, $\varphi([u,v]_L) = [\varphi(u),\varphi(v)]_G B(\varphi(u'),\varphi(v)) = [\varphi(u),\varphi(v)]_L$. $\square$

Замечание. Предположим, что P — нильпотентная p-группа ступени c для некоторого простого p. Тогда для любого k, взаимно простого с p, она содержит единственный k-й корень из любого $g \in P$; на самом деле этот корень лежит в $\langle g\rangle$. (Другими словами, любая p-группа является $\mathbb{Q}_\sigma$-группой, где σ — множество всех простых чисел, отличных от p.) Тогда любая подгруппа вида P^n фактически равна P^{p^m}, где p^m — наибольшая степень p, делящая n. Аддитивные группы колец Ли $\overline{U}$ и $\overline{V}$, построенных в теореме 2, также являются p-группами (так что это $\mathbb{Q}_\sigma$-алгебры Ли), так как для коммутирующих элементов сложение в этих кольцах Ли совпадает с групповым умножением. Функцию $n_9(c)$ здесь можно заменить более точной функцией $p^{m(p,c)}$, где $m(p,c)$ зависит от p, как и от c. Значение этой функции $m(p,c)$ тем лучше (т. е. меньше), чем больше p. В частности, при $p > c$ можно положить $m(p,c) = 0$, что соответствует применимости соответствия Лазара, когда группа P сама превращается в $\mathbb{Q}_\sigma$-алгебру Ли.

3. Сведения к кольцам Ли

Предположим, что конечная p-группа P допускает автоморфизм φ порядка p, имеющий ровно p^m неподвижных точек. По теореме Хухро [8] тогда P обладает подгруппой (p,m)-ограниченного индекса, которая нильпотентна p-ограниченной ступени. (Оценка ступени нильпотентности в [8] была $h(p)+1$, и она была улучшена до $h(p)$ Н. Ю. Макаренко [9], где $h(p)$ — функция Хигмэна, ограничивающая ступень нильпотентности кольца Ли с регулярным автоморфизмом порядка p.) С другой стороны, Ю. А. Медведев [1] доказал, что P обладает также подгруппой (p,m)-ограниченного индекса, которая нильпотентна m-ограниченной ступени $\leq g(m)$. Это вытекает из его же теоремы о кольцах Ли: если кольцо Ли с аддитивной p-группой допускает автоморфизм порядка p, имеющий ровно p^m неподвижных точек, то оно обладает подкольцом (p,m)-ограниченного индекса (в аддитивной группе), которое нильпотентно m-ограниченной ступени $\leq l(m)$. Результат для p-групп получается сведением к кольцам Ли, которое можно осуществить либо с помощью колец Ли униформно мощных p-групп, либо используя соответствие Лазара и вышеупомянутую теорему, дающую подгруппу ограниченного индекса и ступени нильпотентности $\leq h(p)$. Но в обоих случаях функция $g(m)$ для групп получается гораздо больше, чем функция $l(m)$ для колец Ли. (Уточняя рассуждения из [10, 11], основанные на униформно мощных p-группах, можно добиться значения $g(m) = 4ml(m)$, см. [12, гл. 14]. Сведение по соответствию Лазара дает то же значение $g(m) = l(m)$, но только для достаточно больших $p \geq f(m)$.)

Используя соответствие из разд. 2, покажем, что можно всегда брать $g(m) = l(m)$. Здесь мы не заботимся об оценке индекса соответствующей подгруппы (подкольца), лишь бы он оставался (p,m)-ограниченной величиной.

Теорема 3. *Пусть $l(m)$ — функция Медведева для колец Ли, т. е. такая, что если кольцо Ли, аддитивная группа которого является p-группой, допускает автоморфизм порядка p, имеющий ровно p^m неподвижных точек, то оно обладает подкольцом (p,m)-ограниченного индекса (в аддитивной группе), которое нильпотентно ступени $\leq l(m)$. Тогда любая конечная p-группа P, допускающая автоморфизм φ порядка p ровно с p^m неподвижными точками, имеет подгруппу (p,m)-ограниченного индекса, которая нильпотентна ступени $\leq g(m) = l(m)$.*

Доказательство. В силу вышесказанного мы можем считать группу P нильпотентной ступени $c \leq h(p)$. Тогда для некоторого p-ограниченного натурального $n = n(c)$ множество P^{p^n} может быть оснащено структурой кольца Ли U с подкольцом $V = P^{p^{n+n'}}$, удовлетворяющим теореме 2, где $p^{n'}$ — наивысшая степень p, делящая $n_3 n_4 n_6$. По теореме Медведева [1] для некоторого (p,m)-ограниченного натурального $f = f(p,m)$ идеал $p^f V$ нильпотентен ступени $\leq l(m)$. Так как это также идеал в U, по теореме 2(д) это множество является нормальной подгруппой в P^{p^n} и потому совпадает с подгруппой V^{p^f}. По теореме 2(ж) у нее та же ступень нильпотентности $\leq l(m)$. Поскольку ранги всех φ-инвариантных секций в P не превосходят mp (см., например, [12, следствие 2.7]), эта подгруппа имеет (p,m)-ограниченный индекс в P. $\square$

Другое приложение — новый вариант сведения к кольцу Ли в доказательстве следующей теоремы Хухро [2]: если конечная p-группа P допускает автоморфизм порядка p^n ровно с p^m неподвижными точками, то P обладает подгруппой (p,m,n)-ограниченного индекса, которая разрешима ступени $\le 2k$, где $k=k(p^n)$ — функция Крекнина, ограничивающая ступень разрешимости кольца Ли с регулярным автоморфизмом порядка p^n. В первой части доказательства в [2] показывается, что для некоторой подгруппы P_1, имеющей (p,m,n)-ограниченный индекс, ступень нильпотентности подгруппы $P_1^{(k)}$ ограничена в терминах p, m и n. Потом соответствие Мальцева применяется к свободной нильпотентной φ-группе, и результат затем транслируется в существование подгруппы P_2, имеющей (p,m,n)-ограниченный индекс в $P_1^{(k)}$, такой, что P_2 разрешима ступени $\le k$. Из этого требуемый результат выводится по свойствам мощных p-групп.

Покажем, как можно применить соответствие из разд. 2, чтобы найти такую подгруппу P_2 в $H=P_1^{(k)}$. Так как H нильпотентна (p,m,n)-ограниченной ступени c, для некоторого (p,m,n)-ограниченного натурального $f=f(c)$ множество H^{p^f} можно оснастить структурой кольца Ли U с подкольцом $V=H^{p^{f+f'}}$, удовлетворяющим теореме 2, где $p^{f'}$ — наибольшая степень p, делящая $n_3n_4n_6$. По теореме Крекнина $p^m(p^nV)^{(k)}=0$ и, значит, тем более $(p^{n+m}V)^{(k)}=0$. Поскольку $p^{n+m}V$ — идеал в U, по теореме 2(д) множество $p^{n+m}V$ является нормальной подгруппой в H, которая совпадает с $V^{p^{n+m}}$. По теореме 2(е) эта подгруппа разрешима той же ступени $\le k$. Так как ранги всех φ-инвариантных секций не превосходят mp^n (см., например, [12, следствие 2.7]), эта подгруппа имеет (p,m,n)-ограниченный индекс в H.

Хотя это рассуждение не улучшает оценки ступени разрешимости в [2] (которая почти наилучшая, см. следующий раздел), оно дает еще одну иллюстрацию применения нашего соответствия из разд. 2.

4. Примеры с функциями Хигмэна и Крекнина

Теоремы Хигмэна [13] и Крекнина [3] фактически относятся к градуированным кольцам Ли, а их приложения к кольцам Ли с регулярными автоморфизмами конечного порядка основаны на корневом разложении. Может, однако, существовать некоторая разница между этими функциями для колец Ли ($\mathbb{Z}$-алгебр) $h_{\mathbb{Z}}$ и $k_{\mathbb{Z}}$ и для алгебр Ли над полем, скажем, $\mathbb{Q}$, обозначаемыми через $h_{\mathbb{Q}}$ и $k_{\mathbb{Q}}$.

Определим функцию Хигмэна $h_{\mathbb{Z}}(p)$ следующим образом. Для простого числа p пусть $L=L_0\oplus L_1\oplus\dots\oplus L_{p-1}$ — свободное $(\mathbb{Z}/p\mathbb{Z})$-градуированное кольцо Ли ($\mathbb{Z}$-алгебра), где $[L_i,L_j]\subseteq L_{i+j(\mathrm{mod}p)}$. Теорема Хигмэна утверждает, что фактор-кольцо $L/_{\mathrm{id}}\langle L_0\rangle$ нильпотентно p-ограниченной ступени $h_{\mathbb{Z}}(p)$, что и определяет функцию Хигмэна. Отсюда следует, что если кольцо Ли M допускает регулярный автоморфизм φ порядка p, то M нильпотентно ступени $\le h_{\mathbb{Z}}(p)$.

Аналогичное определение, основанное на свободной $(\mathbb{Z}/p\mathbb{Z})$-градуированной $\mathbb{Q}$-алгебре Ли $\mathbb{Q}L$ (где L, как выше), может, в принципе, дать меньшее значение $h_{\mathbb{Q}}(p)$ для ступени нильпотентности фактор-алгебры $\mathbb{Q}L/_{\mathrm{id}}\langle\mathbb{Q}L_0\rangle$. Это может случиться, если аддитивная группа $L/_{\mathrm{id}}\langle L_0\rangle$ имеет большое кручение, содержащее нетривиальные члены нижнего центрального ряда этого фактор-кольца. Пока не ясно, может так быть или нет, так же как неизвестно, всегда ли $h_{\mathbb{Q}}(p)=h_{\mathbb{Z}}(p)$ для простых p. Известно только, что такого кручения вообще нет для $p=2$ и $p=3$, что $h_{\mathbb{Q}}(5)=6=h_{\mathbb{Z}}(5)$ согласно Хигмэну [13], и что $h_{\mathbb{Q}}(7)=12=h_{\mathbb{Z}}(7)$ в силу примеров Хигмэна [13], показывающих, что $h_{\mathbb{Q}}(p)\ge(p^2-1)/4$

для всех простых p, и вычислений Шимеми (не опубликовано) и Хьюза [14], которые показали, что $h_{\mathbb{Z}}(7) \leq 12$. Стоит также заметить, что явная верхняя оценка для $h_{\mathbb{Z}}(p)$, принадлежащая В. А. Крекнину и А. И. Кострикину [3, 15], равна $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$.

Отметим, что для каждого простого p существует нильпотентная $\mathbb{Q}$-алгебра Ли ступени ровно $h_{\mathbb{Q}}(p)$ с регулярным автоморфизмом φ порядка p: просто определим действие φ на образе компоненты $\mathbb{Q}L_j$ в $\mathbb{Q}L/{}_{\mathrm{id}}\langle \mathbb{Q}L_0\rangle$ как умножение на ω^j, где ω — примитивный корень p-й степени из единицы. Но для $h_{\mathbb{Z}}$ не известно, может ли p-кручение в $L/{}_{\mathrm{id}}\langle L_0\rangle$ помешать построить примеры нильпотентных колец Ли ступени ровно $h_{\mathbb{Z}}(p)$ с регулярным автоморфизмом порядка p.

Напомним, что если конечная p-группа допускает автоморфизм порядка p ровно с p^m неподвижными точками, то она обладает подгруппой (p,m)-ограниченного индекса, которая нильпотентна ступени $\leq h(p)$. Хотя в работах [16, 8, 9] использовалась функция $h(p) = h_{\mathbb{Z}}(p)$, можно доказать такой же результат с функцией $h(p) = h_{\mathbb{Q}}(p)$ (может быть, несколько ухудшив (p,m)-ограниченную оценку индекса подгруппы). В самом деле, в доказательстве использовалось включение $p^{h(p)+1}[x_1, \dots, x_{h(p)+1}] \in {}_{\mathrm{id}}\langle C_L(\varphi)\rangle$ для кольца Ли L, допускающего автоморфизм φ порядка p. На самом деле здесь достаточно иметь включение $p^{f(p,m)}[x_1, \dots, x_{h(p)+1}] \in {}_{\mathrm{id}}\langle C_L(\varphi)\rangle$ для некоторого (p,m)-ограниченного натурального $f(p,m)$. Из определения функции $h = h_{\mathbb{Q}}(p)$ вытекает, что в свободной градуированной алгебре Ли коммутатор $[x_1, \dots, x_{h+1}]$ равен рациональной линейной комбинации коммутаторов от компонент элементов x_i, в которых есть подкоммутаторы из L_0. Поэтому существует даже p-ограниченное натуральное число $\alpha(p)$ такое, что $p^{\alpha(p)}[x_1, \dots, x_{h+1}]$ — p-целая линейная комбинация тех же коммутаторов. В силу включения $pL \subseteq L_0 + \dots + L_{p-1}$, где L_j — аналоги корневых пространств, которое выполняется для любого кольца Ли L с автоморфизмом φ порядка p, получаем $p^{\alpha(p)+h+1}[x_1, \dots, x_{h+1}] \in {}_{\mathrm{id}}\langle C_L(\varphi)\rangle$. Применяя остальную часть рассуждений из [8, 9], приходим к требуемому результату.

Теорема 4. *Если конечная p-группа P допускает автоморфизм порядка p ровно с p^m неподвижными точками, то P обладает подгруппой (p,m)-ограниченного индекса, которая нильпотентна ступени $\leq h_{\mathbb{Q}}(p)$.* $\square$

Теперь мы покажем, что функция Хигмэна $h_{\mathbb{Q}}(p)$ для $\mathbb{Q}$-алгебр Ли является наилучшей оценкой для ступени нильпотентности в этом теоретико-групповом результате (если требовать, чтобы она зависела только от p).

Как замечено выше, существует нильпотентная $\mathbb{Q}$-алгебра Ли N ступени ровно $h = h_{\mathbb{Q}}(p)$ с регулярным автоморфизмом φ порядка p. В ней есть элементы $n_1, \dots, n_h \in N$ такие, что $[n_1, \dots, n_h] \neq 0$. Будем считать, что $N = \langle n_i^{\varphi^j}\rangle$. По соответствию Мальцева N можно считать также нильпотентной $\mathbb{Q}$-группой, причем φ — ее автоморфизм, действующий так же на том же множестве.

Пусть σ — множество всех простых чисел, отличных от p, и пусть $\mathbb{Q}_\sigma = \{m/n \mid m, n \in \mathbb{Z},\ p \nmid n\}$ — кольцо *p-целых* чисел. Пусть M — $\mathbb{Q}_\sigma$-подкольцо Ли кольца N, порожденное множеством

$$\{n_i^{\varphi^j} \mid i = 1, \dots, h;\ j = 0, \dots, p-1\},$$

и G — $\mathbb{Q}_\sigma$-группа, порожденная теми же элементами. Семейство групп, дающее требуемые примеры, составят фактор-группы $G_n = G/G^{p^n}$, $n \in \mathbb{N}$. Будучи периода p^n, нильпотентными и конечно порожденными (так же, как абстрактные группы), группы G_n являются конечными p-группами для всех n. Пусть $C_n = \{x \in G \mid \varphi(x) \in xG^{p^n}\}$ — полный прообраз централизатора $C_{G_n}(\varphi)$.

Пусть p^{m_i} обозначает наивысшую степень p, делящую $n_i = n_i(c)$, где n_i — числа из лемм разд. 1.

Лемма 8. *Для любого $n \geq m_8 + 1$ справедливо соотношение*

$$C_n \subseteq p^{n-m_8-1}M.$$

Доказательство. Если $x \in C_n$, то $\varphi^j(x) \in xG^{p^n} \subseteq x + p^{n-m_8}M$ по лемме 6. Так как $C_N(\varphi) = 0$, имеем

$$x + \varphi(x) + \varphi^2(x) + \dots + \varphi^{p-1}(x) = 0.$$

Значит, $px \in p^{n-m_8}M$. Из этого следует, что $x \in p^{n-m_8-1}M$, ибо аддитивная групп M не имеет кручения. $\square$

Лемма 9. *Для любого n порядок $|C_{G_n}(\varphi)|$ является p-ограниченной величиной (не зависящей от n, а зависящей только от p).*

Доказательство. Пусть T — трансверсаль по подгруппе G^{p^n} в группе C_n, так что $|T| = |C_{G_n}(\varphi)|$. Определим отображение

$$\alpha : T \to p^{n-m_8-1}M/p^{n+m_7}M$$

по правилу $\alpha(t) = t + p^{n+m_7}M$. В силу леммы 8 образ действительно лежит в $p^{n-m_8-1}M/p^{n+m_7}M$. Это отображение инъективно по лемме 6. Значит, $|T| \leq |p^{n-m_8-1}M/p^{n+m_7}M|$. Аддитивная группа $p^{n-m_8-1}M/p^{n+m_7}M$ имеет период $p^{m_7+m_8+1}$. Как $\mathbb{Q}_\sigma$-модуль $p^{n-m_8-1}M/p^{n+m_7}M$ порождается p-ограниченным числом элементов, а именно образами p^{n-m_8-1}-х кратных базисных коммутаторов веса $\leq h$ от элементов

$$\left\{n_i^{\varphi^j} \mid i = 1, \dots, h;\ j = 0, \dots, p-1\right\}.$$

Следовательно, будучи p-группой, $p^{n-m_8-1}M/p^{n+m_7}M$ порождается тем же множеством как абстрактная группа. В результате эта группа имеет p-ограниченный порядок, а значит, то же верно для $C_{G_n}(\varphi)$. (Здесь можно считать n достаточно большим числом относительно любой функции от p, так как иначе даже порядок группы G/G^{p^n} p-ограничен.) $\square$

Лемма 10. *Для любого $a \geq 0$ существует $n \geq a$ такое, что ступень нильпотентности группы G^{p^a}/G^{p^n} равна в точности h.*

Доказательство. Для заданного a мы просто покажем, что

$$[n_1^{p^a}, \dots, n_h^{p^a}]_G \notin G^{p^n}$$

для некоторого n. Так как $G^{p^n} \subseteq p^{n-m_4}M$ по лемме 2, достаточно показать, что $[n_1^{p^a}, \dots, n_h^{p^a}]_G \notin p^{n-m_4}M$. Поскольку ступень нильпотентности равна h, групповой коммутатор веса h равен такому же кольцевому коммутатору:

$$\left[n_1^{p^a}, \dots, n_h^{p^a}\right]_G = [p^a n_1, \dots, p^a n_h]_L = p^{ah}[n_1, \dots, n_h]_L.$$

Аддитивная группа M конечно порождена, и потому

$$\bigcap_i p^i M = 0.$$

Так как $[n_1, \dots, n_h]_L \neq 0$, существует j такое, что $[n_1, \dots, n_h]_L \notin p^j M$. Тогда

$$p^{ah}[n_1, \dots, n_h]_L \notin p^{j+ah}M,$$

так как M не имеет кручения. Значит, лемма справедлива при $n \geq j + ah + m_4$. $\square$

В силу лемм 9 и 10 группы G_n дают примеры, доказывающие следующую теорему.

Теорема 5. *Не существует такой функции $g(p,m)$, что для любой конечной p-группы G, допускающей автоморфизм порядка p ровно с p^m неподвижными точками, ступень нильпотентности подгруппы $G^{p^{g(p,m)}}$ не превосходит $h_{\mathbb{Q}}(p)-1$.* $\square$

Теперь обратимся к теореме Хухро [2] о конечных p-группах с автоморфизмом порядка p^n с p^m неподвижными точками. Опять же в работе [2] использовалась функция Крекнина $k = k_{\mathbb{Z}}$, определенная через градуированное $\mathbb{Z}$-кольцо Ли. Но рассуждение, аналогичное проведенному для теоремы 4, позволяет заменить $k_{\mathbb{Z}}(p^n)$ возможно меньшим значением $k_{\mathbb{Q}}(p^n)$, определяемым через градуированную $\mathbb{Q}$-алгебру Ли.

Теорема 6. *Если конечная p-группа P допускает автоморфизм порядка p^n ровно с p^m неподвижными точками, то P обладает подгруппой (p,m,n)-ограниченного индекса, ступень разрешимости которой $\leq 2k_{\mathbb{Q}}(p^n)$.* $\square$

Пока не ясно, можно ли сделать $k(p^n)$ оценкой ступени разрешимости. Сейчас мы покажем, что эта оценка здесь не может быть сделана меньше, чем $k_{\mathbb{Q}}(p^n)$. Остается разрыв между $k_{\mathbb{Q}}(p^n)$ в примерах и $2k_{\mathbb{Q}}(p^n)$ в теореме 6.

Соответствующие примеры можно построить практическим таким же образом, как в доказательстве теоремы 5, если бы мы могли начать с *нильпотентной* $\mathbb{Q}$-алгебры Ли ступени разрешимости ровно $k = k_{\mathbb{Q}}(p^n)$, которая допускает регулярный автоморфизм порядка p^n. Покажем, что такая алгебра действительно существует.

Пусть L — свободная $(\mathbb{Z}/p^n\mathbb{Z})$-градуированная $\mathbb{Q}$-алгебра Ли на счетном числе свободных порождающих. Можно считать L абстрактной свободной $\mathbb{Q}$-алгеброй Ли на свободных порождающих x_{ij}, $i = 0,1,\dots,p^n-1$, $j = 1,2,\dots$, где первый индекс используется для указания компоненты градуировки. Тогда $(\mathbb{Z}/p^n\mathbb{Z})$-градуировка задается разложением $L = L_0 \oplus \dots \oplus L_{p^n-1}$, где L_k натянуто на все коммутаторы от x_{ij}, у которых сумма первых индексов сравнима с $k (\operatorname{mod} p^n)$. Конечно, L однородно относительно свободных порождающих x_{ij}, т. е. $L = \bigoplus\limits_{i=1}^{\infty} W_i$, где W_t натянуто на все коммутаторы веса t от элементов x_{ij}.

Теперь пусть I — идеал алгебры L, порожденный L_0. По теореме Крекнина фактор-алгебра L/I разрешима p^n-ограниченной ступени разрешимости $k = k_{\mathbb{Q}}(p^n)$, что и определяет функцию Крекнина.

Идеал I также однороден: $I = \bigoplus\limits_i (I \cap W_i)$. В самом деле, он натянут на коммутаторы вида $[l_0, y_1, \dots, y_s]$, где $l_0 \in L_0$, а y_i — произвольные элементы из L. Но L_0 натянуто на некоторые коммутаторы от элементов x_{ij}, так же как и L. Отсюда следует, что I натянут на некоторые коммутаторы от x_{ij} и поэтому однороден.

Теперь

$$L/I = \bigoplus_{i\geq 1} (W_i/(I\cap W_i)), \quad \gamma_m(L/I) = \bigoplus_{i\geq m} (W_i/(I\cap W_i))$$

для любого m. Пусть $\delta_n(y_1,\dots,y_{2^n}) = 0$ — тождество разрешимости ступени n. Так как ступень разрешимости фактор-алгебры L/I равна k, существуют некоторые элементы z_i среди образов элементов x_{ij} такие, что $\delta_{k-1}(z_1,\dots,z_{2^{k-1}}) \neq 0$ в L/I. Поскольку $\delta_{k-1}(z_1,\dots,z_{2^{k-1}})$ лежит в образе $W_{2^{k-1}}$, образ элемента $\delta_{k-1}(z_1,\dots,z_{2^{k-1}})$ нетривиален также в $L/(I+\gamma_{2^{k-1}+1}(L))$. Последняя алгебра

Ли нильпотентна ступени 2^{k-1}. Она допускает регулярный автоморфизм порядка p^n, действующий на образе L_i умножением на ω^i, где ω — примитивный корень p^n-й степени из единицы.

Теперь можно использовать ту же конструкцию, что в доказательстве теоремы 5, чтобы доказать следующий результат.

Теорема 7. *Не существует такой функции $g(p, m, n)$, что если конечная p-группа P допускает автоморфизм порядка p^n ровно с p^m неподвижными точками, то ступень разрешимости подгруппы $G^{p^{g(p,m,n)}}$ не превосходит $k_{\mathbb{Q}}(p^n) - 1$.* □

Можно построить подобные же примеры, но основанные на другом простом числе $q \neq p$, т. е. группы G/G^{q^n}, подобные вышепостроенным, где σ — множество всех простых чисел, отличных от q. В результате получается следующий результат.

Теорема 8. *Для любых различных простых чисел p и q существуют конечные q-группы ступени нильпотентности ровно $h_{\mathbb{Q}}(p)$, допускающие регулярный автоморфизм порядка p.* □

В работе Хигмэна [13] такие примеры построены (также с использованием формулы Бейкера — Хаусдорфа) только для достаточно больших простых чисел q. Как мы заметили ранее, в копростой ситуации имеется гипотетический разрыв между $h_{\mathbb{Q}}(p)$, ступенью нильпотентности в примерах, и $h_{\mathbb{Z}}(p)$, верхней оценкой для ступени нильпотентности.

Используя тот же метод, можно построить также примеры конечных q-групп ступени разрешимости ровно $k_{\mathbb{Q}}(n)$, допускающих регулярный автоморфизм копростого порядка n. Но ограничение ступени разрешимости таких групп какой бы то ни было функцией от n пока остается открытой проблемой.

ЛИТЕРАТУРА

1. *Medvedev Yu.* p-Divided Lie rings and p-groups // J. London Math. Soc. (2). 1999. V. 59. P. 787–798.
2. *Хухро Е. И.* Конечные p-группы, допускающие p-автоморфизм с малым числом неподвижных точек // Мат. сб. 1993. Т. 184. С. 53–64.
3. *Крекнин В. А.* Разрешимость алгебр Ли с регулярным автоморфизмом конечного периода // Докл. АН СССР. 1963. Т. 150. С. 467–469.
4. *Lazard M.* Sur les groupes nilpotents et les anneaux de Lie // Ann. Sci. École Norm. Super. 1954. V. 71. P. 101–190.
5. *Weigel T.* Exp and Log functors for the categories of powerful p-central groups and Lie algebras. Habilitationsschrift. Freiburg i. Br. 1994.
6. *Бурбаки Н.* Группы и алгебры Ли. Гл. 2–3. Свободные алгебры Ли и группы Ли. М.: Мир, 1978.
7. *Blackburn N.* Conjugacy in nilpotent groups // Proc. Amer. Math. Soc. 1965. V. 16. P. 143–148.
8. *Хухро Е. И.* Конечные p-группы, допускающие автоморфизм порядка p с малым числом неподвижных точек // Мат. заметки. 1985. Т. 38. С. 652–657.
9. *Макаренко Н. Ю.* Почти регулярные автоморфизмы простого порядка // Сиб. мат. журн. 1992. Т. 33, № 5. С. 206–208.
10. *Medvedev Yu.* p-Groups, Lie p-rings and p-automorphisms // J. London Math. Soc. 1998. V. 58, N 1. P. 27–37.
11. *Shalev A.* On almost fixed point free automorphisms // J. Algebra. 1993. V. 157. P. 271–282.
12. *Khukhro E. I.* p-Automorphisms of finite p-groups. Cambridge: Cambridge Univ. Press, 1998. (London Math. Soc. Lecture Note Ser.; V. 246).
13. *Higman G.* Groups and rings which have automorphisms without non-trivial fixed elements // J. London Math. Soc. (2). 1857. V. 32. P. 321–334.

14. *Hughes I.* Groups with fixed-point-free automorphisms // C. R. Math. Rep. Acad. Sci. Canada. 1985. V. 7. P. 61–66.
15. *Крекнин В. А., Кострикин А. И.* Алгебры Ли с регулярными автоморфизмами // Докл. АН СССР. 1963. Т. 149. С. 249–251.
16. *Alperin J. L.* Automorphisms of solvable groups // Proc. Amer. Math. Soc. 1962. V. 13. P. 175–180.
17. *Мальцев А. И.* Нильпотентные группы без кручения // Изв. АН СССР. Сер. мат. 1949. Т. 13. С. 201–212.

Статья поступила 26 августа 1999 г.

Departamento de Matemáticas — Matematika Saila
Facultad de Ciencias — Zientzi Fakultatea
Universidad del País Vasco — Euskal Herriko Unibertsitatea
Apdo. 644, 48080, Bilbao, Spain
mtbjazaa@lg.ehu.es

Институт математики им. С. Л. Соболева СО РАН,
просп. Коптюга, 4, 630090 Новосибирск, Россия
khukhro@math.nsc.ru