П. А. Кожевников, Об одной независимой бесконечной системе групповых тождеств, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 1997, номер 4, 13–16

линейная комбинация координатных функций σF обладает свойством λ, т.е. для любых $\alpha_i \in \{0,1\}$, не равных одновременно нулю, функция $\sum_{i=1}^{n} \alpha_i \tau_i \sigma F$ обладает свойством λ. Поскольку оператор σ коммутирует с операторами проектирования и является линейным, имеем

$$\sum_{i=1}^{n} \alpha_i \tau_i \sigma F = \sum_{i=1}^{n} \alpha_i \sigma \tau_i F = \sigma \left(\sum_{i=1}^{n} \alpha_i \tau_i F \right).$$

Таким образом, для любой ненулевой линейной комбинации $\sum_{i=1}^{n} \alpha_i \tau_i F$ и любого оператора $\sigma \in \Sigma$ функция $\sigma(\sum_{i=1}^{n} \alpha_i \tau_i F)$ обладает свойством λ. Это и означает, что любая ненулевая линейная комбинация $\sum_{i=1}^{n} \alpha_i \tau_i F$ обладает вторичным свойством (λ, Σ).

Легко убедиться в обратимости проведенных рассуждений. Тем самым доказана сводимость вторичного свойства (λ, Σ), а вместе с ней и теорема.

В заключение укажем один широкий класс LP линейных операторов, коммутирующих с операторами проектирования. Класс LP содержит операторы фиксации части переменных, любой оператор из класса LP индуцируется некоторым преобразованием пространства V_n следующим образом. Пусть $g : V_n \to V_n$ — произвольное преобразование, соответствующий оператор $\overset{\circ}{g} \in LP$ действует на произвольное булево отображение F по правилу $\overset{\circ}{g}F(x) = F(gx)$. Следующее утверждение практически очевидно.

Утверждение. *Любой оператор из класса LP является линейным и коммутирует с операторами проектирования.*

СПИСОК ЛИТЕРАТУРЫ

1. *Siegenthaler T.* Correlation immunity of non-linear combining functions for cryptographic applications //IEEE Trans. Inform. Theory. 1984. **IT–30**. 776–780.
2. *Xiao G.Z.* Correlation immunity of boolean functions //Electron. Lett. 1987. **23**, N 25. 1335–1336.
3. *Xiao G.Z., Massey J.L.* A spectral characterisation of correlation immune combining functions //IEEE Trans. Inform. Theory. 1988. **IT–34**. 569–571.
4. *Camion P., Carlet P.C., Charpin P., Sendrier N.* On correlation-immune functions //Advances in Cryptology. Proc. Crypto'91. Springer Verlag. 1992. 87–100.
5. *Preneel B., Van-Leekwijck W., van Linden L., Covaerts R., Vandewalle J.* Propagation characteristics of boolean functions //Advances in Cryptology. Proc. Eurocrypt'90. Springer Verlag. 1991. 161–173.
6. *Seberry J., Zhang X.M., Zheng X.* Structures of cryptographic functions with strong avalanche characteristics //Advances in Cryptology. Proc. Asiacrypt'94. Springer Verlag. 1995. 96–106.
7. *Youssef A.M., Tavares S.E.* Spectral properties and information leakage of multi-output boolean functions //Proc. 1995 IEEE Intern. symp. on information theory. Whistler, Canada, 1995. 351.

Поступила в редакцию
15.12.95

УДК 512.543.23

ОБ ОДНОЙ НЕЗАВИСИМОЙ БЕСКОНЕЧНОЙ СИСТЕМЕ ГРУППОВЫХ ТОЖДЕСТВ

П.А. Кожевников

Впервые независимая бесконечная система групповых тождеств от двух переменных в явном виде была предложена С.И. Адяном [1]. Она имеет вид $\{[x^{pn}, y^{pn}]^n = 1\}$, где n — нечетное число, $n \geqslant 4361$ (в [2] оценка снижена до $n \geqslant 1003$), p пробегает множество простых чисел.

В настоящей заметке доказывается, что независимой является бесконечная система тождеств более простого вида, а именно справедлива

Теорема. *При достаточно большом нечетном n (можно взять, например, $n > 10^{10}$), равном степени простого, тождества $\{[x^p, y^p]^n = 1\}$, где p пробегает множество простых чисел, независимы.*

Будем строить группу, в которой выполнены все тождества из условия теоремы, кроме одного фиксированного. Построение такой группы будет опираться на материал [3, гл. 4–6].

Пусть $F = F(\mathfrak{A})$ — свободная группа с базисом $\mathfrak{A}$ мощности не меньше двух, $\{N_\alpha\}_{\alpha\in I}$ (I — множество индексов) — система нормальных подгрупп группы F, для которых выполнено условие

$$\text{в факторгруппах } F/N_\alpha \text{ нет элементов порядка 2.} \tag{1}$$

Модифицируем схему выбора определяющих соотношений, предложенную в [3, § 18, п. 1], изменяя определения следующим образом. Периоды $\mathfrak{X}_i$ ранга i выбираем как максимальное подмножество простых в ранге $i-1$ слов длины i со свойствами: а) если $A, B \in \mathfrak{X}_i$ и A графически не равно B, то слово A не сопряжено в $G(i-1)$ с $B^{\pm 1}, i \geqslant 1$; б) если $A \in \mathfrak{X}_i$, то существуют целая степень r ($r \neq 0$) и индекс $\alpha \in I$, такие, что $A^r \in N_\alpha$ в группе F (наименьшее натуральное из таких r для данного A обозначим r_A, в силу условия (1) r_A всегда нечетно). Определяем соотношения ζ_i ранга i равенством $\zeta_i = \{A^{r_A n} | A \in \mathfrak{X}_i\}$. Таким образом, имеем последовательность групп $F = G(0), G(1), \ldots, G(\infty)$, где $G(i) =< \mathfrak{A} \,\|R = 1; R \in \mathfrak{R}_i >$ ($\mathfrak{R}_0 = \emptyset$, $\mathfrak{R}_i = \mathfrak{R}_{i-1} \cup \zeta_i$),

$$G(\infty) =< \mathfrak{A} \| R = 1; R \in \mathfrak{R} = \bigcup_{i=1}^{\infty} \mathfrak{R}_i > .$$

Для группы $G(\infty)$, построенной по системе подгрупп $\{N_\alpha\}$, при достаточно большом нечетном n справедливы аналоги многих утверждений [3, § 18,19]. Сохраним нумерацию таких утверждений, приведенную в [3], помечая их дополнительно буквой "а". В частности, справедливы следующие два утверждения.

Лемма 18.3а. *Если $X \neq 1$ в $G(i)$ и слово X имеет конечный порядок в $G(i)$, то оно сопряжено в $G(i)$ с некоторой степенью какого-то периода ранга $k \leqslant i$.*

Теорема 19.4а. *Период A имеет порядок $r_A \cdot n$ в $G(\infty)$.*

(Лемма 18.3а — аналог леммы 18.3 из [3]. Для ее доказательства нужно повторить цикл утверждений из [3, §18,19], доказываемых совместной индукцией, со следующими изменениями. Вместо нечетности n нужно использовать нечетность $n \cdot r_A$, а вместо того факта, что длина контура клетки ранга j равна nj, использовать соответствующее неравенство. Теорема 19.4а — аналог теоремы 19.4, п.2. В доказательстве равенство $A^n = 1$ нужно заменить на $A^{r_A n} = 1$. Последнее равенство верно, так как это соотношение для группы $G(\infty)$.)

Рассмотрим подгруппу N группы F, равную произведению всех подгрупп $\{N_\alpha{}^n\}_{\alpha\in I}$ (как обычно, G^n — подгруппа, порожденная n-ми степенями элементов из G). Из определения соотношений $\mathfrak{R}$, очевидно, следует $\mathfrak{R} \subseteq N$. Далее, для подгрупп $\{N_\alpha\}$ предполагается выполненным условие

$$N \subseteq N_\alpha \text{ для каждого } \alpha \in I\,. \tag{2}$$

Лемма 1. *Пусть слово X лежит в некоторой подгруппе N_α, а X и Y сопряжены в $G(\infty)$. Тогда и Y лежит в той же подгруппе N_α.*

Доказательство. Так как $\mathfrak{R} \subseteq N$, то G/N — факторгруппа группы $G(\infty)$, а в силу (2) G/N_α — факторгруппа группы G/N. Отсюда вытекает сопряженность X и Y в G/N_α. По условию $X = 1$ в G/N_α, следовательно, $Y = 1$ в G/N_α, что и требуется. □

Лемма 2. *Пусть $X^n = 1$ в $G(\infty)$. Тогда найдется индекс $\alpha \in I$, такой, что $X \in N_\alpha$.*

Доказательство. Если $X = 1$ в $G(\infty)$, то $X \in N_\alpha$ для всех $\alpha \in I$ (это следует из леммы 1, поскольку $1 \in N_\alpha$). Иначе найдется число i, такое, что $X^n = 1$ в $G(i)$ и $X \neq 1$ в $G(i)$. Тогда по лемме 18.3а X сопряжено в $G(i)$ и, следовательно, в $G(\infty)$ со степенью некоторого периода A: $X = YA^sY^{-1}$ в $G(\infty)$. Отсюда $X^n = YA^{sn}Y^{-1} = 1$, $A^{sn} = 1$ в $G(\infty)$. По теореме 19.4а r_A делит s. Значит, $A^s \in N_\alpha$ для некоторого $\alpha \in I$, так как $A^{r_A} \in N_\alpha$, и, следовательно, $X \in N_\alpha$ по лемме 1. □

Лемма 3. *Пусть $X^m \in N_\alpha$ для некоторых $m \in \mathbb{N}$, $\alpha \in I$. Тогда X сопряжено в $G(\infty)$ со степенью некоторого периода.*

Доказательство. Если длина слова X равна i и X не просто в ранге $i-1$, то по определению простых в ранге i слов X сопряжено в $G(i-1)$ и, следовательно, в $G(\infty)$ либо со степенью периода, либо со степенью слова Y меньшей длины. Во втором случае $X = ZY^sZ^{-1}$ в $G(\infty)$, отсюда $Y^{sm} = Z^{-1}X^mZ$ в $G(\infty)$ и $Y^{sm} \in N_\alpha$ по лемме 1. Применяя индукцию по длине слова, получаем сопряженность Y со степенью периода в $G(\infty)$. Поэтому Y^s и X также сопряжены в $G(\infty)$ со степенью периода. Если же

X просто в ранге $i-1$, то по определению $\mathfrak{X}_i$ слово X сопряжено с периодом ранга i в группе $G(i-1)$ и, следовательно, в $G(\infty)$. □

Предположим, что для подгрупп $\{N_\alpha\}$ выполнено также условие

$$\begin{aligned}&\text{если } r\ (r<\infty) \text{ — порядок слова } X \text{ в группе } F/N_\alpha \text{ для некоторого } \alpha,\\ &\text{а } r_X \text{ — наименьший из таких порядков для всех } \alpha\in I, \text{ то } r_X \text{ делит } r.\end{aligned} \tag{3}$$

При выполнении этого условия верна

Лемма 4. *Нормальное замыкание $\mathfrak{R}^F$ соотношений $\mathfrak{R}$ совпадает с N.*

Доказательство. Из леммы 3 вытекает, что если $X\in N_\alpha$ для некоторого $\alpha\in I$, то X сопряжено в $G(\infty)$ со степенью A^s периода A, откуда по лемме 1 имеем $A^s\in N_\alpha$. Но в силу условия (3) r_A делит s, поэтому $A^{ns}=1$ в $G(\infty)$, так как это есть следствие соотношения $A^{r_A n}=1$ из $\mathfrak{R}$. Получаем $X^n=YA^{sn}Y^{-1}=1$ в $G(\infty)$. Всякий элемент из N — конечное произведение n-х степеней слов, каждое из которых лежит в некоторой подгруппе N_α. Следовательно, такой элемент равен 1 в $G(\infty)$. □

Лемма 4 утверждает, что $G(\infty)$ на самом деле совпадает с G/N.

Обозначим через P некоторое множество простых чисел. В качестве системы подгрупп $\{N_\alpha\}$ берем систему вербальных подгрупп

$$\{N_p(F)=[F^p,\ F^p]\cdot[F,F]^n \mid p\in P\}.$$

В следующей лемме существенно используется то, что n — степень простого числа.

Лемма 5. *Для подгрупп $\{N_p\}_{p\in P}$ выполнены условия (1)–(3).*

Доказательство. Легко видеть, что $[F,F]^n\subseteq N_p\subseteq[F,F]$, поэтому ${N_p}^n\subseteq[F,F]^n\subseteq N_p$ для любого $p\in P$. Таким образом, $N\subseteq N_p$, и условие (2) для системы $\{N_p\}_{p\in P}$ выполнено. Любой элемент конечного порядка в F/N_p лежит в $[F,F]/N_p$, так как группа $F/[F,F]$ без кручения. Но $[F,F]/N_p$ является факторгруппой группы $[F,F]/[F,F]^n$, следовательно, в группах $[F,F]/N_p$ и F/N_p конечным порядком какого-то элемента может быть только делитель числа n. Поскольку n — нечетное, являющееся степенью простого, то его делитель — нечетное число, являющееся степенью того же простого. Отсюда следует выполнение условий (1) и (3) для системы $\{N_p\}$. □

По лемме 4 группа $G(\infty)$, построенная по системе подгрупп $\{N_p\}_{p\in P}$, есть группа G/N. Но G/N — свободная группа в многообразии, в котором, в частности, выполняются тождественные соотношения $[x^p,y^p]^n=1$, $p\in P$.

Для завершения доказательства теоремы осталось рассмотреть специальную группу.

Лемма 6. *Пусть $G=Z_n wr Z_p$ — сплетение циклических групп порядков n и p. Тогда*

1) *вербальная подгруппа $N_p(G)$ тривиальна,*

2) *тождество $[x^q,y^q]=1$ не выполнено в G, если q — простое, отличное от p.*

Доказательство. 1. В группе G p-я степень любого элемента и коммутатор любых двух элементов лежат в базе сплетения, следовательно, G^p и $[G,G]$ лежат в базе сплетения. А так как база сплетения — абелева группа периода n, то $[G^p,G^p]=1$ и $[G,G]^n=1$, откуда $N_p(G)=1$.

2. Каждый элемент из Z_p является q-й степенью в силу того, что $p\neq q$, поэтому активная группа Z_p при естественном вложении в G попадает в нормальную подгруппу G^q. Централизатором подгруппы Z_p является, как легко убедиться, подгруппа $Z_p D$, где D — диагональ базы сплетения. Нетрудно выбрать подгруппу, сопряженную в G с Z_p, не лежащую в $Z_p D$. Отсюда получаем, что $G^q\not\subseteq Z_p D$ и G^q неабелева. Значит, в G найдутся элементы g_1,g_2, такие, что $[{g_1}^q,{g_2}^q]\neq 1$. □

Покажем, наконец, что в группе $G(\infty)$ не выполняется тождество $[x^q,y^q]^n=1$, если q — простое, не принадлежащее P. Если бы это было не так, то $[{a_1}^q,{a_2}^q]^n=1$ в $G(\infty)$ для различных элементов a_1,a_2 базиса $\mathfrak{A}$ группы F. По лемме 2 отсюда следовало бы, что $[{a_1}^q,{a_2}^q]\in N_p(F)$ для некоторого $p\in P$. Но согласно лемме 6 при гомоморфизме $\varphi: F\to G$ (G — рассмотренное сплетение), таком, что $\varphi(a_i)=g_i$ ($i=1,2$), справедливо равенство $\varphi(N_p(F))=1$, но $\varphi([{a_1}^q,{a_2}^q])\neq 1$ — противоречие. Если P — множество всех простых чисел, за исключением q, то в $G(\infty)$ будут выполнены все тождества, указанные в теореме, кроме $[x^q,y^q]^n=1$. Это завершает доказательство теоремы.

Замечание. А. Л. Шмелькин указал автору, что сходные системы тождеств были рассмотрены в [4]. Однако при простом n наш результат не следует из [4].

Автор выражает благодарность А. Ю. Ольшанскому за полезные советы.

СПИСОК ЛИТЕРАТУРЫ

1. *Адян С.И.* Бесконечные неприводимые системы групповых тождеств //Изв. АН СССР. 1970. **34**, № 4. 715–734.
2. *Адян С.И.* Проблема Бернсайда и тождества в группах. М., 1975.
3. *Ольшанский А.Ю.* Геометрия определяющих соотношений в группах. М., 1989.
4. *Клейман Ю.Г.* О тождествах в группах //Тр. Моск. матем. о-ва. 1982. **44**. 62–108.

Поступила в редакцию
18.12.95

УДК 517

ОБ ЭКСТРЕМАЛЬНЫХ ПОДПРОСТРАНСТВАХ ДЛЯ КЛАССОВ ФУНКЦИЙ, ЗАДАВАЕМЫХ ЯДРАМИ, НЕ ПОВЫШАЮЩИМИ ОСЦИЛЛЯЦИЮ

В.М. Тихомиров

1. Постановка задачи и формулировка результата. Пусть $W_\infty^r(\mathbf{T})$, $r \in \mathbf{N}$, — это совокупность 2π-периодических функций $x(\cdot)$, принадлежащих $C^{r-1}(\mathbf{T})$ (т.е. имеющих на периоде $r-1$ непрерывную производную), причем $x^{(r-1)}(\cdot)$ удовлетворяет условию Липшица с константой единица: $|x^{(r-1)}(t) - x^{(r-1)}(t')| \leqslant |t-t'|$ (или, что то же, $x^{(r-1)}(\cdot)$ абсолютно непрерывна и $\|x^{(r)}(\cdot)\|_{L_\infty(\mathbf{T})} \leqslant 1$). В 1936 г. французский математик Ж. Фавар [1] доказал следующее соотношение:

$$d(W_\infty^r(\mathbf{T}), \mathcal{T}_{n-1}, C(\mathbf{T})) = K_r/n^r, \tag{1}$$

где $n \in \mathbf{N}$, $\mathcal{T}_{n-1}$ — пространство тригонометрических полиномов степени $\leqslant n-1$, $K_r = \dfrac{4}{\pi}\displaystyle\sum_{k=0}^{\infty} \frac{(-1)^{k(r+1)}}{(2k+1)^{r+1}}$ (это число называют *константой Фавара*), а $d(C, L, X) = \sup_{x\in C} \inf_{y\in L} \|x-y\|$ — *уклонение* подмножества C нормированного пространства X от подпространства L, лежащего в X.

В 1960 г. автором [2] было доказано, что

$$d_{2n-1}(W_\infty^r(\mathbf{T}), C(\mathbf{T})) = K_r/n^r \tag{2}$$

(где $d_n(C, X)$ для множества C, лежащего в нормированном пространстве X, — это *n-поперечник по Колмогорову* множества C в X, см. [3, с. 17]). Несколько позже автором было доказано [4], что, во-первых,

$$d_{2n-1}(W_\infty^r(\mathbf{T}), C(\mathbf{T})) = d_{2n}(W_\infty^r(\mathbf{T}), C(\mathbf{T})), \tag{3}$$

а во-вторых,

$$d_{2n}(W_\infty^r(\mathbf{T}), C(\mathbf{T})) = d(W_\infty^r(\mathbf{T}), S_{2n}^{r-1}, C(\mathbf{T})) = K_r/n^r, \tag{4}$$

где S_{2n}^{r-1} — пространство сплайнов порядка $r-1$ дефекта 1 по равномерному разбиению (определение см. в [3, с. 90]). Из сопоставления (1)–(4) видно, что экстремальными подпространствами для класса $W_\infty^r(\mathbf{T})$ (в смысле приближения в равномерной метрике подпространствами размерности $\leqslant 2n$) могут быть подпространства весьма разной природы: сплайны гладкости $r-1$ и тригонометрические полиномы, являющиеся аналитическими функциями. Естественно было ожидать, что в этом случае существуют подпространства промежуточной гладкости, также являющиеся экстремальными. И действительно, такой результат был получен Лигуном [5], доказавшим, что все пространства сплайнов S_{2n}^m, $m \geqslant r-1$, также являются экстремальными. (При этом теорема Фавара об экстремальности пространства тригонометрических полиномов может быть получена предельным переходом, ибо пространства сплайнов S_{2n}^m при $m \to \infty$ сходятся к пространству тригонометрических полиномов.)

И теорема Фавара, и теорема автора о поперечниках получили многочисленные обобщения. Теорема Фавара оказалась верной для многих периодических ядер (см. [6]), а результат автора об оптимальности сплайнов оказался справедливым и в случае, когда рассматриваются пары $(W_p^K(\mathbf{T}), L_q(\mathbf{T}))$,