УДК 512

Д. А. СУПРУНЕНКО, акад. АН БССР (Ин-т математики АН БССР, Минск)

# О группе Фробениуса

Доказано, что при $l > 1$ подстановочный ранг группы Фробениуса с ядром класса нильпотентности $l$ больше $4^{l-1} + 1$.

Пусть $p$ и $q$ — простые числа, $q \mid p - 1$, $1 < j < q$. Для всех таких $p, q, j$ построены группы Фробениуса порядка $p^{j+1}q$ с ядром класса нильпотентности $j$ и порядка $p^{j+1}$. При $p = 7$, $q = 3$, $j = 2$ получаем известный пример О. Ю. Шмидта.

Доведено, що при $l > 1$ підстановочний ранг групи Фробеніуса з ядром класу нільпотентності $l$ більше $4^{l-1} + 1$.

Нехай $p$ і $q$ — прості числа, $q \mid p - 1$, $1 < j < q$. Для всіх таких $p, q, j$ побудовані групи Фробеніуса порядку $p^{j+1}q$ з ядром класу нільпотентності $j$ і порядку $p^{j+1}$. При $p = 7$, $q = 3$, $j = 2$ одержуємо відомий приклад О. Ю. Шмідта.

1. Пусть $G$ — группа подстановок конечного множества $X$, $a, b \in X$, $a \neq b$. Буквами $G_a$ и $G_{a,b}$ обозначим одноточечный и двуточечный стабилизаторы. Пусть далее выполняются три условия: а) группа $G$ транзитивна; б) $G_a \neq \langle 1 \rangle$; в) $G_{a,b} = \langle 1 \rangle$ для любых двух различных точек из $X$. Тогда группа $G$ называется группой Фробениуса.

Как доказал Фробениус [1], группа Фробениуса $G$ обладает регулярной нормальной подгруппой $N$. Следовательно, $G = NG_a$, $N \cap G_a = \langle 1 \rangle$.

Условие в) означает, что ограничение $G_a|X \setminus a$ является полурегулярной группой подстановок множества $X \setminus a$. Таким образом, число $|G_a|$ делит $|X| - 1$, а все неодноточечные орбиты группы $G_a$ имеют одну и ту же длину. Регулярная нормальная подгруппа $N$ группы Фробениуса $G$ называется ядром группы $G$, а подгруппа $G_a$ — дополнением.

Дважды транзитивные группы Фробениуса изучал еще Жордан [2]. Он доказал, что ядро дважды транзитивной группы Фробениуса абелево. Отсюда и из примитивности дважды транзитивной группы следует, что ядро дважды транзитивной группы Фробениуса является элементарной абелевой $p$-группой. В свою очередь отсюда вытекает, что дважды транзитивная группа Фробениуса содержится в аффинной группе Aff $(m, p)$, где $p^m$ — степень группы подстановок Фробениуса.

Верна также теорема Бернсайда [3]: если дополнение $G_a$ группы Фробениуса $G$ имеет четный порядок, то ядро $N$ группы $G$ абелево. О. Ю. Шмидт [4] построил первый пример группы Фробениуса $G$ с неабелевым ядром $N$. В примере О. Ю. Шмидта $N$ — неабелева группа порядка $7^3$, экспоненты 7, $|G| = 7^3 \cdot 3 = 1029$.

Хигман доказал теорему: если ядро $N$ группы Фробениуса разрешимо, то оно нильпотентно [5]. Наконец, Томпсон [6] установил разрешимость, а следовательно, и нильпотентность ядра группы Фробениуса. В частности, из теоремы Томпсона следует, что ядро примитивной группы подстановок Фробениуса является элементарной абелевой $p$-группой.

Как нетрудно видеть, для любого простого делителя $q$ числа $|G_a|$ существует регулярный автоморфизм порядка $q$ ядра $N$. Согласно Хигману

[5], для каждого простого $q$ есть такое целое $k(q)$, зависящее только от $q$, что группа, допускающая регулярный автоморфизм порядка $q$, имеет показатель нильпотентности, не превышающий числа $k(q)$. В силу теоремы Бернсайда $k(2) = 1$. Далее $k(3) = 2$, $k(5) = 6$. Если $q \geqslant 7$, то $k(q) \geqslant (q^2 - 1)/4$ (Хигман [5]). Согласно работам В. Ф. Крекнина и А. И. Кострикина [7, 8]

$$k(q) \leqslant ((q-1)^{2q-1} - 1)/(q-2).$$

В настоящей работе доказываются следующие утверждения.

Т е о р е м а 1. *Пусть $r$ — подстановочный ранг группы Фробениуса $G$, ядро которой $N$ имеет показатель нильпотентности $l > 1$. Тогда $r > 4^{l-1} + 1$.*

Из теоремы 1 вытекает следующее обобщение теоремы Жордана.

П р е д л о ж е н и е 1. *Пусть $r$ — подстановочный ранг группы Фробениуса $G$, а $N$ — ядро группы $G$. Если $r < 6$, то группа $N$ абелева.*

Т е о р е м а 2. *Пусть $p$ и $q$ — простые числа, $q \mid p - 1$. Тогда для любого $l < q$ существует группа Фробениуса $G$ порядка $p^{l+1}q$, ядро которой $N_1$ имеет порядок $p^{l+1}$ и показатель нильпотентности $l$.*

Теорема 2 доказывается конструктивно, группы $G_l$ полностью построены; если $i < j < q$, то $G_i \subset G_j$. В частности, $N_2$ — неабелева группа порядка $p^3$, экспоненты $p$. При $p = 7$, $q = 3$, $l = 2$ группа $G_l$ совпадает с группой упомянутого выше примера О. Ю. Шмидта.

Т е о р е м а 3. *Неабелева группа порядка $p^3$, экспоненты $p^2$, где $p$ — простое, не может оказаться ядром группы Фробениуса.*

Т е о р е м а 4. *Пусть $n > 1$. Тогда прямое произведение $n$ экземпляров циклической группы порядка $2^m$ является ядром некоторой группы Фробениуса.*

2. Рассмотрим подстановочный ранг группы Фробениуса. Напомним, что подстановочный ранг группы подстановок $\Gamma$ совпадает с числом орбит стабилизатора $\Gamma_a$, считая и точку $a$. Пусть $X$ — конечное множество, $G$ — группа подстановок Фробениуса множества $X$, $N$ — ядро группы $G$, $r$ — подстановочный ранг группы $G$, а $l$ — показатель нильпотентности ядра $N$.

Л е м м а 1.

$$r \geqslant l + 1, \tag{1}$$

*причем равенство $r = l + 1$ верно тогда и только тогда, когда $r = 2$.*

Д о к а з а т е л ь с т в о. Пусть $a \in X$. В силу регулярности группы подстановок $N$ множество $X$ можно таким способом наделить структурой группы $\langle X, . \rangle$, что точка $a$ станет единицей группы $\langle X, . \rangle$, группа $N$ — образом левого регулярного представления группы $\langle X, . \rangle$, а группа $G_a$ — некоторой подгруппой группы $\mathrm{Aut}\,\langle X, . \rangle$.

Пусть $\langle 1 \rangle = Z_l \subset Z_1 \subset \ldots \subset Z_l = \langle X, . \rangle$ — верхний центральный ряд группы $\langle X, . \rangle$. Здесь $Z_1$ — центр группы $\langle X, . \rangle$, а $Z_{i+1}/Z_i$ — центр факторгруппы $\langle X, . \rangle / Z_i$, $i = 1, \ldots, l-1$.

Так как $Z_i$ — характеристические подгруппы группы $\langle X, . \rangle$, а $G_a \subset \mathrm{Aut}\,\langle X, . \rangle$, то подмножества

$$Z_0, Z_1 \setminus Z_0, \ldots, Z_l \setminus Z_{l-1} \tag{2}$$

$G_a$-инвариантны. Ясно, что подмножества (2) попарно не пересекаются. Следовательно, число орбит группы $G_a$ не меньше числа подмножеств (2). Поэтому $r \geqslant l + 1$ и неравенство (1) доказано. Пусть теперь $r = l + 1$. Надо доказать, что $r = 2$. Пусть вопреки лемме 1 $r > 2$. Тогда $l > 1$, а подмножества (2) суть орбиты группы $G_a$. Так как все неодноточечные орбиты группы $G_a$ имеют одну и ту же мощность, то $|Z_1 \setminus Z_0| = |Z_2 / Z_1|$. Но последнее равенство невозможно, ибо его левая часть равна $|Z_1| - 1$, а правая делится на $|Z_1|$. Следовательно, если $r = l + 1$, то $r = 2$ и лемма 1 полностью доказана.

Докажем теорему 1. При $l > 1$ в силу теоремы Бернсайда $|G_a|$ — нечетное число, следовательно, и длина орбиты группы $G_a$ — нечетное число. Обратимся теперь к $G_a$-инвариантным множествам (2). Пусть $\delta$ — длина

неодноточечной орбиты группы $G_a$. Так как $|Z_1 \setminus Z_0| = |Z_1| - 1$ делится на $\delta$, то $(\delta, |Z_1|) = 1$, $|Z_1| \geqslant 4$.

Запишем $|Z_i|$ в виде $|Z_i| = K_i|Z_{i-1}|$, $1 < i \leqslant l$. Тогда

$$(\delta, |Z_i|) = 1, \quad \delta | K_i - 1. \tag{3}$$

Действительно, $|Z_2 \setminus Z_1| = |Z_1|(K_2 - 1)$, $\delta | |Z_2 \setminus Z_1|$, $\delta | K_2 - 1$, $K_2 \geqslant 4$, $(\delta, K_2) = 1$, $(\delta, |Z_2|) = 1$. Поэтому (3) верно при $i = 2$. Пусть (3) верно для $i$. Покажем, что (3) верно для $i+1$. Очевидно, $\delta || Z_{i+1} \setminus Z_i|$, $|Z_{i+1} \setminus Z_i| = (K_{i+1} - 1)|Z_i|$. Следовательно, $\delta | K_{i+1} - 1$, $(\delta, K_{i+1}) = 1$, $(\delta, |Z_{i+1}|) = 1$. Таким образом, (3) полностью доказано. Как легко видеть,

$$|\langle X, \cdot \rangle| = |N| = K_2 K_3 \dots K_l |Z_1|,$$

$$r = \frac{|N| - 1}{\delta} + 1.$$

Так как $\delta | K_i - 1$, $\delta || Z_1| - 1$ и $\delta \geqslant 3$, то

$$\frac{K_2 \dots K_l |Z_1| - 1}{\delta} \geqslant \frac{(\delta+1)^{l-1}(\delta+1) - 1}{\delta} = (\delta+1)^{l-1} + \frac{(\delta+1)^{l-1} - 1}{\delta} >$$

$$> (\delta+1)^{l-1} \geqslant 4^{l-1}.$$

Следовательно, $r > 4^{l-1} + 1$. Теорема 1 доказана.

Учитывая теорему Бернсайда, теорему 1 можно сформулировать так: пусть ядро $N$ группы Фробениуса $G$ неабелево. Тогда $\frac{|N| - 1}{3} + 1 \geqslant r > 4^{l-1} + 1$.

Как вытекает из построений п. 3, для любого простого $p$, подчиненного условию $p \equiv 1 \pmod 3$, существует группа Фробениуса порядка $3p^3$ с неабелевым ядром $N$ порядка $p^3$, для которой

$$r = \frac{|N| - 1}{3} + 1 = \frac{p^3 - 1}{3} + 1.$$

**3.** Пусть $p$ и $q$ — простые числа, причем $p \equiv 1 \pmod q$. Тогда верна следующая теорема, уточняющая теорему 2.

Теорема 2*. *Существует ряд групп*

$$G_2 \subset G_3 \subset \dots \subset G_{q-1}, \tag{4}$$

*обладающий следующими свойствами*:

1) *каждая группа $G_j$ ряда* (4) *является группой Фробениуса*;

2) $G_j = N_j H$, $|N_j| = p^{j+1}$, $|H| = q$, $|G_j| = p^{j+1}q$, *где $N_j$ — ядро группы $G_j$, а $H$ — дополнение*;

3) *показатель нильпотентности ядра $N_j$ равен $j$.*

Ниже дается конструктивное доказательство теоремы 2*, группы $G_j$ будут полностью построены.

1. Будем строить $p$-группы, допускающие регулярный автоморфизм порядка $q$. Так как такие группы мы будем искать среди нильпотентных матричных групп, описанных в статье [9], то приведем сперва в удобной форме некоторые результаты этой статьи. Пусть $\mathbf{C}$ — поле комплексных чисел, $\varepsilon \in \mathbf{C}$, $\varepsilon^p = 1$, $\varepsilon \neq 1$, $E_p$ — единица группы $\mathrm{GL}(p, \mathbf{C})$, где $p$ — пока любое нечетное простое число. Положим

$$c_1 = \varepsilon E_p, \; h = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & & 1 & 0 \end{pmatrix}.$$

Как легко проверить, $c_1, h \in \mathrm{SL}(p, \mathbf{C})$.

Лемма 2. *Пусть $d$ — произвольная диагональная матрица группы* SL $(p, \mathbf{C})$. *Тогда в группе* SL $(p, \mathbf{C})$ *есть такая диагональная матрица $c$, что* $[c, h] = chc^{-1}h^{-1} = d$. *Если $u$ — другая диагональная матрица из группы* SL $(p, \mathbf{C})$, *для которой* $[u, h] = d$, *то* $u \in \langle c_1 \rangle\, c = \langle \varepsilon \rangle\, c$.

Доказательство. По условию

$$d = \operatorname{diag}[\delta_0, \delta_1, \dots, \delta_{p-1}], \quad \delta_0\delta_1 \dots \delta_{p-1} = 1.$$

Пусть $a = \operatorname{diag}[1, \alpha_1, \dots, \alpha_{p-1}]$, где $\alpha_j = \delta_1\delta_2 \dots \delta_j$, $j = 1, \dots, p-1$. Тогда, как показывает прямая проверка, $[a, h] = d$. Пусть $\lambda \in \mathbf{C}$, $\lambda^p \det a = 1$, $c = \lambda a$. Тогда $c$ — диагональная матрица, $c \in \mathrm{SL}(p, \mathbf{C})$ и $[c, h] = d$.

Если $u$ — другая диагональная матрица из $\mathrm{SL}(p, \mathbf{C})$, для которой $[u, h] = d$, то $uhu^{-1}h^{-1} = chc^{-1}h^{-1}$, $c^{-1}uh = hc^{-1}u$. Так как $c^{-1}u$ — диагональная матрица, то из последнего равенства следует $c^{-1}u = \gamma E_p$, $\gamma \in \mathbf{C}$, $u = \gamma c$. Поскольку $\det u = \det c$, то $\gamma^p = 1$, $\gamma \in \langle \varepsilon \rangle$, $u \in \langle \varepsilon \rangle\, c$. Лемма 2 полностью доказана. Из леммы 2 вытекает такое утверждение.

Лемма 3. *Существует бесконечная последовательность диагональных матриц группы* SL $(p, \mathbf{C})$

$$c_1, c_2, \dots, c_j, \dots$$

*такая, что*

$$[c_{j+1}, h] = c_j. \tag{5}$$

В частности, из доказательства леммы 2 вытекает, что можно положить $c_2 = \operatorname{diag}[1, \varepsilon, \dots, \varepsilon^{p-1}]$.

Из (5), легко следует равенство

$$[c_{j+1}^{\alpha}, h] = c_j^{\alpha}, \tag{6}$$

где $\alpha$ — любое целое положительное число.

Для целого положительного $j$ положим $D_j = \langle c_1, \dots, c_j \rangle$. Из (5), (6) следует

$$[c_1^{\alpha_1}c_2^{\alpha_2} \dots c_j^{\alpha_j}, h] = c_1^{\alpha_1}c_2^{\alpha_2} \dots c_{j-1}^{\alpha_j} \in D_{j-1}. \tag{7}$$

Из (6) получаем $[c_3^p, h] = c_2^p = E_p$, $c_3^p \in \langle c_1 \rangle$. Используя (7), индукцией по $j$ доказываем, что

$$c_{j+1}^p \in D_{j-1} \subset D_j. \tag{8}$$

Лемма 4. $D_{j+1} = \langle c_{j+1} \rangle D_j$, $|D_j| = p^j$, $|D_{j+1}/D_j| = p$.

Доказательство. В силу (8) достаточно лишь установить, что $c_{j+1} \notin D_j$. Пусть $c_{j+1} \in D_j$. Тогда в силу (5) и (7) $c_j = [c_{j+1}, h] \in D_{j-1}$, $c_{j-1} \in D_{j-2}$, $c_2 \in D_1 = \langle c_1 \rangle$. Последнее неверно. Отсюда и следует лемма 4.

Как нетрудно видеть,

$$hD_jh^{-1} = D_j. \tag{9}$$

Введем еще группу

$$\mathfrak{N}_j = \langle h \rangle D_j. \tag{10}$$

Из леммы 4 и равенства (9) вытекает такая лемма.

Лемма 5. $|\mathfrak{N}_j| = p^{j+1}$.

Лемма 6. *Показатель нильпотентности группы $\mathfrak{N}_j$ равен $j$.*

*Доказательство.* Пользуясь формулами (5) и (7), легко показать, что $\mathfrak{N}_j \supset D_{j-1} \supset D_{j-2} \supset \dots \supset D_1 \supset \langle E_p \rangle$ — нижний центральный ряд группы $\mathfrak{N}_j$.

2. Из (5) и (10) следует $\mathfrak{N}_j = \langle c_j, h \rangle$.

Пусть теперь $k$ — целое положительное число и $(k, p) = 1$. Тогда $\mathfrak{N}_j = \langle c_j^k, h^k \rangle$, так как $c_j,\ h \in \langle c_j^k, h^k \rangle$.

Позже мы покажем существование в $\mathrm{Aut}\,(\mathfrak{N}_j)$ такого автоморфизма $f$, что

$$f(c_j) = c_j^k, \quad f(h) = h^k. \tag{11}$$

А теперь докажем одну условную лемму.

Лемма 7. *Если* $f \in \mathrm{Aut}(\mathfrak{N}_j)$ *и выполняются условия* (11), *то при* $1 < i < j$

$$f(c_i) = c_i^{k^{j-i+1}} d_{i-1}, \quad d_{i-1} \in D_{i-1}, \tag{12}$$

$$f(c_1) = c_1^{k^j}.$$

Доказательство. Из (5) получаем

$$c_j h^2 = c_{j-1} h c_j h = c_{j-1} h c_{j-1} h c_j = c_{j-1} c_{j-2}^{-1} c_{j-1} h^2 c_j = c_{j-1}^2 c_{j-2}^{-1} h^2 c_j =$$

$$= c_{j-1}^2 d_{j-2} h^2 c_j, \quad d_{j-2} \in D_{j-2},$$

$$c_j h^\beta = c_{j-1}^\beta d_{j-2} h^\beta c_j, \quad d_{j-2} \in D_{j-2}$$

(используя индукцию по $\beta$ и центральный ряд из леммы 6). Следовательно,

$$[c_j, h^\beta] = c_{j-1}^\beta d_{j-2}, \quad d_{j-2} \in D_{j-2}. \tag{13}$$

Отсюда и из (6) находим

$$[c_j^\alpha, h^\beta] = c_{j-1}^{\alpha\beta} d_{j-2}, \; d_{j-2} \in D_{j-2}. \tag{14}$$

В частности,

$$f(c_{j-1}) = f([c_j, h]) = [c_j^k, h^k] = c_{j-1}^{k^2} d_{j-2}, \; d_{j-2} \in D_{j-2}.$$

Далее

$$f(c_{j-2}) = f([c_{j-1}, h]) = [c_{j-1}^{k^2} d_{j-2}, h^k] = c_{j-2}^{k^3} d_{j-3},$$

$$d_{j-3} \in D_{j-3}.$$

Из (13) и (14) и из равенства $f(c_i) = f([c_{i+1}, h])$ при $1 < i < j$ вытекает равенство (12).

При $i = 2$ из (12) получаем

$$f(c_2) = c_2^{k^{j-1}} c_1^\alpha = c_2^{k^{j-1}} \varepsilon^\alpha.$$

Следовательно,

$$f(c_1) = f([c_2, h]) = [c_2^{k^{j-1}} \varepsilon^\alpha, h^k] = c_1^{k^j}.$$

Лемма 7 доказана.

Лемма 8. *В группе* $\mathrm{Aut}(\mathfrak{N}_j)$ *есть такой автоморфизм* $\psi$, *что*

$$\psi(c_j) = c_j^k, \; \psi(h) = h^k.$$

Доказательство. Для удобства введем обозначения

$$h^k = b, \; c_1^{k^j} = a_1, \; c_1^{k^{j-i+1}} d_{i-1} = a_i, \quad 0 < i < j, \; c_j^k = a_j,$$

где элементы $d_{i-1} \in D_{i-1}$ определяются соотношениями (14) и

$$[c_{i+1}^{k^{j-i}} d_i, h^k] = c_i^{k^{j-i+1}} d_{i-1}.$$

Так как $(k, p) = 1$, то

$$|\langle b \rangle| = |\langle h \rangle| = p, \quad |\langle a_i, D_{i-1} \rangle / D_{i-1}| = p. \tag{15}$$

Из (5) и из доказательства леммы 7 вытекает $[a_i, b] = a_{i-1}$, $i = 2, \ldots, j$. Очевидно, любой элемент $x \in \mathfrak{N}_j$ можно единственным способом представить в виде

$$x = h^{\gamma_0} c_1^{\gamma_1} \ldots c_j^{\gamma_j}, \quad 0 \leqslant \gamma_i < p.$$

Введем теперь преобразование

$$\psi : \mathfrak{N}_j \to \mathfrak{N}_j, \quad h^{\gamma_0} c_1^{\gamma_1} \ldots c_j^{\gamma_j} \to b^{\gamma_0} a_1^{\gamma_1} \ldots a_j^{\gamma_j}.$$

Ясно, что $\psi(h) = b = h^k$, $\psi(c_j) = a_j = c_j^k$. Покажем, что $\psi \in \mathrm{Aut}(\mathfrak{N}_j)$. Пусть $y = h^{\beta_0} c_1^{\beta_1} \ldots c_j^{\beta_j}$, $0 \leqslant \beta_i < p$. Тогда

$$\psi(xy) = \psi(h^{\gamma_0} c_1^{\gamma_1} \ldots c_j^{\gamma_j} h^{\beta_0} c_1^{\beta_1} \ldots c_j^{\beta_j}) = \psi(h^{\lambda_0} c_1^{\lambda_1} \ldots c_j^{\lambda_j}) = b^{\lambda_0} a_1^{\lambda_1} \ldots a_j^{\lambda_j},$$

где

$$xy = h^{\gamma_0}c_1^{\gamma_1}\dots c_j^{\gamma_j}h^{\beta_0}c_1^{\beta_1}\dots c_j^{\beta_j} = h^{\lambda_0}c_1^{\lambda_1}\dots c_j^{\lambda_j}, \tag{16}$$

$$\psi(x)\psi(y) = b^{\gamma_0}a_1^{\gamma_1}\dots a_j^{\gamma_j}b^{\beta_0}a_1^{\beta_1}\dots a_j^{\beta_j} = b^{\rho_0}a_1^{\rho_1}\dots a_j^{\rho_j}. \tag{17}$$

Правая часть равенства (16) получается из левой следующим путем. Матрица $h$ последовательно переставляется с матрицами $c_j^{\gamma_j}, c_{j-1}^{\gamma_{j-1}}, \dots, c_1^{\gamma_1}$ и при этом учитывается, что $[c_i, h] = c_{i-1}$. Аналогично правая часть равенства (17) получается из левой перестановками матрицы $b$ с матрицами $a_j^{\gamma_j}, a_{j-1}^{\gamma_{j-1}}, \dots a_1^{\gamma_1}$ при учете равенства $[a_i, b] = a_{i-1}$. Следовательно, $\lambda_i = \rho_i$, $i = 0, 1, \dots, j$, $\psi(xy) = \psi(x)\psi(y)$. Из (15) вытекает инъективность отображения $\psi$. Поэтому $\psi \in \mathrm{Aut}(\mathfrak{N}_j)$. Лемма 8 доказана.

Лемма 9. *Пусть $q$ — простое число, $q \mid p-1$, $q > j$. Тогда в $\mathrm{Aut}(\mathfrak{N}_j)$ есть регулярный автоморфизм порядка $q$.*

Доказательство. Пусть $p^t$ — экспонента группы $D_j$. Так как $q \mid p-1$, то существует такое целое $k$, что

$$k^q \equiv 1 \pmod{p^t},\ k \not\equiv 1 \pmod{p}. \tag{18}$$

В силу леммы 8 в $\mathrm{Aut}(\mathfrak{N}_j)$ есть такой автоморфизм $\psi$, что $\psi(c_j) = c_j^k$, $\psi(h) = h^k$. Так как $\mathfrak{N}_j = \langle c_j, h\rangle$, то в силу (18) порядок автоморфизма $\psi$ равен $q$. Остается показать регулярность $\psi$. Пусть

$$x = h^{\alpha_0}c_1^{\alpha_1}\dots c_j^{\alpha_j} \neq E_p, \quad 0 \leqslant \alpha_i < p.$$

Тогда среди чисел $\alpha_i$ есть отличные от нуля. Покажем, что $\psi(x) \neq x$. Если $a_0 \neq 0$, то $\psi(x) = h^{\alpha_0 k}\psi(c_1^{\alpha_1}\dots c_j^{\alpha_j})$, $\alpha_0 k \not\equiv \alpha_0 \pmod{p}$. Следовательно, $\psi(x) \neq x$. Если $\alpha_0 = 0$, то есть такое $i$, что $\alpha_i \neq 0$, $i > 0$. Выберем $\alpha_i \neq 0$ с наибольшим индексом. Тогда

$$x = c_1^{\alpha_1}\dots c_i^{\alpha_i} \in D_i, \quad \psi(x) = c_1^{\alpha_1 k^j}\dots c_i^{\alpha_i k^{j-i+1}}d_{i-1},\ d_{i-1} \in D_{i-1}.$$

Так как $(\alpha_i, p) = 1$, $k \not\equiv 1 \pmod{p}$, $j - i + 1 < q$, то $a_i k^{j-i+1} \not\equiv \alpha_i \pmod{p}$. Следовательно, если $i > 1$, то элементы $x$ и $\psi(x)$ принадлежат двум разным смежным классам группы $D_i$ по $D_{i-1}$. Если же $i = 1$, то $x = c_1^{\alpha_1}$, $\psi(x) = c_1^{\alpha_1 k^j} \neq c_1^{\alpha_1} = x$. Таким образом, $\psi$ сдвигает с места любой неединичный элемент группы $\mathfrak{N}_j$. Лемма доказана.

Теперь нетрудно доказать теорему 2*. Пусть $N_l$ — образ левого регулярного представления группы $\mathfrak{N}_l$, а $\psi$ — регулярный автоморфизм порядка $q$ группы $\mathfrak{N}_l$. Тогда группа $G_l = N_l\langle\psi\rangle$ обладает свойствами 1—3 из теоремы 2. Отсюда и следует теорема 2*.

3. Из построения группы $G_l = N_l\langle\psi\rangle$ следует, что она задается простыми числами $p$ и $q$, где $q \mid p-1$, и числом $l < q$. Если теперь положить $p = 7$, $q = 3$, $l = 2$, то получим пример О. Ю. Шмидта $|G| = 7^3 \cdot 3 = 1029$. Заметим, что в статье [4], где опубликован этот пример, имеется очевидная опечатка. Равенство $RT = TP^4$ надо заменить равенством $PT = TP^4$. К сожалению, эта опечатка осталась без исправления и в посмертном издании трудов О. Ю. Шмидта [10].

Как нетрудно показать, из групп Фробениуса нечетного порядка с неабелевым ядром группа порядка 1029, построенная О. Ю. Шмидтом, имеет наименьший порядок. В самом деле, пусть $N$ — неабелево ядро группы Фробениуса $G$ нечетного порядка и пусть $|G| < 7^3 \cdot 3$. Тогда $|N| < 7^3$. Если $N_p$ — неабелева $p$-подгруппа Силова в $N$, $X_1 = N_p$-орбита точки $a \in X$, то $N_pG_a$ — группа Фробениуса с ядром $N_p$, действующая на $X_1$, ибо $N_p \Delta N$ ввиду нильпотентности группы $N$. Поэтому можно считать, что либо $|N| = 3^\alpha$, либо $|N| = 5^\alpha$. Однако это невозможно. Действительно, пусть $Z$ — центр $N$, $|Z| = p^\gamma$, $p \in \{3, 5\}$. Тогда $|Z \setminus 1|$ и $|N \setminus Z|$ делятся на нечетное простое число $q$. Поскольку $|Z \setminus 1| = p^\gamma - 1$, $|N \setminus Z| = p^\gamma(p^{\alpha-\gamma} - 1)$, то $q \mid p^{\alpha-\gamma} - 1$. Поэтому $\gamma$, $\alpha - \gamma \geqslant 3$ при $p = 3$ и $\gamma$,

$\alpha - \gamma \geqslant 2$ при $p = 5$. В первом случае $|N| \geqslant 3^6$, во втором $-|N| \geqslant 5^6$. Оба эти числа больше $7^3$.

4. Пусть $K$ — класс всех абстрактных групп, являющихся ядрами групп Фробениуса. Как вытекает из построений п. 3, неабелева группа $N_2$ порядка $p^3$ экспоненты $p$, где $p$ — простое, а $p-1$ делится на некоторое нечетное простое число, принадлежит классу $K$.

Докажем теорему 3. Пусть теперь $p$ — произвольное простое число, $P = \langle a, b\rangle$, $a^p = b^{p^2} = 1$, $aba^{-1} = b^{p+1}$. Тогда, очевидно, $|P| = p^3$, центр $Z(P)$ группы $P$ совпадает с $\langle c\rangle$, где $c = b^p$. Если $p = 2$, то $|Z(P)| = 2$ и при любом автоморфизме $\varphi$ группы $P$ $\varphi(c) = c$. Следовательно, $P \notin K$. Если $p = 2^t + 1$, то число $|Z(P)| - 1 = 2^t$ не имеет нечетных простых делителей, следовательно, в $\mathrm{Aut}(P)$ нет регулярных автоморфизмов простого нечетного порядка. Значит, и в этом случае $P \notin K$.

Итак, остается рассмотреть случай, когда $q \mid p - 1$, где $q$ — нечетное простое число.

Пусть вопреки теореме 3 в $\mathrm{Aut}(P)$ есть регулярный автоморфизм $f$ нечетного простого порядка $q$. Тогда, так как $\langle c\rangle$ — центр группы $P$, то $f(c) = c^r$, $r^q \equiv 1 \pmod p$, $1 < r \leqslant p - 1$, $q \mid p - 1$. Из равенства

$$aba^{-1} = b^{p+1} = bc \tag{19}$$

следует, что порядок элемента $a^\alpha b^\beta$, где $(\beta, p) = 1$, равен $p^2$. Поэтому

$$f(a) = a^\mu c^\nu. \tag{20}$$

Из (19) получаем

$$f(a) f(b) f(a)^{-1} = f(b) c^r. \tag{21}$$

Элемент $f(b)$ можно представить в виде $f(b) = a^k b^l$. Отсюда и из (21) вытекает

$$a^\mu c^\nu a^k b^l c^{-\nu} a^{-\mu} = a^k b^l c^r,$$

$$a^\mu b^l a^{-\mu} = b^l c^r. \tag{22}$$

Далее в силу (19) имеем $a^\mu b^l a^{-\mu} = (a^\mu b a^{-\mu})^l = (bc^\mu)^l = b^l c^{\mu l}$. Отсюда и из (22) получаем

$$b^l c^{\mu l} = b^l c^r, \quad c^{\mu l} = c^r. \tag{23}$$

Используя (19), вычисляем

$$c^r = f(c) = f(b^p) = (a^k b^l)^p = b^{lp} = c^l.$$

Поэтому $r \equiv l \pmod p$. Отсюда и из (23) следует $\mu \equiv 1 \pmod p$. Таким образом, (20) принимает вид

$$f(a) = ac^\nu, \quad \nu \not\equiv 0 \pmod p. \tag{24}$$

Вычислим теперь $f(d)$, где $d = ac^{-\nu\rho}$, $\rho(r - 1) \equiv 1 \pmod p$. Согласно (24) $f(d) = f(a) f(c)^{-\nu\rho} = ac^\nu c^{-\nu\rho r} = ac^{\nu(1-\rho r)}$. Далее $\nu(1 - \rho r) \equiv \nu(\rho(r - 1) - \rho r) \equiv -\nu\rho \pmod p$. Следовательно, $f(d) = ac^{-\nu\rho} = d \neq 1$. Последнее противоречит регулярности автоморфизма $f$. Итак, в $\mathrm{Aut}(P)$ нет регулярного автоморфизма простого порядка, $P \notin K$.

5. Пусть, как в п. 4, $K$ — класс конечных групп, обладающих регулярным автоморфизмом простого порядка. Если $A$ — абелева группа нечетного порядка, то $A \in K$, ибо преобразование $A \to A$, $a \to a^{-1}$ является регулярным автоморфизмом второго порядка. Но абелева группа четного порядка не обязательно попадает в класс $K$. Например, если $\langle a\rangle$ — циклическая 2-группа, то $\langle a\rangle \notin K$, так как любой автоморфизм группы $\langle a\rangle$ оставляет на месте ее единственный элемент второго порядка.

Как легко видеть, элементарная абелева группа $A$ порядка $2^n$ при $n > 1$ принадлежит классу $K$. Группу $A$ можно трактовать как $n$-мерное векторное пространство над полем $GF(2)$. Очевидно, для любого простого де-

лителя $q$ числа $2^n - 1$ в группе GL $(n, 2)$ есть элемент $b$ порядка $q$ такой, что минимальный многочлен $b$ неприводим над GF (2). Ясно, что $b$ — регулярный автоморфизм порядка $q$ группы $A$. Последнее замечание будет использовано при доказательстве теоремы 4.

Прежде, чем доказывать теорему 4, рассмотрим кольцо $\mathbf{Z}_{2^m} = \mathbf{Z}/(2^m)$. Введем гомоморфизм колец $\gamma : \mathbf{Z}_{2^m} \mapsto \mathbf{Z}_2$, $x \mapsto x + 2\mathbf{Z}_{2^m}$ (смежный класс). Гомоморфизм $\gamma$ определяет гомоморфизм групп

$$h_n : \mathrm{GL}(n, Z_{2^m}) \mapsto \mathrm{GL}(n, 2), \quad \| a_{ij} \| \to \| \gamma(a_{ij}) \|.$$

Как нетрудно проверить, $\operatorname{Im} h_n = \mathrm{GL}(n, 2)$, а $\operatorname{Ker} h_n$ состоит из всех матриц вида $E_n + 2r$, $r \in M(n, Z_{2^m})$. Следовательно, $|\operatorname{Ker} h_n| = 2^{(m-1)n^2}$. Как легко вычислить, $(E_n + 2r)^{2^{m-1}} = E_n$.

Доказательство теоремы 4. Пусть $V$ — прямая сумма $n$ экземпляров циклической группы порядка $2^m$, $q$ — простой делитель числа $2^n - 1$, а $b$ — элемент порядка $q$ группы GL $(n, 2)$ с неприводимым над GF (2) минимальным многочленом. Пусть далее $l$ — степень минимального многочлена матрицы $b$. Тогда мы можем считать, что

$$b = \operatorname{diag}[d, \ldots, d], \tag{25}$$

где $d \in \mathrm{GL}(l, 2)$, $d^q = E_l$, $|xE_l - d|$ — неприводимый над GF (2) многочлен. Группу $V$ будем трактовать как $\mathbf{Z}_{2^m}$-модуль столбцов $v$, где

$$v = \begin{pmatrix} v_1 \\ \cdot \cdot \cdot \\ v_n \end{pmatrix}, \quad v_i \in \mathbf{Z}_{2^m}.$$

Регулярный автоморфизм порядка $q$ группы $v$ будем искать в группе $h_n^{-1}(\langle b \rangle)$. Очевидно, $|h_n^{-1}(\langle b \rangle)| = q\,|\operatorname{Ker} h_n|$.

По теореме Силова в группе $h_n^{-1}(\langle b \rangle)$ есть элемент $g$ порядка $q$. Следовательно, $h_n^{-1}(\langle b \rangle) = \langle g \rangle \operatorname{Ker} h_n$. Так как $|\langle g \rangle| = |\langle b \rangle| = q$ и $h_n \langle g \rangle = \langle b \rangle$, то в $h_n^{-1}(\langle b \rangle)$ есть такой элемент $a$ порядка $q$, что $h_n(a) = b$. В силу (1) в $h_n^{-1}(b)$ есть матрица вида $a = \operatorname{diag}[c, \ldots, c]$, $c \in h_l^{-1}(d)$. Согласно предыдущим рассуждениям мы можем считать, что $|\langle c \rangle| = q$.

Итак, можно ограничиться случаем неприводимой группы $\langle b \rangle : (\langle b \rangle) = q$, многочлен $|xE_n - b|$ неприводим над GF (2), а в $h_n^{-1}(b)$ есть элемент $a$ порядка $q$. Матрицу $b$ можно выбрать в виде

$$b = \begin{Vmatrix} 0 & 0 & \cdots & 0 & \beta_0 \\ 1 & 0 & \cdots & 0 & \beta_1 \\ 0 & 1 & \cdots & 0 & \beta_2 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & \beta_{n-1} \end{Vmatrix}, \quad \beta_i \in \mathrm{GF}(2).$$

Очевидно, в $h_n^{-1}(b)$ есть матрица

$$a_0 = \begin{Vmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & \alpha_2 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & \cdot & \alpha_{n-1} \end{Vmatrix}, \quad \alpha_i \in Z_{2^m}, \quad \gamma(\alpha_i) = \beta_i. \tag{26}$$

Для $a$ имеем $a \in a_0 \operatorname{Ker} h_n$, $a = a_0 (E_n + 2r)$, $r \in M(n, Z_{2^m})$. Покажем теперь, что $a$ — регулярный автоморфизм группы $V$. Пусть $v \in V$ и $av = v$. Полагая $v = \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}$, имеем

$$a \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}, \quad v_i \in \mathbf{Z}_{2^m}.$$

Тогда $h_n(a) w = w$, $bw = w$, где

$$w = \begin{pmatrix} \gamma(v_1) \\ \dots \\ \dots \\ \gamma(v_n) \end{pmatrix}.$$

Так как многочлен $(xE_n - b)$ неприводим над GF(2), то

$$w = 0, \quad \gamma(v_i) = 0, \quad v_i \in 2\mathbf{Z}_{2^m}, \quad i = 1, \dots, n.$$

Пусть $v_i \in 2^t \mathbf{Z}_{2^m}$, $0 < t < m$, $i = 1, \dots, n$. Для $av$ можно записать $av = a_0 (E_n + 2r) v = a_0 v + 2a_0 rv = a_0 v + 2^{t+1} u$, $u \in V$. Следовательно, $a_0 v + 2^{t+1} u = v$. Отсюда и из (26) получаем сравнения

$$\left.\begin{aligned} \alpha_0 v_n &\equiv v_1 \\ v_1 + \alpha_1 v_n &\equiv v_2 \\ &\dots \\ v_{n-1} + \alpha_{n-1} v_n &\equiv v_n \end{aligned}\right\} \pmod{2^{t+1} \mathbf{Z}_{2^m}}. \tag{27}$$

Сложив эти сравнения, получим

$$(\alpha_0 + \alpha_1 + \dots + \alpha_{n-1}) v_n \equiv v_n \pmod{2^{t+1} \mathbf{Z}_{2^m}}. \tag{28}$$

Так как $|xE - b|$ — неприводимый над GF(2) многочлен, то

$$\beta_0 + \beta_1 + \dots + \beta_{n-1} + 1 = 1, \ \beta_0 + \beta_1 + \dots + \beta_{n-1} = 0,$$

$$\alpha_0 + \alpha_1 + \dots + \alpha_{n-1} \in 2\mathbf{Z}_{2^m}.$$

Отсюда и из сравнения (28) следует, что

$$v_n \in 2^{t+1} \mathbf{Z}_{2^m}. \tag{29}$$

Из (27) и (29) получаем $v_1 \equiv v_2 \equiv \dots v_{n-1} \equiv 0 \pmod{2^{t+1} \mathbf{Z}_{2^m}}$. Отсюда $v = 2^{t+1} v'$, $v' \in \mathbf{Z}_{2^m}$. Применяя несколько раз предыдущие рассуждения, получаем $v_i = 0$, $i = 1, \dots, n$, $v = 0$. Следовательно, из равенства $av = v$ вытекает равенство $v = 0$, $a$ — регулярный автоморфизм порядка $q$ группы $V$. Теорема 4 доказана.

Из доказательства теоремы 4 вытекают такие утверждения.

Следствие 1. *Пусть $n > 1$, $V_{n,m}$ — прямая сумма $n$ экземпляров циклической группы порядка $2^m$. Тогда для любого простого делителя $q$ числа $2^n - 1$ в* $\operatorname{Aut}(V_{n,m})$ *есть регулярный автоморфизм порядка $q$.*

Очевидно, любую абелеву 2-группу $A$ можно представить в виде прямой суммы $A = V_{n_1, m_1} \oplus \dots \oplus V_{n_k, m_k}$.

Следствие 2. *Пусть наибольший общий делитель $(n_1, \dots, n_k) = d$ чисел $n_1, \dots, n_k$ больше 1. Тогда $A \in K$, ибо для любого простого делителя $q$ числа $2^d - 1$ в* $\operatorname{Aut}(A)$ *есть регулярный автоморфизм порядка $q$.*

Верна следующая теорема.

Теорема 5. *Пусть разложение конечной абелевой 2-группы $A$ в прямое произведение циклических подгрупп содержит $k$ множителей, $n_1, \ldots, n_v$ — кратности циклических множителей разложения, а $d = (n_1, \ldots, n_v)$ — наибольший общий делитель чисел $n_1, \ldots, n_v$. Группа $A$ тогда и только тогда изоморфна ядру некоторой группы Фробениуса, когда $(n_1, \ldots, n_v) = d > 1$.*

Доказательство. В силу следствия 2 остается доказать лишь необходимость условия $d > 1$. Пусть $A \in K$. Надо доказать, что $d > 1$. Так как $A \in K$, то в Aut $(A)$ есть автоморфизм $\psi$ простого порядка $q$. Пусть $m$ — наименьшее положительное целое, для которого $2^m \equiv 1 (\mathrm{mod}\, q)$. Покажем, что $m \mid d$. Пусть $2^{\alpha_1} < 2^{\alpha_2} < \ldots < 2^{\alpha_v}$ — порядки прямых циклических сомножителей группы $A$, а $n_j$ — кратность множителя порядка $2^{\alpha_j}$. Рассмотрим подгруппы $B_j = A^{2^{\alpha_j}}$, $j = 1, \ldots, v-1$. Очевидно, $B_j$ — характеристическая подгруппа группы $A$ и, следовательно, ограничение $\psi_j = \psi \mid B_j$ является регулярным автоморфизмом порядка $q$ группы $B_j$.

Пусть теперь $M$ и $M_j$ — множества всех элементов второго порядка групп $A$ и $B_j$ соответственно. Тогда, очевидно, $\psi(M) = M$, $\psi_j(M_j) = M_j$. Следовательно, $q \mid\mid |M|$, $q \mid\mid |M_j|$, $j = 1, \ldots, v-1$. Как нетрудно вычислить, $|M| = 2^k - 1$, $|M_j| = 2^{k-(n_1+\ldots+n_j)} - 1$. Следовательно, в поле $\mathrm{GF}(2^k)$ есть элемент порядка $q$. В силу выбора числа $m$ имеем $\mathrm{GF}(2^m) \subseteq \mathrm{GF}(2^k)$, $m \mid k$, $m \mid (n_1 + \ldots + n_v)$. Аналогично получаем

$$\mathrm{GF}(2^m) \subseteq \mathrm{GF}(2^{k-(n_1+\ldots+n_j)}), \quad m \mid (k - (n_1 + \ldots + n_j)),$$

$j = 1, \ldots, v-1$. Итак, верны следующие сравнения:

$$\left.\begin{aligned} n_1 + \ldots + n_v &\equiv 0 \\ n_2 + \ldots + n_v &\equiv 0 \\ &\cdots \\ n_v &\equiv 0 \end{aligned}\right\} (\mathrm{mod}\, m).$$

Отсюда получаем $m \mid n_1$, $m \mid n_2$, ..., $m \mid n_v$, $m \mid d$, $d > 1$. Теорема 5 доказана.

Заметим, что если $p$ и $q$ — простые числа и $q \mid p - 1$, то, как легко проверить, любая конечная абелева $p$-группа обладает регулярным автоморфизмом порядка $q$. В более общей ситуации, когда $p$ и $q$ — простые числа, $p \neq q$, а $m$ — такое целое положительное число, что $q \mid p^m - 1$, но $q \nmid p^u - 1$, где $0 < u < m$, верна следующая теорема.

Теорема 6. *Пусть $A$ — конечная абелева $p$-группа, $n_1, \ldots, n_v$ — кратности ее циклических прямых множителей, $d$ — наибольший общий делитель чисел $n_1, \ldots, n_v$. В группе* Aut $A$ *тогда и только тогда существует регулярный автоморфизм порядка $q$, когда $m \mid d$.*

Доказательство аналогично доказательству теорем 4 и 5.


1. *Frobenius G.* Uber auflosbare Gruppen. IV. // Sitzungber. Berliner Akad. Wissenschaften.— 1901.— S. 1216—1230.
2. *Jordan C.* Recherches sur les substitutions // J. Math. Pures Appl.— 1872.— 17.— P. 351—363.
3. *Burnside W.* Theory of groups of finite order.— Cambridge, 1911.
4. *Шмидт О. Ю.* О группе Frobeniusa // Докл. АН СССР.— 1940.— 26, № 1.— С. 3—5.
5. *Higman G.* Groups and rings having automorphisms without non—trivial fixed elements // J. London Math. Soc.— 1957.— 32.— P. 321—334.
6. *Thompson J. G.* Finite groups with fixed point free automorphisms of prime order // Proc. Nat. Acad. Sci.— 1959.— 45.— P. 578—581.
7. *Крекнин В. А., Кострикин А. И.* Об алгебрах Ли с регулярным автоморфизмом // Докл. АН СССР.— 1963.— 149, № 2.— С. 249—251.
8. *Крекнин В. А.* О разрешимости алгебр Ли с регулярным автоморфизмом конечного периода // Там же.— 150, № 3.— С. 467—469.
9. *Супруненко Д. А.* Неприводимые нильпотентные матричные группы простой степени // Мат. сб.— 1952.— 31 (73).— С. 353—358.
10. *Шмидт О. Ю.* Избранные труды. Математика.— М. : Изд-во АН СССР, 1959.— 316 с.


Получено 14.01.91