Владикавказский математический журнал
Апрель–июнь, 2000, Том 2, Выпуск 2

Юрию Леонидовичу Ершову
к его шестидесятилетию

УДК **512.54**

О ГРУППАХ ФРОБЕНИУСА, СОДЕРЖАЩИХ ЭЛЕМЕНТ ПОРЯДКА 3

А. Х. Журтов

Доказывается, что группа Фробениуса G, порожденная двумя элементами порядка 3, конечна. Ядро группы G абелево и число его порождающих не превышает числа 8, а дополнение либо циклическое, либо изоморфно одной из групп $\mathrm{SL}_2(3)$, $\mathrm{SL}_2(5)$.

В работе продолжаются исследования начатые в [1] и [2]. Часть результатов получены совместно с В. Д. Мазуровым.

Напомним, что группой Фробениуса с ядром F и дополнением H называется полупрямое произведение $F \cdot H$, удовлетворяющее следующим условиям:

а) H — собственная подгруппа в G и $H \cap H^f = 1$ для любого неединичного элемента $f \in F$,

б) $F \setminus \{1\} = G \setminus \{H^f | f \in F\}$.

Теорема 1. *Группа Фробениуса G, порожденная двумя элементами порядка 3, конечна. Ядро группы G абелево и число его порождающих не превышает числа 8, а дополнение либо циклическое, либо изоморфно одной из групп $SL_2(3)$, $SL_2(5)$.*

Доказательству предпошлем три леммы. В них под модулем для группы или кольца понимается любая аддитивно записанная абелева группа, на которой данная группа или кольцо действует. Для группы A A-модуль V называется *фробениусовым*, если $v(x-1) \neq 0$ и $V(x-1) = V$ для всех $V \ni v \neq 0$, $1 \neq x \in A$.

Лемма 1. *Пусть m — натуральное число и V — ненулевой RA-модуль, где R — поле простого порядка или $R = \mathbb{Z}[1/m]$ и в этом случае V не имеет кручения, а $A = \langle \mathrm{a} \rangle$ — циклическая группа. Если модуль V конечно порожден как RA-модуль, то существует натуральное число n такое, что $V(a^n - 1) \neq V$.*

$\lhd$ Предположим вначале, что $R = \mathbb{Z}[1/m]$ и V — противоречащий пример с наименьшим числом s образующих v_1, v_2, ... , v_s. Поскольку $V(a-1) = V$, то существует ненулевой полином $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_t x^t \in \mathbb{Z}[x]$ такой, что $v_s f(a) \in v_1 S + \ldots + v_{s-1} S$, где $S = R\langle a\rangle$. Выберем f наименьшей степени t. Тогда $\alpha_0 \neq 0 \neq \alpha_t$ и $v_s \alpha_t a^t$, $v_s \alpha_0 a^{-1} \in \sum\limits_{i=1}^{s-1} v_i S$. Это означает, что $V \le \sum\limits_{i=1}^{s-1} v_i R_1\langle a\rangle + v_s \sum\limits_{j=0}^{t-1} R_1 a^j = V_1$, где $R_1 = \mathbb{Z}[1/m\alpha_0\alpha_t]$, и V_1 является $\langle a\rangle$-модулем над R_1. Далее, $V_1(a^n - 1) = V_1$ для любого $n \in \mathbb{N}$. Если $v_s(\beta_0 + \beta_1 + \ldots + \beta_{t-1}a^{t-1}) \in \sum\limits_{i=1}^{s-1} v_i R_1\langle a\rangle$ для некоторого ненулевого вектора $(\beta_0 + \beta_1 + \ldots + \beta_{t-1}) \in R_1^t$, то умножив на подходящее натуральное число, мы найдем нетривиальный полином $g \in \mathbb{Z}[x]$ степени не больше $s-1$, для которого $v_s g(a) \in \sum\limits_{i=1}^{s-1} v_i S$. Это противоречит выбору f. По выбору V, $V_1 \neq \sum\limits_{i=1}^{s-1} v_i R_1\langle a\rangle = V_2$, $V_3 = V_1/V_2$ — ненулевой конечномерный $\langle a\rangle$-модуль без кручения над R_1 с одним порождающим $v = v_s + V_2$ и $V_3(a^n - 1) = V_3$ для всех $n \in \mathbb{N}$. Теперь мы можем рассматривать R_1 как R, V_3 как V и считать, что V — конечномерный однопорожденный S-модуль.

В этом случае V как S-модуль изоморфен кольцу $S_0 = S/\ker V$. Пусть p — простое число, не делящее m. Если $pV = V$, то $pvg(a) = v$ для некоторого полинома g над R степени не больше $s-1$, и $v(pg-1) = 0$ вопреки выбору f. Поэтому pS_0 — собственный идеал в S_0 и число $|S_0/pS_0| = |V : pV|$ конечно. Пусть M — максимальный идеал из S_0 содержащий pS_0. Тогда $a \notin M$, S_0/M — конечное поле и поэтому существует $n \in \mathbb{N}$, для которого $a^n + M = 1 + M$. Другими словами, $a^n - 1 \in M$, $S_0(a^n - 1) \subseteq M \neq S_0$ и $V(a^n - 1) \neq V$. Это противоречие доказывает лемму для $R = \mathbb{Z}[1/m]$. Те же рассуждения (с некоторыми очевидными упрощениями) годятся и для поля простого порядка. Лемма доказана. $\triangleright$

Лемма 2. *Пусть A — группа, порожденная двумя элементами x, y порядка 3 и V — однопорожденный фробениусов A-модуль. Тогда V — конечная абелева группа.*

$\triangleleft$ Пусть u_0 — порождающий A-модуля V и T — множество всех элементов конечного порядка из V. Тогда T — A-подмодуль и V/T — группа без кручения. Если $T = V$ и m — порядок элемента u_0, то $mV = 0$. Если $m = pn$, где p — простой делитель числа m, то $V_0 = \{x \in V \mid nx = 0\}$ — собственный A-модуль. Пусть $V_1 = V/V_0$. Тогда V_1 — ненулевой однопорожденный фробениусов A-модуль над полем порядка p. Если порядок группы V_1 конечен, то и порядок V конечен. Таким образом, в этом случае достаточно доказать лемму для A-модуля над полем F порядка p.

Если $T \neq V$, то $V_1 = V/T$ — фробениусов A-модуль без кручения и мы можем считать, что $V_1 = V$. Итак, можно предполагать V — RA-модуль, где $R = F$ или $R = \mathbb{Z}$ и в этом последнем случае V не имеет кручения.

Обозначим $a = xy$ и положим $u_i = u_0 a^i$, $v_i = u_0 a^i x$ для $i \in \mathbb{Z}$. Тогда $V = \langle \{u_i, v_i | i \in \mathbb{Z}\} \rangle$

$$u_i x = v_i, \quad v_i x = -u_i - v_i, \quad u_i y = -u_i - v_{i-1}, \quad v_i y = u_{i+1} \tag{1}$$

для всех целых чисел i. Из (1) вытекает, что для любого целого i

$$\begin{gathered} u_i a = u_{i+1}, \quad v_i a - 1 = v_{i-1}, \quad u_i a^{-1} = -u_{i-1}, \\ v_i a^{-1} = -u_i + u_{i+1} + v_{i+1}. \end{gathered} \tag{2}$$

Это показывает, что u_0, v_0 — порождающие для $R\langle a \rangle$-модуля V. По лемме 1 существует $n \in \mathbb{N}$ такой, что $V(a^n - 1) \neq V$. По условию $a^n = 1$. По [1] группа А конечна и V — конечно порожденная группа. Если $R = F$, то V конечна. Предположим, что $R = \mathbb{Z}$. Тогда $V = V(x-1)^2 = V(-3x) = 3V$, что невозможно. Лемма доказана. $\triangleright$

Лемма 3. *Пусть A — конечная группа порожденная двумя элементами x, y порядков ≤ 4 и V — конечная абелева группа с s порождающими, которая является однопорожденным фробениусовым A-модулем. Тогда верно одно из следующих утверждений:*

(1) *группа A циклическая порядка 2, 3, 4, 6 или 12 и s не превосходит числа 1, 2, 2, 2 или 4 соответственно;*

(2) *группа A изоморфна $SL_2(3)$, $GL_2(3)$ или $SL_2(5)$ и s не превосходит числа 4, 4 или 8 соответственно;*

(3) *группа A изоморфна группе $SQ_{2n} = \langle x^{2n} = y^4 = 1 | x^n = y^2, x^y x = 1 \rangle$ порядка $4n$ и $s \leq 4\varphi(n)$, где φ — функция Эйлера.*

$\triangleleft$ Доказательство этой леммы, по существу, содержится в [1]. $\triangleright$

Теперь докажем теорему 1.

$\triangleleft$ Пусть $G = \langle x, z \rangle = AP$, где $x^3 = z^3 = 1$, F — ядро и H — дополнение в G. Можно считать, что $x \in H$. Пусть $z = fy$, где $f \in F$, $y \in H$. Тогда $G = \langle f, x, y \rangle$, $H = \langle x, y \rangle$, $F = \langle f^H \rangle$. Пусть M — максимальная абелева подгруппа в F, содержащая f. Если для всех $h \in H$ выполнено равенство $M^h =$ M, то $F = M$ — абелева группа. Предположим, что $M^h \neq M$ для некоторого элемента $h \in H$. Тогда либо $M^x \neq M$, либо $M^y \neq M$. Из-за симметрии можно считать, что $M^x \neq M$. По выбору $M, [M^x, M] \neq 1$. Пусть a$, b \in M$. Тогда $1 = (a^x b)^2 (a^x b)^x (a^x b) = ab^{x^2} \mathrm{a}^{x^2} b^x a^x b = ab^{x^2} (a^{x^2} a^x)(b^x b) = ab^{x^2} \mathrm{a}^{-1} (b^{-1})^{x^2} = [a^{-1}, (b^{-1})^{x^2}]$ и поэтому $[a, b^x] = 1$. Следовательно, $[M, M^x] = 1$. Это противоречие показывает, что $F = M$ — абелева группа. Теперь заключение теоремы вытекает из лемм 1, 2, 3. $\triangleright$

Следствие. *Пусть (G, H) — пара Фробениуса и H содержит элемент x порядка 3. Если для любого элемента $g \in G$ подгруппа $\langle x, x^g \rangle$ — является группой Фробениуса, то $G = F \cdot H$ для нормальной периодической подгруппы F. При этом, либо подгруппа $V = \langle x^h | \, h \in H \rangle$ изоморфна одной из групп $SL_2(3)$, $SL_2(5)$ и подгруппа F — абелева, либо $\langle x \rangle$ — нормальная подгруппа в H и F двуступенно нильпотентна.*

По теореме 1 выполнены условия (теоремы 5 из [2]) $\{2, 3\}$-группы регулярных автоморфизмов. Пусть C_{p^∞} — бесконечная, локально циклическая p-группа. Это означает, что

$$C_{p^\infty} = \langle a_i | a_1^p = 1, \ a_{i+1}^p = a_i, \ i \in \mathbb{N} \rangle.$$

Бесконечной обобщенной группой кватернионов назовем группу

$$Q^\infty = \langle C_{2^\infty}, t | \, t^2 = a_1, \ a_i^t = a_i^{-1} \rangle.$$

Легко проверить, что каждая подгруппа $Q_i = \langle a_i, t \rangle$ изоморфна обобщенной группе кватернионов порядка 2^{i+1} и $Q^\infty = \bigcup_{i \in \mathbb{N}} Q_i$. Заметим, что $N = \langle a_i | \, i \in \mathbb{N} \rangle$ единственная собственная, бесконечная подгруппа из Q^∞ и любой элемент из Q^∞, порядок которого больше четырех, лежит в $\mathbb{N}$.

Группа Q^∞ порождается элементами порядка 4.

Любая собственная подгруппа из Q^∞ отлична от своего нормализатора и либо конечна и является циклической или обобщенной кватернионной группой, либо совпадает с N.

Утверждение. *Пусть G — группа, в которой любые два элемента x, y со свойством $x^y = x^{-1}$ порождают 2-подгруппу с единственной инволюцией. Любая 2-группа с единственной инволюцией либо является локально циклической, либо обобщенной группой кватернионов (возможно, бесконечной).*

Если в G нет нетривиальных 2-элементов, то доказывать нечего. В противном случае G обладает единственной инволюцией z. Если в G нет элементов порядка 4, то снова доказывать нечего. Пусть в G есть элемент порядка 4. Нам потребуется следующая лемма.

Лемма 4. *Если y — элемент порядка 4 из G, то 2-элементы из $C_G(y)$ составляют локально циклическую подгруппу C_0, а в $N_G(\langle y \rangle)$ 2-элементы составляют нормальную 2-подгруппу, в которой C_0 — подгруппа индекса ≤ 2.*

$\lhd$ Пусть C_0 — максимальная, нормальная локально циклическая 2-подгруппа из $C = C_G(y)$. Если не все 2-элементы из C содержатся в C_0, то найдется такой 2-элемент t из C, что tC_0 — инволюция в C/C_0.

Если $t^c C_0 \neq tC_0$ для некоторого элемента $c \in C$, то $\langle t, t^c, y \rangle$ — конечная не локально циклическая 2-группа с одной инволюцией и центральной подгруппой порядка 4. Поскольку в конечной обобщенной группе кватернионов порядок центра равен двум, эта ситуация невозможна и $\langle t, C_0\rangle$ — нормальная локально конечная подгруппа из C, содержащая центральную подгруппу порядка 4. Поэтому $\langle t, C_0\rangle$ — локально циклическая группа, вопреки выбору подгруппы C_0. Итак C_0 содержит все 2-элементы из C. Если $N = N_G(\langle y\rangle \neq C$, то найдется элемент x из $N \setminus C$, что $y^x = y^{-1}$, поэтому x — 2-элемент.

Если x не централизует C/C_0, то поскольку $\langle C_0, x\rangle$ — неабелева группа, она обобщенная группа кватернионов, x элемент порядка 4 и x^2 централизует C_0. Пусть $cC/C_0 \neq c^xC/C_0$, для некоторого элемента $c \in C$. Тогда $(c^{-1}c^x)^x = (c^{-1}c^x)^{-1}$, $c^{-1}c^x \notin C_0$ и поэтому не является 2-элементом. Это противоречит условию. Поэтому x централизует C/C_0 и $\langle C_0, x\rangle$ обобщенная группа кватернионов, нормальная в N.

Если в G нет элементов порядка 8, то любые два элемента порядка 4 из G перестановочны по модулю $\langle z\rangle$ и поэтому все 2-элементы порождают группу кватернионов порядка 8.

Пусть x — элемент из G порядка 8 и $y = x^2$. Тогда $y^2 = z$. Положим $C = C_G(y)$, $N = N_G(\langle y\rangle)$. По лемме 4 в C существует локально циклическая нормальная силовская 2-подгруппа C_0, а в N — нормальная силовская 2-подгруппа N_0 и $|N_0 : C_0| \leq 2$. Если $N_0 \neq C_0$, то N_0 — обобщенная группа кватернионов (возможно, бесконечная). Если все элементы порядка 4 из G содержатся в N, то в случае $N = C$ подгруппа C совпадает с G, а в случае $N \neq C$ подгруппа N_0 порождается элементами порядка 4 и, следовательно, нормальна в G. Но тогда $\langle y\rangle G$ и $N = G$.

Поэтому пусть существует элемент t порядка 4 из G, который не содержится в N. Подгруппа $\langle y, x\rangle$ — обобщенная группа кватернионов и yt — элемент, порядок которого больше четырех. Пусть $z = (yt)^{2^s}$ — элемент порядка 8. Тогда $\langle x, r\rangle$ нормализует $H = \langle y, r^2\rangle$ и xH, rH — инволюция в $\langle x, r\rangle/H$. Таким образом $\langle x, r\rangle$ — конечная 2-подгруппа из G содержащая две различные циклические подгруппы порядка 8. Это невозможно. $\triangleright$

Теорема 2. *Пусть G — нетривиальная $\{2, 3\}$-группа регулярных автоморфизмов абелевой группы. Если G конечна, то верно одно из следующих утверждений:*

(1) *G — циклическая группа;*

(2) *$G = \langle x, y | x^{3^t} = y^{2^s} = 1,\ y^{-1}xy = x^{-1}\rangle$ для некоторых натуральных чисел t и s, $s \geq 2$;*

(3) *$G = \langle x, y | x^{2^s3^t} = y^4 = 1,\ y^2 = x^{2^{s-1}3^t},\ x^y = x^{-1}\rangle$ для некоторых натуральных чисел t и s, $s \geq 2$;*

(4) *$G = \langle x, y, z | x^4 = z^{3^t} = 1,\ x^2 = y^2,\ y^x = y^{-1},\ x^z = y,\ y^z = xy^{-1}\rangle$, t — натуральное число; другими словами, G — расширение группы кватернионов Q порядка 8 посредством циклической 3-группы, индуцирующей в Q*

нетривиальный автоморфизм;

(5) $G = \langle x, y, z, v\rangle$, *где* $\langle x, y, z\rangle$ — *группа типа* 3, $v^2 = x^2$, $z^v = z^{-1}$, $x^v = y^{-1}$, $y^v = x^{-1}$;

(6) G *изоморфна* $SL_2(5)$;

(7) G *содержит подгруппу индекса* 2, *изоморфную* $SL_2(5)$, *и силовская* 2*-подгруппа из* G — *обобщенная группа кватернионов.*

Если G *бесконечна, то подгруппа из* G *порожденная всеми элементами порядка* 3, *является циклической, и верно одно из следующих утверждений:*

(8) G — *расширение локально циклической* 2*-группы или (возможно, бесконечной) обобщенной группы кватернионов посредством* 3*-группы с единственной подгруппой порядка* 3;

(9) G — *полупрямое произведение локально циклической* 3*-подгруппы* R *и циклической* 2*-подгруппы* $\langle s\rangle$ *порядка* ≥ 4, $r^s = r^{-1}$ *для любого элемента* $r \in R$;

(10) $G = (U \times V)\langle t\rangle$, *где* U — *локально циклическая* 2*-группа или конечная группа кватернионов,* V — *локально циклическая* 3*-группа,* t — *элемент порядка* 4, $U\langle t\rangle$ — *(возможно, бесконечная) обобщенная группа кватернионов и* $v^t = v^{-1}$ *для любого элемента* $v \in V$.

Отметим, что только в случае 8 группа G *может не быть локально конечной (см. примеры 1 и 2 в [3]).*

$\lhd$ Если G конечна, то её строение известно (см. [4, 5, 6]). Пусть G — бесконечна и A-подгруппа из G, порожденная всеми элементами порядка 3. По [2] A — циклическая группа или группа изоморфная одной из групп $\mathrm{SL}_2(3)$, $\mathrm{SL}_2(5)$. Во втором случае $C_G(\mathrm{A}) \leq A$ и поэтому $G = N_G(A)$ — конечная группа. Итак A — циклическая группа.

Если $|A| = 1$, то G — 2-группа и по предложению 1 G удовлетворяет условию 8. Поэтому пусть $|A| = 3$. Если $B = C_G(A)$, то по предложению 1 B удовлетворяет условиям пункта 8 и при $B = G$ теорема доказана.

Если $B \neq G$, то $|G : B| = 2$. Пусть $S = O_2(G)$. Тогда G/S — расширение 3-группы $\overline{R}$ с помощью подгруппы $\langle a\rangle$ порядка 2, индуцирующей в $\overline{R}$ регулярную группу автоморфизмов. Пусть $r \in \overline{R}$. Тогда $[r, a] = a^r a$ — элемент нечетного порядка и поэтому в $\langle a^r, a\rangle$ существует инволюция i, для которой $a^{ri} = a$. Это означает, что $ri = a$, $r = ai$ и $r^a = r^{-1}$. Таким образом, a инвертирует каждый элемент из $\overline{R}$, поэтому $\overline{R}$ абелева и, следовательно, локально циклическая. Пусть t — элемент из $G \setminus B$. Тогда $r^t = r^{-1}$ для любого элемента $r \in \overline{R}$.

Пусть R — силовская 3-подгруппа из G, тогда R локально циклическая группа и $SR = B$. Действительно, если $SR \neq B$, то SR/S — собственная подгруппа в локально циклической 3-группе B/S. Поэтому $R = \langle r\rangle$ — циклическая группа конечного порядка 3^a и существует элемент r_1 в B порядка 3^{a+1}.

Поскольку B локально конечна, подгруппа $\langle r_1\rangle$ сопряжена с подгруппой из $\langle r\rangle$ в конечной группе $\langle r, r_1\rangle$ и мы получаем противоречие. Если R не централизует S, то S — группа кватернионов порядка 8, а R — циклическая группа. В этом случае G — конечная группа вопреки предположению. Если же R централизует S, то R — нормальная подгруппа в G и выполнены условия пункта 9. $\triangleright$

Литература

1. *Журтов А. Х.* Квадратичные автоморфизмы абелевых групп // Алгебра и логика (в печати).
2. *Журтов А. Х.* О регулярных автоморфизмах порядка 3 и парах Фробениуса // Сиб. мат. журн.—2000.—Т. 51, № 2.
3. *Созутов А. П.* О строении неквариантного множителя в некоторых группах Фробениуса // Сиб. мат. журн.—1994.—Т. 35, № 4.—С. 893–901.
4. *Zassenyjuse H.* Kennzeichnung endlichen linearen Gruppen als Permutationsgruppen // Abhandl. Math. Semin., Hamburg.—1936.—V. 11.—P. 17–40.
5. *Буссарин В. М., Горчанов Ю. М.* Конечные расщепляемые группы.—М.: Наука, 1969.
6. *Huppert B., Blackburn N.* Finite groups 3.—Berlin: Springer Verlag, 1982.

г. Нальчик *Статья поступила 30 марта 2000 г.*