Серия «Математика»
2013. Т. 6, № 2. С. 18—25

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 512.517

О необходимых условиях регулярности силовской p-подгруппы группы $GL_n(\mathbb{Z}_{p^m})$ *

С. Г. Колесников
Сибирский федеральный университет,
Сибирский государственный аэрокосмический университет

Аннотация. В связи с вопросом Б. Верфрица 8.3 из Коуровской тетради установлено, что силовская p-подгруппа группы $GL_n(\mathbb{Z}_{p^m})$ при $n \leqslant (p-1)/2$ удовлетворяет известным необходимым условиям регулярности.

Ключевые слова: регулярная p-группа; линейная группа; силовская подгруппа.

1. Введение

Понятие регулярной группы было введено Ф. Холлом в [1]. Им же был установлен следующий критерий регулярности (см., например, [2, теорема 12.4.2]): конечная p-группа G регулярна тогда и только тогда, когда для любых двух элементов $a, b \in G$ существует элемент $c \in \langle a, b\rangle'$ такой,что $(ab)^p = a^p b^p c^p$. И найдены следующие необходимые условия регулярности: если p-группа G регулярна, то для любых $a, b \in G$ а) равенство $a^{p^i} = b^{p^i}$ имеет место тогда и только тогда, когда $(a^{-1}b)^{p^i} = 1$ [2, теорема 12.4.4]; б) $[a^{p^i}, b] = 1$ (или $[a, b^{p^i}] = 1$) тогда и только тогда, когда $[a, b]^{p^i} = 1$ [2, теорема 12.4.3]; в) множества

$$\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}, \quad \mho_i(G) = \{x^{p^i} \mid x \in G\}, \quad i = 1, 2, \ldots,$$

являются характеристическими подгруппами в G [2, теорема 12.4.5].

В 1982 году Б.Верфриц поставил в Коуровской тетради вопрос [3, вопрос 8.3]: для каких натуральных чисел n, m и простого числа p силовская p-подгруппа $P_n(\mathbb{Z}_{p^m})$ общей линейной группы $GL_n(\mathbb{Z}_{p^m})$ над

* Работа выполнена при финансовой поддержке РФФИ, грант 12-01-00968, проекта «Алгебро-логические структуры и компплексный анализ с приложениями к передаче и защите информации», выполняемому в рамках «Задание Минобрнауки РФ», гранта КГПУ им. В. П. Астафьева НШ № 10.

кольцом $\mathbb{Z}_{p^m}$ классов вычетов целых чисел по p-примарному модулю является регулярной? Изучая коммутаторное строение матричных групп, Ю.И. Мерзляков в [4] установил, что ступень нильпотентности группы $P_n(\mathbb{Z}_{p^m})$ равна $nm-1$. Поскольку p-группы ступени нильпотентности меньше, чем p, регулярны [2, стр. 205], группа $P_n(\mathbb{Z}_{p^m})$ регулярна при $nm-1<p$. В работе А. В. Ягжева [5], для случая $m=1$, и работе С. Г. Колесникова [6], для случая $m=2$, было показано, что группа $P_n(\mathbb{Z}_{p^m})$ регулярна тогда и только тогда, когда $n<(p+1)/m$. В [7] автором была установлена регулярность группы $P_n(\mathbb{Z}_{p^m})$ при любых $m\geqslant 1$, когда $n^2<p$. Учитывая, что свойство регулярности наследуется на подгруппы и фактор-группы, из приведенных результатов следует полный ответ на вопрос Б. Верфрица для $n=2$. Когда $n>2$, ответ на вопрос остаётся неизвестным лишь для конечного числа простых чисел заключённых в промежутке от $2n+1$ до n^2. Цель статьи — показать, что в оставшихся случаях группа $P_n(\mathbb{Z}_{p^m})$ удовлетворяет сформулированным выше необходимым условиям регулярности.

Отметим, что автором и Н.В. Мальцевым в работах [7], [8] исследовался и аналог вопроса Б. Верфрица для силовских p-подгрупп групп Шевалле над $\mathbb{Z}_{p^m}$.

2. Определения и основная теорема

Для всякого целого неотрицательного числа l через J^l будем обозначать идеал кольца $\mathbb{Z}_{p^m}$, порождённый элементом p^l, а множество квадратных матриц порядка n, у которых все элементы лежат в идеале J^l, будем обозначать $M_n(J^l)$. Очевидна следующая

Лемма 1. *Для всякого целого неотрицательного числа l множество $M_n(J^l)$ является идеалом кольца всех матриц порядка n с элементами из $\mathbb{Z}_{p^m}$ и имеют место следующие включения:*

А) $M_n(J^l)\cdot M_n(J^k)\subseteq M_n(J^{l+k})$;

Б) $p^kA\in M_n(J^{l+k})$, *если* $A\in M_n(J^l)$.

Множество матриц сравнимых с единичной матрицей по модулю идеала $M_n(J^i)$, $i=1,2,\ldots$, образуют подгруппу в $GL_n(\mathbb{Z}_{p^m})$, которая называется конгруэнц-подгруппой и обозначается $K_n(\mathbb{Z}_{p^m},J^i)$.

Следуя [4], определим последовательность функций $F_n^{(k)}$, $n,k=1,2,\ldots$, от натуральных аргументов i,j, полагая

$$F_n^{(k)}(i,j)=-\left[\frac{i-j-k}{n}\right],$$

здесь $[x]$ — целая часть числа x (ближайшее к x слева целое число). Множество квадратных матриц порядка n, у которых элемент, стоящий на пересечении i-й строки и j-го столбца, лежит в идеале $J^{F_n^{(k)}(i,j)}$, обозначим через $M_n(F_n^{(k)})$. Нетрудно видеть, что имеют место следующие включения:

$$M_n(F_n^{(1)}) \supseteq M_n(F_n^{(2)}) \supseteq \dots .$$

Множество матриц порядка n с элементами из кольца $\mathbb{Z}_{p^m}$ сравнимых с единичной матрицей по модулю $M_n(F_n^{(1)})$ является максимальной p-подгруппой в $GL_n(\mathbb{Z}_{p^m})$ [9, стр. 95, упражнение 7]. Поэтому можем считать, что

$$P_n(\mathbb{Z}_{p^m}) = \{E + A \mid A \in M_n(F_n^{(1)})\},$$

здесь и далее через E обозначаем единичную матрицу порядка n. Также в [9, стр. 138] показано, что k-й централ группы $P_n(\mathbb{Z}_{p^m})$ совпадает с пересечением

$$\gamma_k(P_n(\mathbb{Z}_{p^m})) = (E + M_n(F_n^{(k)})) \cap SL_n(\mathbb{Z}_{p^m}).$$

Оказывается, что включения для произведений матриц из множеств $M_n(F_n^{(k)})$ тоже описываются функциями $F_n^{(k)}$. Более точно, справедлива

Лемма 2. *Пусть $k_1, \dots, k_s$ — произвольные натуральные числа и $A_i \in M_n(F_n^{(k_i)})$, $i = 1, \dots, s$. Тогда*

$$A_1 \cdot A_2 \cdot \dots \cdot A_s \in M_n(F_n^{(k_1+\dots+k_s)}).$$

Доказательство. Лемму достаточно доказать для случая $s = 2$. Пусть $A_1 = ||a_{ij}||$, $A_2 = ||a'_{ij}||$ и $C = A_1A_2 = ||c_{ij}||$. Функции $F_n^{(k)}$ для любых натуральных чисел k_1, k_2 и фиксированных i, j, l больших нуля и не превосходящих n, удовлетворяют неравенству

$$F_n^{(k_1)}(i,l) + F_n^{(k_2)}(l,j) \geqslant F_n^{(k_1+k_2)}(i,j).$$

Отсюда следует, что

$$c_{ij} = \sum_{l=1}^{n} a_{il}a'_{lj} \in \sum_{l=1}^{n} J^{F_n^{(k_1)}(i,l)} J^{F_n^{(k_2)}(l,j)} =$$

$$= \sum_{l=1}^{n} J^{F_n^{(k_1)}(i,l)+F_n^{(k_2)}(l,j)} \subseteq J^{F_n^{(k_1+k_2)}(i,j)}$$

и, значит, $A_1A_2 \in M_n(F_n^{(k_1+k_2)})$. □

Диагональю с номером k, $1-n \leqslant k \leqslant n-1$, квадратной матрицы D порядка n назовём множество таких элементов d_{ij} этой матрицы, что $i-j=k$.

Лемма 3. *Пусть* $B \in M_n(F_n^{(1)})$, $D \in M_n(J^{m-2})$, $m \geqslant 2$, s — *целое число,* $0 \leqslant s < n-1$. *Если все элементы диагоналей* $1-n, \ldots, s$ *матрицы* D *лежат в* J^{m-1}, *то у матриц* BD *и* DB *в идеале* J^{m-1} *лежат все элементы диагоналей* $1-n, \ldots, s+1$.

Доказательство. Пусть натуральные числа i, j удовлетворяют неравенствам: $1 \leqslant i, j \leqslant n$ и $i-j \leqslant s+1$. Запишем элемент c_{ij} матрицы BD в виде следующих двух сумм

$$c_{ij} = \sum_{u=1}^{i-1} b_{iu}d_{uj} + \sum_{u=i}^{n} b_{iu}d_{uj}.$$

Элементы d_{uj} первой суммы лежат в J^{m-1}, поскольку для них $u-j \leqslant i-j-1 \leqslant s$. Во второй сумме элементы b_{iu} лежат в J, так как их индексы удовлетворяют условию $i-u \leqslant 0$, а элементы d_{uj} лежат J^{m-2}. Значит, $c_{ij} \in J^{m-1}$. Доказательство включения в J^{m-1} элемента c'_{ij} произведения DB устанавливается как выше с использованием равенства

$$c'_{ij} = \sum_{u=1}^{j} d_{iu}b_{uj} + \sum_{u=j+1}^{n} d_{iu}b_{uj}.$$

□

При доказательстве справедливости необходимых условий регулярности группы $P_n(\mathbb{Z}_{p^m})$ существенным образом используется следующая основная

Теорема 1. *Пусть* $A, B \in P_n(\mathbb{Z}_{p^m})$, $m \geqslant 2$, $p \geqslant 5$ *и* $2 \leqslant n \leqslant (p-1)/2$. *Равенство* $A^p = B^p$ *имеет место тогда и только тогда, когда* $A = BC$ *для некоторой матрицы* $C \in K_n(\mathbb{Z}_{p^m}, J^{m-1})$.

Доказательство. Пусть $A = E + A'$, $B = E + B'$, где $A', B' \in M_n(F_n^{(1)})$, и $A^p = B^p$. Покажем, что $D = A' - B' \in M_n(F_n^{(mn-n+1)})$.

Включение $D \in M_n(F_n^{(1)})$ очевидно. Пусть включение $D \in M_n(F_n^{(l)})$, $1 \leqslant l < mn-n+1$, уже доказано. Из равенства $A^p = B^p$ следует, что

$$\sum_{i=1}^{p} \binom{i}{p} ((B'+D)^i - B'^i) = O,$$

здесь и далее O — нулевая матрица порядка n. Матрицы $W_i = (B'+D)^i - B'^i$ при $i \geqslant 2$ являются однородными многочленами от B' и D

степени i, причем, матрицу D содержит каждое слагаемое. Значит, по лемме 2

$$W_i \in M_n(F_n^{(l+i-1)}) \subseteq M_n(F_n^{(l+1)}), \qquad i \geqslant 2.$$

В частности, из неравенства $n \leqslant (p-1)/2$ следует, что

$$W_p \in M_n(F_n^{(l+p-1)}) \subseteq M_n(F_n^{(l+n+1)}).$$

Далее, биномиальные коэффициенты $\binom{i}{p}$, когда $1 \leqslant i \leqslant p-1$, кратны p, поэтому

$$\binom{i}{p} W_i \in M_n(F_n^{(l+n+1)}), \qquad 2 \leqslant i \leqslant p-1.$$

Отсюда,

$$pD = -\sum_{i=2}^{p-1} \binom{i}{p} W_i - W_p \in M_n(F_n^{(l+n+1)})$$

и, следовательно, $D \in M_n(F_n^{(l+1)})$. Таким образом, включение $D \in M_n(F_n^{(mn-n+1)})$ доказано.

Индукцией по номеру диагонали s, $1 \leqslant s \leqslant n-1$, матрицы D с помощью леммы 3 и аналогичных рассуждений устанавливаем включение $A' - B' = D \in M_n(J^{m-1})$. Положив сейчас $C' = (E+B')^{-1}D$ и $C = E + C'$, будем иметь

$$BC = (E+B')(E+C') = (E+B')(E+(E+B')^{-1}D) =$$

$$= E + B' + D = E + A' = A.$$

и, очевидно, $C' \in M_n(J^{m-1})$.

Обратно, пусть $E + A' = (E+B')(E+C')$ и $C' \in M_n(J^{m-1})$. Из кратности p биномиальных коэффициентов $\binom{i}{p}$, когда $1 \leqslant i \leqslant p-1$, и равенства $pC' = O$ следует

$$(E + B' + C' + B'C')^p = E + \sum_{i=1}^{p} \binom{i}{p} (B' + C' + B'C')^i =$$

$$= E + (B' + C' + B'C')^p + \sum_{i=1}^{p-1} \binom{i}{p} B'^i.$$

Любое произведение, содержащее не менне двух матриц из идеала $M_n(J^{m-1})$, равно нулевой матрице, поэтому

$$(B' + C' + B'C')^p = B'^p + B'^{p-1}C' + B'^{p-2}C'B + \ldots + C'B'^{p-1}.$$

В произведении $B'^k C' B'^l$, когда $k + l = p - 1$, обязательно $k \geqslant (p - 1)/2 \geqslant n$ или $l \geqslant n$. Значит, по лемме 2 $B'^k \in M_n(F_n^{(n)}) \subseteq M_n(J)$ или $B'^l \in M_n(J)$, откуда

$$B'^k C' B'^l \in M_n(J) \cdot M_n(J^{m-1}) = \{O\}.$$

Поэтому $(B' + C' + B'C')^p = B'^p$ и, следовательно,

$$A^p = (E + B' + C' + B'C')^p = E + \sum_{i=1}^{p} \binom{i}{p} B'^i = (E + B')^p = B^p.$$

Теорема доказана. □

3. Необходимые условия регулярности

Всюду далее предполагаем, что натуральные числа m, n и простое число p удовлетворяют неравенствам: $m \geqslant 2$, $p \geqslant 5$ и $2 \leqslant n \leqslant (p-1)/2$.

Следствие 1. *Пусть $A, B \in P_n(\mathbb{Z}_{p^m})$, $1 \leqslant i \leqslant m - 1$. Равенство $A^{p^i} = B^{p^i}$ имеет место тогда и только тогда, когда $A = BC$ для некоторой матрицы $C \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$.*

Доказательство. Будем вести индукцией по i. Случай $i = 1$ разобран в теореме 1. Пусть $i > 1$ и $A^{p^i} = B^{p^i}$. Тогда $(A^p)^{p^{i-1}} = (B^p)^{p^{i-1}}$ и по предположению индукции существует матрица $D \in K_n(\mathbb{Z}_{p^m}, J^{m-i+1})$ такая, что $A^p = B^p D$. Рассмотрим канонический гомоморфизм ρ кольца $\mathbb{Z}_{p^m}$ на кольцо $\mathbb{Z}_{p^{m-i+1}}$ (взятие вычета по модулю p^{m-i+1}). Он продолжается до гомоморфизма $\bar{\rho}$ группы $P_n(\mathbb{Z}_{p^m})$ на группу $P_n(\mathbb{Z}_{p^{m-i+1}})$. Ядром $\bar{\rho}$ служит конгруэнц-подгруппа $K_n(\mathbb{Z}_{p^m}, J^{m-i+1})$. В группе $P_n(\mathbb{Z}_{p^{m-i+1}})$ имеет место равенство

$$(\bar{\rho}(A))^p = \bar{\rho}(A^p) = \bar{\rho}(B^p D) = \bar{\rho}(B^p)\bar{\rho}(D) = \bar{\rho}(B^p) = (\bar{\rho}(B))^p.$$

По теореме 1 $\bar{\rho}(A) = \bar{\rho}(B)\bar{C}$ для некоторой матрицы $\bar{C}$ из конгруэнц-подгруппы $K_n(\mathbb{Z}_{p^{m-i+1}}, J^{m-i})$ группы $P_n(\mathbb{Z}_{p^{m-i+1}})$. Перейдя к прообразам, получим требуемое равенство.

Обратно, пусть $A = BC$ и $C \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$. Тогда $\bar{\rho}(A) = \bar{\rho}(B)\bar{\rho}(C)$, где $\bar{\rho}(C)$ принадлежит конгруэнц-подгруппе $K_n(\mathbb{Z}_{p^{m-i+1}}, J^{m-i})$ группы $P_n(\mathbb{Z}_{p^{m-i+1}})$. Используя теорему 1, получаем

$$\bar{\rho}(A^p) = (\bar{\rho}(A))^p = (\bar{\rho}(B))^p = \bar{\rho}(B^p)$$

или, переходя к прообразам, $A^p = B^p D$, где $D \in K_n(\mathbb{Z}_{p^m}, J^{m-i+1})$. По индукции $A^{p^i} = (A^p)^{p^{i-1}} = (B^p D)^{p^{i-1}} = B^{p^i}$. □

Следствие 2. *Множества* $\Omega_i(P_n(\mathbb{Z}_{p^m}))$ *и* $\mho_i(P_n(\mathbb{Z}_{p^m}))$, $i = 1, \dots m-1$, *образуют характеристические подгруппы в* $P_n(\mathbb{Z}_{p^m})$.

Доказательство. Множество $\Omega_i(P_n(\mathbb{Z}_{p^m}))$ состоит из эдементов, порядки которых не превышают p^i, а множество $\mho_i(P_n(\mathbb{Z}_{p^m}))$ — из p^i-х степеней всех элементов группы $P_n(\mathbb{Z}_{p^m})$. Характеристичность обоих множеств вытекает из инвариантности порядка и степени элемента относительно автоморфизма.

Покажем, что указанные множества являются подгруппами. Действительно, полагая в следствии 1 $B = E$, видим, что $A^{p^i} = E$ тогда и только тогда, когда A лежит в конгруэнц-подгруппе $K_n(\mathbb{Z}_{p^m}, J^{m-i})$. Значит, $\Omega_i(P_n(\mathbb{Z}_{p^m})) = K_n(\mathbb{Z}_{p^m}, J^{m-i})$. Далее, используя формулу бинома и лемму 2, нетрудно убедится в том, что A^{p^i} лежит в подгруппе $H_i = E + M_n(F_n^{(in+1)})$ для любой матрицы $A \in P_n(\mathbb{Z}_{p^m})$. Порядок подгруппы H_i равен

$$p^{(m-i)\frac{(n-1)n}{2}+(m-i-1)\frac{n(n+1)}{2}}$$

и совпадает с порядком $\mho_i(P_n(\mathbb{Z}_{p^m}))$, который ввиду следствия 1 равен

$$|P_n(\mathbb{Z}_{p^m})|/|K_n(\mathbb{Z}_{p^m}, J^{m-i})| = p^{m\frac{(n-1)n}{2}+(m-1)\frac{n(n+1)}{2}}/p^{in^2}.$$

Значит, множество $\mho_i(P_n(\mathbb{Z}_{p^m}))$ совпадает с подгруппой H_i. □

Следствие 3. *Пусть* $A, B \in P_n(\mathbb{Z}_{p^m})$, $i \geqslant 0$ – *целое. Равенство* $A^{p^i} = B^{p^i}$ *имеет место тогда и только тогда, когда* $(A^{-1}B)^{p^i} = E$.

Доказательство. Пусть $A^{p^i} = B^{p^i}$. Если $i \geqslant m$, то $E = A^{p^i} = B^{p^i} = (AB^{-1})^{p^i}$ и доказывать нечего. При $i < m$ ввиду следствия 1 имеем $A = BC$, где $C \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$. Отсюда, $(A^{-1}B)^{p^i} = (C^{-1}B^{-1}B)^{p^i} = (C^{-1})^{p^i} = E$. Обратное утверждение очевидно. □

Следствие 4. *Пусть* $A, B \in P_n(\mathbb{Z}_{p^m})$, $i \geqslant 0$ – *целое. Равенство* $[A^{p^i}, B] = E$ *(или* $[A, B^{p^i}] = E$*) имеет место тогда и только тогда, когда* $[A, B]^{p^i} = E$.

Доказательство. В самом деле, если $[A^{p^i}, B] = E$, то

$$E = [A^{p^i}, B] = (A^{-1})^{p^i} B^{-1} A^{p^i} B = (A^{-1})^{p^i} (B^{-1}AB)^{p^i},$$

или $(B^{-1}AB)^{p^i} = A^{p^i}$. По следствию 1 $B^{-1}AB = AC$ для некоторой матрицы $C \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$, откуда

$$[A, B]^{p^i} = (A^{-1}B^{-1}AB)^{p^i} = (A^{-1}AC)^{p^i} = E.$$

Обратно, из равенства $[A,B]^{p^i} = E$ следует включение $A^{-1}B^{-1}AB \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$, то есть $B^{-1}AB = AC$ для некоторой матрицы $C \in K_n(\mathbb{Z}_{p^m}, J^{m-i})$. По следствию 1 $(AC)^{p^i} = A^{p^i}$, поэтому

$$[A^{p^i}, B] = (A^{-1})^{p^i}(AC)^{p^i} = (A^{-1})^{p^i}A^{p^i} = E.$$

□

Список литературы

1. Hall P. A contribution to the theory of groups of prime-power order / P. Hall // Proc. London Math. Soc. – 1934. – Vol. 36, N 1. – P. 29–95.
2. Холл М. Теория групп / М. Холл. – М. : Иностр. лит., 1962. – 468 с.
3. Коуровская тетрадь. Нерешённые вопросы теории групп / ред. В. Д. Мазуров, Е. И. Хухро. – 16-е изд. – Новосибирск : ИМ СО РАН, 2006. – 180 с.
4. Мерзляков Ю.И. Центральные ряды и ряды коммутантов матричных групп / Ю. И. Мерзляков // Алгебра и логика. – 1964. – Т. 3, № 4. – С. 49–58.
5. Ягжев А.В. О регулярности силовских p-подгрупп полных линейных групп над кольцами вычетов / А. В. Ягжев // Мат. заметки. – 1994. – Т. 56, № 6. – С. 106–116.
6. Колесников С.Г. О регулярности силовских p-подгрупп групп $GL_n(\mathbb{Z}_{p^m})$ / С. Г. Колесников // Исследования по математическому анализу и алгебре. – Томск : ТГУ, 2001. – Т.3. – С. 117–124.
7. Колесников С. Г. О регулярных силовских p-подгруппах групп Шевалле над кольцом $\mathbb{Z}_{p^m}$ / С. Г. Колесников // Сиб. мат. журн. – 2006. – Т. 46, № 6. – С. 1289–1295.
8. Колесников С. Г. О регулярности силовских p-подгрупп симплектических и ортогональных групп над кольцом $\mathbb{Z}_{p^m}$ / С. Г. Колесников, Н. В. Мальцев // Журн. Сиб. федер. ун-та. Математика и физика. – 2011. – Т. 4, № 4. – С. 489–497.
9. Каргаполов М. И. Основы теории групп / М. И. Каргаполов, Ю. И. Мерзляков. – М. : Наука, 1972. – 240 с.

S. G. Kolesnikov

On necessary conditions of regularity of Sylow p-subgroups of the group $GL_n(\mathbb{Z}_{p^m})$

Abstract. In connect to B. Vehrfritz's problem 8.3 from Kourovka notebook we prooved that Sylow p-subgroup of group $GL_n(\mathbb{Z}_{p^m})$ when $n \leqslant (p-1)/2$ satisfies well-known necessary coditions of regularity.

Keywords: regular p-group; linear group; Sylow subgroup.

Колесников Сергей Геннадьевич, доктор физико-математических наук, профессор, Институт математики и фундаментальной информатики, Сибирский федеральный университет, 660041, Красноярск, пр. Свободный, 79, тел.: (3912)206-20-76 (sklsnkv@mail.ru)

Kolesnikov Sergei, Siberian Federal University, 79, Svobodny av., Krasnoyarsk, 660041, professor, Phone: (3912)206-20-76 (sklsnkv@mail.ru)