Сибирский математический журнал
Ноябрь—декабрь, 2006. Том 47, № 6

УДК 519.54

О РЕГУЛЯРНЫХ СИЛОВСКИХ p–ПОДГРУППАХ ГРУПП ШЕВАЛЛЕ НАД КОЛЬЦОМ $\mathbb{Z}_{p^m}$

С. Г. Колесников

Аннотация: Доказано, что силовская p-подгруппа общей линейной группы размерности n над кольцом вычетов по модулю p^m является регулярной при $n^2 < p$ и мощной тогда и только тогда, когда $n = 2$ и $m = 1$. Аналогичные результаты получены для силовских p-подгрупп групп Шевалле нормальных типов над тем же кольцом.

Ключевые слова: регулярная p-группа, мощная p-группа, силовская p-подгруппа.

Введение

Свойства конечной p-группы в значительной степени определяются соотношениями между коммутаторами и p-ми степенями ее элементов. Фиксируя в определении некоторые из таких соотношений, получаем различные классы p-групп. Классическим примером является класс регулярных p-групп, введенный Холлом. Согласно [1, теорема 12.4.2] регулярность конечной p-группы равносильна тому, что для любых двух ее элементов a и b найдется такой элемент c из коммутанта подгруппы, порожденной a и b, что $(ab)^p = a^p b^p c^p$. Более современный и интенсивно исследующийся класс групп, появившийся на этом пути, это класс мощных p-групп, введенный Манном. Напомним (см., например, [2, § 6.1], что p-группа называется *мощной*, если для любых двух ее элементов a и b коммутатор $[a, b]$ разложим при $p > 2$ в произведение p-х степеней элементов группы, а при $p = 2$ — четвертых степеней.

В 1982 г. Верфриц в «Коуровской тетради» поставил следующий вопрос [3, вопрос 8.3]: для каких целых положительных чисел m, n и простого числа p группа $P_n(\mathbb{Z}_{p^m})$ всех таких $(n\times n)$-матриц (a_{ij}) над целыми числами по модулю p^m, что $a_{ii} \equiv 1(\mathrm{mod}\ p)$ для всех i и $a_{ij} \equiv 0(\mathrm{mod}\ p)$ для всех $i < j$ ($i > j$ — в оригинале), является регулярной? Отметим, что, заменяя неравенство $i > j$ на $i < j$, получаем изоморфные группы, изоморфизм между ними устанавливает отображение, которое переводит произвольную обратимую матрицу A в $(A^{-1})^t$.

Как известно [4], группа $P_n(\mathbb{Z}_{p^m})$ является силовской p-подгруппой группы $GL_n(\mathbb{Z}_{p^m})$, а ее ступень нильпотентности равна $mn - 1$. Так как p-группа ступени нильпотентности, меньшей, чем p, является регулярной [1, с. 205], то $P_n(\mathbb{Z}_{p^m})$ регулярна, если $mn \le p$. При $m = 1$ в [5], а при $m = 2$ в [6] доказано, что группа $P_n(\mathbb{Z}_{p^m})$ является регулярной тогда и только тогда, тогда ее ступень нильпотентности меньше p. Можно было ожидать, и предыдущие результаты подтверждают это, что группа $P_n(\mathbb{Z}_{p^m})$ не является регулярной, если $mn > p$. Однако справедлива

Работа выполнена при финансовой поддержке гранта Президента РФ (код проекта МК–1133.2005.1) и Красноярского краевого фонда науки (код проекта 15G090).

Теорема 1. *Если $n^2 < p$, то группа $P_n(\mathbb{Z}_{p^m})$ регулярна при любом $m \geq 1$.*

Условия, при которых группа $P_n(\mathbb{Z}_{p^m})$ является мощной, выявляет

Теорема 2. *Группа $P_n(\mathbb{Z}_{p^m})$ является мощной тогда и только тогда, когда $n = 2$ и $m = 1$.*

В § 2 приводится аналог теорем 1 и 2 для силовских p-подгрупп групп Шевалле нормальных типов над кольцом $\mathbb{Z}_{p^m}$.

§ 1. Доказательства теорем 1 и 2

Определим последовательность функций f_n, $n = 1, 2, \dots$, от целочисленных аргументов i, j, k, полагая $f_n(i, j, k) = -[(i - j - k)/n]$, здесь $[x]$ — целая часть числа x. Для всякого целого неотрицательного числа l через J^l будем обозначать идеал кольца $\mathbb{Z}_{p^m}$, порожденный элементом p^l, а множество квадратных матриц порядка n, у которых элемент, стоящий на пересечении i-й строки и j-го столбца, лежит в идеале $J^{f_n(i,j,k)}$, обозначим через $M_n(k)$. Нетрудно видеть, что имеют место следующие включения $M_n(1) \supseteq M_n(2) \supseteq \dots$, а согласно [4] $P_n(\mathbb{Z}_{p^m}) = E_n + M_n(1)$, здесь и далее через E_n обозначаем единичную матрицу порядка n. Также в [4] показано, что k-й централ группы $P_n(\mathbb{Z}_{p^m})$ совпадает с пересечением

$$\gamma_k(P_n(\mathbb{Z}_{p^m})) = (E_n + M_n(k)) \cap SL_n(\mathbb{Z}_{p^m}). \tag{1}$$

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

$$A_1 \cdot A_2 \cdot \ldots \cdot A_s \in M_n(k_1 + \dots + k_s).$$

Доказательство. Лемму, очевидно, достаточно доказать для случая $s = 2$. Пусть $A_1 = (a_{ij})$, $A_2 = (a'_{ij})$ и $C = A_1 A_2 = (c_{ij})$. Функция f_n для любых натуральных чисел k_1, k_2 и фиксированных i, j, l, больших нуля и не превосходящих n, удовлетворяет неравенству

$$f_n(i, l, k_1) + f_n(l, j, k_2) \geq f_n(i, j, k_1 + k_2).$$

Отсюда следует, что

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

и, значит, $A_1 A_2 \in M_n(k_1 + k_2)$. Лемма доказана.

Лемма 2. *Пусть $a = E_n + A$ и $A \in M_n(k)$. Тогда $a^p \in E_n + M_n(k + n) + M_n(pk)$.*

Доказательство. Имеем

$$a^p = (E_n + A)^p = E_n + C_p^1 A + \dots + C_p^{p-1} A^{p-1} + A^p.$$

Из леммы 1 следует, что $A^p \in M_n(kp)$. Пусть целое число l удовлетворяет неравенствам $1 \leq l \leq p - 1$. Тогда биномиальные коэффициенты C_p^l кратны p и, поскольку $f_n(i, j, k) + 1 = f_n(i, j, k + n)$, имеет место включение $C_p^l A \in M_n(k + n)$. Снова применяя лемму 1, получаем $C_p^l A^l \in M_n(lk + n)$. Таким образом,

$$a^p \in E_n + M_n(k + n) + \dots + M_n((p - 1)k + n) + M_n(pk) \subseteq E_n + M_n(k + n) + M_n(pk).$$

Лемма доказана.

Лемма 3. *Для всякого идеала J^l, $l \geq 1$, кольца $\mathbb{Z}_{p^m}$ множество $1 + J^l$ является группой относительно умножения, причем циклической, если $p > 2$. Кроме того, $(1 + J^l)^p \subset 1 + J^{l+1}$.*

Доказательство. Пусть $1 + x \in 1 + J^l$. По формуле бинома

$$(1+x)^p = 1 + C_p^1 x + \dots + C_p^{p-1} x^{p-1} + x^p.$$

Биномиальные коэффициенты $C_p^1, \dots, C_p^{p-1}$ кратны p и $x^p \in J^{lp} \subseteq J^{l+1}$, поскольку $p \geq 2$. Поэтому $(1+x)^p \in 1 + J^{l+1}$.

Докажем первое утверждение леммы. Множество $1 + J^l$, очевидно, замкнуто относительно умножения, содержит единичный элемент и ввиду равенства

$$(1 + p^l t)^{-1} = 1 + (-p^l t) + (-p^l t)^2 + \dots + (-p^l t)^m$$

замкнуто относительно взятия обратного элемента, а значит, является группой.

Покажем, что при $p > 2$ группа $1 + J$ порождается элементом $1 + p$. Пусть целое положительное число i удовлетворяет неравенству $i < m - 1$. Используя формулу бинома, получаем

$$(1+p)^{p^i} = 1 + p^{i+1} + \sum_{j=2}^{p^i - 1} C_{p^i}^j p^j + p^{p^i}.$$

Так как $p > 2$, то $p^i \geq i + 2$ и поэтому $p^{p^i} \in J^{i+2}$. Далее, пусть j удовлетворяет неравенствам $2 \leq j \leq p^i - 1$, и пусть $j = p^s z$, где НОД$(p, z) = 1$. Тогда биномиальный коэффициент $C_{p^i}^j$ делится на p^{i-s}. Снова ввиду неравенства $p > 2$ имеем $j \geq p^s \geq s + 2$, а значит, произведение $C_{p^i}^j p^j$ тоже лежит в J^{i+2}. Таким образом, $(1+p)^{p^i} \equiv 1 + p^{l+1} (\mathrm{mod}\ J^{i+2})$, и поэтому порядок элемента $1 + p$ не меньше, чем p^{m-1}. С другой стороны, $|1 + J| = |J| = p^{m-1}$. Значит, группа $1 + J$ циклическая.

Цикличность групп $1 + J^l$ вытекает из включения $1 + J^l \subseteq 1 + J$. Лемма доказана.

Для конечной группы G через G^p будем обозначать подгруппу, порожденную p-ми степенями всех элементов из G. Следующее утверждение можно найти в [2, лемма 1.2.11].

Лемма 4. *Конечная p-группа G является регулярной, если $|G : G^p| < p^p$.*

Докажем теорему 1. По лемме 2

$$[P_n(\mathbb{Z}_{p^m})]^p = [E_n + M_n(1)]^p \subseteq E_n + M_n(n+1),$$

поскольку $p > n^2 > n$. С другой стороны, группа $E_n + M_n(n+1)$ порождается трансвекциями из множеств $E_n + J e_{ij}$ и $E_n + J^2 e_{ji}$ $(i > j)$ и диагональными матрицами из $E_n + J^2 e_{ii}$ (здесь и далее через e_{ij} обозначаем матрицу, у которой на месте (i, j) стоит единица и нули на остальных местах). Ввиду того, что идеалы J и J^2 порождаются элементами p и p^2 соответственно, а группа $1 + J^2$ в силу условия $p > n^2 > 2$ и леммы 3 — элементом $(1+p)^p$, матрицы $E_n + pe_{ij} = (E_n + e_{ij})^p$, $E_n + p^2 e_{ji} = (E_n + pe_{ji})^p$ $(i > j)$ и $(E_n + pe_{ii})^p$ порождают группу $E_n + M_n(n+1)$ и, очевидно, содержатся в $[P_n(\mathbb{Z}_{p^m})]^p$. Следовательно, имеет место равенство $E_n + M_n(n+1) = [P_n(\mathbb{Z}_{p^m})]^p$. Так как $f_n(i, j, n+1) = f_n(i, j, 1) + 1$ для любых i, j, индекс подгруппы $[P_n(\mathbb{Z}_{p^m})]^p$ в группе $P_n(\mathbb{Z}_{p^m})$ равен p^{n^2}. Значит, по лемме 4 группа $P_n(\mathbb{Z}_{p^m})$ регулярна. Теорема 1 доказана.

Докажем теорему 2. По лемме 2 $[P_n(\mathbb{Z}_{p^m})]^p \subseteq E_n + M_n(p) + M_n(n+1)$ и $[P_n(\mathbb{Z}_{p^m})]^4 \subseteq E_n + M_n(4)$, в то время как по формуле (1) коммутант группы $P_n(\mathbb{Z}_{p^m})$ при любом простом p совпадает с пересечением $(E_n + M_n(2)) \cap SL_n(\mathbb{Z}_{p^m})$. Если $n \geq 3$, то матрица $E_n + e_{31}$ лежит в коммутанте и не содержится в $E_n + M_n(p) + M_n(n+1)$ при $p \geq 3$ и в $E_n + M_n(4)$ при $p = 2$. Если же $m \geq n = 2$, то коммутатор

$$\left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1-p & -p^2 \\ p & 1+p+p^2 \end{pmatrix}$$

содержится в коммутанте и не лежит в множествах $E_n + M_n(p) + M_n(n+1)$ и $E_n + M_n(4)$ при $p \geq 3$ и $p = 2$ соответственно. Следовательно, группа $P_n(\mathbb{Z}_{p^m})$ не может быть мощной, когда $n \geq 3$ или $m \geq 2$. В то же время группа $P_2(\mathbb{Z}_p)$ циклическая простого порядка и поэтому содержится в классе мощных p-групп. Теорема 2 доказана.

§ 2. Регулярные силовские p-подгруппы групп Шевалле

Обозначим через Φ приведенную неразложимую систему корней простой комплексной алгебры Ли классического или исключительного типа, а через $\Pi(\Phi)$ — ее базу. Группу Шевалле, ассоциированную с системой корней Φ, решеткой корней $L(\Phi)$ и кольцом $\mathbb{Z}_{p^m}$, обозначим через $G\Phi(\mathbb{Z}_{p^m})$ (определение группы Шевалле над произвольным коммутативным кольцом и перенесение основных понятий можно найти в [7]). Справедлива

Теорема 3. *Силовская p-подгруппа группы $G\Phi(\mathbb{Z}_{p^m})$ является регулярной при $|\Phi| + |\Pi(\Phi)| < p$ и является мощной тогда и только тогда, когда Φ типа A_1 и $m = 1$.*

Доказательство теоремы 3 опирается на ряд вспомогательных утверждений.

Лемма 5. *Пусть p — простое число. Произведение $(a_1 \dots a_k)^p$ элементов группы G представимо в виде*

$$\big(a_1 \dots a_k\big)^p = a_1^p \dots a_k^p c_1^{pn_1} \dots c_j^{pn_j} c_{j+1}^{n_{j+1}} \dots c_{j+l}^{n_{j+l}}, \tag{2}$$

где степени $n_1, \dots, n_{j+l}$ являются целыми положительными числами, а $c_1, \dots, c_{j+l}$ — коммутаторы от элементов $a_1, \dots, a_k$, причем вес коммутаторов $c_1, \dots, c_j$ не превосходит $p - 1$, а вес коммутаторов $c_{j+1}, \dots, c_{j+l}$ не меньше, чем p.

Доказательство следует из [1, теорема 12.3.1].

В группе Шевалле $G\Phi(\mathbb{Z}_{p^m})$, как обычно (см., например, [7; 8, § 4.3, 7.1], выделяем корневые $x_r(t)$, $r \in \Phi$, $t \in \mathbb{Z}_{p^m}$, и диагональные $h_r(u)$, $u \in \mathbb{Z}_{p^m}^{\#}$, элементы.

Обозначим через $U\Phi(J^i)$ $(i \geq 0)$ унипотентную подгруппу, порожденную элементами $x_r(p^i)$, r пробегает систему положительных корней Φ^+, и для всякого натурального числа n определим подгруппу $U_n \subseteq U\Phi(\mathbb{Z}_{p^m})$, положив $U_n = 1$, если $n \geq h$, и $U_n = \langle x_r(1) \mid ht(r) \geq n\rangle$, если $n < h$ (здесь и далее через ht обозначаем функцию высоты корня, а через h — число Кокстера системы корней Φ). Справедлива

Лемма 6. *Имеет место включение* $[U\Phi(\mathbb{Z}_{p^m})]^p \subseteq U\Phi(J) \cdot U_p$, *а если* $p \geq h$, *то* $[U\Phi(\mathbb{Z}_{p^m})]^p = U\Phi(J)$.

Доказательство. Согласно коммутаторной формуле Шевалле [8, § 5.2] если r и s — положительные корни, то коммутатор $[x_s(u), x_r(t)]$ равен единице, когда $r + s \notin \Phi$, а в случае $r + s \in \Phi$ — раскладывается в произведение $\prod x_{ir+js}(c_{ijrs}(-t)^i u^j)$, которое берется по всем целым $i, j > 0$ таким, что $ir + js \in \Phi$. Отсюда следует, что группа $U\Phi(J)$ нормальна в группе $U\Phi(\mathbb{Z}_{p^m})$. Кроме того, из аддитивности функции ht вытекает соотношение

$$[U_n, U_l] \subseteq U_{n+l}. \tag{3}$$

Индукцией по i докажем включение $U_i^p \subseteq U\Phi(J) \cdot U_p$, отсюда при $i = 1$ получим первое утверждение леммы. Включение очевидно, когда $i \geq h$. Пусть уже доказано, что $U_i^p \subseteq U\Phi(J) \cdot U_p$ для всех i, больших некоторого целого $n \geq 1$, и пусть $x_{r_1}(t_1) \dots x_{r_k}(t_k) \in U_n$. По формуле (2)

$$(x_{r_1}(t_1) \dots x_{r_k}(t_k))^p = x_{r_1}(t_1)^p \dots x_{r_k}(t_k)^p c_1^{pn_1} \dots c_j^{pn_j} c_{j+1}^{n_{j+1}} \dots c_{j+l}^{n_{j+l}}.$$

Элементы $x_{r_i}(t_i)^p = x_r(pt_i)$ лежат в $U\Phi(J)$, а коммутаторы $c_{j+1}, \dots, c_{j+l}$ имеют вес $\geq p$ и в силу (3) содержатся в U_p. Коммутаторы $c_1, \dots, c_j$ также ввиду (3) содержатся в U_{2n}, а по предположению индукции $U_{2n}^p \subseteq U\Phi(J) \cdot U_p$. Таким образом, $[U\Phi(\mathbb{Z}_{p^m})]^p \subseteq U\Phi(J) \cdot U_p$.

Если $p \geq h$, то $U_p = 1$, а потому $[U\Phi(\mathbb{Z}_{p^m})]^p \subseteq U\Phi(J)$. С другой стороны, группа $U\Phi(J)$ порождается элементами $x_r(p) = x_r(1)^p$, где r пробегает Φ^+, которые лежат в $[U\Phi(\mathbb{Z}_{p^m})]^p$. Поэтому при $p \geq h$ имеет место равенство $[U\Phi(\mathbb{Z}_{p^m})]^p = U\Phi(J)$. Лемма доказана.

Унипотентную подгруппу, порожденную элементами $x_r(p^i)$, r пробегает множество отрицательных корней Φ^-, обозначим через $U\Phi^-(J^i)$ $(i \geq 0)$, а диагональную подгруппу, порожденную элементами $h_r(1 + u)$, r пробегает $\Pi(\Phi)$, u пробегает идеал J^i, — через $H(1 + J^i)$ $(i \geq 1)$. Ядро гомоморфизма групп $G\Phi(\mathbb{Z}_{p^m}) \to G\Phi(\mathbb{Z}_{p^i})$, который индуцирован кольцевым гомоморфизмом $\mathbb{Z}_{p^m} \to \mathbb{Z}_{p^i}$ (взятие вычета по модулю p^i), обозначим через $\Phi(J^i)$. Согласно [9, теорема 2] разложение

$$\Phi(J^i) = U\Phi(J^i) \cdot H(1 + J^i) \cdot U\Phi^-(J^i) \tag{4}$$

является каноническим, а соотношение

$$[\Phi(J^i), \Phi(J^j)] \subseteq \Phi(J^{i+j}) \tag{5}$$

верно для любых целых $i, j > 0$. Справедлива

Лемма 7. *Имеет место включение* $[\Phi(J^i)]^p \subseteq \Phi(J^{i+1})$.

Доказательство. Пусть $g \in \Phi(J^i)$. Согласно (4) элемент g разлагается в произведение корневых $x_s(t_s)$ и диагональных $h_r(1 + u_r)$ элементов. Возводя g в степень p и применяя формулу (2), видим, что g^p является произведением p-х степеней элементов $x_s(t_s)$ и $h_r(1 + u_r)$ и коммутаторов от них. Так как $x_s(t_s)^p = x_s(pt_s)$ и $h_r(1 + u_r)^p = h_r((1 + u_r)^p)$, а по лемме 3 $(1 + J^i)^p = 1 + J^{i+1}$, то элементы $x_s(u_s)^p$ и $h_r(1 + u_r)^p$ содержатся в $\Phi(J^{i+1})$. Коммутаторы от $x_s(u_s)$ и $h_r(1 + u_r)$ согласно (5) лежат в $\Phi(J^{2i})$. Значит, $g^p \in \Phi(J^{i+1})$. Лемма доказана.

Далее, с учетом [9] группа

$$S\Phi(\mathbb{Z}_{p^m}) = U\Phi(\mathbb{Z}_{p^m}) \cdot H(1 + J) \cdot U\Phi^-(J) \tag{6}$$

является силовской p-подгруппой группы $G\Phi(\mathbb{Z}_{p^m})$, а разложение (6) — ее каноническим разложением. Справедлива

Лемма 8. *Имеет место включение* $[S\Phi(\mathbb{Z}_{p^m})]^p \subseteq \Phi(J)\cdot U_p$, *а если* $p > h$, *то* $[S\Phi(\mathbb{Z}_{p^m})]^p = U\Phi(J)\cdot\Phi(J^2)$.

Доказательство. Из (6) и (4) получаем следующую факторизацию:

$$S\Phi(\mathbb{Z}_{p^m}) = U\Phi(\mathbb{Z}_{p^m})\cdot\Phi(J). \tag{7}$$

Пусть g — произвольный элемент из $S\Phi(\mathbb{Z}_{p^m})$. Ввиду (7) $g = ab$ для некоторых элементов $a \in U\Phi(\mathbb{Z}_{p^m})$ и $b \in \Phi(J)$. По формуле (2) $g^p = a^p b^p c$, где элемент c лежит в коммутанте подгруппы, порожденной a и b. По лемме 6 $a^p \in U\Phi(J)\cdot U_p$. Так как подгруппа $\Phi(J)$ нормальна в $S\Phi(\mathbb{Z}_{p^m})$, то $c \in \Phi(J)$, а по лемме 7 $b^p \in \Phi(J^2)$. Из доказанных включений вытекает первое утверждение леммы.

Пусть теперь $p > h$. Тогда по лемме 6 $a^p \in U\Phi(J)$, а по формуле (2) элемент c разложим в произведение коммутаторов

$$c_1^{pn_1}\dots c_j^{pn_j}c_{j+1}^{n_{j+1}}\dots c_{j+l}^{n_{j+l}},$$

зависящих от a и b, причем вес коммутаторов $c_{j+1},\dots,c_{j+l}$ не меньше, чем p. По доказанному выше коммутаторы $c_1,\dots,c_j$ лежат в $\Phi(J)$ и, следовательно, по лемме 7 $c_1^p,\dots,c_j^p \in \Phi(J^2)$. Коммутаторы $c_{j+1},\dots,c_{j+l}$ вследствие условия $p > h$ имеют вес, не меньший, чем $h+1$, и поэтому содержатся в $(h+1)$-м централе группы $S\Phi(\mathbb{Z}_{p^m})$, который согласно [9, следствие 1] имеет вид $U\Phi(J)\cdot\Phi(J^2)$. Таким образом, $g^p \in U\Phi(J)\cdot\Phi(J^2)$.

Докажем обратное включение. Так как идеалы J и J^2 порождаются элементами p и p^2 соответственно, а ввиду леммы 3 и условия $p > h \geq 2$ мультипликативная группа $1+J^2$ порождается элементом $(1+p)^p$, то подгруппа $U\Phi(J)\cdot\Phi(J^2)$ порождается корневыми элементами $x_r(p) = x_r(1)^p$ и $x_{-r}(p^2) = x_{-r}(p)^p$, где r пробегает Φ^+, и диагональными элементами $h_s((1+p)^p) = h_s(1+p)^p$, где s пробегает $\Pi(\Phi)$. Указанные элементы, очевидно, лежат в $[S\Phi(\mathbb{Z}_{p^m})]^p$. Поэтому $U\Phi(J)\cdot\Phi(J^2) \subseteq [S\Phi(\mathbb{Z}_{p^m})]^p$. Лемма доказана.

Докажем теорему 3. В силу разложения (6) порядок группы $S\Phi(\mathbb{Z}_{p^m})$ равен p^M, где $M = m(|\Phi| + |\Pi(\Phi)|) - |\Phi^+| - |\Pi(\Phi)|$.

Пусть $p > h$. Из леммы 8 и разложения (4) следует, что

$$[S\Phi(\mathbb{Z}_{p^m})]^p = U\Phi(J)\cdot\Phi(J^2) = U\Phi(J)\cdot H(1+J^2)\cdot U\Phi^-(J^2),$$

поэтому порядок группы $[S\Phi(\mathbb{Z}_{p^m})]^p$ равен p^{M_1}, где $M_1 = (m-1)(|\Phi|+|\Pi(\Phi)|) - |\Phi^+| - |\Pi(\Phi)|$. Отсюда заключаем, что индекс подгруппы $[S\Phi(\mathbb{Z}_{p^m})]^p$ в группе $S\Phi(\mathbb{Z}_{p^m})$ равен $p^M/p^{M_1} = p^{|\Phi|+|\Pi(\Phi)|}$. Следовательно, группа $S\Phi(\mathbb{Z}_{p^m})$ регулярна, когда $|\Phi| + |\Pi(\Phi)| < p$.

Докажем второе утверждение теоремы. Предположим, что ранг системы корней Φ не меньше двух, и пусть r, s — простые корни такие, что $r + s \in \Phi$. Тогда $c_{11,rs} = \pm 1$ и по коммутаторной формуле Шевалле $\left[x_s(1), x_r\left(c_{11,rs}^{-1}\right)\right] = x_{r+s}(1) \bmod (U_3)$, в то время как по лемме 8 $[S\Phi(\mathbb{Z}_{p^m})]^p \subseteq \Phi(J)\cdot U_p \subseteq \Phi(J)\cdot U_3$ при $p \geq 3$ и $[S\Phi(\mathbb{Z}_{2^m})]^4 \subseteq [\Phi(J)\cdot U_2]^2 \subseteq \Phi(J)\cdot U_4$. Поэтому группа $S\Phi(\mathbb{Z}_{p^m})$ не может быть мощной, когда ранг Φ больше 1.

Рассмотрим группу $SA_1(\mathbb{Z}_{p^m})$. Она циклическая и, следовательно, мощная, если $m = 1$. Пусть $m \geq 2$. Тогда коммутант группы $SA_1(\mathbb{Z}_{p^m})$ содержит коммутатор

$$[x_r(1), x_{-r}(p)] = x_r((1-p)^{-1}p)h_r(1-p)x_{-r}(-(1-p)^{-1}p^2).$$

Вместе с тем по лемме 8 при $p \geq 3$ имеет место включение $[SA_1(\mathbb{Z}_{p^m})]^p \subseteq UA_1(J)\cdot A_1(J^2)$, а если $p = 2$, то $[SA_1(\mathbb{Z}_{2^m})]^4 \subseteq [A_1(J)]^2 \subseteq A_1(J^2)$. Теорема 3 доказана.

ЛИТЕРАТУРА

1. *Холл М.* Теория групп. М.: Изд-во иностр. лит., 1962.
2. *Leedham-Green C. R., McKay S.* The structure of groups of prime power order. Oxford: Oxford Univ. Press, 2002.
3. *Коуровская* тетрадь. Новосибирск: НГУ, 2002.
4. *Мерзляков Ю. И.* Центральные ряды и ряды коммутантов матричных групп // Алгебра и логика. 1964. Т. 3, № 4. С. 49–53.
5. *Ягжев А. В.* О регулярности силовских подгрупп полных линейных групп над кольцами вычетов // Мат. заметки. 1994. Т. 56, № 6. С. 106–116.
6. *Колесников С. Г.* О регулярности силовских p-подгрупп групп $GL_n(Z_{p^m})$ // Исследования по математическому анализу и алгебре. 2001. Т. 3. С. 117–124.
7. *Stein M. R.* Generators, relations and covering of Chevalley groups over commutative ring // Am. J. Math. 1971. V. 93, N 4. P. 965–1004.
8. *Carter R.* Simple groups of Lie type. New York: Wiley and Sons, 1972.
9. *Левчук В. М.* Коммутаторное строение некоторых подгрупп групп Шевалле // Укр. мат. журн. 1992. Т. 44, № 6. С. 786–795.

Статья поступила 14 февраля 2006 г.

Колесников Сергей Геннадьевич
Красноярский гос. университет, пр. Свободный, 79, Красноярск 660041
sklsnkv@mail.ru