Journal of Siberian Federal University. Mathematics & Physics 2011, 4(4), 489–497

УДК 512.54

О регулярности силовских p-подгрупп симплектических и ортогональных групп над кольцом $\mathbb{Z}/p^m\mathbb{Z}$

Сергей Г. Колесников*
Институт математики,
Сибирский федеральный университет,
Свободный 79, Красноярск, 660041,
Россия

Николай В. Мальцев†
Институт фундаментальной подготовки,
Сибирский федеральный университет,
Киренского 26, Красноярск, 660074,
Россия

Получена 31.05.2011, окончательный вариант 25.08.2011, принята к печати 10.09.2011

Для симплектических $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ и ортогональных $O^{+}_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ групп над кольцом классов вычетов целых чисел $\mathbb{Z}/p^m\mathbb{Z}$, p — простое число, $m \geqslant 1$, исследуется аналог вопроса 8.3 Верфрица из Коуровской тетради: при каких n, m, p силовские p-подгруппы групп $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ и $O^{+}_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ регулярны?

Ключевые слова: регулярная p-группа, симплектическая группа, ортогональная группа, силовская подгруппа.

Введение

Понятие регулярной p-группы (p — простое число) было введено Ф. Холлом в [1], как обобщение понятия абелевой p-группы, которые легко классифицируются. Согласно [1] конечная p-группа G называется регулярной, если для любых $a, b \in G$ и любого натурального n существует натуральное число k и элементы $c_1, \ldots, c_k \in \langle a, b, \rangle'$ такие, что $(ab)^{p^n} = a^{p^n} b^{p^n} c_1^{p^n} \ldots\ c_k^{p^n}$.

В этой же статье (см. также [2, теорема 12.4.2]) был доказан следующий критерий регулярности: конечная p-группа G регулярна тогда и только тогда, когда для любых $a, b \in G$ существует элемент $c \in \langle a, b\rangle'$ такой, что $(ab)^p = a^p b^p c^p$. Примеры регулярных групп дают p-группы порядка $< p^p$, а также p-группы ступени нильпотентности $< p$.

В 1982 г. Верфриц поставил в Коуровской тетради вопрос [3, вопрос 8.3]: для каких n, m, p силовская p-подгруппа общей линейной группы $GL_n(\mathbb{Z}/p^m\mathbb{Z})$ над кольцом классов вычетов целых чисел $\mathbb{Z}/p^m\mathbb{Z}$ по p-примарному модулю является регулярной? Ответ на него получен в [4] для случая $m = 1$ и в [5], [6] во всех случаях, за исключением следующих: $m, n > 2$ и $2n - 1 < p \leqslant \min\{nm, n^2\}$. В [6] также рассматривался аналогичный вопрос для силовских p-подгрупп групп Шевалле над этим же кольцом.

*sklsnkv@mail.ru
†nvmatsev@mail.ru

В настоящей статье аналог вопроса Верфрица рассматривается для симплектических $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ и ортогональных $O^+_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ групп. Более точно доказаны следующие две теоремы.

Теорема 1. *Силовская p-подгруппа симплектической группы $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ нерегулярна при любом $m \geqslant 1$, если $p < 2n$, и при любом $m \geqslant 2$, когда $p < 4n$.*

Теорема 2. *Силовская p-подгруппа ортогональной группы $O^+_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ нерегулярна при любом $m \geqslant 1$, если $p < 2n-2$, и при любом $m \geqslant 2$, когда $p < 4n-4$.*

1. Вспомогательные результаты

Определим последовательность функций f_n, $n = 1, 2, \ldots$, от целочисленных аргументов i, j, k, полагая $f_n(i,j,k) = -[(j-i-k)/n]$, здесь $[x]$ — целая часть числа x. Для всякого целого неотрицательного числа l через J^l будем обозначать идеал кольца $\mathbb{Z}/p^m\mathbb{Z}$, порождённый элементом p^l. Множество идеалов $\mathfrak{A}^{(k)}_m = \{J_{ij} = J^{f_n(i,j,k)} \mid 1 \leqslant i,j \leqslant n\}$ кольца $\mathbb{Z}/p^m\mathbb{Z}$ образует ковер [7, стр. 195]. Положим $M_n(\mathfrak{A}^{(k)}_m) = \{||c_{ij}|| \mid c_{ij} \in J_{ij}\}$ и обозначим через $\Gamma(\mathfrak{A}^{(k)}_m) = \{E_n + C \mid C \in M_n(\mathfrak{A}^{(k)}_m)\}$ конгруэнц-подгруппу группы $GL_n(\mathbb{Z}/p^m\mathbb{Z})$ по модулю ковра идеалов $\mathfrak{A}^{(k)}_m$ (E_n — единичная матрица порядка n). Множество квадратных матриц порядка n, все элементы которых лежат в фиксированном идеале J^l, будем обозначать через $M_n(J^l)$.

Нетрудно видеть, что имеют место следующие включения $M_n(\mathfrak{A}^{(1)}_m) \supseteq M_n(\mathfrak{A}^{(2)}_m) \supseteq \ldots$. Следующая лемма доказана в [6].

Лемма 1. *Пусть $k_1, \ldots, k_s$ — произвольные натуральные числа и $A_i \in M_n(\mathfrak{A}^{(k_i)}_m)$, $i = 1, \ldots, s$. Тогда $A_1 \cdot A_2 \cdot \ldots \cdot A_s \in M_n(\mathfrak{A}^{(k_1+\ldots+k_s)}_m)$.*

Далее нам потребуется следующий теоретико-числовой факт.

Лемма 2. *Для всякого целого простого числа $p > 2$ и целого k, $1 \leqslant k < p$, сумма биномиальных коэффициентов*

$$(-1)^k \binom{k}{p+k-1} + \binom{k}{p}$$

делится на p^2.

Доказательство. При $k = 1$ сумма равна нулю. Пусть $k > 1$. Имеют место следующие равенства: $(p+(k-1))\ldots(p+1) = sp+(k-1)!$, $\quad (p-(k-1))\ldots(p-1) = tp+(-1)^{k-1}(k-1)!$, для некоторых $s, t \in \mathbb{Z}$. Поэтому число

$$(-1)^k(p+k-1)! + p!(p-k+1)\ldots(p-1) =$$

$$= p!((-1)^k(p+(k-1))\ldots(p+1) + (p-(k-1))\ldots(p-1)) =$$

$$= p!((-1)^k sp + (-1)^k(k-1)! + tp + (-1)^{k-1}(k-1)!) = p!p(t+(-1)^k s)$$

делится на p^2. Оно также делится на взаимно простое с p число $k!(p-1)!$. Значит, сумма

$$(-1)^k \binom{k}{p+k-1} + \binom{k}{p} = (-1)^k \frac{(p+k-1)!}{k!(p-1)!} + \frac{p!(p-k+1)\ldots(p-1)}{k!(p-1)!}$$

делится на p^2. $\square$

2. Симплектические группы

Пусть $p > 2$ — простое число и $f = \begin{pmatrix} O_n & H \\ -H & O_n \end{pmatrix}$, где

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ . & . & . & . & . \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

— квадратная матрица порядка n, O_n — нулевая матрица порядка n. Множество матриц $\{x \in GL_{2n}(\mathbb{Z}/p^m\mathbb{Z}) \mid xfx^t = f\}$ образуют группу относительно умножения матриц, которая называется симплектической группой и обозначается $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$. Пересечение $Sp_{2n}(\mathfrak{A}_m^{(1)}) = Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z}) \cap \Gamma_{2n}(\mathfrak{A}_m^{(1)})$, где $\mathfrak{A}_m^{(1)}$ — ковер, определенный выше, является силовской p-подгруппой в $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ (см., например, [8]).

Предложение 1. *Для всякого простого числа $p \geqslant 3$ силовская p-подгруппа симплектической группы $Sp_{p+1}(\mathbb{Z}/p\mathbb{Z})$ не является регулярной.*

Доказательство. Положим $n = (p+1)/2$ и пусть $a = \begin{pmatrix} E_n + C & O_n \\ O_n & E_n + D \end{pmatrix}$ — клеточно-диагональная матрица с клетками

$$E_n + C = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & \dots & 1 & 1 \\ . & . & . & . & . \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \qquad E_n + D = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 & -1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Пусть также $b = E_{2n} + e_{n,n+1}$ (через e_{ij} обозначаем матрицу, у которой на пересечении i-й строки и j-го столбца стоит единица и нули на остальных местах; порядок матрицы e_{ij} всегда ясен из контекста). Матрицы a и b лежат в силовской p-подгруппе $Sp_{2n}(\mathfrak{A}_1^{(1)})$.

Вычислим a^p и b^p. Имеем $b^p = E_{2n} + p\, e_{n,n+1} = E_{2n}$. Далее, $C^p = D^p = O_n$, так как C и D нильпотентны степени $n < p$. Биномиальные коэффициенты $\binom{p}{i}$, $i = 1, \dots, p-1$, кратны p, поэтому $(E_n + C)^p = E_n + \sum\limits_{i=1}^{p-1} \binom{p}{i} C^i + C^p = E_n$ и, аналогично, $(E_n + D)^p = E_n$. Значит, $a^p = E_{2n}$.

Найдем $(ab)^p$. Пусть $Q = ab - E_{2n} = e_{1,2} + \ldots + e_{n,n+1} - e_{n+1,n+2} - \ldots - e_{2n-1,2n} + \sum\limits_{j-i>1} \alpha_{ij} e_{ij}$.

Тогда $(ab)^p = (E_{2n} + Q)^p = E_{2n} + \sum\limits_{i=1}^{p-1} \binom{p}{i} Q^i + Q^p = E_{2n} + Q^p$. Для того чтобы вычислить произведение Q^p, подставим в него вместо матрицы Q ее разложение в сумму элементарных матриц. После раскрытия всех скобок мы получим сумму произведений элементарных матриц, где каждое произведение содержит ровно $p = 2n-1$ сомножителей. Теперь заметим, что произведение элементарных матриц $e_{i_1,j_1} \cdot e_{i_2,j_2} \cdot \ldots \cdot e_{i_s,j_s}$ отлично от нулевой матрицы только, если $j_k = i_{k+1}$, $k = 1, \dots, s-1$. В случае, когда указанное произведение отлично от нулевой матрицы, оно равно e_{i_1,j_s}, а сумма разностей $j_k - i_k$, $k = 1, \dots, s$, равна $j_s - i_1$. Так как максимальное значение разности $j - i$ для верхней нильтреугольной матрицы e_{ij} порядка $2n$ равно $2n-1$, а число $2n-1$ раскладывается в сумму $2n-1$ натуральных чисел единственным способом (только в сумму единиц), то существует единственное ненулевое произведение p

элементарных верхних нильтреугольных матриц порядка $2n$, а именно, $e_{1,2}\cdot e_{2,3}\cdot\ldots\cdot e_{2n-1,2n}$, и равно оно $e_{1,2n}$. Поэтому $Q^p = e_{12}\cdot\ldots\cdot e_{n,n+1}(-e_{n+1,n+2})\cdot\ldots\cdot(-e_{2n-1,2n}) = (-1)^{n-1}e_{1,2n}$ и, значит, $(ab)^p = E_{2n} + (-1)^{n-1}e_{1,2n}$.

Вычислим теперь G'^p, где $G = \langle a,b\rangle$. Согласно [8, стр. 647] $[Sp_{2n}(\mathfrak{A}_1^{(1)}), Sp_{2n}(\mathfrak{A}_1^{(1)})] = Sp_{2n}(\mathfrak{A}_1^{(2)})$. Так как $Sp_{2n}(\mathfrak{A}_1^{(2)}) \subseteq \Gamma(\mathfrak{A}_1^{(2)})$ и по лемме 1 $\left[\Gamma(\mathfrak{A}_1^{(2)})\right]^p \subseteq \Gamma(\mathfrak{A}_1^{(2p)}) = \{E_{2n}\}$ $(f_{2n}(i,j,2p) \geqslant 1$ для всех $i,j)$, то $G'^p = \{E_{2n}\}$. Однако, $b^{-p}a^{-p}(ab)^p \neq E_{2n}$, поэтому группа $Sp_{2n}(\mathfrak{A}_1^{(1)})$ нерегулярна. □

Предложение 2. *Для всякого простого числа $p > 3$ такого, что число $n = (p+1)/4$ — целое, силовская p-подгруппа симплектической группы $Sp_{2n}(\mathbb{Z}/p^2\mathbb{Z})$ не является регулярной.*

Доказательство. Прежде чем приступить к доказательству предложения, слелаем два замечания. Во-первых, из равенства $2n = (p+1)/2$ и леммы 1 следует, что произведение любых $(p+1)$-й матрицы из $M_{2n}(\mathfrak{A}_2^{(1)})$ равно нулевой матрице. Во-вторых, произведение числа, кратного p на любую матрицу из $M_{2n}(J)$, тоже равно нулевой матрице.

Пусть $a = E_{2n} + A$, где $A = \begin{pmatrix} C & Q \\ O_n & D \end{pmatrix}$ и C, D, Q следующие квадратные матрицы порядка n :

$$C = \begin{pmatrix} 0 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 0 & 1 & \ldots & 1 & 1 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \\ . & . & . & . \\ 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{pmatrix},$$

$$D = -e_{12} - e_{23} - \ldots - e_{n-1,n}.$$

Матрицы a и $b = E_{2n} + B = E_{2n} + p\,e_{2n,1}$ лежат в силовской p-подгруппе $Sp_{2n}(\mathfrak{A}_2^{(1)})$.

Вычислим $(ab)^p$. Имеем $(ab)^p = (E_{2n}+A+B+AB)^p = E_{2n} + \sum\limits_{k=1}^{p}\binom{k}{p}(A+B+AB)^k$. Матрица B лежит в нильпотентном ступени 2 идеале $M_{2n}(J)$ кольца $M_{2n}(\mathbb{Z}/p^2\mathbb{Z})$. Поэтому любое произведение, составленное из матриц A или B, содержащее не менее двух сомножителей, равных B, равно нулевой матрице. Отсюда при $k > 1$ следует

$$(A+B+AB)^k = ((A+B)+AB)\ldots((A+B)+AB) =$$
$$= (A+B)^k + AB(A+B)^{k-1} + (A+B)AB(A+B)^{k-2} + \ldots + (A+B)^{k-1}AB =$$
$$= (A+B)^k + ABA^{k-1} + A^2BA^{k-2} + \ldots + A^kB$$

и, значит,

$$\binom{k}{p}(A+B+AB)^k = \binom{k}{p}\left[(A+B)^k + ABA^{k-1} + A^2BA^{k-2} + \ldots + A^kB\right] =$$
$$= \binom{k}{p}(A+B)^k = \binom{k}{p}A^k$$

для $k = 2,\ldots,p-1$. Поэтому

$$(ab)^p = E_{2n} + \binom{1}{p}(A+B+AB) + \sum_{k=2}^{p-1}\binom{k}{p}A^k + (A+B+AB)^p =$$

$$= E_{2n} + (A+B)^p + \sum_{k=1}^{p-1} \binom{k}{p} A^k.$$

Вычислим a^{-p} и b^{-p}. Имеем $b^{-p} = (E_{2n} + p^2 e_{2n,1})^{-1} = E_{2n}^{-1} = E_{2n}$. Для вычисления a^{-p} воспользуемся разложением в ряд Маклорена функции $(1+x)^{-p}$:

$$(E_{2n} + A)^{-p} = E_{2n} + \sum_{k=1}^{p-1} (-1)^k \binom{k}{p+k-1} A^k.$$

Ряд конечный, поскольку $A^p = O_{2n}$ (матрица A является верхней нильтреугольной и ее степень нильпотентности равна $2n < p$.

Используя полученные равенства, находим

$$b^{-p}a^{-p}(ab)^p = \left(E_{2n} + \sum_{k=1}^{p-1} (-1)^k \binom{k}{p+k-1} A^k \right) \left(E_{2n} + (A+B)^p + \sum_{k=1}^{p-1} \binom{k}{p} A^k \right) =$$

$$E_{2n} + (A+B)^p + \sum_{k=1}^{p-1} \left((-1)^k \binom{k}{p+k-1} A^k + \binom{k}{p} A^k \right).$$

Ввиду леммы 2 для $k = 1, \dots, p-1$ имеют место равенства

$$(-1)^k \binom{k}{p+k-1} A^k + \binom{k}{p} A^k = \left((-1)^k \binom{k}{p+k-1} + \binom{k}{p} \right) A^k = O_{2n},$$

следовательно, $b^{-p}a^{-p}(ab)^p = E_{2n} + (A+B)^p$.

Найдем p-ю степень произвольной матрицы $W = ||w_{ij}|| \in M_{2n}(\mathfrak{A}_2^{(1)})$. По лемме 1 элемент $w_{ij}^{(p)}$ матрицы W^p лежит в идеале $J^{f_{2n}(i,j,p)}$. Значение функции $f_{2n}(i,j,p)$ равно единице при $i = 1$, $j = 2n$ и больше единицы в остальных случаях. Поэтому $W^p = w_{1,2n}^{(p)} e_{1,2n}$. Для вычисления элемента $w_{1,2n}^{(p)}$ представим матрицу W в виде суммы элементарных матриц и воспользуемся формулами их умножения. Так как все элементы матрицы W, лежащие на главной диагонали и ниже нее, принадлежат идеалу J, то любое произведение, содержащее не менее двух матриц $w_{ij}e_{ij}$ с $i > j$, равно нулю. Ненулевым будет только единственное произведение

$$\left(\prod_{k=1}^{2n-1} w_{k,k+1} e_{k,k+1} \right) w_{2n,1} e_{2n,1} \left(\prod_{k=1}^{2n-1} w_{k,k+1} e_{k,k+1} \right).$$

Стало быть, $w_{1,2n}^{(p)} = w_{2n,1} \prod\limits_{k=1}^{2n-1} w_{k,k+1}^2$.

Используя последнее равенство, находим $b^{-p}a^{-p}(ab)^p = E_{2n} + (A+B)^p = E_{2n} + p\, e_{1,2n} \neq E_{2n}$. Однако, элемент b, а, следовательно, и коммутант подгруппы $\langle a, b \rangle$, лежат в нормальной подгруппе $H = \langle E_{2n} + ||w_{ij}|| \mid w_{ij} \in J,\ 1 \leqslant i, j \leqslant 2n \rangle \cap Sp_{2n}(\mathfrak{A}_2^{(1)})$. Так как H является элементарной абелевой p-группой, то p-я степень любого элемента из $\langle a, b \rangle'$ равна единице. Поэтому элемент $E_{2n} + p\, e_{1,2n}$ не представим в виде произведения p-х степеней элементов из $\langle a, b \rangle'$. Значит, группа $Sp_{2n}(\mathfrak{A}_2^{(1)})$ нерегулярна. Предложение доказано. □

Поскольку подгруппы и фактор группы регулярной группы тоже регулярны, то из предложений 1 и 2 вытекает теорема 1.

Заметим также, что согласно [8] ступень нильпотентности группы $Sp_{2n}(\mathfrak{A}_m^{(1)})$ равна $2nm - 1$, а p-группы ступени нильпотентности меньше, чем p регулярны [2, стр. 205]. Поэтому из теоремы 1 следует полное решение вопроса о регулярности силовской p-группы группы $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ при $m = 1, 2$.

3. Ортогональные группы

Пусть $p > 2$ — простое число и

$$f = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ . & . & . & . & . \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

— квадратная матрица порядка $2n$. Множество матриц

$$\{x \in GL_{2n}(\mathbb{Z}/p^m\mathbb{Z}) \mid xfx^t = f,\ \det(x) = 1\}$$

образуют группу относительно умножения матриц, которая называется унимодулярной ортогональной группой и обозначается $O^+_{2n}(\mathbb{Z}/p^m\mathbb{Z})$. Пересечение

$$O^+_{2n}(\mathfrak{A}^{(1)}_m) = O^+_{2n}(\mathbb{Z}/p^m\mathbb{Z}) \cap \Gamma_{2n}(\mathfrak{A}^{(1)}_m),$$

где $\mathfrak{A}^{(1)}_m$ — ковер, определенный в п.1, является силовской p-подгруппой в $O^+_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ (см., например, [9, §1.2]).

Предложение 3. *Пусть $p > 2$ — простое число. Силовская p-подгруппа ортогональной группы $O^+_{p+3}(\mathbb{Z}/p\mathbb{Z})$ не является регулярной.*

Доказательство. Положим $2n = p + 3$. Рассмотрим матрицы

$$a = \begin{pmatrix} E_n + C & O_n \\ O_n & E_n + D \end{pmatrix},$$

где

$$C = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}, \qquad D = \begin{pmatrix} 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

и

$$b = E_{2n} + e_{n-1,n+1} - e_{n,n+2}.$$

Так как произведение $e_{n-1,n+1} \cdot e_{n,n+2}$ равно нулевой матрице, то

$$b^p = E_{2n} + p\, e_{n-1,n+1} - p\, e_{n,n+2} = E_{2n}.$$

Далее, степень нильпотентности матриц C и D равна $n < p$, поэтому

$$(E_n + C)^p = E_n + \sum_{k=1}^{p-1} \binom{k}{p} C^k + C^p = E_n$$

и, аналогично, $(E_n + D)^p = E_n$. Отсюда

$$a^p = \begin{pmatrix} (E_n + C)^p & O_n \\ O_n & (E_n + D)^p \end{pmatrix} = \begin{pmatrix} E_n & O_n \\ O_n & E_n \end{pmatrix} = E_{2n}.$$

Вычислим $(ab)^p$. Имеем
$$ab = \begin{pmatrix} E_n + C & R \\ O_n & E_n + D \end{pmatrix},$$
где
$$R = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 \\ 1 & -1 & 0 & \dots & 0 \\ . & . & . & . & . \\ 1 & -1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \end{pmatrix}.$$
Пусть
$$Q = ab - E_{2n} = \sum_{j-i>2} \alpha_{ij} e_{ij} +$$
$$+e_{1,2} + \ldots + e_{n-1,n} - e_{n+1,n+2} - \ldots - e_{2n-1,2n} + e_{1,3} + \ldots + e_{n-1,n+1} - e_{n,n+2}.$$
Тогда
$$(ab)^p = (E_{2n} + Q)^p = E_{2n} + \sum_{k=1}^{p-1} \binom{k}{p} Q^k + Q^p = E_{2n} + Q^p.$$
Из леммы 1 следует, что все элементы матрицы $Q^p = ||q_{ij}^{(p)}||$, кроме, быть может, $q_{1,2n-1}^{(p)}$, $q_{1,2n}^{(p)}$ и $q_{2,2n}^{(p)}$, равны нулю. Вычислим $q_{1,2n-1}^{(p)}$. Число $2n-2$ представляется в виде суммы из $p = 2n-3$ натуральных чисел единственным образом $2n-2 = 2+1+\ldots+1$. Поэтому элементарную матрицу $e_{1,2n-1}$ можно представить в виде произведения $(2n-3)$-х верхних треугольных элементарных матриц только, если разность между вторым и первым индексом одной из матриц произведения равна 2, а у остальных 1. Учитывая, что коэффициент при $e_{n,n+1}$ в разложении Q равен нулю, как и коэффициенты при $e_{i,i+2}$, $i = n+1, \ldots, 2n-2$, получим
$$q_{1,2n-1}^{(p)} e_{1,2n-1} = e_{1,2} \ldots e_{n-1,n}(-e_{n,n+2})(-e_{n+2,n+3}) \ldots (-e_{2n-2,2n-1}) +$$
$$+e_{1,2} \ldots e_{n-2,n-1} e_{n-1,n+1}(-e_{n+1,n+2}) \ldots (-e_{2n-2,2n-1}) = 2(-1)^{n-1} e_{1,2n-1}.$$
Таким образом,
$$b^{-p} a^{-p} (ab)^p = E_{2n} + 2(-1)^{n-1} e_{1,2n-1} + q_{2,2n}^{(p)} e_{2,2n} + q_{1,2n}^{(p)} e_{1,2n} \neq E_{2n}.$$

Вычислим теперь G'^p, где $G = \langle a, b \rangle$. По теореме 1.2.4. из [9] имеем
$$[O_{2n}^+(\mathfrak{A}_1^{(1)}), O_{2n}^+(\mathfrak{A}_1^{(1)})] \subseteq O_{2n}^+(\mathfrak{A}_1^{(2)}).$$
Так как $O_{2n}^+(\mathfrak{A}_1^{(2)}) \subseteq \Gamma(\mathfrak{A}_1^{(2)})$ и по лемме 1
$$\left[\Gamma(\mathfrak{A}_1^{(2)})\right]^p \subseteq \Gamma(\mathfrak{A}_1^{(2p)}) = \{E_{2n}\},$$
то $G'^p = \{E_{2n}\}$. Однако, $b^{-p} a^{-p} (ab)^p \neq E_{2n}$, поэтому группа $O_{2n}^+(\mathfrak{A}_1^{(1)})$ нерегулярна. □

Предложение 4. *Для всякого простого числа p такого, что число $n = (p+5)/4$ — целое, силовская p-подгруппа ортогональной группы $O_{2n}^+(\mathbb{Z}/p^2\mathbb{Z})$ не является регулярной.*

Доказательство. Простые вычисления с матрицами
$$a = E_4 + e_{13} - e_{24}, \quad b = E_4 + 3e_{31} - 3e_{42}.$$

показывают, что силовская 3-подгруппа группы $O_4^+(\mathbb{Z}/3^2\mathbb{Z})$ не является регулярной.

Пусть $p > 3$. Положим

$$A = \begin{pmatrix} C & Q \\ O_n & D \end{pmatrix},$$

где C, D, Q следующие квадратные матрицы порядка n :

$$C = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 \\ 1 & -1 & 0 & \dots & 0 \\ . & . & . & . & . \\ 1 & -1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \end{pmatrix},$$

$$D = -e_{12} - e_{23} - \dots - e_{n-1,n},$$

и

$$B = p\, e_{2n-1,1} - p\, e_{2n,2}.$$

Матрицы $a = E_{2n} + A$ и $b = E_{2n} + B$ лежат в силовской p-подгруппе $O_{2n}^+(\mathfrak{A}_2^{(1)})$. Дословно повторив рассуждения из предложения 2, получим равенство

$$b^{-p}a^{-p}(ab)^p = E_{2n} + (A+B)^p.$$

По лемме 1 имеем $(A+B)^p \in M_{2n}(\mathfrak{A}_2^{(p)})$. Так как $f_{2n}(i,j,p) \geqslant 2$ для всех пар (i,j), отличных от $(1, 2n-1)$, $(1, 2n)$, $(2, 2n)$, то

$$(A+B)^p = \alpha e_{1,2n-1} + \beta e_{1,2n} + \gamma e_{2,2n}.$$

Вычислим коэффициент α. Для этого, как обычно, разложим $A+B$ в сумму элементарных матриц и выберем те произведения, которые дают $e_{1,2n-1}$:

$$\Big(e_{1,2} \dots e_{n-2,n-1}\big(e_{n-1,n+1}(-e_{n+1,n+2}) + e_{n-1,n}(-e_{n,n+2})\big)(-e_{n+2,n+3}) \dots (-e_{2n-1,2n})\Big) \times$$
$$\times(-p\, e_{2n,2})\times$$
$$\times\Big(e_{2,3} \dots e_{n-2,n-1}\big(e_{n-1,n+1}(-e_{n+1,n+2}) + e_{n-1,n}(-e_{n,n+2})\big)(-e_{n+2,n+3}) \dots (-e_{2n-2,2n-1})\Big) +$$
$$\Big(e_{1,2} \dots e_{n-2,n-1}\big(e_{n-1,n+1}(-e_{n+1,n+2}) + e_{n-1,n}(-e_{n,n+2})\big)(-e_{n+2,n+3}) \dots (-e_{2n-2,2n-1})\Big) \times$$
$$\times(p\, e_{2n-1,1})\times$$
$$\Big(e_{1,2} \dots e_{n-2,n-1}\big(e_{n-1,n+1}(-e_{n+1,n+2}) + e_{n-1,n}(-e_{n,n+2})\big)(-e_{n+2,n+3}) \dots (-e_{2n-2,2n-1})\Big) =$$
$$= 8p\, e_{1,2n-1}.$$

Таким образом, $\alpha = 8p \neq 0$ и, следовательно, $b^{-p}a^{-p}(ab)^p \neq E_{2n}$. Завершают доказательство предложения рассуждения, аналогичные тем, что и в заключении доказательства предложения 2. □

Из предложений 3 и 4 следует теорема 2. Как и в случае симплектических групп заметим, что ступень нильпотентности группы $O_{2n}^+(\mathfrak{A}_m^{(1)})$ согласно [10, следствие 1] равна $(2n-2)m-1$. Поэтому из теоремы 2 вытекает полное решение вопроса о регулярности группы $O_{2n}^+(\mathfrak{A}_m^{(1)})$ при $m = 1, 2$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 09-01-00717)

Список литературы

[1] P.Hall, A conribution to the theory of groups of prime-power order, *Proc. London Math. Soc.,* **s2-36**(1934), №1, 29–95.

[2] *М.Холл*, Теория групп, М., ИЛ, 1962.

[3] Коуровская тетрадь, Нерешенные вопросы теории групп, ред. Мазуров В.Д., Хухро Е.И.,16-е издание, 2006, http://www.math.nsc.ru/

[4] А.В.Ягжев, О регулярности силовских p-подгрупп полных линейных групп над кольцами вычетов, *Матем. заметки,* **56**(1994), №6, 106–116.

[5] С.Г.Колесников, О регулярности силовских p-подгрупп групп $GL_n(\mathbb{Z}_{p^m})$, *Иссл. по матем. анализу и алгебре,* **3**(2001), 117–124.

[6] С.Г.Колесников, О регулярных силовских p-подгруппах групп Шевалле над кольцом $\mathbb{Z}_{p^m}$, *Сиб. матем. журнал,* **46**(2006), №6, 1289–1295.

[7] М.И.Каргаполов, Ю.И.Мерзляков Основы теории групп, М., Наука, 1977.

[8] Ю.В.Сосновский, Коммутаторное строение симплектических групп, *Матем. заметки,* **24**(1978), №5, 641–648.

[9] Ю.В.Сосновский, Коммутаторное строение и изоморфизмы классических групп, Диссертация на соискание уч. степ. к.ф.-м.н., Новосибирск, 1980.

[10] В.М.Левчук, Коммутаторное строение некоторых подгрупп групп Шевалле, *Укр. мат. журнал,* **44**(1992), №6, 786–795.

On the Regularity Sylow's p-subgroups of Symplectic and Orthogonal Groups over Ring $\mathbb{Z}/\mathrm{p}^{\mathrm{m}}\mathbb{Z}$

Sergey G. Kolesnikov
Nikolay V. Maltsev

For symplectic $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ and orthogonal $O_{2n}^+(\mathbb{Z}/p^m\mathbb{Z})$ groups over residue ring of integers $\mathbb{Z}/p^m\mathbb{Z}$, p — prime integer, $m \geqslant 1$, we investigate analog Wehrfritz's question 8.3 from Kourovka notebook: for which n, m, p Sylow p-subgroups of groups $Sp_{2n}(\mathbb{Z}/p^m\mathbb{Z})$ and $O_{2n}^+(\mathbb{Z}/p^m\mathbb{Z})$ are regular?

Keywords: regular p-group, symplectic group, orthogonal group, Sylow subgroup.