



МАТЕМАТИКА

УДК 512.54

А.А. Шлепкин, И.В. Сабодах,
А.Н. Дарзиев, Е.А. ПронинаО ПОДГРУППАХ ГРУПП $GL_2(p^n)$

В статье рассмотрено понятие насыщенности группы. Установлена структура 2-групп, насыщенных фиксированным набором конечных 2-групп.

Ключевые слова: группа, насыщенность, теорема, доказательство.

А.А. Shlepin, I.V. Sabodakh,
A.N. Darzиеv, E.A. ProninaABOUT THE SUBGROUPS OF GROUPS $GL_2(p^n)$

The concept of the group saturation is considered in the article. The structure of 2-groups, saturated by the fixed set of finite 2-groups is established.

Key words: group, saturation, theorem, proof.

Введение. В обзоре [1] поставлена следующая задача: как устроена группа G насыщенная $GL_2(q)$. Для ее решения необходимо знать структуру подгрупп $GL_2(q)$, а также структуру силовой 2-подгруппы исследуемой группы. Решению этих двух задач посвящена данная работа.

1. Группы насыщенные конечными 2-группами специального вида

Пусть X – множество конечных полудиэдральных 2-групп, Y – множество конечных групп периода 2, а Z – множество сплетенных конечных 2-групп. Положим $\mathfrak{M} = X \cup Y \cup Z$.

Теорема 1. Пусть G – 2-группа и G насыщена группами из множества $\mathfrak{M}$. Тогда G изоморфна одной из следующих групп:

1. $G = \langle a, b | a^{2^n} = b^2 = e, a^b = a^{2^{n-1}-1} \rangle$ – группа полудиэдра.
2. G – группа периода два.
3. $G = (A \times B) \rtimes \langle \omega \rangle$, ω^2 – инволюция, $A^\omega = B$ и A – (локально) циклическая 2-группа.

Доказательство теоремы 1. Утверждение теоремы очевидно, если G конечная группа. Поэтому в дальнейшем будем предполагать, что G – бесконечная группа.

Лемма 1 (В.П. Шунков). В бесконечной 2-группе T любая конечная подгруппа отлична от своего нормализатора. В частности, T содержит бесконечную локально конечную подгруппу [2, 3].

Лемма 2. G – 2-группа.

Доказательство. Пусть $b \in G$ и $|b| < \infty$. По условиям теоремы $b \in K$ и поскольку $K \in \mathfrak{M}(1)$, то K – 2-группа. Следовательно, b – 2-элемент. Лемма доказана.

Лемма 3. Если $\mathfrak{M}(1)$ содержит полудиэдральную подгруппу, то либо G группа полудиэдра, либо G насыщена сплетенными 2-группами.

Доказательство. Покажем, что G конечная группа. Предположим обратное. По лемме 1 $N_G(K) \neq K$. Здесь $K \in \mathfrak{M}(1)$ и K полудиэдральная группа. Возьмем $b \in N_G(K) \setminus K$ и положим $K_1 = \langle K, b \rangle$. Очевидно, K_1 конечная группа.

По условию насыщенности $K_1 \subseteq K_2 \in \mathfrak{M}(1)$. Из определения множества $\mathfrak{M}$ следует, что K_2 одна из следующих групп:

1. K_2 – группа полудиэдра.

2. K_2 – конечные элементарные абелевы 2-группы.

3. K_2 – сплетенная 2-группа.

Так как K собственная подгруппа K_2 , то ни одна из ситуаций 1, 2 невозможна и, следовательно, либо $K = G$, либо G насыщена сплетенными 2-группами. Лемма доказана.

В дальнейшем будем считать, что $\mathfrak{M}(1)$ не содержит полудиэдральных групп.

Лемма 4. Если $\mathfrak{M}(1)$ содержит элементарную абелеву группу K и $|K| \geq 8$, то G группа периода два.

Доказательство. Пусть G содержит элементарную абелеву подгруппу $|K| \geq 8$. Из леммы 1 и условия насыщенности вытекает, что в этом случае G содержит бесконечную элементарную абелеву подгруппу I и будем считать I максимальной в указанном смысле (Лемма Цорна [4]).

Если $G = I$, то все доказано. Предположим, что $x \in G \setminus I \neq \emptyset$. Покажем, что x можно выбрать так, что $xz = zx$ для некоторой инволюции $z \in I$.

Если $|x| = 2$, то группа $\langle x, z \rangle$ конечна, для любой инволюции z из I . Пусть t инволюция из $Z(\langle x, z \rangle)$. Если $t \in I$, то положим $z = t$. Если $t \notin I$, то положим $x = t$. Подгруппа $\langle z \rangle \times \langle x \rangle = K_1$, очевидно, не лежит в I и $K_1 \cap I = \langle z \rangle$. Возьмем в I инволюцию $t \neq z$. Ясно, что $tz = zt$.

Рассмотрим конечную подгруппу $\langle z, x, t \rangle$. Данные подгруппы, очевидно, не лежат в I и $\langle z, x, t \rangle \cap I \geq (\langle x \rangle \times \langle t \rangle)$. В силу леммы 1, в $\langle z, x, t \rangle$ существует элемент v такой, что $v \in N_G(\langle z \rangle \times \langle t \rangle) \setminus I$ и $v^2 \in I$. Тогда группа $K_2 = \langle v, z, x, t, t_1 \rangle$, где $t_1 \in I \setminus (\langle z \rangle \times \langle t \rangle)$ конечна.

По условию насыщенности $K_2 \leq K_3 \in \mathfrak{M}(1)$. Так как K_3 содержит подгруппу $\langle t \rangle \times \langle t_1 \rangle \times \langle z \rangle$, то из структуры $\mathfrak{M}$ вытекает, что K_3 – элементарная абелева 2-группа. В силу произвольности t_1 как инволюции, из I получим, что x перестановочен с любой инволюцией из I . Таким образом, $I \times \langle x \rangle$ элементарная абелева 2-группа, что противоречит максимальной, I – как элементарная абелева 2-группа.

Пусть $|x| > 2$. Возьмем $x_1 = x^{|x|/2}$. По доказанному выше $x_1 \in I$. В дальнейшем, дословно повторяя рассуждения для случая $|x| = 2$, получим, что $x \in K_4$ – элементарная абелева 2-группа. Противоречие с тем, что $|x| > 2$. Лемма доказана.

В дальнейшем будем считать, что G не содержит элементарных абелевых групп порядка более четырех.

Лемма 5. $G = (A \times B) \rtimes \langle w \rangle$, где $A^w = B$, A (локально) – циклическая группа, w – инволюция.

Доказательство. Так как G бесконечная группа, то можно считать в силу доказанных выше лемм, что $\mathfrak{M}$ состоит только из сплетенных 2-групп и по [5] G требуемого вида. Лемма доказана.

Из лемм 2–5 вытекает доказательство теоремы.

2. Структура сплетенной 2-группы

Теорема 2. Пусть $G = (A \times B) \rtimes \langle w \rangle$ – конечная сплетенная 2-группа, т.е.

$A = \langle a \rangle, B = \langle b \rangle, a^w = b, a^{2^k} = b^{2^k} = w^2 = 1$. Тогда:

1. Центр G – $Z(G) = \langle ab \rangle = \langle z \rangle$, где $z = ab$.

2. $G = (Z \times A) \rtimes \langle w \rangle = (Z \times B) \rtimes \langle w \rangle, z^w = z, a^w = b = aba^{-1} = za^{-1}, a^{w^2} = (za^{-1})^w = z(za^{-1})^{-1} = zz^{-1}a = a$.

3. $G = (Z \times B), z^w = z, b^w = a = abb^{-1} = zb^{-1}, b^{w^2} = (zb^{-1})^w = z(zb^{-1})^{-1} = zz^{-1}b = b$.

4. Пусть $x \in (A \times B)$ и $|x| = 2^m$. Тогда $|xw| = 2^{m+1}, (xw)^2 \in Z$, в частности, если $x = a$, то $(aw)^2 = ab = z$ и если $x = b$, то $(bw)^2 = ab = z$.

5. $(aw)(bw) = abz^{-1} = ab^{-1}z, z \in \langle ab^{-1} \rangle$.

6. $(ab^{-1})^w = a^wb^{w^{-1}} = ba^{-1}$ и $R = \langle ab^{-1} \rangle \rtimes \langle w \rangle$ – группа диэдра.

7. Пусть $d = a^{2^m-l}b^l$, тогда $d^w = b^{2^m-l}a^l, (l, |2^k|) = 1, dd^w = a^{2^m-l}b^lb^{2^m-l}a^l = a^{2^m}b^{2^m} = z^{2^m}, d^w = d^{-1}a^{2^m}b^{2^m} = d^{-1}z^{2^m}, |d| = 2^k$.

8. Если $m = k$, то $\langle d \rangle = \langle ab^{-1} \rangle$ и $\langle d \rangle \rtimes \langle w \rangle = \langle ab^{-1} \rangle \rtimes \langle w \rangle = R$ – группа диэдра.

9. Если $m = k - 1$, то a^{2^m} – инволюция из A, b^{2^m} – инволюция из $B, a^{2^m}b^{2^m} = z_1$ – инволюция из $D \cap Z = \langle z_1 \rangle$ и $dd^w = z_1$ или $d^w = d^{-1}z_1$. Тогда $D = \langle d \rangle \rtimes \langle w \rangle$ – полудиэдральная группа.

10. $N(\langle bw \rangle) = \langle bw \rangle \rtimes \langle z_b, z_b \rangle$ – инволюция из $\langle b \rangle$.

Доказательство. Непосредственные вычисления и данные 5.

3. Структура $GL_2(q)$, где q – нечетно

Теорема 3. Пусть $L = GL_2(q)$, где $q = p^n$ и p – нечетно. Тогда:

1. $R = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \alpha \in GF(q) \right\}$ – силовская 2-подгруппа группы L .
2. $N_L(R) = R \rtimes (Z \times T)$, где $Z = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \right\rangle$ – центр группы L , $T = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$, $|\alpha| = q - 1$.
3. R – абелева группа периода p и $R \subset SL_2(2p^n)$.
4. $C_L(R) = (R \times Z)$.
5. Все силовские p -подгруппы группы L сопряжены и пересекаются тривиально.
6. $N_L(Z \times T) = (Z \times T) \rtimes \langle w \rangle$, где $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
7. Пусть $M = \langle a \rangle \times \langle b \rangle$, где $|a| = |b| = k > 2$, подгруппа L . Тогда k делит $q - 1$ и для некоторого $g = L$, $M^g \subset (Z \times T)$ и $N_L M^g = N_L(Z \times T)$.
8. $L = SL_2(p^n) \cdot T$, где $T = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ и $\alpha \in GF(p^k)$.
9. $L = (SPGL_2(q) \cdot Z \cdot \langle v \rangle)$, где $v = \begin{pmatrix} h & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $v^2 = w = \begin{pmatrix} h & 0 \\ 0 & h \end{pmatrix} \in Z$, где h – элемент поля $GF(p^n)$, из которого не извлекается корень квадратный.
10. Если $4 \nmid (q - 1)$, то $L = (SL_2(q) \cdot Z \cdot \langle a \rangle)$, где $a = \begin{pmatrix} 0 & 1 \\ h & 0 \end{pmatrix}$ и h – элемент поля $GF(q)$, из которого не извлекается квадратный корень.
11. Если $4 \mid (q - 1)$, то $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in SL_2(q) \cdot Z(GL_2(q))$.
12. Если $4 \nmid (q - 1)$, то $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin SL_2(q) \cdot Z(GL_2(q))$.
13. Если $q \equiv 1 \pmod{4}$, $2^s - 2$ часть числа $q - 1$, ξ – примитивный корень степени 2^s из 1 в $GF(q)$, то силовская 2-подгруппа S группы L имеет порядок 2^{s+1} и является сплетением групп Z_{2^s} и Z_2 , $S = \left\langle \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$.
14. Если $q \equiv -1 \pmod{4}$, $2^s - 2$ часть числа $q + 1$, ξ – примитивный корень степени 2^{s+1} из 1 в $GF(q^2)$, то силовская 2-подгруппа S группы L является полудиэдральной группой порядка 2^{s+2} и $S = \left\langle \begin{pmatrix} \xi & 0 \\ 0 & \xi + \xi^q \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$.
15. Пусть $G = PGL_2(q)$ и $4 \nmid (q - 1)$. Тогда $C_G(w) = \{D \times w\}$, где D – группа диэдра порядка $(q - 1)$, $D = A \rtimes \langle t \rangle$, $A = \langle a \rangle$ – циклическая группа порядка $\frac{(q-1)}{2}$, t – инволюция, $a^t = a^{-1}$ для любого $a \in A$.
16. Если $4 \mid (q - 1)$, то $PGL_2(q) = L_2(q) \rtimes \langle \bar{a} \rangle$, где $|\bar{a}| = 2$.
17. Если $4 \nmid (q - 1)$, то $PGL_2(q) = L_2(q) \rtimes \langle \bar{w} \rangle$, где $\bar{w} = wZ(GL_2(q))$.

Доказательство пунктов 1–8 можно найти в [6].

Доказательство пункта 9. Пусть $\sqrt{h}$ существует в $GF(p^n)$. Тогда:

$$\begin{aligned} L &= Z \cdot SL_2(p^n) \cdot \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \\ &= SL_2(p^n) \cdot Z \cdot \begin{pmatrix} \sqrt{h}^{-1} & 0 \\ 0 & \sqrt{h} \end{pmatrix} \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \\ &= SL_2(p^n) \cdot Z \begin{pmatrix} \sqrt{h}\sqrt{h} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{h}^{-1} & 0 \\ 0 & \sqrt{h} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \\ &= SL_2(p^n) \cdot Z \begin{pmatrix} \sqrt{h} & 0 \\ 0 & \sqrt{h} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = SL_2(p^n) \cdot Z. \end{aligned}$$

Пункт доказан.

Доказательство пункта 10. Покажем, что $\alpha \notin SL_2(q)Z$. Предположим обратное $\alpha \in SL_2(q)Z$. Тогда $\alpha = sz$, где $s \in SL_2(q)Z$, а $z \in Z$. Посчитаем определители матриц: $-h = |\alpha| = |sz| = |s||z| = 1 \cdot$

$|z| = |z| = \alpha^2$, где $z = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$. Поскольку $4|(q-1)$, то $\sqrt{-1}$ элемент поля $GF(q)$. Следовательно, $h = -\alpha^2 = (\sqrt{-1})^2 \alpha^2 = (\sqrt{-1} \cdot \alpha)^2$. Противоречие с тем, что из h не извлекается корень квадратный. Пункт доказан.

Доказательство пункта 11. Так как $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(q)$, то достаточно показать, что $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(q)Z$. Так как $4|(q-1)$, то $\sqrt{-1} \in GF(q)$ и $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & (\sqrt{-1})^{-1} \end{pmatrix} \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \in SL_2(q)Z$. Потому что $\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & (\sqrt{-1})^{-1} \end{pmatrix} \in SL_2(q)$, $\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \in Z$. Пункт доказан.

Доказательство пункта 12. Предположим обратное. Тогда $w = sz$ для некоторых $s \in SL_2(q)$ и $z \in Z(GL_2(q))$. Посчитаем определители $-1 = |w| = |sz| = |s| \cdot |z| = 1 \cdot |z| = |z| = \alpha^2$, где $z = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$. Следовательно, в $GF(q)$ существует $\sqrt{-1}$. Но тогда $|\sqrt{-1}| = 4$ и 4 делит $q-1$, что невозможно. Пункт доказан.

Доказательство пунктов 13, 14 можно найти в [6].

Доказательство пункта 15. Из условия $wgw = gd, d \in Z$ получаем

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & v \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ z & v \end{pmatrix} d \Rightarrow \quad (1)$$

$$\begin{pmatrix} v & z \\ y & x \end{pmatrix} \begin{pmatrix} dx & dy \\ dz & dv \end{pmatrix} \Rightarrow \quad (2)$$

$$\begin{cases} v = dx \\ z = dy \\ y = dz \\ x = dv \end{cases} \Rightarrow \quad (3)$$

$$\begin{matrix} d^2x=x \\ d^2y=y \end{matrix} \Rightarrow \quad (4)$$

$$d = \pm 1 \quad (5)$$

$$C_G(w) = \left\{ \begin{smallmatrix} xy \\ dydx \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} xy \\ yx \end{smallmatrix} \right\} \cup \left\{ \begin{smallmatrix} xy \\ -y & -x \end{smallmatrix} \right\}. \quad (6)$$

Имеют места следующие ограничения $x^2 - y^2 \neq 0$ для первого множества и $-x^2 + y^2 \neq 0$ для второго множества. Равенство 6 можно записать в следующем виде:

$$C_G(w) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} Z \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} Z \right\} \cup \left\{ \begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix} Z \right\} \cup \left\{ \begin{pmatrix} x & 1 \\ -1 & -x \end{pmatrix} \right\}. \quad (7)$$

Посчитаем количество элементов в каждом из этих множеств:

$$\left| \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} Z \right\} \right| = (q-1) \quad (8)$$

$$\left| \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} Z \right\} \right| = (q-1) \quad (9)$$

$$\left| \left\{ \begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix} Z \right\} \right| = (q-2)(q-1). \quad (10)$$

В случае (10) выбрасываются матрицы с $x = \pm 1$. Так как в этом случае $\det \begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix} = 0$.

Аналогично

$$\left| \left\{ \begin{pmatrix} x & 1 \\ -1 & -x \end{pmatrix} Z \right\} \right| = (q-2)(q-1). \quad (11)$$

Нетрудно увидеть, что все указанные 4 множества пересекаются по пустому множеству попарно. Следовательно, общее число элементов равно:

$$\begin{aligned} & (q-1) + (q-1) + (q-2)(q-1) + (q-2)(q-1) = \\ & = (q-1)(2 + 2(q-2)) = 2(q-2-1) = 2(q-1)^2. \end{aligned} \quad (12)$$

Переходим к фактор-группе $GL_2(q)/Z$, получаем: $|C_G(w)| = 2(q-1)$.

Пункт доказан.

Доказательство пунктов 16, 17 вытекает из пунктов 10–12.

4. Структура $SL_2(q)$, где q – нечетно

Теорема 4. Группа $SL_2(p^n)$ при $p \neq 2$ содержит точно одну инволюцию.

Доказательство. Предположим обратное. И пусть $v = \begin{pmatrix} \alpha & \beta \\ \Delta & \sigma \end{pmatrix}$ и инволюция из $SL_2(p^n)$, отличная от инволюции $z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, т.е. $v \neq z$.

Так как $v \in SL_2(p^n)$, то $1 = |v| = \alpha\Delta - \beta\sigma$. Так как $v^2 = e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, то

$$v^2 = \begin{pmatrix} \alpha & \beta \\ \Delta & \sigma \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \Delta & \sigma \end{pmatrix} = \begin{pmatrix} \alpha^2 + \beta\Delta & \alpha\beta + \sigma\beta \\ \alpha\Delta + \sigma\Delta & \beta\Delta + \sigma^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Следовательно, имеем систему уравнений:

$$(1) \quad \begin{cases} \alpha\sigma - \beta\Delta = 1 & (1) \\ \alpha^2 + \beta\Delta = 1 & (2) \\ \beta\Delta + \sigma^2 = 1 & (3) \\ \alpha\beta + \sigma\beta = 0 & (4) \\ \alpha\Delta + \sigma\Delta = 0 & (5). \end{cases}$$

Вычитая из уравнения (3) уравнение (2), получаем $\sigma^2 - \alpha^2 = 0$ или $(\sigma - \alpha)(\sigma + \alpha) = 0$.

I. $\sigma = \alpha$. Тогда система (1) приобретает вид:

$$(2) \quad \begin{cases} 1. \alpha^2 - \beta\Delta = 1 \\ 2. \alpha^2 + \beta\Delta = 1 \\ 3. \Delta\beta + \alpha^2 = 1 \\ 4. 2\alpha\beta = 0 \\ 5. 2\alpha\Delta = 0. \end{cases}$$

Складываем уравнение (1) с уравнением (2). Получим $\alpha^2 = 1$.

Вычитая из уравнения (2) уравнение (1), получаем $2\beta\Delta = 0$. Из уравнений (4) и (5) следует, что $\beta = \Delta = 0$. Значит $\alpha = -1 = \sigma$ и $v = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

II. $\alpha = -\sigma$. Тогда система (1) приобретает вид:

$$(3) \quad \begin{cases} 1. \alpha^2 - \beta\Delta = 1 \\ 2. \alpha^2 + \beta\Delta = 1 \\ 3. \alpha^2 + \beta\Delta = 1 \\ 4. \alpha\beta - \alpha\beta = 0 \\ 5. \alpha\Delta - \alpha\Delta = 0. \end{cases}$$

Точно так же, как и выше (в случае $|\alpha| = \sigma$), получим $\alpha^2 = 1$, $\beta\Delta = 0$ и $1=|v| = -\alpha\sigma = -\alpha^2 = -1$. Противоречие.

Итак, случай II, $\alpha = -\sigma$ невозможно и теорема доказана.

5. Об инволюции в $GL_2(p^n)$

Теорема 5. Пусть $b \in G \geq GL_2(p^n)$, $2 \nmid |b|$ и $C_G(b)$ содержит две различные инволюции. Тогда $|b| \mid p^n - 1$.

Доказательство. Пусть z, v инволюции из условия теоремы. Без ограничения общности можно считать, что $z \in Z(G)$. Несложно видеть, что $G = SL_2(p^n) \rtimes T$, где $T = \left\langle \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ и $t \in GF(p^n)$. Так как $|b|$ нечетное число, то $|b|$ делит либо $p^n - 1$, либо $|b|$ делит $(p^n + 1)$.

Если $|b|$ делит $p^n - 1$, то все доказано.

Рассмотрим случай, когда $|b|$ делит $p^n + 1$. В этом случае $b \in SL_2(p^n) = S$ и по теореме 4 $C_S(b)$ содержит точно одну инволюцию и это инволюция z .

Следовательно, $v \notin S$ и $v = z^\delta t_1$, где $t_1 \in T$ и $t_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, а $\delta \in \{0, 1\}$.

Посчитаем $C_S(t_1)$:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & v \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -x & -y \\ z & v \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & -y \\ -z & v \end{pmatrix}$$

$$\begin{aligned} y &= -y = 0 \\ z &= -z = 0. \end{aligned}$$

Таким образом, $C_S(t_1) = \left\{ \begin{pmatrix} x & 0 \\ 0 & v \end{pmatrix} \right\}$.

Получаем $y = \begin{pmatrix} x & 0 \\ 0 & v \end{pmatrix}$ и $|y|$ делит $p^n - 1$, для любого $y \in C_S(t_1)$.

Противоречие. Так как $b \in C_S(t_1)$, то $|b|$ делит $p^n - 1$. Противоречие с тем, что $|b|$ делит $p^n + 1$, поскольку $(p^n - 1, p^n + 1) = 1$.

Теорема доказана.

Литература

1. Кузнецов А.А. Филиппов К.А. Группы, насыщенные заданным множеством групп // Сибирские электронные математические известия. – 2011. – Т. 8. – С. 230–246.
2. Шлепкин А.К. Сопряженно бипримитивно конечные группы, содержащие конечные неразрешимые подгруппы // Сб. тез. 3-й междунар. конф. по алгебре. – Красноярск, 1993. – С. 396.
3. Лыткина Д.В., Тухватуллина Л.Р., Филиппов К.А. О периодических группах, насыщенных конечным множеством конечных простых групп // Сибир. мат. журн. – 2008. – Т. 49. – № 2. – С. 394–399.
4. Курош А.Г. Лекции по общей алгебре. – М.: Наука, 1973. – 400 с.
5. Шлепкин А.А. Периодические группы, насыщенные сплетенными группами // Сибир. электронные математические известия. – 2013. – Т. 10. – С. 56–64.
6. Harada K. Indecomposable Sylow 2 – subgroups of Simple Groups // Acta Applicandae Mathematicae. – 2005. – Vol. 85. – P. 161–194.

