*Сибирский математический журнал*
*Сентябрь—октябрь, 2005. Том 46, № 5*

*УДК 512.54*

# КОНЕЧНЫЕ СИЛОВСКИЕ ПОДГРУППЫ ПРОСТЫХ ЛОКАЛЬНО КОНЕЧНЫХ ГРУПП ЛИЕВА ТИПА

**М. Кузуджуоглу, В. Д. Мазуров**

**Аннотация:** Основным результатом статьи является следующая

**Теорема.** *Пусть $S = \{r_0, r_1, \dots, r_n\}$ — конечное непустое множество простых чисел и $L$ — лиев тип групп Шевалье. Тогда существует такое локально конечное поле $F$ характеристики $r_0$, что силовские $r$-подгруппы простой группы $L(F)$ типа $L$ над $F$ конечны в том и только в том случае, когда $r \notin S$.*

**Ключевые слова:** силовские подгруппы, локальная конечность, простая группа.

Хартли и Шуте доказали (теорема B в [1]), что бесконечная локально конечная простая группа $G$ удовлетворяет условию min-$p$ для некоторого простого числа $p$ тогда и только тогда, когда $G$ изоморфна группе лиева типа над бесконечным локально конечным полем. В частности, если силовская $p$-подгруппа локально конечной простой группы $G$ является черниковской, то $G$ — простая группа лиева типа. Очевидно, что если характеристика бесконечного локально конечного поля $F$ равна $p$, то силовские $p$-подгруппы простой группы $L(F)$ лиева типа $L$ над $F$ бесконечны. Поэтому если все силовские подгруппы простой локально конечной группы $G$ бесконечны, то $G$ конечна.

Основная цель настоящей работы — доказательство следующего результата.

**Теорема 1.** *Пусть $S = \{r_0, r_1, \dots, r_n\}$ — конечное непустое множество простых чисел и $L$ — лиев тип групп Шевалье. Тогда существует такое локально конечное поле $F$ характеристики $r_0$, что силовские $r$-подгруппы простой группы $L(F)$ типа $L$ над $F$ конечны в том и только в том случае, когда $r \notin S$.*

**Предварительные результаты.**

**Лемма 1.** *Пусть $n > 1$ — натуральное число, $r$ — простое число, не делящее $n$, $s = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, где каждое $p_i$ — простое число, большее чем $r$, и $k_i \geq 1$, $i = 1, \dots, t$. Тогда $r$ не делит $(n^s - 1)/(n - 1)$.*

Доказательство. Пусть $N = (n^s - 1)/(n - 1) = n^{s-1} + \dots + 1$.

Предположим вначале, что $r \mid n - 1$. Если $r$ делит $N$, то

$$N - s = (n^{s-1} - 1) + \dots + (n - 1)$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта № 05–01–00797), гранта Президиума СО РАН (№ 86–197), гранта программы «Университеты России» (№ УР.04.01.028), гранта программы Рособразования «Развитие научного потенциала высшей школы» (№ 511), а также Совета по грантам президента РФ и государственной поддержке ведущих научных школ (грант НШ–2069.2003.1).

и каждое слагаемое делится на $n-1$, поэтому правая часть делится на $r$. Следовательно, $N-s$ делится на $r$ и $r \mid s$, что невозможно.

Пусть $r \nmid n-1$ и $u$ — наименьшее целое положительное число, удовлетворяющее сравнению $n^u \equiv 1(\operatorname{mod} r)$. Тогда $1 \neq u < r$ и если $r$ делит $n^s-1$, то $u$ делит $s$. Это невозможно, поскольку $u < r < p_i$.

**Предложение 1.** *Для любого простого числа $p$ существует несчетное множество бесконечных локально конечных полей $F$ характеристики $p$ таких, что силовские $r$-подгруппы в $\mathrm{PSL}(2,F)$ конечны для любого простого $r \neq p$.*

Доказательство. Пусть $q_0$ — степень $p$ и $F_0 = GF(q_0)$. Существует простое число $p_1$, которое больше, чем любой простой делитель числа $q_0^2-1$. Пусть $q_1 = q_0^{p_1}$ и $F_1 = GF(q_1)$. Пусть $p_i, q_i$, и $F_i$ уже определены. Пусть $p_{i+1}$ — простое число, которое больше $p$ и больше, чем любой простой делитель числа $q_i^2-1$, $q_{i+1} = q_i^{p_{i+1}}$ и $F_{i+1} = GF(q_{i+1})$. Положим $F = \bigcup\limits_i F_i$ и $G = \mathrm{PSL}(2,F)$.

Предположим, что силовская $r$-подгруппа группы $G$ нетривиальна для простого числа $r \neq p$, и выберем элемент $x \in G$ порядка $r$. Тогда $x \in \mathrm{PSL}(2,F_i)$ для некоторого $i$ и поэтому $r \mid \left(q_i^2-1\right)$. Утверждается, что силовская $r$-подгруппа из $\mathrm{PSL}(2,F_i)$ является силовской $r$-подгруппой в $G$. В противном случае существует такое число $j$, что $|\mathrm{PSL}(2,F_{i+j}) : \mathrm{PSL}(2,F_i)|$ делится на $r$, т. е. $\left(q_{i+j}^2-1\right)/\left(q_i^2-1\right)$ делится на $r$. Теперь положим $n = q_i^2$, $s = p_{i+1}\dots p_{i+j}$. Тогда $q_{i+j}^2 = q_i^{2p_{i+1}\dots p_{i+j}} = n^s$ и поэтому $(n^s-1)/(n-1)$ делится на $r$. Это противоречит лемме 1.

Используя, к примеру, [2, с. 26], легко показать, что существует несчетное множество неизоморфных локально конечных полей, удовлетворяющих условиям предложения.

**Лемма 2.** *Пусть $n \neq 1$ — целое число и $r$ — целое число, делящее $n-1$. Тогда*

(а) *число $r^i$ делит $n^{r^{i-1}}-1$ для всех $i \in \mathbb{N}$;*

(б) *число $r$ делит $(n^s-1)/(n-1)$ для натурального числа $s$ в том и только в том случае, когда $r$ делит $s$.*

Доказательство. П. (а) легко доказывается индукцией по $i$, если заметить, что

$$(n^{r^i}-1)/(n^{r^{i-1}}-1) = q^{r-1} + q^{r-2} + \dots + 1 \equiv 0(\operatorname{mod} r),$$

где $q = n^{r^{i-1}}$.

Докажем п. (b). Предположим, что $r$ делит $s$. Тогда $r$ делит

$$(n^{s-1}-1) + (n^{s-2}-1) + \dots + (n-1) + s = (n^s-1)/(n-1).$$

Обратно, предположим, что $r$ делит $(n^s-1)/(n-1)$. Тогда

$$r \mid n^{s-1} + n^{s-2} + \dots + 1 = (n^{s-1}-1) + (n^{s-2}-1) + \dots + (n-1) + s.$$

Следовательно, $r \mid s$. Лемма доказана.

Следующее определение взято из [2]. *Числом Штейница* называется символ вида

$$N = p_1^{x_1} p_2^{x_2} p_3^{x_3} \dots = \prod_{i=1}^{\infty} p_i^{x_i},$$

где $p_i$ — это $i$-е простое число, а $x_i$ содержится в расширенном множестве натуральных чисел $\{0, 1, 2, \dots, \infty\}$.

Пусть $N$ — число Штейница и $p$ — простое число. Поле $GF(p^N)$ определяется как

$$GF(p^N) = \bigcup_{d|N} GF(p^d)$$

с объединением по всем обыкновенным натуральным числам $d$, делящим $N$. Любое локально конечное поле изоморфно $GF(p^N)$ для некоторого простого числа $p$ и некоторого числа Штейница $N$.

Пусть $F = GF(p^N)$ — локально конечное поле характеристики $p$. Тогда $F$ — объединение конечных полей $F_0 < F_1 < \dots F_s < \dots$, где $|F_0| = p$ и степень $m_j = |F_j : F_{j-1}|$ расширения $F_j$ над $F_{j-1}$ — простое число, $j = 1, 2, \dots$. Последовательность $F_0, F_1, \dots, F_s, \dots$ не является однозначно определенной для $F$, но число $\gamma_r(F)$ тех $j$, для которых $m_j$ равно данному простому числу $r$, зависит только от $F$. Действительно, $x_i$ в определении числа Штейница $N$ равно $\gamma_r(F)$, если $p_i = r$.

Для $m \in \mathbb{N}$ и простого числа $r$ положим $v_r(m) = s$, если $r^s \mid m$ и $r^{s+1} \nmid m$. Для $u, t$ из $\mathbb{N}$ определим $v_r(u/t)$ как $v_r(u) - v_r(t)$. Тогда число $v_r(\rho)$ определено корректно для каждого положительного рационального числа $\rho$ и $v_r(\rho) \in \mathbb{Z}$.

Следуя [3, с. 112], поле $F$ будем называть *$r$-замкнутым*, если $F$ не обладает расширением степени $r$.

**Лемма 3.** *Пусть $F$ — локально конечное поле. Следующие утверждения эквивалентны:*

(a) *поле $F$ является $r$-замкнутым;*

(b) $\gamma_r(F) = \infty$.

Доказательство. Предположим, что $F$ является $r$-замкнутым и $\gamma_r(F)$ конечно. Среди подполей $F_i$, определенных выше, выберем такое, что $m_j \neq r$ при всех $j > i$. Выберем полином $f(x) \in F_i[x]$ так, чтобы степень $f(x)$ равнялась $r$ и $f(x)$ был неразложим над $F_i$. Тогда $f(x)$ разложим над $F$. Выберем $g(x) \in F[x]$ так, что $g(x) \mid f(x)$ и $g(x)$ неприводим ненулевой степени $u$. Тогда коэффициенты $g$ лежат в некотором поле $F_j \geq F_i$, где $F_j \neq F_i$. Пусть $Q = F_j(\alpha)$, где $\alpha$ — корень полинома $g(x)$. Тогда $|Q : F_j| = u < r$ и $|Q : F_i| = m_{i+1} \dots m_j u$ не делится на $r$. С другой стороны,

$$|Q : F_i| = |Q : F_i(\alpha)|\, |F_i(\alpha) : F_i|$$

делится на $r$; противоречие.

Предположим теперь, что $\gamma_r(F) = \infty$ и $F$ не является $r$-замкнутым. Пусть $f \in F[x]$ и $f$ неразложим над $F$ степени $r$. Все коэффициенты $f$ лежат в $F_i$ для некоторого числа $i$. Поэтому $f$ — неразложимый полином степени $r$ из $F_i[x]$. По предположению существует такое число $j$, что $|F_j : F_i|$ делится на $r$. Пусть $Q$ — подполе поля $F(\alpha)$, порожденное полями $F_j$ и $F_i(\alpha)$, где $\alpha$ — корень $f$. Тогда $Q$ конечно и поэтому $F_j$ содержит $F_i(\alpha)$. Но тогда $\alpha \in F$; противоречие. Лемма доказана.

**Следствие 1.** *Если $F$ — $r$-замкнутое локально конечное поле и $K$ — подполе $F$ такое, что степень расширения $|F : K|$ конечна, то $K$ также $r$-замкнуто.*

Обозначим через $F^*$ мультипликативную группу поля $F$.

**Следствие 2.** *Если $F$ — локально конечное $r$-замкнутое поле, то силовская $r$-подгруппа $F^*$ либо бесконечна, либо тривиальна.*

Доказательство. Предположим, что силовская $r$-подгруппа $F^*$ нетривиальна. Тогда существует такое $i$, что $|F_i^*|$ делится на $r$. По лемме 3 $\gamma_r(F) = \infty$ и, следовательно, существует такая бесконечная возрастающая последовательность $i_1, i_2, \dots, i_s \dots$, что $i < i_1$ и $m_{i_j} = r$ $(j = 1, 2, \dots)$. По лемме 2(б)

$$v_r(|F^*_{i_{j+1}}|/|F^*_{i_j}|) \geq 1$$

для всех $j$. Это показывает, что силовская $r$-подгруппа в $F^*$ бесконечна.

**Теорема 2.** *Пусть $F$ — локально конечное поле характеристики $p$.*

(а) *Если $F$ не является $r$-замкнутым для некоторого простого числа $r \neq p$, то силовские $r$-подгруппы в $\mathrm{GL}(n, F)$ конечны для любого натурального числа $n$.*

(б) *Если $F$ является $r$-замкнутым для некоторого простого числа $r$, то для любого натурального числа $n$ силовские $r$-подгруппы в $\mathrm{GL}(n, F)$ либо бесконечны, либо тривиальны.*

Доказательство. Сохраним введенные выше обозначения. Пусть $q_i = |F_i|$, $i = 1, 2, \dots$.

(а) Заметим вначале, что силовская $r$-подгруппа $R$ группы $F^*$ конечна. Действительно, если $R \neq 1$, то существует $i$, для которого $|F_i^*|$ содержит элемент порядка $r$. По лемме 3 существует такое число $j$, что степень расширения $|F_k : F_{k-1}|$ взаимно проста с $r$ для любого $k \geq j+1$. Пусть $l = \max\{i, j\}$. Тогда по лемме 2(б) $v_r((q_k - 1)/(q_{k-1} - 1)) = 0$ для любого $k > l$, поэтому $R$ содержится в $F_l$ и, следовательно, конечна.

Положим теперь $s_1 = \min\{i \in \mathbb{N} : F_i$ содержит силовскую $r$-подгруппу группы $F^*\}$. Для $j = 2, \dots, n$ положим $S_j = \{i \in \mathbb{N} : |F_i|^j - 1$ делится на $r\}$ и $s_j = \min\{i : i \in S_j\}$, если $S_j \neq \varnothing$, и $s_j = 1$, если $S_j = \varnothing$.

По лемме 3 $\gamma_r(F) < \infty$ и поэтому существует $t \in \mathbb{N}$ такое, что $m_j \neq r$ для всех $j > t$. Пусть $s_{n+1}$ — наименьшее среди всех таких $t$. Пусть $s = \max\{s_j : j = 1, 2, \dots, n+1\}$, $Q = F_s$ и $q = q_s$. По лемме 2(б)

$$v_r((q^{kj} - 1)/(q^j - 1)) = 0$$

для всех $k = |F_i : Q|$, где $i > s$ и $j = 1, 2, \dots, n$. Следовательно, $\mathrm{GL}(n, Q)$ содержит силовскую $r$-подгруппу группы $\mathrm{GL}(n, F)$, и поэтому силовская $r$-подгруппа в $\mathrm{GL}(n, F)$ конечна.

(б) Если $p = r$, то поле $F$ бесконечно, значит, силовские $r$-подгруппы в $\mathrm{GL}(n, F)$ бесконечны. Предположим, что $r \neq p$ и что силовская $r$-подгруппа в $\mathrm{GL}(n, F)$ нетривиальна. Тогда существует такое число $i$, что $\mathrm{GL}(n, F_i)$ содержит элемент порядка $r$ и поэтому $r$ делит $|F_i|^t - 1$ для некоторого $t \leq n$. По лемме 3 $\gamma_r(F) = \infty$ и, следовательно, существует бесконечная возрастающая последовательность $i_1, i_2, \dots, i_s \dots$ такая, что $i < i_1$ и $m_{i_j} = r$ $(j = 1, 2, \dots)$. По лемме 2(б)

$$v_r((|F_{i_{j+1}}|^t - 1)/(|F_{i_j}|^t - 1)) \geq 1$$

для всех $j$, так что $r$ делит $|\,\mathrm{GL}(n, F_{i_{j+1}}) : \mathrm{GL}(n, |F_{i_j})|$ для любого $j$. Отсюда вытекает, что силовские $r$-подгруппы в $\mathrm{GL}(n, F)$ бесконечны. Теорема доказана.

Следующий пример показывает, что обе возможности в п. (б) теоремы 2 реализуются даже в случае, когда силовская $r$-подгруппа в $F^*$ тривиальна.

Пример 1. (а) Пусть $F$ — объединение конечных полей порядков $5^{3^i}$, $i = 0, 1, \dots$. Тогда поле $F$ является 3-замкнутым, силовская 3-подгруппа в $F^*$ тривиальна, но силовская 3-подгруппа в $\mathrm{GL}(2, F)$ бесконечна.

(б) Пусть $F$ — объединение конечных полей порядков $3^{5^i}$, $i = 0, 1, \dots$. Тогда поле $F$ является 5-замкнутым и силовские 5-подгруппы в $\mathrm{GL}(2, F)$ тривиальны.

**Доказательство основного результата.** Этот пункт посвящен доказательству теоремы 1.

Пусть

$$m = (r_1 - 1) \dots (r_n - 1).$$

Тогда $r_i$ делит $p^m - 1$ для всех $i = 1, \dots, n$. Пусть $F_1$ — конечное поле порядка $r_0$, если $n = 0$, и порядка $r_0^m$, если $n > 0$. Положим $q_1 = |F_1|$. Пусть $p_1$ — простое число, которое больше, чем любой простой делитель числа $|L(F_1)|$. Пусть $F_2$ — поле порядка $q_2 = q_1^{p_1 r_1 \dots r_n}$. Пусть $p_2$ — простое число, которое больше, чем любой простой делитель числа $|L(F_2)|$, $F_3$ — поле порядка $q_3 = q_2^{p_2, r_1 \dots r_n}$, и т. д. Пусть $F$ — объединение полей $F_i$, $i = 1, 2, \dots$.

Очевидно, что для любого простого числа $r \notin S$ поле $F$ не является $r$-замкнутым. Поскольку $L(F)$ обладает конечномерным проективным представлением над $F$, силовские $r$-подгруппы в $L(F)$ конечны для $r \notin S$ по теореме 2.

Очевидно, что силовские $r_0$-подгруппы в $L(F)$ бесконечны. Пусть $r = r_i \neq r_0$. Тогда по лемме 2(б)

$$v_r((q_i - 1)/(q_{i-1} - 1)) \geq 1$$

для всех $i$ и поэтому $v(q_i - 1) \geq i$ для всех $i$.

Поскольку $|L(F_i)|$ делится на $(q_i - 1)/d_i$, где $d_i$ делит некоторое фиксированное натуральное число $d$, зависящее только от $L$ (см. [4, табл. 6]), имеем

$$v_r(|L(F_i)|) \geq i - v_r(d).$$

Отсюда вытекает, что силовские $r$-подгруппы в $L(F)$ бесконечны, и теорема 1 доказана.

Для бесконечных множеств $S$ теорема 1 не верна, как показывает следующий пример.

Напомним, что простое число $r$ называется *примитивным простым делителем* числа $p^n - 1$, если $r \mid (p^n - 1)$, но $r \nmid (p^m - 1)$ для всех $m = 1, 2, \dots, n-1$. По теореме Жигмонди [5] такой делитель существует для любого простого числа $p$ и любого $n$, исключая

(а) $p = 2, n = 6$,

(б) $p = 2^t - 1, n = 2$.

Пример 2. Положим $r_0 = 3$ и для любого $i \geq 1$ обозначим через $r_i$ примитивный простой делитель числа $3^{2^{i+1}} - 1$. Пусть $G = \mathrm{PSL}(2, F)$, где $F$ — локально конечное поле характеристики 3, и пусть $S = \{r_0, r_1, \dots\}$. Очевидно, $S$ — бесконечное множество, состоящее из нечетных чисел. Предположим, что $G$ содержит нетривиальные элементы порядков $r_i$ для всех $i = 1, 2, \dots$. Покажем, что силовская 2-подгруппа группы $G$ бесконечна. Действительно, если порядок элемента из $G$ равен $r_i$, то существует конечное подполе $F_i$ поля $F$ такое, что $r_i \mid |\mathrm{PSL}(2, F_i)|$ и поэтому $r_i \mid (3^{2l} - 1)$, где $|F_i| = 3^l$. По выбору $r_i$ число $l$ делится на $2^i$ и, следовательно, $2^i \mid (3^l - 1)$ по лемме 2(а). Отсюда вытекает, что силовские 2-подгруппы в $G$ бесконечны.

*ЛИТЕРАТУРА*

**1.** *Hartley B., Shute G.* Monomorphisms and direct limits of finite groups of Lie type // Quart. J. Math. (2). 1982. V. 33. P. 309–323.
**2.** *Brawley J., Schnibben G.* Infinite algebraic extensions of finite fields. Providence, RI: Amer. Math. Soc., 1989. (Contemp. Mathematics; V. 95).
**3.** *Dixon M. R.* Sylow theory, formations and Fitting classes in locally finite groups. Singapore: World Sci., 1994. (Ser. Algebra; V. 2).
**4.** *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. Oxford: Clarendon Press, 1985.
**5.** *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.

*Статья поступила 21 марта 2005 г.*

*M. Kuzucuoğlu*
*Department of Mathematics,*
*Middle East Technical University,*
*Ankara, 06531 Turkey*
matmah@metu.edu.tr

*Мазуров Виктор Данилович*
*Институт математики им. С. Л. Соболева СО РАН,*
*пр. Академика Коптюга, 4, Новосибирск 630090*
mazurov@math.nsc.ru