УДК 519.41/47

И. Д. Иванюта

Силовские p-подгруппы группы $U(q^2)$

В работе [1] описано строение силовских p-подгрупп предельной полной линейной группы $GL(q)$ над конечным полем $GF(q)$ из q элементов, когда p и q взаимно простые, $p \neq 2$. Теми же методами удается описать строение силовских p-подгрупп предельной унитарной группы $U(q^2)$ над конечным полем $GF(q^2)$ при указанных ограничениях на p и q. Группа $U(q^2)$ является объединением бесконечной цепи унитарных групп $U(n, q^2)$ конечных степеней над полем $GF(q^2)$ при естественном вложении $U(n, q^2)$, в $U(n + 1, q^2)$: матрица $a \in U(n, q^2)$ отождествляется с матрицей $\mathrm{diag}\,[a, 1] \in U(n+1, q^2)$. Строение силовских p-подгрупп группы $U(q^2)$ оказалось аналогичным строению силовских p-подгрупп группы $GL(q)$.

1. Силовские p-подгруппы классических линейных групп конечных степеней над конечным полем $GF(q)$ при p взаимно простом с q и $p \neq 2$ изучены в [2]. Пусть l — наименьшее из чисел, такое, что $q^l \equiv 1 \pmod p$, $q^l - 1 = p^r m$, $(p, m) = 1$. Рассматривая $GF(q^l)$ как l-мерное линейное пространство V_l над полем $GF(q)$, получаем естественное вложение мультипликативной группы поля $GF(q^l)$ в полную линейную группу $GL(l, q)$. Следовательно, группа $GL(l, q)$ содержит циклическую подгруппу (a) порядка $q^l - 1 = p^r m$, и элемент a перемещает все $q^l - 1$ ненулевые векторы пространства V_l одним циклом. Тогда $P_0 = (a^m)$ — силовская p-подгруппа группы $GL(l, q)$, и элемент a^m является произведением m независимых циклов одной и той же длины p^r. Пусть Z_p — циклическая подгруппа порядка p симметрической группы S_p степени p, $P_i = P_0 \wr Z_p \wr \ldots \wr Z_p$ — сплетение группы P_0 и i экземпляров группы подстановок Z_p. Предположим $n = \gamma + l\alpha$, $0 \leqslant \gamma < l$, $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_\nu p^\nu$, $0 \leqslant \alpha_i < p$, $i = 0, 1, 2, \ldots, \nu$. Тогда прямое произведение $\prod\limits_{i=0}^{\nu} P_i^{\alpha_i}$ является силовской p-подгруппой группы $GL(n, q)$.

Пусть $l = 2k$ четное. Если k нечетное, то силовская p-подгруппа группы $U(n, q^2)$ является силовской p-подгруппой группы $G(n, q^2)$. Из равенства $q^l - 1 = q^{2k} - 1 = p^r m$ следует, что k — наименьшее из чисел такое, что $(q^2)^k = 1 \pmod p$. Следовательно, циклическая подгруппа P_0 порядка p^r степени k группы $GL(k, q^2)$ является ее силовской p-подгруппой.

Предположим $n = \delta + k\alpha$, $0 \leqslant \delta < k$, $\alpha = \sum\limits_{i=0}^{\nu} \alpha_i p^i$, $0 \leqslant \alpha_i < p$, $i = 0, 1, 2, \ldots, \nu$. Тогда прямое произведение $\prod\limits_{i=0}^{\nu} P_i^{\alpha_i}$ является силовской p-подгруппой групп $U(n, q^2)$ и $GL(n, q^2)$.

Если k четное, то циклическая подгруппа P_0 порядка p^r степени l группы $U(l, q^2)$ является ее силовской p-подгруппой. Предположим $n = \gamma + l\alpha$, $0 \leqslant \gamma < l$, $\alpha = \sum\limits_{i=0}^{\nu} \alpha_i p^i$, $0 \leqslant \alpha_i < p$. Тогда $\prod\limits_{i=0}^{\nu} P_i^{\alpha_i}$ является силовской p-подгруппой группы $U(n, q^2)$.

Пусть l нечетное. В этом случае циклическая подгруппа P_0 порядка p^r степени $2l$ группы $U(2l, q^2)$ является ее силовской p-подгруппой. Если $n = \gamma + 2l\beta$, $0 \leqslant \gamma < 2l$, $\beta = \sum\limits_{i=0}^{\nu} \beta_i p^i$, $0 \leqslant \beta_i < p$, то прямое произведение $\prod\limits_{i=0}^{\nu} P_i^{\beta_i}$ является силовской p-подгруппой группы $U(n, q^2)$.

Пусть

$$s = \begin{cases} k, & \text{если } l = 2k \text{ четное, } k \text{ нечетное;} \\ l, & \text{если } l = 2k \text{ четное, } k \text{ четное;} \\ 2l, & \text{если } l \text{ нечетное,} \end{cases}$$

где l — наименьшее из чисел такое, что $q^l \equiv 1 \pmod p$, $q^l - 1 = p^r m$, $(p, m) = 1$.

Лемма 1. *Каждый неединичный элемент силовской p-подгруппы P_0 группы $U(s, q^2)$ перемещает все ненулевые векторы s-мерного линейного пространства V_s над полем $GF(q^2)$, и является произведением независимых циклов одной и той же длины p^μ, $1 \leqslant \mu \leqslant r$.*

Доказательство. Пусть $l = 2k$, k нечетное. Тогда силовская p-подгруппа P_0 группы $U(k, q^2)$ является силовской p-подгруппой группы $GL(k, q^2)$. Если $P_0 = (a)$, то элемент a, как отмечалось выше, является произведением m независимых циклов одной и той же длины p^r и перемещает все $q^{2k} - 1$ ненулевые векторы пространства V_k. Следовательно, любой неединичный элемент из P_0 является произведением независимых циклов одной и той же длины p^μ, где $1 \leqslant \mu \leqslant r$.

Пусть $l=2k$, k четное. Из равенства $(q^2)^k=p^r m$ следует, что k — наименьшее из чисел такое, что $(q^2)^k \equiv 1 \pmod p$. Следовательно, силовской p-подгруппой группы $GL(k,q^2)$ является циклическая группа (c_1) порядка p^r, и элемент c_1 является произведением m независимых циклов одной и той же длины p^r, а силовской p-подгруппой группы $GL(l,q^2)$ — прямое произведение $(c_1)\times(c_2)$ двух таких циклических групп порядков p^r. Силовская p-подгруппа P_0 группы $U(l,q^2)$ — циклическая группа порядка p^r. Покажем, что $P_0=(bd)$, где b и d — некоторые образующие групп (c_1) и (c_2) соответственно. Предположим, что P_0 порождается элементом bh, где $h\in(c_2)$, $h^{pj}=1$ при $j<r$. Тогда $(bh)^{p^j}=b^{p^j}\in P_0\cap GL(k,q^2)$, что невозможно, так как $|U(k,q^2)|=\prod\limits_{i=1}^{k} q^{\frac{k(k-1)}{2}}(q^i-(-1)^i)$ очевидно не делится на p.

Линейное пространство V_l представляется в виде прямой суммы $V_l=V_k\oplus V'_k$, где элемент b перемещает ненулевые векторы из V_k, а элемент d — ненулевые векторы из V'_k.

Обозначим через $L_1, L_2, \ldots, L_m$ области транзитивности элемента b, а через $L'_1, L'_2, \ldots, L'_m$ области транзитивности элемента d. Множество $L_i+L'_j$ векторов вида $u_i+u'_j$, где $u_i\in L_i$, $u'_j\in L'_j$, $i,j=1,2,\ldots,m$, состоящее из p^{2r} векторов, содержит p^r независимых циклов одной и той же длины p^r элемента bd. Число множеств $L_i+L'_j$ равно m^2. Таким образом, элемент bd является произведением $2m+p^r m^2$ независимых циклов одной и той же длины p^r, и перемещает $p^r(2m+p^r m^2)=q^{2l}-1$ векторов из V_l, т. е. перемещает все нулевые векторы пространства V_l.

Пусть l нечетное. Тогда $|GL(l,q^2)|=q^{l(l-1)}\prod\limits_{i=1}^{l}(q^{2i}-1)$, из множителей произведения только $q^{2l}-1=p^r m(q^l+1)$ делится на p. Следовательно, силовской p-подгруппой группы $GL(l,q^2)$ является циклическая подгруппа (c_1) порядка p^r, где c_1 — произведение $m(q^l+1)$ независимых циклов одной и той же длины p^r. Прямое произведение $(c_1)\times(c_2)$ таких циклических групп порядков p^r является силовской p-подгруппой группы $GL(2l,q^2)$. Силовская p-подгруппа P_0 группы $U(2l,q^2)$-циклическая группа порядка p^r. Как и выше, можно показать, что $P_0=(bd)$, где b и d — некоторые образующие групп (c_1) и (c_2), элемент bd является произведением независимых циклов одной и той же длины p^r и перемещает все ненулевые векторы пространства V_{2l}.

Естественно, вкладывая P_n в P_{n+1}, получаем возрастающую цепь групп $P_0\subset P_1\subset P_2\subset \ldots$, объединение которой обозначим через P.

2. Силовские p-подгруппы группы $U(q^2)$ можно строить следующим образом. Пусть $l=2k$ четное, k нечетное. Представим бесконечномерное линейное пространство V над полем $GF(q^2)$ в виде прямой суммы следующих подпространств: γ экземпляров одномерных подпространств, $0\leqslant\gamma<k$ (если $k>1$), α_i экземпляров kp^i-мерных подпространств, $0\leqslant\alpha_i<p$, $i=0, 1, 2, \ldots$, не более чем счетное множество J бесконечномерных подпространств. В унитарных группах указанных kp^i-мерных подпространств берем по одной силовской p-подгруппе (они подобны P_i), а в унитарных группах бесконечномерных подпространств — по одной силовской p-подгруппе $P^{(j)}$, подобной P. Прямое произведение $\prod\limits_{i=0}^{\infty} P_i^{\alpha_i}\times\prod\limits_{j\in J} P^{(j)}$ выбранных групп и будет силовской p-подгруппой группы $U(q^2)$. (P_0 — циклическая группа порядка p_r степени k).

Пусть $l=2k$ четное, k четное. Представим V в виде прямой суммы следующих подпространств: γ экземпляров одномерных подпространств, $0\leqslant\gamma<l$, α_i экземпляров lp^i-мерных подпространств, $0\leqslant\alpha_i<p$, $i=0, 1, 2, \ldots$, не более чем счетное множество J бесконечномерных подпространств. В унитарных группах указанных подпространств выбираем по

по одной силовской p-подгруппе. Их прямое произведение $\prod\limits_{i=0}^{\infty} P_i^{\alpha_i} \times \prod\limits_{j\in J} P^{(j)}$ является силовской p-подгруппой группы $U(q^2)$. Отметим, что здесь P_0- циклическая группа порядка p^r степени l.

Пусть l нечетное. Представим V в виде прямой суммы γ экземпляров одномерных подпространств, $0 \leqslant \gamma < 2l$, α_i экземпляров $2lp^i$-мерных подпространств, $0 \leqslant \alpha_i < p$, не более чем счетное множество J бесконечномерных подпространств. Аналогично получим, что прямое произведение $\prod\limits_{i=0}^{\infty} P_i^{\alpha_i} \times \prod\limits_{j\in J} P^{(j)}$ является силовской p-подгруппой группы $U(q^2)$. Здесь P_0— циклическая группа порядка p^r степени $2l$.

Таким образом, справедливо следующее утверждение.

Лемма 2. *Прямое произведение*

$$\prod_{i=0}^{\infty} P_i^{\alpha_i} \times \prod_{j\in J} P^{(j)}, \tag{1}$$

где $P_i^{\alpha_i}$ — прямое произведение α_i экземпляров групп P_i, $0 \leqslant \alpha_i < p$, $i = 0, 1, 2, \ldots$, для каждого $j \in J$ группа $P^{(j)}$ изоморфна P, множество J не более чем счетно, причем если $J = \varnothing$, то множество тех i, для которых $\alpha_i > 0$, бесконечно, является силовской p-подгруппой группы $U(q^2)$.

Доказательство аналогично доказательству леммы 2 из [1].

3. Указанными в лемме 2 группами исчерпываются все силовские p-подгруппы группы $U(q^2)$.

Теорема 1. *Пусть R — произвольная силовская p-подгруппа группы $U(q^2)$. Тогда R имеет вид* (1).

Под импримитивностью произвольной линейной группы G линейного пространства V будем понимать некоторую эквивалентность θ на V такую, что для $u, v \in V$, $u \equiv v \pmod{\theta}$ имеем $ug \equiv vg \pmod{\theta}$ для всех $g \in G$. Соответствующие классы эквивалентности — это системы импримитивности группы G. Импримитивность группы G будем называть конечной и однородной, если все системы импримитивности — линейные подпространства пространства V одинаковой конечной размерности. Это число назовем рангом импримитивности. Будем говорить, что G действует на V эффективно, если каждый ненулевой вектор перемещается по крайней мере одним элементом из G.

Из строения силовских p-подгрупп группы $U(n, q^2)$ следует лемма.

Лемма 3. *Если R — p-подгруппа группы $U(n, q^2)$, действующая эффективно на пространстве V_n, то R обладает на V_n по крайней мере одной однородной импримитивностью ранга s, указанного в лемме* 1.

Лемма 4. *Если R — некоторая p-подгруппа группы $U(q^2)$, действующая эффективно на V, то она обладает на V по крайней мере одной однородной импримитивностью ранга s из леммы* 1.

Доказательство. Пусть $\Phi = \{R_\alpha\}$ — множество всех конечных подгрупп из R. Множество Φ частично упорядочено по включению: $R_\alpha \subseteq R_\alpha$.

Пусть $s = k$, $l = 2k$ четное, k нечетное. В этом случае силовские p-подгруппы группы $U(n, q^2)$ являются силовскими p-подгруппами группы $GL(n, q^2)$, следовательно, утверждение следует из аналогичной леммы 4 работы [1].

Пусть $s = l = 2k$, k четное. Пусть T_α — подпространство V, на котором R_α действует эффективно. T_α обладает по крайней мере одной однородной импримитивностью ранга l на T_α. Пусть $A_\alpha = \{\theta_\alpha\}$ — всевозможные такие импримитивности R_α.

Рассмотрим R_α и R_β из Φ такие, что $R_\alpha \subset R_\beta$. Очевидно $T_\alpha \subset T_\beta$. Отметим следующий важный факт. В импримитивности $\theta_\beta \in A_\beta$ группы R_β в одной системе не могут быть векторы из T_α и векторы, не лежащие в T_α, т. е. $u \not\equiv v \pmod{\theta_\beta}$ для всех $\theta_\beta \in A_\beta$, если $u \in T_\alpha$, $v \notin T_\alpha$, $v \in T_\beta$, так как в противном случае элементы из R_α, оставляя на месте v, оставлял бы на месте u, что противоречит определению R_α. Действительно, любой элемент из R_α, переводя систему импримитивности в себя, либо все ее векторы оставляет на месте, либо все ненулевые векторы перемещает независимыми циклами длины p^μ, $1 \leqslant \mu \leqslant r$.

Система Ψ конечных множеств A_α, A_β, ... станет частично упорядоченной, если положим $A_\alpha \leqslant A_\beta$ при $R_\alpha \subseteq R_\beta$. Если $A_\alpha \leqslant A_\beta$, то отображение множества A_β в множество A_α — ограничение θ_β на пространстве T_α.

Легко проверить условия существования в Ψ полного проекционного множества. Иными словами, в каждом из множеств A_α можно так выбрать по одной импримитивности, что любые два из них будут содержаться в некоторой третьей, являющейся общим прообразом первых двух.

Полное проекционное множество является импримитивностью группы R, поскольку $\bigcup\limits_\alpha R_\alpha = R$.

При $s = 2l$ доказательство аналогично.

Доказательство теоремы 1 аналогично доказательству соответствующей теоремы работы [1] с использованием леммы 4.

Следствие. *При $l = 2k$, k нечетном силовские p-подгруппы группы $U(q^2)$ являются силовскими p-подгруппами группы $GL(q^2)$.*

Теорема 2. *Пусть Q и R — силовские p-подгруппы группы $U(q^2)$, причем*

$$Q = \prod_{i=0}^{\infty} P_i^{\alpha_i} \times \prod_{j \in J} P^{(j)}, \quad R = \prod_{i=0}^{\infty} P_i^{\beta_i} \times \prod_{\gamma \in \Gamma}^{(\gamma)}.$$

Группы Q и R изоморфны тогда и только тогда, когда $\alpha_i = \beta_i$, $i = 0, 1, 2, \ldots$ и множества J и Γ равномощны.

Доказательство аналогично доказательству теоремы 2 из [1].

1. *Иванюта И. Д.* Силовские p-подгруппы группы $GL(q)$ // Укр. мат. журн.— 1980.— **32**, № 6.— С. 813—818.
2. *Weir A. J.* Sylow n-subgroups of the classical groups over finite fields with characteristic prime to p // Proc. Amer. Math. Soc.— 1955.— **6**, N 4.— P. 529—533.

Киев. автомоб.-дор. ин-т

Получено 03.06.87