УДК 512.542

Г.В. Пастухова

ОПИСАНИЕ ОДНОГО КЛАССА КОНЕЧНЫХ ГРУПП

Доказаны две леммы о свойствах централизатора элемента в конечной группе, с помощью которых в дальнейшем описаны неабелевы группы порядка 2^3p с условием нормальности своей силовской p-подгруппы.

Ключевые слова: *конечная группа, силовская подгруппа, централизатор элемента.*

Классификационная задача Кэли, которая заключается в том, чтобы дать полную классификацию всех групп, порядки которых равны заданному натуральному числу n, решаема по двум направлениям. Первое – это фиксирование порядка и изучение неабелевой группы, исходя или из размеров центра, или нормальности силовской подгруппы, или иных характеристик группы, абелевы же конечные группы имеют полное описание. Для решения этой задачи привлекается различные математические пакеты, которые имеют богатую библиотеку конечных групп. Например, система GAP 4.5.4 включает в себя группы порядка не более 2000, за исключением групп порядка 1024, и всего рассмотрены 423 164 062 группы. Второе направление – это рассмотрение целого класса групп порядка n с определенным каноническим разложением ее порядка. Так, например, известно, что если n – простое число, то существует единственная группа такого порядка. Классический пример описания групп порядка $n = pq$, где p и q – различные простые числа, реализован с помощью теорем Силова [1, с. 101]. Проблема в общем случае не имеет рационального решения, в связи с чем она на сегодняшний день претерпела некоторые изменения, например, описание группы порядка ap, где a – некоторый множитель (в общем случае не являющийся простым числом) и такой, что $(a,p) = 1$.

Опишем группы порядка 2^3p с условием нормальности своей силовской p-подгруппы. Заметим, что порядок 2^3 первый представил всю линейку групп. С таким порядком имеют место помимо существующей для любого порядка циклическая и две абелевых нециклических групп, и две неабелевых. В связи в этим описание этих групп является традиционной задачей при изучении групп и встречается в классических сборниках задач [3, с. 239].

Рассмотрим леммы о свойстве 2-элемента конечной группы и о делимости порядка группы, с помощью которых в дальнейшем опишем вышеупомянутые группы.

Лемма 1. Если x – такой 2-элемент конечной группы, что β – наименьшее с условием $x^{2^\beta} \in C_H(a)$, то $x^{-2^{\beta-1}}ax^{2^{\beta-1}} = a^{-1}$.

Доказательство. Так как $\langle a\rangle \trianglelefteq H$, то $x^{-1}ax \in \langle a\rangle$, то есть существует такое r целое положительное, что $x^{-1}ax = a^r$. Тогда

$$x^{-2}ax^2 = x^{-1}(x^{-1}ax)x = x^{-1}a^r x = \underbrace{(x^{-1}ax)...(x^{-1}ax)}_{r\ раз} = \underbrace{a^r...a^r}_{r\ раз} = (a^r)^r = a^{r^2}.$$

Индукцией по k показывается, что $x^{-k}ax^{k}=a^{r^{k}}$. Так как $x^{-2^{\beta}}ax^{2^{\beta}}=a^{r^{2^{\beta}}}=a$, то $r^{2^{\beta}}\equiv 1(\mathrm{mod}\,p)$. Это сравнение равносильно $(r^{2^{\beta-1}})^{2}\equiv 1(\mathrm{mod}\,p)$ и $r^{2^{\beta-1}}$ – решение сравнения *t*. Поэтому $r^{2^{\beta-1}}\equiv \pm 1(\mathrm{mod}\,p)$. Предположим, что $r^{2^{\beta-1}}\equiv 1(\mathrm{mod}\,p)$. Тогда $x^{-2^{\beta-1}}ax^{2^{\beta-1}}=a^{r^{2^{\beta-1}}}=a$, что противоречит выбору *x*. Следовательно, $x^{-2^{\beta-1}}ax^{2^{\beta-1}}=a^{-1}$. Лемма доказана.

Лемма 2. Если *P* – циклическая группа порядка *p*, то $N_G(P)/C_G(P)$ – циклическая и порядок *r* группы $N_G(P)/C_G(P)$ делит $p-1$.

Доказательство. Сначала докажем следующий факт: *Для любой подгруппы H группы G* $N_G(N)/C_G(N)\tilde{\to} Aut\,H$. Заметим, что $N_G(H)$ можно гомоморфно вложить в *AutH*. Действительно, произвольный элемент *a* из $N_G(H)$ индуцирует некоторый автоморфизм *c*(*a*) из *AutH*, то есть для любых $x,y\in H$ имеем $(xy)^{c(a)}=x^{c(a)}y^{c(a)}$.

Найдем ядро этого гомоморфизма: *ker c* = $\{\,a\in N_G(H)|c(a)$ – тождественный автоморфизм$\}$. Покажем, что $ker\,c=C_G(H)$. Действительно, для любого $a\in ker\,c$ и любого $x\in H$ имеем, что $x^{c(a)}=x^{a}=x$, то есть $a\in C_G(H)$. Значит, $ker\,c=C_G(H)$. Следовательно, по теореме о гомоморфизмах, $N_G(P)/C_G(P)\tilde{\to} Aut\,H$.

Пусть теперь *P* – циклическая группа порядка *p*. Тогда по только что доказанному $N_G(P)/C_G(P)$ – циклическая и изоморфно вкладывается в *Aut P*, где $Aut\,P\tilde{\to} Z_{p-1}$. Это значит, что $N_G(P)/C_G(P)$ можно считать подгруппой группы Z_{p-1} порядка *p*–1. Значит, порядок $N_G(P)/C_G(P)$ делит *p*–1. Лемма доказана.

Теорема. Пусть *H* – неабелева группа порядка 2^3p, силовская *p*-подгруппа *P* группы *H* – нормальна в *H*. Тогда *H* изоморфна одной из следующих групп:

1. $H=\langle a\rangle\leftthreetimes\langle b\rangle, o(a)=p, o(b)=8, b^{-1}ab=a^{r}, r^{i}\not\equiv 1(\mathrm{mod}\,p)$, где $1\le i<8$, $p\equiv 1(\mathrm{mod}\ 8)$.
2. $H=\langle a\rangle\leftthreetimes\langle b\rangle, o(a)=p, o(b)=8, b^{-1}ab=a^{r}, r^{i}\not\equiv 1(\mathrm{mod}\,p)$, где $1\le i<4$, $ab^{4}=b^{4}a,\ \ p\equiv 1(\mathrm{mod}\,4)$.
3. $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle,\ o(a)=p,\ o(b)=4,\ o(c)=2,\ bc=cb,\ b^{-i}ab^{i}=a^{r^{i}}$, $r^{i}\equiv 1(\mathrm{mod}\,p)$, где $1\le i<4, p\equiv 1(\mathrm{mod}\,4)$.
4. $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle, o(a)=p, o(b)=4, o(c)=2, b^{-1}ab=a^{-1}, ab^{2}=b^{2}a, bc=cb$.
5. $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle, o(a)=p, o(b)=4, o(c)=2, c^{-1}ac=a^{-1}, bc=cb$.
6. $H=(\langle a\rangle\times\langle b\rangle\times\langle c\rangle)\leftthreetimes\langle d\rangle, o(a)=p, o(b)=o(c)=o(d)=2,\ d^{-1}ad=a^{-1}$, $bd=db,\ \ cd=dc$.
7. $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle, o(a)=p, o(b)=4, b^{-1}ab=a^{-1}, ab^{2}=b^{2}a, c^{-1}bc=b.$

Доказательство. Конструирование группы основывается на *лемме Фраттини*: пусть *K* – нормальная подгруппа группы *H* и $P\in Syl_p(H)$, тогда $H=N_H(P)K$

[1, с. 115].Обозначим через a образующий элемент подгруппы $P: P=\langle a\rangle$. Рассмотрим всевозможные случаи:

Случай 1. $S=\langle b\rangle$ – циклическая группа. Тогда $H=\langle a\rangle \rtimes \langle b\rangle$.

Случай 1.1. $|C_H(a)|=p$. Покажем, что в этом случае $p\equiv 1(\mathrm{mod}\, 8)$ и если $b^{-1}ab=a^r$, то $r^i\neq 1(\mathrm{mod}\, p)$, при никаких *i*, что $1\le i<8$, а $r^8=1(\mathrm{mod}\, p)$.

Допустим, для некоторого *i*, такого, что $1\le i<8$, имеем $r^i\equiv 1(\mathrm{mod}\, p)$. Это означает, что $b^{-i}ab^i=a^{r^i}=a$ и $b^i\in C_H(a)$, причём $b^i\neq e$. Это противоречит тому, что $|C_H(a)|=p$. Далее, $|a^H|=8$, причём $a^H=\{a,a^r,a^{r^2},...,a^{r^7}\}$. Действительно, если предположить, что для некоторых $i\neq j$, $a^{r^i}=a^{r^j}$, то это будет означать, что $r^i\equiv r^j(\mathrm{mod}\, p)$, что равносильно $(r^j(r^{i-j}-1))\equiv 0(\mathrm{mod}\, p)$, причём можно считать, что $i>j$. Это невозможно, так как $r\neq 0$ и $r^{i-j}\not\equiv 1(\mathrm{mod}\, p)$. Аналогично показывается, что для любой степени a^k, $(a^k)^H=\{a^k,a^{kr},a^{kr^2},...,a^{kr^7}\}$.

Следовательно, $\langle a\rangle=\{e\}\cup\{a,a^r,a^{r^2},...,a^{r^7}\}\cup\{a^k,a^{kr},a^{kr^2},...,a^{kr^7}\}\cup\ldots$. Это означает, что $|\langle a\rangle|=p=1+8l$, где l – число неединичных сопряжённых классов.

Таким образом,

$$H=\left\langle a,b\mid a^p=b^8=e, b^{-1}ab=a^r, r^i\not\equiv 1(\mathrm{mod}\, p), 1\le i<8, p=1(\mathrm{mod}\, 8)\right\rangle.$$

Случай 1.2. $|C_H(a)|=2p$.

Покажем, что в этом случае $p\equiv 1(\mathrm{mod}\, 4)$ и из $b^{-1}ab=a^r$ вытекает, что 4 – наименьшее *i*, такое, что $r^i\equiv 1(\mathrm{mod}\, 4)$. Действительно, аналогично предыдущему случаю, если $i<4$ и $r^i\equiv 1(\mathrm{mod}\, 4)$, то $b^{-i}ab^i=a$ и $b^i\in C_H(a)$. Это означает, что или *b*, или $b^2\in C_H(a)$. Тогда 4 делит $|C_H(a)|$, что противоречит условию. Как и в предыдущем случае, доказывается, что $\langle a\rangle=\{e\}\cup\{a,a^r,a^{r^2},a^{r^3}\}\cup\ldots$ $\ldots\cup\{a^k,a^{kr},a^{kr^2},a^{kr^3}\}\cup\ldots$ и $|\langle a\rangle|=p=1+4t$, где t – число классов сопряжённых неединичных элементов группы.

Таким образом,

$$H=\left\langle a,b\mid a^p=b^8=e, b^{-1}ab=a^r, b^{-4}ab^4=a, r^i\not\equiv 1(\mathrm{mod}\, p), 1\le i<4, p\equiv 1(\mathrm{mod}\, 4)\right\rangle.$$

Случай 1.3. $|C_H(a)|=4p$.

Аналогично доказывается, что $H=\left\langle a,b\mid a^p=b^8=e, b^{-1}ab=a^r, b^{-2}ab^2=a\right\rangle$. Так как H – неабелева, то случай $|C_H(a)|=8p$ невозможен.

Случай 2. $S=\langle b\rangle\times\langle c\rangle$, где $o(b)=4, o(c)=2$. Тогда $H=\langle a\rangle\rtimes(\langle b\rangle\times\langle c\rangle)$.

Для любого $s\in S$, такого, что $o(s)=2$, имеем $s^{-1}as=a^{-1}$. Поэтому $(b^2c)^{-1}a(b^2c)=c^{-1}(b^{-2}ab^2)c=c^{-1}a^{-1}c=a$ и $b^2c\in C_H(a)$, причём $o(b^2c)=2$. Поэтому либо $|C_H(a)|=2p$, либо $|C_H(a)|=4p$.

Случай 2.1. $|C_H(a)|=2p$. Тогда $b\notin C_H(a)$. Допустим, $b^2\in C_H(a)$. Так как $b^{-2}ab^2=a^{-1}$ и $c^{-1}ac=a^{-1}$, то $(b^2c)^{-1}a(b^2c)=a$ и e,b^2,b^2c – элементы из S, входят в $C_H(a)$. Но e, b^2, b^2c – элементы подгруппы четвёртого порядка группы S: $\langle b^2\rangle\times\langle c\rangle$. Поэтому $\langle b^2\rangle\times\langle c\rangle \le C_H(a)$, что невозможно по условию. Это означает, что $\langle b\rangle \cap C_H(a)=\langle e\rangle$, и поэтому $C_H(a)=\langle a\rangle\times\langle c\rangle$. Таким образом, $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle$, где $bc=cb, b^{-i}ab^i=a^{r^i}$, при всех $i=1, 2, 3$ и $p\equiv 1(\mathrm{mod}\, 4)$. Это вытекает аналогично случаю 1.2.

Случай 2.2. $|C_H(a)|=4p$.

Случай 2.2.1. Допустим $b\notin C_H(a)$, но $b^2\in C_H(a)$.

Тогда $\langle b^2\rangle\times\langle c\rangle\le C_H(a)$ и $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle, b^{-1}ab=a^{-1}, ab^2=b^2a$ и $bc=cb$.

Случай 2.2.2. Пусть $b\in C_H(a)$.

Тогда $\langle b\rangle\le C_H(a)$ и $H=(\langle a\rangle\times\langle b\rangle)\leftthreetimes\langle c\rangle, c^{-1}ac=a^{-1}, bc=cb$. Как и в предыдущем случае, $|C_H(a)|=8p$ невозможно.

Случай 3. $S=\langle b\rangle\times\langle c\rangle\times\langle d\rangle$, где $o(b)=o(c)=o(d)=2$.

Случай 3.1. $|C_H(a)|=p$.

Так как $b^{-1}ab=a^{-1}, c^{-1}ac=a^{-1}$, то $(bc)^{-1}a(bc)=c^{-1}(b^{-1}ab)c=c^{-1}a^{-1}c=a$ и $bc\in C_H(a)$ – невозможно.

Случай 3.2. $|C_H(a)|=2p$. Можем считать, что $\langle b\rangle\le C_H(a)$. Тогда $c,d\notin C_H(a)$ и, как и в случае 3.1, $(cd)^{-1}a(cd)=d^{-1}(c^{-1}ac)d=d^{-1}a^{-1}d=a$, то есть $cd\in C_H(a)$ и $\langle b\rangle\times\langle cd\rangle\le C_H(a)$, то есть 4 делит $|C_H(a)|$ – противоречие.

Случай 3.3. $|C_H(a)|=4p$. Можем считать, что $\langle b\rangle\times\langle c\rangle\le C_H(a)$. Тогда, очевидно, $H=(\langle a\rangle\times\langle b\rangle\times\langle c\rangle)\leftthreetimes\langle d\rangle, d^{-1}ad=a^{-1}, bd=db, cd=dc$.

Случай 4. $S=\langle b\rangle\leftthreetimes\langle c\rangle$ – неабелева группа. Тогда $H=\langle a\rangle\times S$ или $H=\langle a\rangle\leftthreetimes S$.

Первая возможность однозначна. Рассмотрим вторую возможность: $H=\langle a\rangle\leftthreetimes S$. Как мы выше заметили (в случае 2), $(b^2c)^{-1}a(b^2c)=a$, поэтому либо $|C_H(a)|=2p$, либо $|C_H(a)|=4p$.

Случай 4.1. $|C_H(a)|=2p$. В этом случае, дословными рассуждениями, как и в случае 2.1, приходим к тому, что $\langle b\rangle\cap C_H(a)=\langle e\rangle$ и $C_H(a)=\langle a\rangle\times\langle c\rangle$. Тогда $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle$, причем $c^{-1}bc=b^{-1}, b^iab^i=a^{r^i}$, на i и p налагаются такие же условия, как и в случае 2.1.

Случай 4.2. $|C_H(a)|=4p$. Здесь возможны два случая:

Случай 4.2.1. Допустим, $b\notin C_H(a)$, но $b^2\in C_H(a)$. Тогда $\langle b^2\rangle\times\langle c\rangle\le C_H(a)$ и $H=(\langle a\rangle\times\langle c\rangle)\leftthreetimes\langle b\rangle, b^{-1}ab=a^{-1}, ab^2=b^2a$ и $b^{-1}cb=c$.

Случай 4.2.2. Пусть $b\in C_H(a)$.

Тогда $\langle b\rangle\le C_H(a)$ и $H=(\langle a\rangle\times\langle b\rangle)\leftthreetimes\langle c\rangle, c^{-1}ac=a^{-1}, c^{-1}bc=b^{-1}$. Случай, когда $|C_H(a)|=8p$, уже отмечен.

Случай 5. $S \cong Q_8$ – группа кватернионов.

$$Q_8 = \left\langle b,c \mid b^4 = c^4 = e,\ b^2 = c^2,\ c^{-1}bc = b^{-1} \right\rangle .$$

Пусть $b^{-1}ab = a^r$ и $c^{-1}ac = a^t$ для некоторых целых положительных r и t. Они являются решениями сравнений $r^2 \equiv 1(\operatorname{mod} p)$ и $t^2 \equiv 1(\operatorname{mod} p)$, так как $b^{-2}ab = a^{r^2}$ и $c^{-2}ac = a^{t^2}$. Значит $r \equiv t(\operatorname{mod} p)$. Тогда $a^t = a^r$, что равносильно, в этом случае либо $|C_H(a)| = 2p$, либо $|C_H(a)| = 4p$.

Покажем, что в $|C_H(a)|$ существует подгруппа порядка H. Если это не так, то $b^{-1}ab = c^{-1}ac = a^{-1}$ и снова получаем, что $bc^{-1} \in C_H(a)$. Но $(bc^{-1})(bc^{-1}) = = b(c^{-1}bc)c^{-2} = bb^{-1}b^2 = b^2$ и $o(bc^{-1}) = 4$. Это означает, что в $C_H(a)$ существует подгруппа порядка 4. Можно считать, что $b \in C_H(a)$ и тогда $H = (\langle a\rangle \times \langle b\rangle) \rtimes \langle c\rangle$, где $c^{-1}bc = b^{-1}, c^{-1}ac = a^r, r^i \not\equiv 1(\operatorname{mod} p)$ при $i = 1,2,3$ $p \equiv 1(\operatorname{mod} 4)$. Теорема доказана.

ЛИТЕРАТУРА

1. *Каргаполов М.И.*, *Мерзляков Ю.И.* Основы теории групп. М.: Наука, 1982.
2. *Курош А.Г.* Теория групп. М.: Наука, 1962.
3. *Сборник* задач по алгебре / под. ред. А.И. Кострикина: учебник для вузов. М.: ФИЗМАТЛИТ, 2001.

Статья поступила 28.11.2011 г.

Pastuhova G.V. DESCRIPTION OF A CLASS OF FINITE GROUPS.

The Cayley classification problem, which is to give a complete classification of all groups whose orders are equal to a given natural number n, is solved in two ways. First, it is order fixing and studying non-Abelian groups proceeding from the size of the center or from a normality of a Sylow subgroup or other characteristics of the group.

The second direction is to consider the whole class of groups of order n with a certain canonical decomposition of its order. For example, we know that if n is a prime number, there exists a unique group of this order. A classical example of the description of groups of order n = pq, where p and q are different prime numbers, is implemented using Sylow theorems. The problem in the general case has no rational solutions; at present, in connection with this, it has undergone some changes. One of new formulations is as follows: to describe groups of order ap, where a is a factor (in the general case, not prime) such that $(a, p) = 1$.

The author describes a group of order with the condition of normality of its Sylow p-subgroup. Note that the order 23 is the first one that presents the full range of groups. In addition to a cyclic group, which exists for any order, this order is inherent to two Abelian noncyclic groups and two non-Abelian groups.

Keywords: finite group, Sylow subgroup, centralizer of the elements.

Pastuhova Galina Vitalyevna (M. Sc, Perm State Humanitarian Pedagogical University, Perm, Moscow State Pedagogical University, Moscow, Russian Federation)
E-mail: pastuhova13@yandex.ru

REFERENCES

1. Kargapolov M.I., Merzlyakov Yu.I. Osnovy teorii grupp. Moscow, Nauka Publ., 1982. (in Russian)
2. Kurosh A.G. Teoriya grupp. Moskow, Nauka Publ., 1962. (in Russian)
3. Sbornik zadach po algebre / pod. red. A.I. Kostrikina. Moscow, Fizmatlit Publ., 2001. (in Russian)