Math-Net.Ru

Общероссийский математический портал

В. П. Буриченко, О группах, элементы малых порядков которых порождают малую подгруппу, *Матем. заметки*, 2012, том 92, выпуск 3, 361–367

DOI: <https://doi.org/10.4213/mzm8972>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.205.19.152

26 апреля 2023 г., 11:47:04

О группах, элементы малых порядков которых порождают малую подгруппу

В. П. Буриченко

Показано, что любая конечная группа G может быть представлена как факторгруппа некоторой конечной группы K такой, что все элементы “небольших” примарных порядков в K порождают абелеву нормальную подгруппу.

Библиография: 5 названий.

1. Введение. Пусть A – конечная абелева группа, $m = \exp(A)$ – ее экспонента, т.е. наименьшее натуральное число такое, что $x^m = 1$ для всех $x \in A$. Тогда для любого собственного делителя $n \mid m$, $n < m$ множество $\{x \in A \mid x^n = 1\}$ является собственной подгруппой в A . Однако для произвольной группы это совершенно неверно. Например, если G – конечная простая группа, порядок которой делится на простое число p , то подгруппа $\langle x \mid x \in G, x^p = 1 \rangle$ совпадает со всей G . Вообще, чем дальше группа от разрешимости, тем менее вероятно, что элементы фиксированого “небольшого” порядка порождают собственную подгруппу.

Беркович и Казарин поставили следующий вопрос [1; вопрос 5.1].

ВОПРОС 1. Предположим, что все элементы простых порядков и порядка 4 в конечной группе G содержатся в $\Phi(G)$. Верно ли, что G разрешима?

Отметим, что в [2] были построены примеры групп, у которых все элементы простого порядка, но не порядка 4, лежат в $\Phi(G)$, но G не разрешима.

Кроме того, в [3] содержится следующий вопрос.

ВОПРОС 2 (Зеленюк). Верно ли, что для каждой конечной группы G имеется конечная группа F и сюръективный гомоморфизм $f: F \rightarrow G$ такие, что для каждой нетривиальной подгруппы H группы F ограничение $f|_H$ не инъективно? (см. [3; вопрос 17.50]).

Мы докажем следующую теорему.

ТЕОРЕМА 1. Пусть G – конечная группа, $\pi(G) = \{p_1, \dots, p_k\}$ есть множество простых делителей ее порядка $|G|$ и $b_1, \dots, b_k$ – неотрицательные целые числа. Тогда существуют конечная группа K и ее нормальная подгруппа $N \triangleleft K$ такие, что

- (1) N абелева и $K/N \cong G$;
- (2) $\pi(K) = \pi(G)$;
- (3) любой элемент из K порядка p_i^c , где $1 \leq i \leq k$ и $0 \leq c \leq b_i$, лежит в N .

Покажем, что из этой теоремы следует отрицательный ответ на вопрос 1. Пусть G есть неабелева конечная простая группа, например, $G = A_5$, и $\pi(G) = \{p_1, \dots, p_k\}$, причем $p_1 = 2$. Возьмем $b_1 = 2$, $b_2 = \dots = b_k = 1$. Пусть K и N – группы, существующие согласно теореме. Возьмем подгруппу $L \subseteq K$, минимальную среди подгрупп, удовлетворяющих условию $NL = K$, и пусть $Q = N \cap L$. Тогда $L/Q \cong G$, в частности L , неразрешима. Кроме того, любой элемент из L порядка p_i^c с $c \leq b_i$ лежит в N , а потому и в Q . Осталось показать, что $Q \subseteq \Phi(L)$.

Допустим, что это не так. Тогда существует максимальная подгруппа $M \subset L$, не содержащая Q . Поскольку $Q \triangleleft L$, то QM – подгруппа, а поскольку $Q \not\subseteq M$, QM содержит M собственным образом и потому должна совпадать с L . Теперь имеем

$$NM = (NQ)M = N(QM) = NL = K.$$

Получили противоречие с выбором подгруппы L . Этим включение $Q \subseteq \Phi(L)$ доказано.

Покажем, что из теоремы 1 следует положительный ответ на вопрос 2. Пусть G – любая конечная группа; возьмем $b_1 = \dots = b_k = 1$, и пусть K, N – группы, существующие согласно теореме. Положим $F = K$, и пусть $f: F = K \rightarrow G$ – эпиморфизм с ядром N . Любой элемент простого порядка из F лежит в N ; значит, любая нетривиальная подгруппа $H \subseteq F$ нетривиально пересекает N , поэтому ограничение $f|_H$ не инъективно.

В следующем пункте мы напомним необходимые сведения о когомологиях, а в п. 3 докажем теорему 1.

2. Предварительные сведения о когомологиях. В этом пункте мы напомним наиболее элементарные сведения о расширениях и 2-когомологиях групп.

Пусть G есть группа, M – G -модуль (т.е. $\mathbf{Z}G$ -модуль). Под 2-коцепью понимается любое отображение $f: G \times G \rightarrow M$. Очевидно, 2-коцепи образуют абелеву группу относительно обычного сложения функций, обозначаемую $C^2(G, M)$. Далее, 2-коцепь называется 2-коциклом, если

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz)$$

для любых $x, y, z \in G$, и 2-кограницей, если существует отображение $h: G \rightarrow M$ такое, что $f(x, y) = xh(y) + h(x) - h(xy)$. (В этом случае пишут $f = \partial h$ и говорят, что f является кограницей 1-коцепи $h \in C^1(G, M)$).

Группа 2-когомологий $H^2(G, M)$ определяется как

$$H^2(G, M) = Z^2(G, M)/B^2(G, M),$$

где $Z^2(G, M)$ и $B^2(G, M)$ суть группы всех 2-коциклов и 2-кограниц соответственно.

Далее, под расширением M с помощью G мы понимаем короткую точную последовательность групп

$$E: 1 \longrightarrow M \xrightarrow{i} \tilde{G} \xrightarrow{\rho} G \longrightarrow 1, \quad (2.1)$$

согласованую со структурой G -модуля на M , т.е. такую, что $gi(m)g^{-1} = i(\rho(g)m)$ для любых $m \in M$, $g \in \tilde{G}$. Два расширения E_1 и E_2 называются *эквивалентными*, если существует коммутативная диаграмма вида

$$\begin{array}{ccccccccc} E_1: & 1 & \longrightarrow & M & \xrightarrow{i_1} & \tilde{G}_1 & \xrightarrow{\rho_1} & G & \longrightarrow & 1 \\ & & & \parallel & & \tau \downarrow & & \parallel & & \\ E_2: & 1 & \longrightarrow & M & \xrightarrow{i_2} & \tilde{G}_2 & \xrightarrow{\rho_2} & G & \longrightarrow & 1, \end{array}$$

где $\tau: \tilde{G}_1 \rightarrow \tilde{G}_2$ – изоморфизм.

Множество классов эквивалентности расширений обозначается через $\mathcal{E}(G, M)$. Между $\mathcal{E}(G, M)$ и $H^2(G, M)$ существует соответствие, которое вкратце может быть описано так.

Пусть E – расширение, как выше. Для каждого $x \in G$ выберем ρ -прообраз $\tilde{x} \in \tilde{G}$. Тогда для любых x, y имеем $\rho(\tilde{x}\tilde{y}(\tilde{x}\tilde{y})^{-1}) = 1$. Положим $c(x, y) = i^{-1}(\tilde{x}\tilde{y}(\tilde{x}\tilde{y})^{-1})$. Можно показать, что c – коцикл, и его класс $[c] \in H^2(G, M)$ зависит лишь от класса $[E] \in \mathcal{E}(G, M)$.

Наоборот, если c есть 2-коцикл, то мы можем определить на множестве $\tilde{G} = M \times G$ структуру группы по правилу $(m, g)(l, h) = (m + gl + c(g, h), gh)$. Тогда

$$E = E(c): \quad 1 \longrightarrow M \xrightarrow{i} \tilde{G} = \tilde{G}(c) \xrightarrow{\rho} G \longrightarrow 1,$$

где i и ρ определены правилами $i(m) = (m, 1)$, $\rho((m, x)) = x$, является расширением M с помощью G , и его класс $[E]$ зависит лишь от $[c]$. Мы называем $E(c)$ *каноническим расширением*, ассоциированным с c . Легко видеть, что если E есть произвольное расширение (2.1), а $\{\tilde{x} \in \tilde{G} \mid x \in G\}$ – некоторый набор прообразов для элементов из G и $c(x, y)$ – соответствующий коцикл, то E эквивалентно $E(c)$.

Можно показать, что описанные соответствия между $\mathcal{E}(G, M)$ и $H^2(G, M)$ на самом деле являются взаимно обратными биекциями. Детали могут быть найдены в [4; гл. 4], и [5; гл. 4].

Пусть $\varphi: M \rightarrow N$ – гомоморфизм G -модулей. Он индуцирует гомоморфизм абелевых групп $\varphi_*: C^2(G, M) \rightarrow C^2(G, N)$ обычным образом, а именно,

$$(\varphi_* f)(x, y) = \varphi(f(x, y)).$$

Легко видеть, что φ_* переводит $Z^2(G, M)$ и $B^2(G, M)$ в $Z^2(G, N)$ и $B^2(G, N)$ соответственно, и потому индуцирует гомоморфизм $H^2(G, M) \rightarrow H^2(G, N)$, который тоже будем обозначать через φ_* .

Далее, пусть когомологический класс $\theta \in H^2(G, M)$ представлен коциклом $z \in Z^2(G, M)$, и $H \subseteq G$ – подгруппа. Ограничение z на $H \times H$ есть 2-коцикл на H , и его класс $[z|_{H \times H}] \in H^2(H, M)$ зависит только от θ . Получаем отображение ограничения $\text{res}_H^G: H^2(G, M) \rightarrow H^2(H, M)$.

Нам потребуются также сведения о когомологиях индуцированных модулей.

Пусть G – группа, $H \subseteq G$ – подгруппа, M есть H -модуль, и M^G есть индуцированный G -модуль. Хорошо известно, что если $|G:H| < \infty$, то $H^k(G, M^G) \cong H^k(H, M)$ для любого $k \geq 0$ (“лемма Шапиро”), см. [4; предложение III.6.2]. Нам потребуется это утверждение лишь для $k = 2$.

Фактически, нам нужно следующее уточнение леммы Шапиро. Пусть G, H, M, M^G как выше, и пусть R – некоторое множество представителей правых смежных классов G/H , так что $G = \bigsqcup_{x \in R} xH$. Будем предполагать, что $1 \in R$. Тогда M^G можно представить как $\bigoplus_{x \in R} xM$. Оба $M = 1 \cdot M$ и $L = \bigoplus_{x \in R \setminus \{1\}} xM$ являются H -подмодулями в M^G , и $M^G = M \oplus L$.

ПРЕДЛОЖЕНИЕ 2. При сделанных выше предположениях сквозное отображение в композиции

$$H^k(G, M^G) \xrightarrow{\text{res}} H^k(H, M^G) \xrightarrow{\varphi_*} H^k(H, M)$$

является изоморфизмом. Здесь $\text{res} = \text{res}_H^G$ есть ограничение когомологий с G на H , $\varphi: M^G \rightarrow M$ есть проекция на прямое слагаемое, и φ_* – индуцированное отображение в когомологиях.

Это предложение является частным случаем упражнения 2 из § III.8 в [4]. (Иногда само предложение 2 и называют леммой Шапиро.)

Ниже нам потребуется следующая лемма. Для краткости мы пишем $t|_H$ вместо $t|_{H \times H}$.

ЛЕММА 3. Пусть G, H, M, M^G, L как выше, и $z \in Z^2(H, M)$ есть 2-коцикл. Тогда существует 2-коцикл $t \in Z^2(G, M^G)$ такой, что $t_M = z$. Здесь $t_M: H \times H \rightarrow M$ есть M -компонента ограничения $t|_H$, т.е. $t(x, y) = t_M(x, y) + t_L(x, y)$, $x, y \in H$, $t_M(x, y) \in M$, $t_L(x, y) \in L$.

ДОКАЗАТЕЛЬСТВО. Пусть $\theta = [z] \in H^2(H, M)$ есть класс коцикла z , пусть

$$H^k(G, M^G) \xrightarrow{\text{res}} H^k(H, M^G) \xrightarrow{\varphi_*} H^k(H, M)$$

есть композиция из предыдущего предложения, $\tau \in H^2(G, M^G)$ есть класс, соответствующий θ относительно этой композиции, и $u \in Z^2(G, M^G)$ есть коцикл, представляющий τ . Очевидно, ограничение $u|_H$ есть коцикл, представляющий класс $\text{res}(\tau) = \tau|_H$.

Далее, пусть $v \in Z^2(H, M^G)$ есть произвольный коцикл, $\sigma = [v]$ его класс, v_L и v_M его L - и M -компоненты соответственно. Легко видеть, что v_L и v_M суть 2-коциклы на H со значениями в L и M соответственно, и

$$[v_M] = [\varphi_* v] = \varphi_*([v]) = \varphi_* \sigma.$$

В частности, если u_M есть M -компонента ограничения $u|_H$, то

$$[u_M] = \varphi_*([u|_H]) = \varphi_*(\tau|_H) = \varphi_*(\text{res}(\tau)) = \theta.$$

Поскольку $[u_M] = \theta = [z]$, u_M и z отличаются на кограницу: $u_M - z = \partial b$ для некоторого $b \in C^1(H, M)$. Продолжим b до коцепи $b_1 \in C^1(G, M^G)$ произвольным образом (например, дополним нулями вне H). Положим $t = u - \partial b_1$ и покажем, что коцикл t искомым.

Имеем $t|_H = u|_H - (\partial b_1)|_H$. Далее,

$$(\partial b_1)|_H = \partial(b_1|_H) = \partial b = u_M - z.$$

Отсюда

$$t|_H = u|_H - (u_M - z) = z + u|_H - u_M = z + u_L.$$

Поэтому M -компонента в $t|_H$ есть в точности z , что и требовалось.

3. Доказательство теоремы 1.

ЛЕММА 4. Пусть G – конечная группа, $x \in G$ – элемент простого порядка p , и $k \geq 1$. Тогда существуют G -модуль M , являющийся абелевой p -группой экспоненты p^{k-1} , и расширение

$$E: 1 \longrightarrow M \xrightarrow{i} \tilde{G} \xrightarrow{\rho} G \longrightarrow 1$$

такие, что порядок любого $\tilde{x} \in \tilde{G}$ такого, что $\rho(\tilde{x}) = x$, есть $|\tilde{x}| = p^k$.

ДОКАЗАТЕЛЬСТВО. Пусть $H = \langle x \rangle \subseteq G$, и пусть A и $\tilde{H}$ суть циклические группы порядков p^{k-1} и p^k с порождающими a и y соответственно, и гомоморфизмы $j: A \rightarrow \tilde{H}$ и $\sigma: \tilde{H} \rightarrow H$ определены тем, что $j(a) = y^p$ и $\sigma(y) = x$. Будем рассматривать A как H -модуль с тривиальным действием. Тогда

$$D: 1 \longrightarrow A \xrightarrow{j} \tilde{H} \xrightarrow{\sigma} H \longrightarrow 1$$

есть расширение, соответствующее этим данным. Для элементов x^m , $0 \leq m \leq p-1$, выберем какие-нибудь прообразы $\tilde{x}^m \in \tilde{H}$, и пусть $c \in Z^2(H, A)$ есть коцикл, соответствующий этому выбору прообразов. (Например, если выбрать $\tilde{x}^m = y^m$, то легко видеть, что $c(x^i, x^j) = 0$ при $0 \leq i+j \leq p-1$ и $= a$ при $p \leq i+j \leq 2(p-1)$.)

Далее, пусть $M = A^G$, $L \subset M$ есть H -подмодуль в M , дополнительный к A . Согласно лемме 3 существует 2-коцикл $z \in Z^2(G, M)$ такой, что $z_A = c$, где z_A есть A -компонента ограничения $z|_H$. Пусть

$$E = E(z): 1 \longrightarrow M \xrightarrow{i} \tilde{G} \xrightarrow{\rho} G \longrightarrow 1$$

есть каноническое расширение, связанное с z . Мы покажем, что E искомое.

Заметим следующий общий факт. Пусть X – произвольная группа, V – X -модуль, $t \in Z^2(X, V)$ – коцикл, и

$$E(t): 1 \longrightarrow V \xrightarrow{i} \tilde{X} \xrightarrow{\rho} X \longrightarrow 1$$

– соответствующее расширение. Далее, предположим, $g \in X$ – элемент порядка m , и $\tilde{g} = (v, g)$ – какой-либо его прообраз в $\tilde{X}$. Тогда $\tilde{g}^m = d \in V$, и $|\tilde{g}| = m|d|$. Кроме того,

$$d = \sum_{l=0}^{m-1} g^l v + \sum_{l=1}^{m-1} t(g^l, g).$$

Действительно, для каждого $j \geq 0$ имеем $(v, g)^j = (d_j, g^j)$ для некоторого $d_j \in V$. При этом $d_0 = 0$, $d_1 = v$ и

$$(d_j, g^j) = (d_{j-1}, g^{j-1})(v, g) = (d_{j-1} + g^{j-1}v + t(g^{j-1}, g), g^j),$$

откуда $d_j = d_{j-1} + g^{j-1}v + t(g^{j-1}, g)$, и индукцией по j получаем, что

$$d_j = \sum_{l=0}^{j-1} g^l v + \sum_{l=1}^{j-1} t(g^l, g)$$

для всех $j \geq 1$, откуда при $j = m$ получаем требуемое.

Теперь пусть $\tilde{x}$ – произвольный прообраз для x в $\tilde{G}$. Тогда $\tilde{x} = (b, x)$ для некоторого $b \in M$. Нам достаточно показать, что элемент

$$d = \sum_{l=0}^{p-1} x^l b + \sum_{l=0}^{p-1} z(x^l, x)$$

имеет порядок p^{k-1} в M . Для этого, в свою очередь, достаточно доказать, что его A -компонента d_A имеет порядок p^{k-1} . Но

$$d_A = \sum_{l=0}^{p-1} x^l b_A + \sum_{l=0}^{p-1} z_A(x^l, x) = \sum_{l=0}^{p-1} x^l b_A + \sum_{l=0}^{p-1} c(x^l, x).$$

Последний же элемент имеет порядок p^{k-1} в силу того, что c есть коцикл, соответствующий расширению D , а в последнем расширении любой прообраз для x имеет порядок p^k .

Теперь можно завершить ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Пусть $\mathcal{K}_1, \dots, \mathcal{K}_s$ – все классы сопряженности в G , состоящие из элементов простых порядков, и $x_i \in \mathcal{K}_i$ – их представители. Пусть $|x_l| = p_r$. По лемме 4 существуют расширения

$$1 \longrightarrow M_l \xrightarrow{i_l} \tilde{G}_l \xrightarrow{\rho_l} G \longrightarrow 1$$

такие, что M_l – абелева группа экспоненты $p_r^{b_r}$ и любой ρ_l – прообраз элемента x_l имеет порядок $p_r^{b_r+1}$. В прямом произведении $G \times \tilde{G}_1 \times \dots \times \tilde{G}_s$ рассмотрим подгруппу $\tilde{G}$ всех элементов $\bar{g} = (g, g_1, \dots, g_s)$ таких, что $\rho_l(g_l) = g$ для всякого $l = 1, \dots, s$. Определим $\rho: \tilde{G} \rightarrow G$ тем, что $\rho((g, g_1, \dots, g_s)) = g$. Ясно, что ρ – сюръекция, и $\text{Ker } \rho = \{1\} \times i_1(M_1) \times \dots \times i_s(M_s)$.

Мы утверждаем, что $K = \tilde{G}$ и $N = \text{Ker } \rho$ удовлетворяют заключению теоремы. Очевидно, что N абелева, $K/N \cong G$, и легко видеть, что $\pi(K) = \pi(G)$. Остается доказать, что любой элемент $\bar{g} \in K$ порядка p_r^c , где $c \leq b_r$, лежит в N .

Допустим противное, и пусть $\bar{g}$ – такой элемент, не лежащий в N . Пусть $g = \rho(\bar{g})$. Очевидно, $|g|$ есть степень простого p_r . Поэтому для некоторого $d = p_r^a$ элемент $h = g^d$ имеет порядок p_r . Также очевидно, что $\bar{h} = \bar{g}^d$ имеет порядок $p_r^{c_1}$ с $c_1 \leq c$. Поэтому мы можем предполагать без ограничения общности, что g – порядка p_r . Очевидно, g сопряжено с элементом x_l для некоторого l ; $x_l = aga^{-1}$, $a \in G$. Пусть $\tilde{a} \in \tilde{G}$ – любой представитель для a . Тогда $\bar{h} = \tilde{a}\bar{g}\tilde{a}^{-1}$ является представителем для x_l и имеет порядок p_r^c . Поэтому можно считать, что $g = x_l$. Теперь мы имеем $\bar{g} = (g, g_1, \dots, g_s)$. Элемент g_l является ρ_l -прообразом для x_l . Поэтому $|g_l| = p_r^{b_r+1}$, и, тем более, $|\bar{g}| \geq |g_l| = p_r^{b_r+1} > p_r^c$; противоречие.

Доказательство теоремы 1 окончено.

В заключение автор выражает благодарность И. Д. Супруненко за поддержку и В. Н. Тютянову, обратившему внимание автора на вопрос из [1].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Y. Berkovich, L. Kazarin, “Indices of elements and normal structure of finite groups”, *J. Algebra*, **283**:2 (2005), 564–583.

- [2] В. Н. Тютянов, “Конечные группы, у которых все элементы простых порядков содержатся в подгруппе Фраттини”, *Изв. Гомельск. гос. ун-та им. Ф. Скорины*, **41**:2 (2007), 59–61.
- [3] *Нерешенные вопросы теории групп. Коуровская тетрадь*, 17-е изд., ред. В. Д. Мазуров, Е. И. Хухро, Ин-т матем. СО РАН, Новосибирск, 2010.
- [4] К. С. Браун, *Когомологии групп*, Наука, М., 1987.
- [5] С. Маклейн, *Гомология*, Мир, М., 1966.

В. П. Буриченко

Институт математики НАН Беларуси

E-mail: vpburich@gmail.com

Поступило

14.01.2011