

В. Н. Шокуев

## ОСНОВЫ ТЕОРИИ ПЕРЕЧИСЛЕНИЯ ДЛЯ КОНЕЧНЫХ НИЛЬПОТЕНТНЫХ ГРУПП

Теорема Силова о  $p$ -подгруппах конечной группы играет фундаментальную роль в теории групп, являясь одной из важнейших среди теорем, выводящих глубокие свойства конечных групп из арифметических свойств их порядков. Различным уточнениям и обобщениям теоремы Силова было посвящено много работ (Фробениус, Миллер, Шмидт, Кулаков, Ф. Холл, Дюбюк, Беркович, Тазава, Хушерт и др.). Наибольшего успеха в этом направлении достиг Кулаков [13]; он доказал, что в нециклической группе порядка  $p^m$  ( $p$  — простое  $> 2$ ) число подгрупп порядка  $p^n$  ( $1 \leq n < m$ ) сравнимо с  $1 + p$  по модулю  $p^2$ . Впоследствии вокруг теоремы Кулакова проводилось много исследований, а в 1972 году автор [6] получил точную формулу для числа подгрупп любого порядка в произвольной конечной  $p$ -группе. К настоящему времени накопился ряд перечислительных задач теории групп, как старых, так и нерешенных, но отсутствует систематическая техника, пригодная для конкретных и наиболее важных перечислений.

Цель этой работы — показать, что обращение Мебиуса является весьма эффективным рабочим инструментом для решения основных задач теории перечисления для конечных нильпотентных групп. Ключ к такому подходу — в заметке [9], где автор вычислил функцию Мебиуса на любой подгруппе конечной  $p$ -группы (см. также [9, 10, 11]).

Все рассматриваемые группы предполагаются конечными.

Наш метод перечисления основывается на гауссовых коэффициентах [2, с. 330]

$$(m, n) = \prod_{k=0}^{n-1} (p^{m-k} - 1)(p^{n-k} - 1)^{-1}, \quad (1)$$

выражающих число подгрупп порядка (индекса)  $p^n$  в элементарной (абелевой)  $p$ -группе порядка  $p^m$  [5, с. 225].

Непосредственная проверка показывает, что выполняется тождество [12]

$$\sum_{n=0}^m (-1)^n p^{\binom{n}{2}} (m, n) = 0, \quad (2)$$

представляющее обобщение биномиального тождества

$$\sum_{n=0}^m (-1)^n \binom{m}{n} = 0. \quad (3)$$

Определенное место занимают и майорантные подгруппы [12], т.е. подгруппы, содержащие подгруппу Фраттини. Для нильпотентных групп майорантные подгруппы — это в точности те подгруппы, которые являются пересечениями каких-то максимальных подгрупп [10].

Важную роль играет следующее предложение [11]:

**Основная теорема (обращение Мебиуса).** Пусть  $G$  — нильпотентная группа порядка  $p_1^{\alpha_1} \dots p_k^{\alpha_k}$  ( $p_1, \dots, p_k$  — различные простые),  $L$  — решетка подгрупп  $G$ ,  $K$  — поле характеристики нуль и  $f$  — функция на  $L$  со значениями в  $K$ . Пусть  $S$  — суммирующая функция для  $f$ , т.е. для  $X \in L$  выполняется равенство

$$\left. \begin{aligned} S(X) &= \sum_{Y \leq X} f(Y). \\ \text{Тогда ему равносильно равенство} \\ f(X) &= \sum_{Y \leq X} \mu(Y, X) S(Y) \quad (X \in L), \end{aligned} \right\} \quad (4)$$

где  $\mu$  — функция Мебиуса алгебры инцидентности решетки  $L$  — вычисляется следующим образом:

$$\mu(X, Y) = \begin{cases} \prod_{i=0}^k (-1)^{n_i} p_i^{\binom{n_i}{2}}, & \text{если } X \text{ — майорантная подгруппа} \\ & \text{индекса } p_1^{n_1} \dots p_k^{n_k} \text{ в } Y, \\ 0 & \text{в остальных случаях.} \end{cases} \quad (5)$$

**Доказательство.** Пусть сначала  $G$  есть  $p$ -группа,  $|G| = p^m$ , и пусть  $X, Y$  — какие угодно подгруппы в  $G$ . Если  $X \not\leq Y$ , то согласно определению функции Мебиуса [1–3]  $\mu(X, Y) = 0$ . Поэтому можно считать, что  $X \leq Y$ . Пусть  $|Y : X| = p^n$  — индекс  $X$  в  $Y$ . Если  $X = Y$ , то  $\mu(X, Y) = 1 = (-1)^0 p^{\binom{0}{2}}$ , и это примем за базу индукции по числу  $n$ .

По самому определению  $\mu$  имеем при  $X < Y$ :

$$\mu(X, Y) = - \sum_{X < Z \leq Y} \mu(Z, Y). \quad (6)$$

Если  $X$  майоранта в  $Y$ , то для любой промежуточной подгруппы  $Z$ ,  $X < Z \leq Y$ , факторгруппы  $Z/X$  и  $Y/Z$  элементарны. Здесь имеем биективное соответствие между подгруппами группы  $Y/X$  и группами  $Y/Z$ , на компонентах которых  $(Z, Y)$  функция Мебиуса осуществляет индуктивный вклад  $\mu(Z, Y)$  в (6). Пусть  $|Z/X| = p^\nu$ , тогда  $|Y : Z| = p^{n-\nu}$ ,  $1 \leq \nu \leq n$ , поэтому число  $Z$  с  $|Z/X| = p^\nu$  есть  $(n, \nu) = (n, n - \nu)$ , а вклад  $\mu(Z, Y)$  в (6) равен (согласно индуктивному предположению) числу  $(-1)^{n-\nu} p^{\binom{n-\nu}{2}}$ . Следовательно, суммарный вклад за счет таких  $Z$  равен

$$(-1)^k p^{\binom{k}{2}}(n, k), \quad k = n - \nu, \quad 0 \leq k \leq n - 1,$$

и в силу (2) и (6) получаем требуемое:

$$\mu(X, Y) = - \sum_{k=0}^{n-1} (-1)^k p^{\binom{k}{2}}(n, k) = (-1)^n p^{\binom{n}{2}}(n, n) = (-1)^n p^{\binom{n}{2}}.$$

Пусть теперь  $X$  не майоранта в  $Y$ . Пусть  $M$  – множество майорантных в  $Y$  промежуточных подгрупп  $Z$ ,  $X < Z \leq Y$  и  $D$  – их пересечение. Тогда  $D$  майоранта в  $Y$  и  $Y/D$  элементарна, причем

$$Z/D \leq Y/D \Leftrightarrow Z \in M.$$

Если  $|Y/D| = p^\alpha$ , то правая часть (6) в силу (2) и предположения индукции равна  $\sum_{\beta=0}^{\alpha} (-1)^\beta p^{\binom{\beta}{2}}(\alpha, \beta) = 0$ , т.е.  $\mu(X, Y) = 0$ , и теорема для  $p$ -групп доказана.

**Замечание.** Относительно проведенной части доказательства основной теоремы мы не ссылаемся на [9] в связи с тем, что изложенное в [9] доказательство опирается на задачи, ради систематического решения которых строится теория перечисления. Чтобы избавиться от недостатков первоначального доказательства, здесь мы воспользовались определением (6) функции Мебиуса посредством рекуррентности со свободным левым концом, в противоположность [9], где свободным был правый конец интервала  $[X, Y]$ .

Переходя к доказательству для нильпотентных групп, заметим, что как и выше, используется (2) и метод индукции; кроме того, учитывается мультипликативность  $\mu$  на прямых сомножителях групп. Подробные выкладки можно восстановить по статье [10].

Теорема доказана.

Благодаря соотношениям (4), (5) на решетке  $L$  возникает исчисление инверсий, которое полностью определяется значением  $\mu$ . "Рассматривая суммирующую функцию как дискретный аналог

неопределенного интеграла в математическом анализе, мы можем считать обращение Мебиуса аналогом производной в дискретном случае," [1, с. 165].

В работе [10] для любого натурального числа  $n$  строится отрезок  $[1, m]$ ,  $m = m(n)$ , натурального ряда и нильпотентная группа  $G(m)$ , такие, что решетка подгрупп  $G(m)$  изоморфна отрезку, упорядоченному отношением делимости. Это позволяет установить тот факт, что классическое исчисление инверсий содержится в качестве частного случая в исчислении инверсий на решетке подгрупп  $L$  нильпотентной группы. Там же доказывается, что исчисление инверсий (4), (5) включает в себя как особый случай и исчисление инверсий на решетке подмножеств любого конечно-го множества, причем здесь играет роль "предельный переход"  $\lim_{p \rightarrow 1} \binom{m}{n} = \binom{m}{n}$  и подсказанная им аналогия между соотношениями (2) и (3), связанными таким же переходом. Эти результаты позволяют трактовать классические факты с новой точки зрения, рассматривая их как частные проявления структуры группы, и потому некоторым образом раскрывающие определенные свойства последней.

Перейдем к типичным примерам комбинаторных ситуаций, в которых обращение Мебиуса на нильпотентных группах возникает естественно и приводит к точным результатам.

На первый план выдвигается, естественно, задача перечисления подгрупп любого порядка (хотя бы благодаря исследованиям по теореме Силова).

**Теорема о числе подгрупп.** В  $p$ -группе  $G$  порядка  $p^m$  число подгрупп порядка  $p^{m-n}$ ,  $n = 1, \dots, m$ , определяется по формуле

$$\sigma_n = \sum_{k=1}^n (-1)^{k-1} p^{\binom{k}{2}} \sum_{d_{n-k}} (d_{n-k}, k), \quad (7)$$

где  $d_{n-k}$  пробегает ранги подгрупп индекса  $p^{n-k}$  в  $G$ . В нильпотентной группе порядка  $p_1^{m_1} \dots p_r^{m_r}$  число подгрупп порядка  $p_1^{m_1-n_1} \dots p_r^{m_r-n_r}$  равно  $\sigma_{n_1} \dots \sigma_{n_r}$ , где каждое  $\sigma_{n_i}$  вычисляется согласно (7) в соответствующей  $p_i$ -силовой подгруппе.

**Доказательство.** Пусть  $\mathcal{H}$  — множество подгрупп индекса  $p^n$  в группе  $G$  порядка  $p^m$ . Для  $H \in \mathcal{H}$  имеем

$$\sum_{H \leq X \leq G} \mu(H, X) = 0,$$

где по основной теореме  $\mu(H, X) = (-1)^k p^{\binom{k}{2}}$ , если  $H$  майорантна в  $X$  подгруппа с  $|X : H| = p^k$ , и  $\mu(H, X) = 0$  в противном случае; следовательно,

$$\sum_{H \in \mathcal{H}} \sum_{H \leq X \leq G} \mu(H, X) = 0. \quad (8)$$

Пусть  $X$  — фиксированная подгруппа в (8), для которой  $|G : X| = p^{n-k}$  ( $0 \leq k \leq n$ ) и пусть  $d_{n-k}$  — ее ранг, так что  $|X/\Phi(X)| = p^{d_{n-k}}$ . Так как  $|X/\Phi(X) : H/\Phi(X)| = |X : H| = p^k$  при  $\mu(H, X) = 0$ , то число ненулевых слагаемых вида  $\mu(H, X)$  равно гауссову коэффициенту  $(d_{n-k}, k)$ , поэтому (8) имеет вид

$$\sum_{k=0}^n (-1)^k p^{\binom{k}{2}} \sum_{d_{n-k}} (d_{n-k}, k) = 0, \quad (9)$$

где  $d_{n-k}$  побегает ранги всех подгрупп индекса  $p^{n-k}$  в  $G$ . Так как  $(d_n, 0) = 1$  и число таких слагаемых в (9) равно  $\sigma_n$ , то из (9) следует (7).

Утверждение о подгруппах нильпотентной группы выполняется очевидным образом. Теорема доказана.

Относительно первоначального вывода формулы (7), содержащегося в [6], дело обстоит примерно так же, как и с доказательством основной теоремы.

Вопрос о существовании точной формулы (7) оставался открытым целое столетие (1872–1972), если отсчет вести с теоремы Силова, и может возникнуть сомнение в том, что является ли (7) именно той формулой, которую так долго искали? Другими словами, насколько естественно и неизбежно присутствие в ней параметров  $d_{n-k}$ ?

Рассматривая известную формулу Найссера [5, с. 247] для числа максимальных подгрупп  $p$ -группы  $G$  ранга  $d_0$ ,  $\sigma_1 = 1 + p + \dots + p^{d_0-1}$ , замечаем, что  $\sigma_1$  является функцией от  $d_0$  (и, разумеется, от  $p$ ); в свою очередь число максимальных подгрупп в каждой из этих первых максимальных подгрупп группы  $G$  определяется по той же формуле, поэтому в формуле для  $\sigma_2$  должны фигурировать наряду с  $d_0$  и все  $d_1$  и т.д., так что  $\sigma_n$  должно зависеть от всех  $d_{n-k}$ ,  $k = n, n-1, \dots, 1$ . Сила метода обращения как раз проявляется в том, что позволяет исключить возникающие здесь повторения.

В дальнейшем через  $G$  будет обозначаться  $p$ -группа порядка  $p^m$  и ранга  $d$ .

Рассмотрим некоторые полезные следствия из основной теоремы, которые найдут применение к  $p$ -группам. Пусть  $X \leq G$  и  $|X/\Phi(X)| = p^{d(X)}$ . Пусть  $M_n$  пробегает множество  $W_n$  майорантных подгрупп индекса  $p^n$  в  $X$ . Тогда из основной теоремы следует, что

$$\left. \begin{aligned} S(X) &= \sum_{Y \leq X} f(Y) \\ \text{тогда и только тогда, если} \\ f(X) &= \sum_{n=0}^{d(X)} (-1)^n p^{\binom{n}{2}} \sum_{M_n \in W_n} S(M_n). \end{aligned} \right\} \quad (10)$$

Для некоторых задач суммирующая функция постоянна на  $W_n$  (при фиксированном  $n = 0, \dots, d(X)$ ), и для них (10) принимает более удобный вид

$$\left. \begin{aligned} S(X) &= \sum_{Y \leq X} f(Y) \quad (X \leq G) \\ \text{тогда и только тогда, когда} \\ f(X) &= \sum_{n=0}^{d(X)} (-1)^n p^{\binom{n}{2}} (d(X), n) c_n. \end{aligned} \right\} \quad (11)$$

Пусть  $T$  – некоторое множество элементов группы  $G$ . Для  $X \leq G$  пусть  $S(X)$  есть число содержащихся в  $X$  элементов из  $T$ , и  $f(X)$  – число элементов из  $T$ , порождающих  $X$ . Тогда в силу (10) имеем формулу для  $f(G)$ :

$$f(G) = \sum_{n=0}^d (-1)^n p^{\binom{n}{2}} \sum_{M_n \in W_n} S(M_n), \quad (12)$$

где  $W_n$  – множество майорантных подгрупп  $M_n$  индекса  $p^n$  в  $G$ .

Если ни один из элементов (т.е. комплексов) множества  $T$  не является системой образующих  $G$ , то (12) превращается в “принцип перечисления” Ф. Холла [12]:

$$\sum_{n=0}^d (-1)^n p^{\binom{n}{2}} \sum_{M_n \in W_n} S(M_n) = 0. \quad (13)$$

С помощью “обобщенного принципа перечисления” (12) можно решить ряд задач; в частности, можно коротким и единообразным путем передоказать классические перечислительные теоремы (Кулакова и др.) [7, 12].

Систему образующих  $G$  мощности  $n$  назовем  $n$ -системой образующих  $G$ . Пусть  $T$  – множество  $n$ -подмножеств  $G$  и  $S(M_n)$  – число тех из них, которые содержатся в  $M_n$ . Тогда из (12) в силу тривиальных равенств  $S(M_k) = \binom{m-k}{n}$ ,  $|W_k| = (d, k)$  получается

**Теорема о числе  $n$ -систем образующих.** Число  $f_n(G)$   $n$ -систем образующих  $G$  определяется по формуле

$$f_n(G) = \sum_{k=0}^d (-1)^k p^{\binom{k}{2}} \binom{d-k}{n} \binom{p^{m-k}}{n}, \quad (14)$$

$$(1 \leq n \leq p^m).$$

В частности,  $f_n(G) = 0$  при  $1 \leq n \leq d-1$  и  $f_d(G)$  есть число базисов  $G$ , ([12], [3, с. 199]).

Упорядоченная система  $a_1, \dots, a_n$  не обязательно различных элементов  $G$ , в совокупности порождающих  $G$ ,  $G = \langle a_1, \dots, a_n \rangle$ , называется  $n$ -последовательностью образующих  $G$ .

Как и предыдущая, из (12) легко следует

**Теорема о числе  $n$ -последовательностей образующих.** Число  $\pi_n(G)$   $n$ -последовательностей образующих  $G$  представляется формулой

$$\pi_n(G) = p^{(m-d)n} \prod_{k=0}^{d-1} (p^n - p^k). \quad (15)$$

**Следствие 1.** Порядок  $G$  допускает следующее "предельное" представление:

$$|G| = \lim_{n \rightarrow \infty} \frac{\pi_{n+1}(G)}{\pi_n(G)}.$$

**Следствие 2.** Вероятность  $v_n(G)$  того, что  $n$ -последовательность элементов  $G$  является образующей  $G$ , определяется формулой

$$v_n(G) = \prod_{k=0}^{d-1} (1 - p^{k-n}); \quad (16)$$

в частности,  $\lim_{n \rightarrow \infty} v_n(G) = 1$ .

В силу (16)  $v_n(G)$  есть функция на множестве классов (конечных)  $p$ -групп одинаковых рангов при каждом фиксированном  $n$ .

Назовем [4]  $n$ -й экспонентой группы  $G$  максимальный порядок  $p^{l_n}$  в системе порядков подгрупп  $G$ , имеющих ранг  $n$  ( $1 \leq n \leq \log_p |G|$ ); в частности,  $p^{l_1}$  — это обычная экспонента  $p^l$  группы  $G$ . Число подгрупп порядка  $p^i$  и ранга  $j$  группы  $G$  обозначим  $\sigma_{ij}$ . Теоретико-числовая формула Гаусса применительно к  $G$  представляется соотношением

$$|G| = \sum_{k=0}^l \varphi(p^k) \sigma_{k1} \quad (\varphi - \text{функция Эйлера}).$$

Его непосредственным обобщением является

**Следствие 3.** Для любого натурального числа  $n$

$$|G|^n = 1 + (p^n - 1)(\sigma_{11} + p^{1 \cdot n} \sigma_{21} + \dots + p^{(l_1 - 1) \cdot n} \sigma_{l_1, 1}) + \\ + (p^n - 1)(p^n - p)(\sigma_{22} + p^{1 \cdot n} \sigma_{32} + \dots + p^{(l_2 - 2) \cdot n} \sigma_{l_2, 2}) + \dots + \\ + (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})(\sigma_{nn} + p^{1 \cdot n} \sigma_{n+1, n} + \dots + p^{(l_n - n) \cdot n} \sigma_{l_n, n}). \quad (17)$$

**Следствие 4.** Имеют место соотношения

$$\sum_{\beta=0}^{\gamma} \sum_{\alpha=\beta}^{m+\beta-\gamma} (-1)^\beta p^{\binom{\beta}{2}} (\alpha, \beta) \sigma_{m+\beta-\gamma, \alpha} = 0, \quad \gamma = 1, \dots, m.$$

Если  $G$  — элементарная  $p$ -группа, из (17) следует полезное тождество относительно произвольных переменных  $x, y, z$ :

$$x^m - y^m = \sum_{k=1}^m (m, k)_z y^{m-k} \prod_{t=0}^{k-1} (x - yz^t),$$

где  $(m, k)_z$  получается из  $(m, k)$  заменой  $p$  на  $z$ .

Если  $n$  делит порядок конечной группы, то по теореме Фробениуса [3, с. 157], число решений уравнения  $x^n = 1$  (в группе) кратно  $n$ . Следующий точный результат [8] представляет усиление теоремы Фробениуса применительно к группе  $G$ :

**Теорема о числе решений уравнения  $x^{p^n} = 1$ .** Число  $k_n$  решений уравнения  $x^{p^n} = 1$  ( $1 \leq n \leq l$ ) в  $G$  определяется формулой

$$k_n = p^n \sum_{\lambda=0}^n \sum_{t=\lambda+1}^{m-n-\lambda} (-1)^{1+t} p^{\binom{t}{2}} \sum_{d_{n+t-\lambda}} (d_{n+t-\lambda}, t),$$

где  $d_\alpha$  пробегает ранги подгрупп порядка  $p^\alpha$  группы  $G$ .

**Следствие 1.** Порядок  $G$  связан с ее экспонентой  $p^l$  равенством

$$|G| = p^l \sum_{\lambda=0}^l \sum_{t=\lambda+1}^{m-l+\lambda} (-1)^{t+1} p^{\binom{t}{2}} \sum_{d_{l+t-\lambda}} (d_{l+t-\lambda}, t). \quad (18)$$

Понятно, что (18) имеет непосредственное отношение к ослабленной проблеме Бернсайда.

**Следствие 2.** Число  $\theta_n$  элементов порядка  $p^n$  ( $1 \leq n \leq l$ ) группы  $G$  определяется по формуле

$$\theta_n = p^n \sum_{t=1}^{m-n} (-1)^{t+1} p^{\binom{t}{2}} \sum_{d_{n+t}} (d_{n+t}, t) + \\ + \sum_{t=1}^n (-1)^t p^{n+t(t+3)/2} \sum_{d_n} (d_n, t).$$

**Следствие 3.** Число  $c_n$  циклических подгрупп порядка  $p^n$  ( $1 \leq n \leq l$ ) группы  $G$  определяется формулой

$$c_n = p(p-1)^{-1} \left[ \sum_{t=1}^{m-n} (-1)^{t+1} p^{\binom{t}{2}} \sum_{d_{n+t}} (d_{n+t}, t) + \right. \\ \left. + \sum_{t=1}^n (-1)^t p^{t(t-3)/2} \sum_{d_n} (d_n, t) \right].$$

Обзор дальнейших применений основной теоремы остается за пределами данной статьи; частично она восполняется результатами из цитированной литературы.

#### ЛИТЕРАТУРА

1. М. Айгнер, *Комбинаторная теория*. М.: Мир, 1982, 556 с.
2. *Перечислительные задачи комбинаторного анализа*. М.: Мир, 1979, 368 с.
3. М. Холл, *Теория групп*. М.: Мир, 1962, 468 с.
4. Т. А. Цатурян, В. Н. Шокуев, *О некоторых соотношениях между теоретико-групповыми инвариантами конечных  $p$ -групп*. II. Алгебра и теория чисел, Межвуз. сборник, Вып. 2, Нальчик: КБГУ, 1977, 139–146.
5. О. Ю. Шмидт, *Избранные труды. Математика*. М.: Изд. АН СССР, 1959, 315 с.
6. В. Н. Шокуев, *Формула для числа подгрупп данного порядка конечной  $p$ -группы*. — Мат. заметки, 12, No. 5 (1972), 561–568.
7. В. Н. Шокуев, *О числе подгрупп конечной  $p$ -группы*. — Мат. записки Уральского ун-та, 8, No. 3 (1972), 133–138.
8. В. Н. Шокуев, *О некоторых соотношениях между теоретико-групповыми инвариантами конечных  $p$ -групп*. — Мат. заметки, 17, No. 4 (1975), 571–578.
9. В. Н. Шокуев, *Исчисление универсий на решетке подгрупп конечной  $p$ -группы*. Кольца и модули. Предельные теоремы теории вероятностей, Вып. 2, Изд. Ленингр. ун-та, 1988, с. 92–97.
10. В. Н. Шокуев, *Функция Мебиуса решетки подгрупп конечной nilпотентной группы*. Кольца и модули. Предельные теоремы теории вероятностей, Вып. 3, Изд. С.-Петербург. ун-та, 1993, с. 99–110.

11. В. Н. Шокуев, *Теория перечисления для конечных нильпотентных групп*. Тезисы докладов по теории групп. Межд. конф. по алгебре, Новосибирск, 1991, с. 129.
12. P. A. Hall, *A contribution to the theory of groups of prime-power order*. — Proc. London Math. Soc. **36** (1933), 29–95.
13. A. Kulakoff, *Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in  $p$ -Gruppen*. — Math. Ann. **104** (1933), 778–793.

Кабардино-Балкарский  
государственный университет

Поступило 18 августа 1994 г.