Journal of Siberian Federal University. Mathematics & Physics 2009, 2(2), 189-205

УДК 512.5

Метаполя и описание метабелевых групп без инволюций

Сергей В.Ларин*
Красноярский государственный педагогический университет им. В.П.Астафьева,
Лебедевой 89, Красноярск, 660049,
Россия

Получена 18.02.2009, окончательный вариант 20.03.2009, принята к печати 20.04.2009

Для описания метабелевых групп без инволюций вводится понятие метаполя, которое имеет и самостоятельное значение. Доказано, что всякая конечно порожденная метабелева группа без инволюций содержит порождающее множество, относительно которого всякий элемент имеет однозначную запись. Элементы группы перемножаются по формуле, которая определяется характеристическим числовым набором. При этом характеристический числовой набор определяет группу однозначно с точностью до изоморфизма.

Ключевые слова: метаполе, метабелева группа, инволюции, конечно порожденная группа, изоморфизм групп.

Введение

С целью описания метабелевых групп без инволюций в статье вводится понятие метаполя $\langle F, +, \cdot \rangle$ (определение 2), которое имеет и самостоятельное значение. Доказано, что всякая метабелева группа без инволюций является подгруппой мультипликативной группы некоторого метаполя (следствие из теоремы 6). Это позволяет изучать метабелевы группы без инволюций в рамках теории метаполей, привлекая помимо умножения еще и сложение.

С каждым конечно порожденным метаполем связывается характеристический набор чисел (определение 3), который характеризует умножение. Найдены необходимые и достаточные условия, которым он должен удовлетворять, чтобы существовало соответствующее ему конечно порожденное метаполе (теоремы 3 и 4).

Доказано, что всякая конечно порожденная метабелева группа G без инволюций содержится в минимальном метаполе, аддитивная группа которого представима в виде прямой суммы циклических подгрупп, содержащихся в G (теорема 7). Это позволяет представить всякий элемент группы в стандартной аддитивной или мультипликативной записи и указать формулу умножения таких записей (теорема 8). Доказано, что характеристический числовой набор определяет конечно порожденную метабелеву группу без инволюций однозначно с точностью до изоморфизма (теорема 9). Такой способ описания конечно порожденных метабелевых групп без инволюций позволяет свести решение некоторых задач к вычислительным процедурам. Например, выяснение вопроса, является ли коммутатором произведение двух данных коммутаторов, сводится к решению системы уравнений. Используя этот метод, удалось построить метабелевы группы, в которых произведение двух коммутаторов не является коммутатором.

Работа является продолжением исследований, анонсированных в [1].

*e-mail: Larin_Serg@mail.ru

1. Определение и основные свойства метаполей

Для группы G, следуя [2], будем обозначать коммутант $G' = [G, G]$, центр $C(G)$, а централизатор подгруппы H в группе G — через $C_G(H)$. Группу G будем называть метабелевой, если она нильпотентна ступени нильпотентности 2, то есть коммутант $G' = [G, G]$ лежит в центре $C(G)$ [2, с. 87].

Определение 1. *Будем говорить, что в метабелевой группе F из элемента a извлекается квадратный корень, если в F существует элемент, который будем обозначать $\sqrt{a}$, квадрат которого равен a.*

Лемма 1. *Пусть метабелева группа F не содержит инволюций.*

1) Для всякого элемента группы F существует не более одного квадратного корня.

2) Если G является подгруппой группы F и для элемента $a \in C(G)$ существует элемент $\sqrt{a} = b \in F$, то $b \in C_F(G)$.

Доказательство. 1) В метабелевой группе F из равенства $a^2 = b^2$ следует, что $[a,\ b]^4 = [a^2, b^2] = e$, а так как в F нет элементов порядка 2, то $[a,\ b] = e$. Но тогда из равенства $a^2 = b^2$ получаем $(ab^{-1})^2 = e$, откуда $ab^{-1} = e$ и $a = b$.

Кстати, заметим, что доказанное утверждение является частным случаем более общей теоремы [3, 16.2.8] об однозначности операции извлечения корней в произвольной нильпотентной группе.

2) Пусть G является подгруппой группы F и для элемента $a \in C(G)$ существует элемент $\sqrt{a} = b \in F$ такой, что $b^2 = a$. Тогда для любого $g \in G$ имеем $[g,\ b]^2 = [g,\ b^2] = [g,\ a] = e$, а так как в F нет инволюций, то $[g,\ b] = e$. Следовательно, $b \in C_F(G)$. □

Введем понятие, являющееся объектом нашего исследования.

Определение 2. *Метаполем назовем систему $\langle F,\ +\ ,\ \cdot\ \rangle$, где $\langle F,\ +\ \rangle$ является абелевой группой без инволюций, которую будем называть аддитивной группой метаполя, $\langle F,\ \cdot\ \rangle$ является группой, которую будем называть мультипликативной группой метаполя, и для любых $x, y \in F$ имеет место равенство $x \cdot y \cdot x = x + y + x$.*

Метаполе назовем тривиальным, если в нем умножение совпадает со сложением, и нетривиальным в противном случае.

Два метаполя назовем изоморфными, если существует взаимно однозначное отображение одного метаполя на другое, сохраняющее операции сложения и умножения.

Рангом метаполя без кручения назовем ранг его аддитивной группы (мощность максимальной линейно независимой системы элементов аддитивной группы без кручения).

Подмножество $H \subseteq F$ назовем подметаполем метаполя $\langle F,\ +\ ,\ \cdot\ \rangle$, если H является метаполем относительно сужения на H операций сложения и умножения.

Установим некоторые общие свойства метаполей.

Теорема 1. *Пусть дано метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$.*

1) Если 0 — нулевой элемент аддитивной группы, а e — единичный элемент мультипликативной группы данного метаполя, то $e = 0$.

2) Для любого $a \in F$ и любого целого n имеет место равенство $a^n = na$. Другими словами, мультипликативная циклическая группа $\langle a \rangle$ совпадает с аддитивной циклической группой $\langle a \rangle$.

3) Для любых элементов $x, y \in F$ существует элемент $v(x,y) \in F$ такой, что $x \cdot y = x + y - v(x,y)$, причем $(v(x,y))^2 = [y,x]$.

4) Элемент $v = v(x,y)$ принадлежит центру $C(F)$, а значит, мультипликативная группа метаполя $\langle F, +, \cdot \rangle$ метабелева.

5) Для элементов $x, y \in F$имеем $x + y = x \cdot y$ тогда и только тогда, когда $x \cdot y = y \cdot x$. Следовательно, $x + y = x \cdot y \cdot v(x,y)$.

6) Подгруппа H мультипликативной группы метаполя $\langle F, +, \cdot \rangle$ является подметаполем тогда и только тогда, когда в H из всякого коммутатора извлекается квадратный корень.

7) Метаполе без кручения, ранга не превосходящего двух, тривиально.

8) Два метаполя изоморфны тогда и только тогда, когда изоморфны их мультипликативные группы.

9) Для любых $a, b, c \in F$ $a \cdot (b+c) = a \cdot b + a \cdot c - a$, $(b+c) \cdot a = b \cdot a + c \cdot a - a$ и $[a,b] = a \cdot b - (b \cdot a)$.

10) Определим на F операцию $*$, положив для любых $a, b \in F$ $a * b = [a,b]$. Тогда система $\langle F, +, * \rangle$ является кольцом. Это кольцо имеет единицу тогда и только тогда, когда оно нулевое, то есть $F = \{0\}$.

Доказательство. 1) Из равенства $e = e \cdot e \cdot e = e + e + e$ получаем $0 = 2e$, а так как, по определению, аддитивная группа метаполя не содержит элементов порядка 2, то $e = 0$.

2) Для любого элемента $a \in F$, используя 1), получаем $a^0 = e = 0 = 0a$. Далее, $a^1 = a = 1a$. Для любого натурального n имеем:

$$a^{2n} = \underbrace{a \cdot a \cdot ... \cdot a}_{n} \cdot e \cdot \underbrace{a \cdot a \cdot ... \cdot a}_{n} = \underbrace{a + a + ... + a}_{n} + 0 + \underbrace{a + a + ... + a}_{n} = 2na,$$

$$a^{2n+1} = \underbrace{a \cdot a \cdot ... \cdot a}_{n} \cdot a \cdot \underbrace{a \cdot a \cdot ... \cdot a}_{n} = \underbrace{a + a + ... + a}_{n} + a + \underbrace{a + a + ... + a}_{n} = (2n+1)a.$$

Из равенства $a^{-1} = a^{-1} \cdot a \cdot a^{-1} = a^{-1} + a + a^{-1}$ получаем $0 = a + a^{-1}$, откуда $a^{-1} = -a$. Наконец,

$$a^{-n} = (a^n)^{-1} = -(na) = (-n)a.$$

3) Для любых $x, y \in F$ обозначим $v(x,y) = x + y - x \cdot y$. Тогда $x \cdot y = x + y - v(x,y)$ и

$$(v(x,y))^2 = 2(x + y - x \cdot y) = x + y - 2(x \cdot y) + y + x = x + y + (x \cdot y)^{-2} + y + x =$$

$$= x \cdot y \cdot (x \cdot y)^{-2} \cdot y \cdot x = [y,x].$$

4) Пусть $x, y, z \in F$. Обозначим $v = v(x,y)$. Используя 3), получаем

$$x \cdot y \cdot z \cdot x \cdot y = y \cdot x \cdot [x,y] \cdot z \cdot x \cdot y = y + x + v^{-2} \cdot z + x + y =$$

$$= x \cdot y + v + v^{-2} \cdot z + x \cdot y + v = x \cdot y \cdot v \cdot v^{-2} \cdot z \cdot v \cdot x \cdot y,$$

откуда $z = v^{-1} \cdot z \cdot v$. Следовательно, $v \in C(F)$ и $[y,x] = v^2 \in C(F)$. Таким образом, мультипликативная группа метаполя метабелева.

5) Из 3) следует, что $x \cdot y = x + y$ тогда и только тогда, когда $v(x,y) = 0 = e$, а так как $(v(x,y))^2 = [y,\ x]$ и в F нет инволюций, то $v(x,y) = e$ равносильно условию $[x,y] = e$. Поскольку $v(x,y)$ лежит в центре, то $x + y = x \cdot y + v(x,y) = x \cdot y \cdot v(x,y)$.

6) Пусть подгруппа H мультипликативной группы метаполя $\langle F,\ +\ ,\ \cdot\ \rangle$ является подметаполем. Следовательно, множество H замкнуто относительно сложения и умножения. По 3), для любых элементов $x, y \in H$ существует элемент v такой, что $v = x + y - x \cdot y \in H$, причем $v^2 = [y,x]$.

Обратно, пусть в подгруппе H мультипликативной группы метаполя $\langle F,\ +\ ,\ \cdot\ \rangle$ для любых $x, y \in H$ существует элемент $v \in H$ такой, что $v^2 = [y,\ x]$. Тогда по 5) $x + y = x \cdot y \cdot v \in H$. Следовательно, H является подметаполем.

7) Пусть дано метаполе без кручения $\langle F,\ +\ ,\ \cdot\ \rangle$ ранга $\leqslant 2$. По 3), для любых элементов $x, y \in F$ существует элемент $v \in F$ такой, что $x \cdot y = x + y - v$, причем $v^2 = [y,x]$. Предположим, что $v \neq e$. По условию, ранг аддитивной группы $\langle F,\ +\ \rangle$ не превосходит 2, поэтому существуют целые числа k, m, n, среди которых есть отличные от нуля такие, что $kx + my = nv$. По 2) и 3), получаем $kx + my = x^k + y^m = x^k \cdot y^m + v(kx, my)$, а по 4) элементы v и $v(kx, my)$ принадлежат центру группы $\langle F,\ \cdot\ \rangle$. Следовательно, $x^k \cdot y^m = kx + my - v(kx, my) = nv - v(kx, my) \in C(F)$. Используя метабелевость группы $\langle F,\ \cdot\ \rangle$, получаем $v^{2k} = [y,x]^k = [y, x^k y^m] = e$, откуда $k = 0$. Аналогично $v^{2m} = [y,x]^m = [x^k y^m, x] = e$, откуда $m = 0$. Но тогда $nv = 0$, а так как порядок элемента v бесконечен, то $n = 0$. Пришли к противоречию. Следовательно, $v = e$, откуда $[y,x] = v^2 = e$ и $x \cdot y = x + y$, то есть метаполе тривиально.

8) Необходимость вытекает из определения изоморфизма метаполей.

Докажем достаточность. Пусть φ — изоморфизм мультипликативной группы $\langle F,\ \cdot\ \rangle$ метаполя $\langle F,\ +\ ,\ \cdot\ \rangle$ на мультипликативную группу $\langle F_1,\ \cdot\ \rangle$ метаполя $\langle F_1,\ +,\ \cdot\ \rangle$. Используя обозначения, принятые в 3), заметим сначала, что для любых $x, y \in F$ имеем

$$\varphi(v(x,y))^2 = \varphi([y,x]) = [\varphi(y), \varphi(x)] = (v(\varphi(x), \varphi(y))^2,$$

откуда $\varphi(v(x,y)) = v(\varphi(x), \varphi(y))$. Теперь, используя свойство 5), получаем $\varphi(x + y) = \varphi(x \cdot y \cdot v(x,y)) = \varphi(x) \cdot \varphi(y) \cdot \varphi(v(x,y)) = \varphi(x) \cdot \varphi(y) \cdot v(\varphi(x), \varphi(y)) = \varphi(x) + \varphi(y)$.

9) Используем формулы $x \cdot y = x + y - v(x,y)$, $(v(x,y))^2 = [y,\ x]$ и принадлежность элемента $v(x,y)$ центру метабелевой группы $\langle F,\ \cdot\ \rangle$. Поскольку $(v(a, b+c))^2 = [b+c,\ a] = [b,\ a] \cdot [c,\ a] = (v(a,b) + v(a,c))^2$, то $v(a, b+c) = v(a,b) + v(a,c)$. Отсюда $a(b+c) = a + b + c - v(a, b+c) = a + b - v(a,b) + a + c - v(a,c) - a = a \cdot b + a \cdot c - a$. Аналогично доказывается равенство $(b+c)a = ba + ca - a$. Далее, $(v(a,b))^2 = [b,\ a] = [a,\ b]^{-1} = (-v(b,a))^2$, откуда $v(a,b) = -v(b,a)$. Следовательно, $a \cdot b - b \cdot a = a + b - v(a,b) - (b + a - v(b,a)) = -2v(a,b) = ((v(a,b))^2)^{-1} = [b,\ a]^{-1} = [a,\ b]$.

10) Используя метабелевость группы $\langle F,\ \cdot\ \rangle$, легко доказать, что операция $*$ ассоциативна и дистрибутивна относительно сложения. Предположим, что элемент $e_* \in F$ является единицей относительно операции $*$. Тогда, используя 9), получаем $e_* = e_* * e_* = [e_*, e_*] = e_* \cdot e_* - (e_* \cdot e_*) = 0$. Но тогда для любого $x \in F$ имеем $x = x * e_* = x * 0 = 0$. □

Теорема 2. *Группа F без инволюций является мультипликативной группой некоторого метаполя тогда и только тогда, когда она метабелева и из всякого коммутатора извлекается квадратный корень.*

Доказательство. Необходимость вытекает из пунктов 3 и 4 теоремы 1.

Достаточность. Пусть F — мультипликативная метабелева группа без инволюций и для любых элементов $x, y \in F$ существует элемент $v(x, y)$ такой, что $(v(x, y))^2 = [y, x]$. По лемме 1, $v(x, y) \in C(F)$.

Определим операцию сложения на множестве F, положив $x + y = x \cdot y \cdot v(x, y)$.

1. Операция сложения ассоциативна. Действительно, для любых $a, b, c \in F$ имеем:

$$(a + b) + c = ab \cdot v(a, b) + c = ab \cdot v(a, b) \cdot c \cdot v(ab \cdot v(a, b), c),$$

$$a + (b + c) = a + bc \cdot v(b, c) = a \cdot bc \cdot v(b, c) \cdot v(a, bc \cdot v(b, c)).$$

Используя принадлежность центру элементов вида $v(x, y)$ и метабелевость группы F, получаем:

$$(v(a, b) \cdot v(ab \cdot v(a, b), c))^2 = (v(a, b))^2 (v(ab \cdot v(a, c), c))^2 = [b, a][c, ab] = [b, a][c, a][c, b],$$

$$(v(b, c) \cdot v(a, bc \cdot v(b, c))^2 = (v(b, c))^2 (v(a, bc \cdot v(b, c))^2 = [c, b][bc, a] = [c, b][b, a][c, a].$$

Это на основании леммы 1 доказывает тождество ассоциативности.

2. Если e — единица группы F, то, как легко видеть, для любого $a \in F$ имеем: $a + e = e + a = a$. Следовательно, e является нулевым элементом.

3. Легко доказать, что $a + a^{-1} = a^{-1} + a = e$. Следовательно, $-a = a^{-1}$.

4. Группа $\langle F,\ + \rangle$ абелева. Действительно, $a + b = ab \cdot v(a, b)$, $b + a = ba \cdot v(b, a) = ab[b, a] \cdot v(b, a)$. Но $([b, a] \cdot v(b, a))^2 = [b, a]^2 [a, b] = [b, a] = (v(a, b))^2$, откуда по лемме 1 $[b, a] \cdot v(b, a) = v(a, b)$. Следовательно, $a + b = b + a$.

5. Непосредственным подсчетом убеждаемся, что для любых элементов $a, b \in F$ имеет место равенство $a \cdot b \cdot a = a + b + a$.

Таким образом, система $\langle F,\ +\ ,\ \cdot\ \rangle$ является метаполем. □

2. Конечно порожденные метаполя

Определение 3. *Пусть дано конечно порожденное метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ и его аддитивная группа $\langle F,\ + \rangle = \langle a_1 \rangle \oplus ... \oplus \langle a_n \rangle$. Напомним, что $v(x, y)$ обозначает такой элемент центра $C(F)$, квадрат которого равен $[y,\ x]$. Если $v(a_i,\ a_j) = \sum\limits_{k=1}^{n} p_{ijk} a_k$, то набор целых чисел $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ назовем характеристическим числовым набором данного метаполя относительно порождающего множества $\{a_1, ..., a_n\}$.*

Лемма 2. *Пусть дано метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ и его характеристический числовой набор $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ относительно порождающего множества $\{a_1, ..., a_n\}$. Тогда для любых $x = \sum\limits_{k=1}^{n} \alpha_k a_k$, $y = \sum\limits_{k=1}^{n} \beta_k a_k$*

$$[y,\ x] = 2 \sum_{k=1}^{n} \left(\sum_{1 \leqslant i < j \leqslant n} p_{ijk} (\alpha_i \beta_j - \alpha_j \beta_i) \right) a_k, \tag{1}$$

$$x \cdot y = \left(\sum_{k=1}^{n} \alpha_k a_k\right) \cdot \left(\sum_{k=1}^{n} \beta_k a_k\right) = \sum_{k=1}^{n} \left(\alpha_k + \beta_k + \sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j \beta_i - \alpha_i \beta_j)\right) a_k. \quad (2)$$

Доказательство. В соответствии с определением 3, аддитивная группа метаполя $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$ и $[a_j,\ a_i] = (v(a_i,\ a_j))^2 = 2\sum\limits_{k=1}^{n} p_{ijk}a_k$. Пользуясь пунктами 3) и 4) теоремы 1, для любых $x = \sum\limits_{k=1}^{n} \alpha_k a_k$, $y = \sum\limits_{k=1}^{n} \beta_k a_k$ получаем

$$[y, x] = [a_1^{\beta_1}...a_n^{\beta_n},\ a_1^{\alpha_1}...a_n^{\alpha_n}] = \prod_{1 \leqslant i < j \leqslant n} [a_j, a_i]^{\alpha_i\beta_j - \alpha_j\beta_i} =$$

$$= 2\sum_{1 \leqslant i < j \leqslant n} (\alpha_i\beta_j - \alpha_j\beta_i)\left(\sum_{k=1}^{n} p_{ijk}a_k\right) = 2\sum_{k=1}^{n}\left(\sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_i\beta_j - \alpha_j\beta_i)\right) a_k.$$

Следовательно, $v(x, y) = \sum\limits_{k=1}^{n}\left(\sum\limits_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_i\beta_j - \alpha_j\beta_i)\right) a_k$. По пункту 3) теоремы 1 для любых $x, y \in F$ имеем

$$x \cdot y = x + y - v(x, y) = \sum_{k=1}^{n}\left(\alpha_k + \beta_k + \sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j\beta_i - \alpha_i\beta_j)\right) a_k,$$

что и требовалось доказать. □

Доказанные ниже теоремы 3 и 4 устанавливают необходимые и достаточные условия, при которых набор целых чисел $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ является характеристическим числовым набором некоторого конечно порожденного метаполя.

Теорема 3. *Пусть дано метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$, его аддитивная группа $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$ и характеристический числовой набор $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ относительно порождающего множества $\{a_1, ..., a_n\}$. Тогда*

$$\begin{pmatrix} 0 & p_{12k} & \cdots & p_{1n-1k} & p_{1nk} \\ -p_{12k} & 0 & \cdots & p_{2n-1k} & p_{2nk} \\ \multicolumn{5}{c}{\dotfill} \\ -p_{1n-1k} & -p_{2n-1k} & \cdots & 0 & p_{n-1nk} \\ -p_{1nk} & -p_{2nk} & \cdots & -p_{n-1nk} & 0 \end{pmatrix} \cdot \begin{pmatrix} p_{121} & p_{131} & \cdots & p_{n-1\,n\,1} \\ p_{122} & p_{132} & \cdots & p_{n-1\,n\,2} \\ \multicolumn{4}{c}{\dotfill} \\ p_{12n-1} & p_{13n-1} & \cdots & p_{n-1\,n\,n-1} \\ p_{12n} & p_{13n} & \cdots & p_{n-1nn} \end{pmatrix} \equiv 0 \ (\mod |a_k|) \quad (3)$$

для любого $k = 1,\ ...\ ,\ n$, где в случае $|a_k|\ = \infty$ сравнение вида $t \equiv 0\ (\mod\ |a_k|)$ означает $t = 0$.

Доказательство. По определению 3, аддитивная группа данного метаполя $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$ и $[a_j,\ a_i] = (v(a_i,\ a_j))^2 = 2\sum\limits_{k=1}^{n} p_{ijk}a_k$ для любых $i,\ j,\ 0 \leqslant i < j \leqslant n$. Поскольку $v(a_i, a_j) \cdot a_m = a_m \cdot v(a_i, a_j)$ для любого $m = 1, ..., n$, то

$$\left(\sum_{k=1}^{n} p_{ijk}a_k\right) \cdot a_m = a_m \cdot \left(\sum_{k=1}^{n} p_{ijk}a_k\right). \quad (4)$$

При $m = 1$ отсюда получаем

$$\left(\sum_{k=1}^{n} p_{ijk}a_k\right) \cdot a_1 = a_1 \cdot \left(\sum_{k=1}^{n} p_{ijk}a_k\right). \tag{5}$$

Для вычисления левой части этого равенства положим в формуле (2) $\alpha_k = p_{ijk}$ для фиксированных $i,\ j$, где $1 \leqslant i < j \leqslant n$, и $k = 1,\ \dots\ ,\ n$, а также $\beta_1 = 1$ и $\beta_2 = \dots = \beta_n = 0$. Тогда

$$(p_{ij1}a_1 + p_{ij2}a_2 + \dots + p_{ijn}a_n) \cdot a_1 =$$

$$= (p_{ij1} + 1 + p_{121}p_{ij2} + p_{131}p_{ij3} + \dots + p_{1n1}p_{ijn})a_1 +$$

$$+(p_{ij2} + p_{122}p_{ij2} + p_{132}p_{ij3} + \dots + p_{1n2}p_{ijn})a_2 + \dots +$$

$$+(p_{ijn} + p_{12n}p_{ij2} + p_{13n}p_{ij3} + \dots + p_{1nn}p_{ijn})a_n.$$

Для вычисления правой части равенства (5) положим в формуле (2) $\alpha_1 = 1$, $\alpha_2 = \dots = \alpha_n = 0$ и $\beta_k = p_{ijk}$ для тех же фиксированных $i,\ j$ и $k = 1,\ \dots\ ,\ n$. Тогда

$$a_1 \cdot (p_{ij1}a_1 + p_{ij2}a_2 + \dots + p_{ijn}a_n) =$$

$$= (1 + p_{ij1} + p_{121}(-p_{ij2}) + p_{131}(-p_{ij3}) + \dots + p_{1n1}(-p_{ijn}))a_1 +$$

$$+(p_{ij2} + p_{122}(-p_{ij2}) + p_{132}(-p_{ij3}) + \dots + p_{1n2}(-p_{ijn}))a_2 + \dots +$$

$$+(p_{ijn} + p_{12n}(-p_{ij2}) + p_{13n}(-p_{ij3}) + \dots + p_{1nn}(-p_{ijn}))a_n.$$

Сравнивая соответствующие коэффициенты, получаем сравнения

$$p_{121}p_{ij2} + p_{131}p_{ij3} + \dots + p_{1n1}p_{ijn} \equiv -p_{121}p_{ij2} - p_{131}p_{ij3} - \dots - p_{1n1}p_{ijn} \pmod{|a_1|},$$

$$p_{122}p_{ij2} + p_{132}p_{ij3} + \dots + p_{1n2}p_{ijn} \equiv -p_{122}p_{ij2} - p_{132}p_{ij3} - \dots - p_{1n2}p_{ijn} \pmod{|a_2|},$$

. . . .

$$p_{12n}p_{ij2} + p_{13n}p_{ij3} + \dots + p_{1nn}p_{ijn} \equiv -p_{12n}p_{ij2} - p_{13n}p_{ij3} - \dots - p_{1nn}p_{ijn} \pmod{|a_n|}.$$

Так как нет инволюций, отсюда заключаем, что

$$p_{121}p_{ij2} + p_{131}p_{ij3} + \dots + p_{1n1}p_{ijn} \equiv 0 \pmod{|a_1|},$$

$$p_{122}p_{ij2} + p_{132}p_{ij3} + \dots + p_{1n2}p_{ijn} \equiv 0 \pmod{|a_2|},$$

. . . .

$$p_{12n}p_{ij2} + p_{13n}p_{ij3} + ... + p_{1nn}p_{ijn} \equiv 0 \;(\mod |a_n|).$$

Таким образом, для любого $k = 1, \ ... \ , n$ получаем матричную запись сравнений

$$(0 \; p_{12k} \; p_{13k} \; ... \; p_{1nk}) \begin{pmatrix} p_{ij1} \\ p_{ij2} \\ p_{ij3} \\ ... \\ p_{ijn} \end{pmatrix} \equiv 0 \;(\mod |a_k|).$$

Аналогично из равенства $\left(\sum\limits_{k=1}^{n} p_{ijk}a_k\right) \cdot a_2 = a_2 \cdot \left(\sum\limits_{k=1}^{n} p_{ijk}a_k\right)$ получаем

$$(-p_{12k} \;\; 0 \;\; p_{23k} \;\; ... \;\; p_{2nk}) \begin{pmatrix} p_{ij1} \\ p_{ij2} \\ p_{ij3} \\ ... \\ p_{ijn} \end{pmatrix} \equiv 0 \;(\mod |a_k|).$$

И так далее, в итоге из (4) получаем матричное сравнение (3). □

Теорема 4. *Пусть дана абелева группа* $\langle F, + \rangle = \langle a_1 \rangle \oplus ... \oplus \langle a_n \rangle$ *и множество целых чисел* $M = \{p_{ijk} \mid 1 \leqslant i < j \leqslant n, \; k = 1, ..., n\}$ *удовлетворяет условию* (3). *Определим на множестве* F *операцию умножения формулой* (2). *Тогда система* $\langle F, +, \cdot \rangle$ *является метаполем с характеристическим числовым набором* M *относительно порождающего множества* $\{a_1, ..., a_n\}$.

Доказательство. Докажем ассоциативность операции умножения, которая определена на F формулой (2). Пусть $x = \sum\limits_{k=1}^{n} \alpha_k a_k$, $y = \sum\limits_{k=1}^{n} \beta_k a_k$, $z = \sum\limits_{k=1}^{n} \gamma_k a_k$. Тогда

$$(x \cdot y) \cdot z = \left(\left(\sum_{k=1}^{n} \alpha_k a_k\right) \cdot \left(\sum_{k=1}^{n} \beta_k a_k\right)\right) \cdot z =$$

$$= \left(\sum_{k=1}^{n}\left(\alpha_k + \beta_k + \sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j\beta_i - \alpha_i\beta_j)\right) a_k\right) \cdot \left(\sum_{i=1}^{n} \gamma_i a_i\right) =$$

$$= \sum_{k=1}^{n} \Bigg(\alpha_k + \beta_k + \sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j\beta_i - \alpha_i\beta_j) + \gamma_k +$$

$$+ \sum_{1 \leqslant i < j \leqslant n} p_{ijk}\left(\alpha_j + \beta_j + \sum_{1 \leqslant i_1 < j_1 \leqslant n} p_{i_1 j_1 j}(\alpha_{j_1}\beta_{i_1} - \alpha_{i_1}\beta_{j_1})\right)\gamma_i -$$

$$- \left(\alpha_i + \beta_i + \sum_{1 \leqslant i_2 < j_2 \leqslant n} p_{i_2 j_2 i}(\alpha_{j_2}\beta_{i_2} - \alpha_{i_2}\beta_{j_2})\right)\gamma_j \Bigg) a_k.$$

С другой стороны,

$$x\cdot(y\cdot z)=\left(\sum_{k=1}^{n}\alpha_k a_k\right)\cdot\left(\left(\sum_{k=1}^{n}\beta_k a_k\right)\cdot\left(\sum_{k=1}^{n}\gamma_k a_k\right)\right)=$$

$$\left(\sum_{k=1}^{n}\alpha_k a_k\right)\cdot\left(\sum_{k=1}^{n}\left(\beta_k+\gamma_k+\sum_{1\leqslant i<j\leqslant n}p_{ijk}(\beta_j\gamma_i-\beta_i\gamma_j)\right)a_k\right)=$$

$$=\sum_{k=1}^{n}\left(\alpha_k+\beta_k+\gamma_k+\sum_{1\leqslant i<j\leqslant n}p_{ijk}(\beta_j\gamma_i-\beta_i\gamma_j)+\right.$$

$$+\sum_{1\leqslant i<j\leqslant n}p_{ijk}\left(\alpha_j\left(\beta_i+\gamma_i+\sum_{1\leqslant i_3<j_3\leqslant n}p_{i_3j_3i}(\beta_{j_3}\gamma_{i_3}-\beta_{i_3}\gamma_{j_3})\right)-\right.$$

$$\left.\left.-\alpha_i\left(\beta_j+\gamma_j+\sum_{1\leqslant i_4<j_4\leqslant n}p_{i_4j_4j}(\beta_{j_4}\gamma_{i_4}-\beta_{i_4}\gamma_{j_4})\right)\right)\right)a_k.$$

Находим разность $(x\cdot y)\cdot z-x\cdot(y\cdot z)$. Коэффициент при a_k в этой разности равен

$$K_a=\sum_{1\leqslant i<j\leqslant n}p_{ijk}\left(\left(\sum_{1\leqslant i_1<j_1\leqslant n}p_{i_1j_1j}(\alpha_{j_1}\beta_{i_1}-\alpha_{i_1}\beta_{j_1})\right)\gamma_i-\left(\sum_{1\leqslant i_2<j_2\leqslant n}p_{i_2j_2i}(\alpha_{j_2}\beta_{i_2}-\alpha_{i_2}\beta_{j_2})\right)\gamma_j\right)-$$

$$-\sum_{1\leqslant i<j\leqslant n}p_{ijk}\left(\alpha_j\left(\sum_{1\leqslant i_3<j_3\leqslant n}p_{i_3j_3i}(\beta_{j_3}\gamma_{i_3}-\beta_{i_3}\gamma_{j_3})\right)-\ \alpha_i\left(\sum_{1\leqslant i_4<j_4\leqslant n}p_{i_4j_4j}(\beta_{j_4}\gamma_{i_4}-\beta_{i_4}\gamma_{j_4})\right)\right)=$$

$$=\sum_{1\leqslant i<j\leqslant n}p_{ijk}\left(\sum_{1\leqslant i_1<j_1\leqslant n}p_{i_1j_1j}\left((\alpha_{j_1}\beta_{i_1}-\alpha_{i_1}\beta_{j_1})\gamma_i+\alpha_i(\beta_{j_1}\gamma_{i_1}-\beta_{i_1}\gamma_{j_1})\right)-\right.$$

$$\left.-\left(\sum_{1\leqslant i_2<j_2\leqslant n}p_{i_2j_2i}((\alpha_{j_2}\beta_{i_2}-\alpha_{i_2}\beta_{j_2})\gamma_j+\alpha_j(\beta_{j_2}\gamma_{i_2}-\beta_{i_2}\gamma_{j_2}))\right)\right).$$

Обозначим $u_{ijk}=(\alpha_j\beta_i-\alpha_i\beta_j)\gamma_k+\alpha_k(\beta_j\gamma_i-\beta_i\gamma_j)$, где $1\leqslant i<j\leqslant n$, $k=1,\ \dots\ ,\ n$. Тогда

$$K_a=\sum_{1\leqslant i<j\leqslant n}p_{ijk}\left(\sum_{1\leqslant i_1<j_1\leqslant n}p_{i_1j_1j}u_{i_1j_1i}-\sum_{1\leqslant i_2<j_2\leqslant n}p_{i_2j_2i}u_{i_2j_2j}\right)=$$

$$=p_{12k}\left(\sum_{i_1<j_1}p_{i_1j_12}u_{i_1j_11}-\sum_{i_1<j_1}p_{i_1j_11}u_{i_1j_12}\right)+p_{13k}\left(\sum_{i_1<j_1}p_{i_1j_13}u_{i_1j_11}-\sum_{i_1<j_1}p_{i_1j_11}u_{i_1j_13}\right)+\ldots+$$

$$+p_{23k}\left(\sum_{i_1<j_1}p_{i_1j_13}u_{i_1j_12}-\sum_{i_1<j_1}p_{i_1j_12}u_{i_1j_13}\right)+\ldots+p_{2nk}\left(\sum_{i_1<j_1}p_{i_1j_1n}u_{i_1j_12}-\sum_{i_1<j_1}p_{i_1j_12}u_{i_1j_1n}\right)+\ldots+$$

$$+p_{n-1nk}\left(\sum_{i_1<j_1} p_{i_1j_1n}u_{i_1j_1n-1} - \sum_{i_1<j_1} p_{i_1j_1n-1}u_{i_1j_1n}\right) =$$

$$= p_{12k}\sum_{i_1<j_1} p_{i_1j_12}u_{i_1j_11} + p_{13k}\sum_{i_1<j_1} p_{i_1j_13}u_{i_1j_11} + ... + p_{1nk}\sum_{i_1<j_1} p_{i_1j_1n}u_{i_1j_11})+$$

$$+\left(-p_{12k}\sum_{i_1<j_1} p_{i_1j_11}u_{i_1j_12} + p_{23k}\sum_{i_1<j_1} p_{i_1j_13}u_{i_1j_12} + ... + p_{2nk}\sum_{i_1<j_1} p_{i_1j_1n}u_{i_1j_12}\right)+$$

$$+\left(-p_{13k}\sum_{i_1<j_1} p_{i_1j_11}u_{i_1j_13} - p_{23k}\sum_{i_1<j_1} p_{i_1j_12}u_{i_1j_13} + ... + p_{3nk}\sum_{i_1<j_1} p_{i_1j_1n}u_{i_1j_13}\right)+ ...+$$

$$+\left(-p_{1nk}\sum_{i_1<j_1} p_{i_1j_11}u_{i_1j_1n} - p_{2nk}\sum_{i_1<j_1} p_{i_1j_12}u_{i_1j_1n} - ... - p_{n-1nk}\sum_{i_1<j_1} p_{i_1j_1n-1}u_{i_1j_1n}\right) =$$

$$= (\ 0\ p_{12k}\ p_{13k}\ ...\ p_{1nk}) \begin{pmatrix} \sum\limits_{i_1<j_1} p_{i_1j_11}u_{i_1j_11} \\ \sum\limits_{i_1<j_1} p_{i_1j_12}u_{i_1j_11} \\ \sum\limits_{i_1<j_1} p_{i_1j_13}u_{i_1j_11} \\ \dotfill \\ \sum\limits_{i_1<j_1} p_{i_1j_1n}u_{i_1j_11} \end{pmatrix} +$$

$$+ (-p_{12k}\ 0\ p_{23k}\ ...\ p_{2nk}) \begin{pmatrix} \sum\limits_{i_1<j_1} p_{i_1j_11}u_{i_1j_12} \\ \sum\limits_{i_1<j_1} p_{i_1j_12}u_{i_1j_12} \\ \sum\limits_{i_1<j_1} p_{i_1j_13}u_{i_1j_12} \\ \dotfill \\ \sum\limits_{i_1<j_1} p_{i_1j_1n}u_{i_1j_12} \end{pmatrix} +$$

$$+ (-p_{13k}\ \ -p_{23k}\ 0\ \ ...\ p_{2nk}) \begin{pmatrix} \sum\limits_{i_1<j_1} p_{i_1j_11}u_{i_1j_12} \\ \sum\limits_{i_1<j_1} p_{i_1j_12}u_{i_1j_12} \\ \sum\limits_{i_1<j_1} p_{i_1j_13}u_{i_1j_12} \\ \dotfill \\ \sum\limits_{i_1<j_1} p_{i_1j_1n}u_{i_1j_12} \end{pmatrix} + ...+$$

$$+(-p_{1nk}\ -p_{2nk}\ -\ ...\ -p_{n-1nk}\ 0\ )\begin{pmatrix} \sum\limits_{i_1<j_1} p_{i_1j_11}u_{i_1j_1n} \\ \sum\limits_{i_1<j_1} p_{i_1j_12}u_{i_1j_1n} \\ \sum\limits_{i_1<j_1} p_{i_1j_13}u_{i_1j_1n} \\ \dots\dots\dots\dots \\ \sum\limits_{i_1<j_1} p_{i_1j_1n}u_{i_1j_1n} \end{pmatrix} =$$

$$=(\ 0\ p_{12k}\ p_{13k}\ ...\ p_{1nk})\begin{pmatrix} p_{121}\ p_{131}\ p_{141}\ \cdots\ p_{n-1n1} \\ p_{122}\ p_{132}\ p_{142}\ \cdots\ p_{n-1n2} \\ p_{123}\ p_{133}\ p_{143}\ \cdots\ p_{n-1n3} \\ \dots\dots\dots\dots\dots\dots \\ p_{12n}\ p_{13n}\ p_{14n}\ \cdots\ p_{n-1nn} \end{pmatrix}\begin{pmatrix} u_{121} \\ u_{131} \\ u_{141} \\ \dots\dots \\ u_{n-1n1} \end{pmatrix}+$$

$$+(-p_{12k}\ 0\ p_{23k}\ ...\ p_{2nk})\begin{pmatrix} p_{121}\ p_{131}\ p_{141}\ \cdots\ p_{n-1n1} \\ p_{122}\ p_{132}\ p_{142}\ \cdots\ p_{n-1n2} \\ p_{123}\ p_{133}\ p_{143}\ \cdots\ p_{n-1n3} \\ \dots\dots\dots\dots\dots\dots \\ p_{12n}\ p_{13n}\ p_{14n}\ \cdots\ p_{n-1nn} \end{pmatrix}\begin{pmatrix} u_{122} \\ u_{132} \\ u_{142} \\ \dots\dots \\ u_{n-1n2} \end{pmatrix}+$$

$$+(-p_{13k}\ -p_{23k}\ 0\ ...\ p_{3nk})\begin{pmatrix} p_{121}\ p_{131}\ p_{141}\ \cdots\ p_{n-1n1} \\ p_{122}\ p_{132}\ p_{142}\ \cdots\ p_{n-1n2} \\ p_{123}\ p_{133}\ p_{143}\ \cdots\ p_{n-1n3} \\ \dots\dots\dots\dots\dots\dots \\ p_{12n}\ p_{13n}\ p_{14n}\ \cdots\ p_{n-1nn} \end{pmatrix}\begin{pmatrix} u_{123} \\ u_{133} \\ u_{143} \\ \dots\dots \\ u_{n-1n3} \end{pmatrix}+...+$$

$$+(-p_{1nk}\ -p_{2nk}\ -p_{3nk}\ ...\ -p_{n-1nk}\ 0\ )\begin{pmatrix} p_{121}\ p_{131}\ p_{141}\ \cdots\ p_{n-1n1} \\ p_{122}\ p_{132}\ p_{142}\ \cdots\ p_{n-1n2} \\ p_{123}\ p_{133}\ p_{143}\ \cdots\ p_{n-1n3} \\ \dots\dots\dots\dots\dots\dots \\ p_{12n}\ p_{13n}\ p_{14n}\ \cdots\ p_{n-1nn} \end{pmatrix}\begin{pmatrix} u_{12n} \\ u_{13n} \\ u_{14n} \\ \dots\dots \\ u_{n-1nn} \end{pmatrix}\equiv$$

$$\equiv 0\ (\mod |a_k|),$$

что вытекает из условия (3).

Легко видеть, что нуль аддитивной группы $\langle F,\ +\ \rangle$ является единичным элементом относительно умножения и для любого элемента $x \in F$ противоположный элемент $-x$ является обратным для x. Следовательно, $\langle F,\ \cdot\ \rangle$ является группой. Непосредственной проверкой устанавливается, что для любых $x, y \in F$ имеет место равенство $x \cdot y \cdot x = x + y + x$. Таким образом, система $\langle F,\ +\ ,\ \cdot\ \rangle$ является метаполем.

Вычислением находим, что $[a_j,\ a_i] = 2\sum\limits_{k=1}^{n} p_{ijk}a_k$, откуда $v(a_i,\ a_j) = \sum\limits_{k=1}^{n} p_{ijk}a_k$ и в соответствии с определением (3) M является характеристическим числовым набором метаполя относительно порождающего множества $\{a_1, ..., a_n\}$. □

Заметим, что при $n \geqslant 3$ существует набор целых чисел $M = \{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ такой, что группа $\langle F,\ \cdot\ \rangle$ неабелева, а значит, соответствующее метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ нетривиально.

Следствие 1. *Всякая конечно порожденная абелева группа без кручения ранга* $\geqslant 3$ *является аддитивной группой некоторого нетривиального метаполя.*

Следствие 2. *Всякий набор целых чисел* $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$*, удовлетворяющий условию* (3)*, является характеристическим набором некоторого метаполя без кручения ранга* n.

3. Применение метаполей для описания конечно порожденных метабелевых групп без инволюций

Теорема 5. *Для любой метабелевой группы* G *без инволюций и любого* $a \in C(G)$ *существует метабелева группа* G_1 *без инволюций и изоморфное вложение* f *группы* G *в группу* G_1 *такое, что если* $f(G) = G_0$, $f(a) = a_0$*, то существует* $\sqrt{a_0} \in C_{G_1}(G_o)$ *и группа* G_1 *порождается множеством* $\{G_0,\ \sqrt{a_0}\}$*. При этом* $G_0 \triangleleft G_1$ *и* $G_0' = G_1'$.

Доказательство. Пусть группа G с единицей e не содержит элементов порядка 2 и $a \in C(G)$. Если существует $\sqrt{a} \in G$, то $G_1 = G$ по лемме 1 $\sqrt{a} \in C(G)$ и теорема доказана. Предположим теперь, что в группе G не существует $\sqrt{a}$, и будем использовать символы $\varnothing$, $\sqrt{a}$. Рассмотрим множество пар $G_1 = \{(g, \varnothing),\ (g, \sqrt{a}) \mid g \in G\}$. Две пары из G_1 считаем равными, если равны соответствующие компоненты пар. Определим на множестве G_1 операцию умножения, положив для любых пар (g_1, x), (g_2, y) из G_1 $(g_1, x) \cdot (g_1, y) = (g, z)$, где

$$z = \begin{cases} \sqrt{a}, \text{ если } x = \varnothing,\ y = \sqrt{a} \text{ или } x = \sqrt{a},\ y = \varnothing, \text{ и тогда } g = g_1 g_2; \\ \varnothing, \text{ если } x = \varnothing,\ y = \varnothing, \text{ и тогда } g = g_1 g_2; \\ \varnothing, \text{ если } x = \sqrt{a},\ y = \sqrt{a}, \text{ и тогда } g = g_1 g_2 a. \end{cases}$$

Легко доказать, что определенное таким образом умножение пар ассоциативно, единицей будет пара $(e, \varnothing)$ и для любого элемента $g \in G$ имеем $(g, \varnothing)^{-1} = (g^{-1}, \varnothing)$, $(g, \sqrt{a})^{-1} = (g^{-1}a^{-1}, \sqrt{a})$. Таким образом, система $\langle G_1, \cdot \rangle$ является группой. Легко проверить также, что для любых пар (g_1, x), (g_2, y) из G_1 коммутатор $[(g_1, x),\ (g_2, y)] = ([g_1, g_2], \varnothing)$ и принадлежит центру группы G_1. Следовательно, группа $\langle G_1, \cdot \rangle$ метабелева.

Докажем, что G_1 не содержит инволюций. Предположим противное: пусть пара (g, x) имеет порядок 2, то есть $g \neq e$ и $(g, x) \cdot (g, x) = (e, \varnothing)$. Тогда при $x = \varnothing$ получаем $(g, \varnothing) \cdot (g, \varnothing) = (g^2, \varnothing) = (e, \varnothing)$, откуда $g^2 = e$, что противоречит условию. При $x = \sqrt{a}$ получаем $(g, \sqrt{a}) \cdot (g, \sqrt{a}) = (g^2 a, \varnothing) = (e, \varnothing)$, откуда $g^2 a = e$ и $a = g^{-2}$. Следовательно, $\sqrt{a} = g^{-1} \in G$, что снова противоречит условию.

Легко видеть, что $(e,\ \sqrt{a})^2 = (a, \varnothing)$. Обозначим $G_0 = \{(g, \varnothing) \mid g \in G\}$. Очевидно, G_0 является подгруппой группы $\langle G_1, \cdot \rangle$, и последняя порождается множеством $\{G_0,\ (e, \sqrt{a})\}$. Наконец, отображение $f(g) = (g, \varnothing)$ для любого $g \in G$ является изоморфизмом группы G на подгруппу G_0. Если обозначить $f(a) = (a, \varnothing) = a_0$, то в соответствии с определением квадратного корня из элемента a_0 имеем $\sqrt{a_0} = (e,\ \sqrt{a})$, и группа G_1 порождается множеством $\{G_0,\ \sqrt{a_0}\}$. По лемме 1, $\sqrt{a_0} \in C_{G_1}(G_o)$, откуда $G_0 \triangleleft G_1$ и $G_0' = G_1'$. □

Определение 4. *Пусть метабелева группа* F *не содержит инволюций,* G *— подгруппа группы* $F, a \in C(G)$ *и существует* $\sqrt{a} \in C_F(G)$*. Тогда группу, порожденную множеством* $\{G,\ \sqrt{a}\}$*, будем называть простым квадратичным расширением группы* G *и обозначать*

$G(\sqrt{a})$. Группу F будем называть квадратичным расширением группы G, если существует цепочка подгрупп

$$G = G_0 \leqslant G_1 \leqslant ... \leqslant G_n = F,$$

такая, что для любого $i = 0,\ 1,\ \dots\ ,\ n-1$ группа G_{i+1} является простым квадратичным расширением группы G_i.

Теорема 6. *Для всякой конечно порожденной метабелевой группы G без инволюций существует квадратичное расширение F, в котором из всякого коммутатора извлекается квадратный корень, причем $F = G \cdot \sqrt{G'}$, где $\sqrt{G'} = \{\sqrt{[x,y]} \mid x, y \in G\}$ и $G' = F'$.*

Доказательство. В метабелевой группе G коммутант G' лежит в центре, а поскольку G конечно порождена, то абелева группа G' разлагается в прямое произведение циклических подгрупп. Пусть $G' = \langle a_1\rangle \times \langle a_2\rangle \times \ldots \langle a_k\rangle \times \langle b_1\rangle \times \langle b_2\rangle \times \ldots \times \langle b_m\rangle$, где для любого $i = 1, \ldots, k$ в G существует элемент $\sqrt{a_i}$, а для любого $j = 1, \ldots, m$ в G не существует элемента $\sqrt{b_j}$. По лемме 1, $\sqrt{a_i} \in C(G)$. Обозначим $G_0 = G$. По теореме 6 существует простое квадратичное расширение $G_1 = G_0(\sqrt{b_1})$, содержащее G, причем $G_1' = G'$. Обозначив $c_1 = \sqrt{b_1}$, получим $G_1' = \langle a_1\rangle \times \langle a_2\rangle \times \ldots \times \langle a_k\rangle \times \langle c_1^2\rangle \times \langle b_2\rangle \times \ldots \times \langle b_m\rangle$ и повторим рассуждения для b_2. На m-м шаге получим квадратичное расширение $F = G_m = G_{m-1}(\sqrt{b_m})$, где $F' = G_m' = G_0' = \langle a_1\rangle \times \ldots \times \langle a_k\rangle \times \langle c_1^2\rangle \times \ldots \times \langle c_m^2\rangle$. При этом $F = \langle G,\ c_1, \ldots, c_m\rangle$, и для любых элементов $a, b \in F$ существует, причем, как следует из леммы 1, только один элемент $v \in C(F)$ такой, что $v^2 = [a,\ b]$. □

Из доказанной теоремы 6 и теоремы 2 вытекает

Следствие 3. *Всякая метабелева группа без инволюций является подгруппой мультипликативной группы некоторого метаполя.*

Очевидно, пересечение подметаполей есть подметаполе, поэтому можно говорить о минимальном подметаполе, содержащем данное множество элементов.

Определение 5. *Будем говорить, что метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ содержит мультипликативную группу G, если мультипликативная группа метаполя содержит подгруппу G_1, изоморфную G. При этом группы G и G_1 будем отождествлять. Метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ будем называть минимальным метаполем, содержащим данную мультипликативную группу G, если оно содержит группу G и нет подметаполей, отличных от данного метаполя, содержащих G.*

Лемма 3. *Пусть метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ содержит мультипликативную группу G. Метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ является минимальным метаполем, содержащим данную мультипликативную группу G, тогда и только тогда, когда $F = G \cdot \sqrt{G'}$, где $\sqrt{G'} = \{\sqrt{[x,y]} \mid x, y \in G\}$.*

Доказательство. Пусть метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ является минимальным метаполем, содержащим данную мультипликативную группу G. В подгруппе $H = G \cdot \sqrt{G'}$ из всякого коммутатора извлекается квадратный корень. По пункту 6) теоремы 1, H является подметаполем. По условию минимальности $F = H = G \cdot \sqrt{G'}$.

Обратно, пусть метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ содержит мультипликативную группу G и $F = G \cdot \sqrt{G'}$. Предположим, что группа G является подгруппой мультипликативной группы подметаполя F_1. Тогда по пункту 6) теоремы 1 $G \cdot \sqrt{G'} \subseteq F_1$. Следовательно, $F = F_1$. □

Теорема 7. *Всякая конечно порожденная метабелева группа G без инволюций содержится в минимальном метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$, аддитивная группа которого представима в виде прямой суммы циклических групп, содержащихся в G :*

$$\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle,$$

где $a_i \in G$ для любого $i = 1,\ \dots\ ,\ n$ и произвольный элемент $x \in G$ однозначно представим в виде $x = \alpha_1 a_1 + ... + \alpha_n a_n$. Если $y = \beta_1 a_1 + ... + \beta_n a_n$, то

$$x \cdot y = \left(\sum_{k=1}^{n} \alpha_k a_k\right) \cdot \left(\sum_{k=1}^{n} \beta_k a_k\right) = \sum_{k=1}^{n} \left(\alpha_k + \beta_k + \sum_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j\beta_i - \alpha_i\beta_j)\right) a_k, \qquad (6)$$

где $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ — характеристический числовой набор данного метаполя относительно порождающего множества $\{a_1, ..., a_n\}$. Если при любом разложении аддитивной группы $\langle F,\ +\rangle$ в прямую сумму циклических подгрупп циклические прямые слагаемые принадлежат группе G, то $G = F$.

Доказательство. Пусть дана конечно порожденная метабелева группа G без инволюций. По следствию из теоремы 6, G является подгруппой мультипликативной группы некоторого минимального метаполя $\langle F,\ +\ ,\ \cdot\ \rangle$. По лемме 3, $F = G \cdot \sqrt{G'}$. Следовательно, аддитивная группа метаполя $\langle F,\ +\rangle$ конечно порождена, а значит, представима в виде прямой суммы конечного числа циклических подгрупп.

Поскольку для любого $x \in F$ элемент $x^2 \in G$, то рассмотрим сначала случай, когда $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_r\rangle \oplus \langle b_1\rangle \oplus ... \oplus \langle b_s\rangle$, где $a_i \in G$ для любого $i = 1,\ \dots\ ,\ r$, а $b_j \notin G$, но $b_j^2 \in G$ для любого $j = 1,\ \dots\ ,\ s$. Пусть $r + s = n$ и s максимально. Если предположить, что $a_1 + b_j \notin G$, то, заменив в разложении $\langle F,\ +\rangle$ прямое слагаемое $\langle a_1\rangle$ на $\langle a_1 + b_j\rangle$, мы увеличим s, что противоречит его максимальности. Следовательно, $a_1 + b_j \in G$ для любого $j = 1,\ \dots\ ,\ s$. Заменив в разложении $\langle F,\ +\rangle$ прямое слагаемое $\langle b_j\rangle$ на $\langle a_1 + b_j\rangle$, получим искомое разложение $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$, где $a_i \in G$ для любого $i = 1,\ \dots\ ,\ n$. Всякий элемент группы G однозначно представим в виде $g = \alpha_1 a_1 + ... + \alpha_n a_n$, и элементы, представленные в таком виде, перемножаются по формуле (6).

Рассмотрим теперь случай, когда при любом разложении в прямую сумму циклических подгрупп имеем $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$, где $a_i \in G$ для любого $i = 1,\ 2,\ \dots\ ,\ n$ и докажем, что $F = G$. Предположим противное: пусть элемент $h = \alpha_1 a_1 + ... + \alpha_n a_n \notin G$. Поскольку $F^2 \subseteq G$, то все коэффициенты не могут быть четными. Пусть $\alpha_1 = 2k_1 + 1, \dots, \alpha_r = 2k_r + 1$, $\alpha_{r+1} = 2k_{r+1}, \dots, \alpha_{r+s} = 2k_{r+s=n}$. Тогда $h = a_1 + ... + a_r + 2k_1 a_1 + ... + 2ka_r + 2k_{r+1}a_{r+1} + ... + 2k_{r+s=n}a_n \notin G$, откуда $b = a_1 + ... + a_r \notin G$. В то же время $\langle F,\ +\rangle = \langle b_1\rangle \oplus \langle a_2\rangle \oplus ... \oplus \langle a_n\rangle$, что противоречит предположению. Следовательно, $F = G$. □

Теорема 8. *Для всякой конечно порожденной метабелевой группы G без инволюций существуют порождающее множество $\{a_1,\ \dots\ ,\ a_n\}$ и набор целых чисел $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$, удовлетворяющий условию (3) такие, что в минимальном метаполе, содержащем данную группу, произвольный элемент $x \in G$ однозначно представим в виде $x = \prod\limits_{k=1}^{n} a_k^{\alpha_k} \prod\limits_{1 \leqslant i < j \leqslant n} \sqrt{[a_j, a_i]^{\alpha_i\alpha_j}}$ и если $y = \prod\limits_{k=1}^{n} a_k^{\beta_k} \prod\limits_{1 \leqslant i < j \leqslant n} \sqrt{[a_j, a_i]^{\beta_i\beta_j}}$, то $x \cdot y = \prod\limits_{k=1}^{n} a_k^{\gamma_k} \prod\limits_{1 \leqslant i < j \leqslant n} \sqrt{[a_j, a_i]^{\gamma_i\gamma_j}}$, где $\gamma_k = \alpha_k + \beta_k + \sum\limits_{1 \leqslant i < j \leqslant n} p_{ijk}(\alpha_j\beta_i - \alpha_i\beta_j)$, $k = 1,\ \dots\ ,\ n$.*

Доказательство. Данная метабелева группа G содержится в некотором минимальном метаполе $\langle F, +, \cdot \rangle$. По теореме 7, $\langle F, +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$, где $a_k \in G$ для любого $k = 1, ..., n$. Пусть $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ является характеристическим числовым набором данного метаполя относительно порождающего множества $\{a_1, \ldots, a_n\}$. По определению 3 это означает, что для любых элементов $x, y \in G$ существует элемент центра $v(a_i, a_j) = \sum\limits_{k=1}^{n} p_{ijk}a_k$, квадрат которого равен $[a_j, a_i]$. Произвольный элемент $x \in G$ однозначно представим в виде $x = \alpha_1 a_1 + ... + \alpha_n a_n$. По пунктам 3) и 5) теоремы 1, для любых элементов $x, y \in F$ имеем $x + y = x \cdot y \cdot \sqrt{[y, x]}$. Используя эту формулу, элемент $x = \sum\limits_{k=1}^{n} \alpha_k a_k$ можно записать в виде $x = \prod\limits_{k=1}^{n} a_k^{\alpha_k} \prod\limits_{1\leqslant i<j\leqslant n} \sqrt{[a_j, a_i]^{\alpha_i\alpha_j}}$, а формула умножения (2) перепишется в виде, указанном в формулировке теоремы. □

Определение 6. *Как доказано в теореме 7, конечно порожденная метабелева группа без инволюций G содержится в минимальном метаполе $\langle F, +, \cdot \rangle$, аддитивная группа которого имеет вид $\langle F, +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_n\rangle$, где $a_k \in G$ для любого $k = 1, ..., n$. Характеристический числовой набор данного метаполя $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ относительно порождающего множества $\{a_1, \ldots, a_n\}$ назовем характеристическим числовым набором группы G относительно этого же порождающего множества данной группы.*

Теорема 9. *Конечно порожденные метабелевы группы G и G_1 без инволюций изоморфны тогда и только тогда, когда они имеют один и тот же характеристический числовой набор относительно некоторых порождающих множеств $\{a_1, ..., a_n\}$ и $\{b_1, ..., b_n\}$ соответственно групп G и G_1, где $|a_k| = |b_k|$ для $k = 1, ..., n$.*

Доказательство. Необходимость. Пусть φ — изоморфизм конечно порожденных метабелевых групп G и G_1 без инволюций, которые содержатся в минимальных метаполях соответственно $\langle F, +, \cdot \rangle$ и $\langle F_1, +, \cdot \rangle$. По теореме 7, $\langle F, + \rangle = \langle a_1\rangle \oplus \ \ldots\ \oplus \langle a_n\rangle$, где $a_k \in G$ для любого $k = 1, ..., n$. Обозначим $\varphi(F) = \{\alpha_1\varphi(a_1) + ... + \alpha_n\varphi(a_n) \mid \alpha_1, ..., \alpha_n \in Z\}$. Легко видеть, что $\langle \varphi(F), +, \cdot \rangle$ является подметаполем метаполя $\langle F_1, +, \cdot \rangle$, содержащим группу $G_1 = \varphi(G)$. В силу минимальности метаполя $\langle F_1, +, \cdot \rangle$ получаем $F_1 = \varphi(F)$. Пусть $\{p_{ijk} \mid 1 \leq i < j \leqslant n,\ k = 1, ..., n\}$ является характеристическим числовым набором метаполя $\langle F, +, \cdot \rangle$ относительно порождающего множества $\{a_1, ..., a_n\}$. Используя формулу умножения (2), убеждаемся, что отображение $f : F \to F_1$, при котором для любого $x \in F$ $f(x) = f(\alpha_1 a_1 + ... + \alpha_n a_n) = \alpha_1\varphi(a_1) + ... + \alpha_n\varphi(a_n)$, является изоморфизмом метаполя $\langle F, +, \cdot \rangle$ на метаполе $\langle F_1, +, \cdot \rangle$. В соответствии с определением 3 имеем $v(a_i, a_j) = \sum\limits_{k=1}^{n} p_{ijk}a_k$ и $(v(a_i, a_j))^2 = [a_j, a_i]$. Поскольку $\varphi([a_j, a_i]) = [\varphi(a_j), \varphi(a_i)]$, то $v(\varphi(a_i), \varphi(a_j)) = \sum\limits_{k=1}^{n} p_{ijk}\varphi(a_k)$. Отсюда следует, что метаполе $\langle F_1, +, \cdot \rangle$, а вместе с ним и группа G_1, имеют тот же характеристический числовой набор относительно порождающего множества $\{\varphi(a_1), ..., \varphi(a_n)\}$, что и группа G относительно порождающего множества $\{a_1, ..., a_n\}$.

Достаточность. Пусть конечно порожденные метабелевы группы G и G_1 имеют один и тот же характеристический числовой набор $\{p_{ijk} \mid 1 \leqslant i < j \leqslant n,\ k = 1, ..., n\}$ относительно порождающих $\{a_1, ..., a_n\}$ и $\{b_1, ..., b_n\}$ соответственно групп G и G_1, где $|a_k| = |b_k|$ для $k = 1, ..., n$. Как вытекает из теоремы 8, искомым изоморфизмом группы G на группу G_1 является отображение $\varphi(x) = \varphi\left(\prod\limits_{k=1}^{n} a_k^{\alpha_k} \prod\limits_{1\leqslant i<j\leqslant n} \sqrt{[a_j, a_i]^{\alpha_i\alpha_j}}\right) = \prod\limits_{k=1}^{n} b_k^{\alpha_k} \prod\limits_{1\leqslant i<j\leqslant n} \sqrt{[b_j, b_i]^{\alpha_i\alpha_j}}$. □

4. Примеры групп, в которых произведение двух коммутаторов не является коммутатором

В [3] рассматривается пример группы порядка 2^{20}, в которой произведение двух коммутаторов не является коммутатором. Построим примеры метабелевых групп с таким же свойством, основываясь на вложении метабелевых групп без инволюций в метаполя.

Рассмотрим метаполе $\langle F,\ +\ ,\ \cdot\ \rangle$ с аддитивной группой $\langle F,\ +\rangle = \langle a_1\rangle \oplus \langle a_2\rangle \oplus ... \oplus \langle a_8\rangle$ и характеристическим числовым набором $\{p_{ijk} \mid 1 \leqslant i < j \leqslant 8,\ k = 1,\ \dots\ ,\ 8\}$, где $p_{125} = p_{137} = p_{236} = p_{248} = 1$, а остальные $p_{ijk} = 0$. Легко видеть, что условие (3) выполняется, а значит, по теореме 4, такое метаполе существует, причем $[a_1,\ a_2] = 2a_5$ $[a_2,\ a_3] = 2a_6$, $[a_1,\ a_3] = 2a_7$, $[a_2,\ a_4] = 2a_8$, $[a_1, a_r] = [a_2, a_s] = [a_3,\ a_r] = [a_i, a_j] = 1$, где $4 \leq r \leqslant 8$, $5 \leqslant s \leqslant 8$, $4 \leqslant i < j \leqslant 8$. Отсюда $[a_1,\ a_3] \cdot [a_2,\ a_4] = 2a_7 + 2a_8$.

Формула умножения (2) элементов данного метаполя принимает вид

$$x \cdot y = \left(\sum_{k=1}^{8} \alpha_k a_k\right) \cdot \left(\sum_{k=1}^{8} \beta_k a_k\right) =$$

$$= (\alpha_1 + \beta_1)a_1 + (\alpha_2 + \beta_2)a_2 + (\alpha_3 + \beta_3)a_3 + (\alpha_4 + \beta_4)a_4 +$$

$$+(\alpha_5 + \beta_5 + \alpha_2\beta_1 - \alpha_1\beta_2)a_5 + (\alpha_6 + \beta_6 + \alpha_3\beta_2 - \alpha_2\beta_3)a_6 +$$

$$+(\alpha_7 + \beta_7 + \alpha_3\beta_1 - \alpha_1\beta_3)a_7 + (\alpha_8 + \beta_8 + \alpha_4\beta_2 - \alpha_2\beta_4)a_8. \tag{7}$$

Используя формулу (7), вычислением находим

$$[x,\ y] = 2(\alpha_2\beta_1 - \alpha_1\beta_2)a_5 + 2(\alpha_3\beta_2 - \alpha_2\beta_3)a_6 + 2(\alpha_3\beta_1 - \alpha_1\beta_3)a_7 + 2(\alpha_4\beta_2 - \alpha_2\beta_4)a_8.$$

Если теперь предположить, что при некоторых $x, y \in F$ справедливо равенство $[a_1,\ a_3] \cdot [a_2,\ a_4] = [x,\ y]$, то приходим к равенствам $\alpha_2\beta_1 - \alpha_1\beta_2 = 0$, $\alpha_3\beta_2 - \alpha_2\beta_3 = 0$, $\alpha_3\beta_1 - \alpha_1\beta_3 = 1$, $\alpha_4\beta_2 - \alpha_2\beta_4 = 1$. Умножим первое равенство на β_3, а второе равенство на β_1 и сложим полученные равенства. Получим $\beta_2(\alpha_3\beta_1 - \alpha_1\beta_3) = 0$, а так как $\alpha_3\beta_1 - \alpha_1\beta_3 = 1$, то $\beta_2 = 0$. Аналогично, умножая первое равенство на α_3, а второе на α_1 и складывая, получим равенство $\alpha_2(\alpha_3\beta_1 - \alpha_1\beta_3) = 0$, откуда $\alpha_2 = 0$. Но тогда равенство $\alpha_4\beta_2 - \alpha_2\beta_4 = 1$ превращается в противоречивое равенство $0 = 1$. Следовательно, в мультипликативной группе данного метаполя произведение $[a_1,\ a_3] \cdot [a_2,\ a_4]$ не является коммутатором.

Наметим прямой путь построения этого примера, без обращения к теории метаполей. Вместо проверки равенства (3) и использования теоремы 4 можно взять аддитивную группу без кручения $\langle F,\ +\rangle = \langle a_1\rangle \oplus ... \oplus \langle a_8\rangle$ и на ее элементах определить умножение формулой (7); затем доказать, что $\langle F,\ \cdot\ \rangle$ является искомой метабелевой группой.

Заметим, что эти рассуждения можно повторить, считая порядки всех элементов равными простому числу $p \neq 2$. При $p = 3$ получаем метабелеву группу $\langle F,\ \cdot\ \rangle = \langle a_1,\ a_2,\ a_3,\ a_4\rangle$ экспоненты 3, где $[a_1,\ \ a_4] = [a_3,\ a_4] = e$, коммутант $F' = \langle b_1,\ b_2,\ b_3,\ b_4\rangle$, $b_1 = [a_1,\ a_2]$, $b_2 = [a_1,\ a_3]$, $b_3 = [a_2,\ a_3]$, $b_4 = [a_2,\ a_4]$, порядок группы равен $3^8 = 6561$ и произведение коммутаторов $[a_1,\ a_3] \cdot [a_2,\ a_4]$ не является коммутатором. В связи с этим возникает предположение, что во всякой группе, порядок которой меньше 6561, произведение двух коммутаторов является коммутатором.

Работа поддержана грантом КГПУ 09-09-1/НШ.

Список литературы

[1] С.В.Ларин, Метабелевы квазиполя без кручения, Всероссийская конференция по математике и механике, Тезисы докл, Томск, 2008, 52-53.

[2] А.Г.Курош, Теория групп, М., Наука, 1967.

[3] М.И.Каргаполов, Ю.И.Мерзляков, Основы теории групп, М., Наука, 1982.

Metafields and Description of Metabelian Groups without the Involutions

Sergey V.Larin

The term quasifield is introduced for the description of metabelian groups but it also bears an independent meaning. It is proved that any finally generated metabelian group contains a generating set compared to which any element has a uniquely represented record. The elements of a group are multiplied under the formula that is defined by a characteristic numerical set. In addition, the characteristic numerical set defines the group uniquely up to isomorphisms.

Keywords: metabelian group, involution, metafield, isomorphism.