ЧЕБЫШЕВСКИЙ СБОРНИК
Том 21. Выпуск 1.

УДК 512.55 DOI 10.22405/2226-8383-2020-21-1-82-100

Конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом натуральных чисел[1]

Е. М. Вечтомов, Д. В. Чупраков

Вечтомов Евгений Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой фундаментальной математики, Вятский государственный университет (г. Киров).
e-mail: vecht@mail.ru
Чупраков Дмитрий Вячеславович — кандидат физико-математических наук, доцент кафедры фундаментальной математики, Вятский государственный университет (г. Киров).
e-mail: chupdiv@yandex.ru

Аннотация

В работе исследуются конечные циклические полукольца с полурешеточным сложением, определенные как конечные циклические мультипликативные моноиды $\langle S, \cdot \rangle$ с введенной на них операцией сложения $(+)$, так, что алгебраическая структура $\langle S, + \rangle$ является верхней полурешеткой и выполняются законы дистрибутивности умножения относительно сложения.

Описано строение конечных циклических полуколец с полурешеточной аддитивной операцией, заданной двухпорожденным идеалом полукольца целых неотрицательных чисел.

Результатом работы является теорема о строении циклических полуколец с полурешеточной аддитивной операцией, заданной двухпорожденным идеалом полукольца целых неотрицательных чисел. Полученный результат, в частности, позволяет установить количество циклических полуколец, соответствующих каждому двухпорожденному идеалу полукольца целых неотрицательных чисел.

В работе используется аппарат идеалов полукольца целых неотрицательных чисел. Получены некоторые свойства идеалов полукольца целых неотрицательных чисел, определяющих структуру конечных циклических полуколец.

Работа дополняет исследования Е. М. Вечтомова и И. В. Орловой, где строение конечных циклических полуколец с идемпотентным некоммутативным сложением описано через конечные циклические полуполя и конечные циклические полукольца с полурешеточным сложением.

Ключевые слова: конечное циклическое полукольцо, полурешеточное сложение, полукольцо целых неотрицательных чисел, идеал.

Библиография: 27 названий.

Для цитирования:
Е. М. Вечтомов, Д. В. Чупраков. Конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом натуральных чисел // Чебышевский сборник, 2020, т. 21, вып. 1, с. 82–100.

[1]Работа выполнена при финансовой поддержке государственного задания Минобрнауки РФ «Полукольца и их связи», проект № 1.5879.2017/8.9.

CHEBYSHEVSKII SBORNIK
Vol. 21. No. 1.

UDC 512.55 DOI 10.22405/2226-8383-2020-21-1-82-100

Finite cyclic semirings with semilattice additive operation defined by two-generated ideal of natural numbers

E. M. Vechtomov, D. V. Chuprakov

E. M. Vechtomov — Doctor of Physical and Mathematical Sciences, Professor, Head of Department fundamental mathematics, Vyatka State University (Kirov).
e-mail: vecht@mail.ru
D. V. Chuprakov — Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Fundamental Mathematics, Vyatka State University (Kirov).
e-mail: chupdiv@yandex.ru

Abstract

The article deals with finite cyclic semirings with a semilattice addition which are defined as finite cyclic multiplicative monoids $\langle S, \cdot \rangle$ with an operation of addition $(+)$ such that the algebraic structure $\langle S, + \rangle$ is an upper semilattice and laws of distributivity of multiplication over addition are satisfied.

The structure of finite cyclic semirings with a semilattice additive operation defined by a two-generated semiring of nonnegative integers is described.

The result of the work is a theorem about a structure of cyclic semirings with the semilattice additive operation defined by a two-generated ideal of non-negative numbers. This fact, in particular, allows to calculate the number of cyclic semirings corresponding to each two-generated ideal of non-negative integers.

The method of ideals of a semiring of nonnegative integers is used in the article. Some properties of ideals of semirings of nonnegative integers determining the structure of finite cyclic semirings are obtained.

This work complements the research of E. M. Vechtomova and I. V. Orlova where the structure of finite cyclic semirings with idempotent noncommutative addition is described in terms of cyclic semifields and finite cyclic semirings with semilattice addition.

Keywords: finite cyclic semiring, semilattice addition, semiring of non-negative integers, ideal.

Bibliography: 27 titles.

For citation:
E. M. Vechtomov, D. V. Chuprakov, 2020, "Finite cyclic semirings with semilattice additive operation defined by two-generated ideal of natural numbers" , *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 82–100.

1. Введение. Основные понятия

Работа посвящена исследованию конечных мультипликативно циклических полуколец с *полурешеточным* (т. е. идемпотентным коммутативным) сложением.

Полукольцом [27] называется алгебраическая структура $\langle S, +, \cdot \rangle$, представляющая собой непустое множество S с заданными на нем двумя ассоциативными бинарными операциями сложения $(+)$ и умножения $(\cdot)$, такими, что умножение дистрибутивно относительно сложения

с обеих сторон: $x(y+z) = xy+xz$, $(x+y)z = xz+yz$. При этом $\langle S, + \rangle$ — аддитивная полугруппа полукольца S, а $\langle S, \cdot \rangle$ — его мультипликативная полугруппа.

Полукольцо может обладать выделенными элементами: нулем 0 — нейтральным по сложению ($x + 0 = 0 + x = x$) и поглощающим по умножению ($x \cdot 0 = 0 \cdot x = 0$) и единицей 1 — нейтральным элементом по умножению ($x \cdot 1 = 1 \cdot x = x$). Полукольцо, мультипликативная полугруппа которого является абелевой группой, называется *полуполем*.

В любом полукольце S с полурешеточным сложением естественным образом вводится разностный порядок:

$$a \leqslant b \Longleftrightarrow \exists c \in S \; a + c = b, \qquad \text{для всех } a, b \in S. \tag{1}$$

При этом $a + b = \sup\{a, b\}$.

Полукольцо S называется (*мультипликативно*) *циклическим* с образующим α, в обозначениях $S = (\alpha)$, если его мультипликативная полугруппа $\langle S, \cdot \rangle$ является циклической полугруппой $\{\alpha, \alpha^2, \ldots, \alpha^n\}$, элемент α — образующий этой полугруппы. При этом, если циклическое полукольцо S содержит единицу 1, то $1 = \alpha^0$.

Циклическая структура играет важную роль в современной математике. Хорошо известно строение циклических групп, их значение в теории групп [12]. Полностью описаны циклические (моногенные) полугруппы [14]. Класс неодноэлементных циклических колец в точности совпадает с классом конечных полей [13]. Также известна структура полуколец с циклическим сложением [18]. Обзор основных результатов теории циклических полуколец приведен в работе [6]. Циклические и идемпотентные алгебраические структуры находят приложения в теории кодирования и криптологии [24, 25, 26], в частности теория конечных полей положена в основу названных дисциплин [15].

Напомним, что циклической полугруппой $\langle S, \cdot \rangle$ называется множество S с заданной на нем ассоциативной операцией умножения $(\cdot)$, имеющей образующий элемент α, натуральные степени которого α^k, $k \in \mathbb{N}$, исчерпывают множество S. Любая конечная циклическая полугруппа S с образующим α однозначно характеризуется парой натуральных чисел $k, l \in \mathbb{N}$ такими, что $S = \{\alpha, \alpha^2, \ldots, \alpha^n, \ldots, \alpha^{n+l-1}\}$ и $\alpha^{n+l} = \alpha^n$ [14]. Множество $\{\alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ называют хвостом, а множество $\{\alpha^n, \ldots, \alpha^{n+l-1}\}$ — циклом полугруппы S. При наличии единицы n-элементная циклическая полугруппа имеет вид $T = \{1, \alpha, \ldots, \alpha^{n-1}, \ldots, \alpha^{n+l-2}\}$, где $a^{n+l-1} = a^{n-1}$.

Конечные циклические полугруппы без хвоста ($k = 1$) и только они являются конечнными группами. При $l = 1$, в свою очередь, будем иметь n-элементную циклическую полугруппу $S = \{\alpha, \alpha^2, \ldots, \alpha^n\}$ с поглощающим элементом α^n.

Далее будем рассматривать только конечные циклические полугруппы, не являющиеся группами, иными словами $n \geqslant 2$.

Задавая на мультипликативных полугруппах S и T всевозможные полукольцевые операции сложения, мы получим все конечные циклические полукольца, отличные от полуполей. Биекция $a^m \leftrightarrow a^{m-1}$, $m \in \{1, ..., n+l-1\}$, между ними позволяет переносить операцию сложения с S на T, и обратно [10]. Таким образом, между классом всех циклических полуколец без единицы и классом всех циклических полуколец с единицей существует естественное взаимно однозначное соответствие.

Отметим, что мультипликативная полугруппа любого конечного циклического полукольца с коммутативным сложением имеет одноэлементный цикл $\{\alpha^n\}$ (см. [2]), иными словами, выполняется свойство $\alpha^n = \alpha^{n+1}$. Таким образом, α^n является поглощающим элементом как по сложению, так и по умножению.

Задача исследования циклических полуколец с коммутативным сложением поставлена Е. М. Вечтомовым в 2000 году [5, задача 8]. В этой работе описаны бесконечные циклические полукольца с коммутативным сложением [5, теорема 4].

Систематическое изучение конечных циклических полуколец ведется с 2010 года [22]. Подробный обзор результатов исследований циклических полуколец приведен в статье [6]. Мы отметим только основные вехи изучения конечных циклических полуколец с идемпотентным сложением.

Начиная с доклада [2], Е. М. Вечтомовым и И. В. Орловой исследуются циклические полукольца с некоммутативным сложением [7, 8, 9, 16]. В частности, изучение конечных циклических полуколец с идемпотентным некоммутативным сложением сведено к конечным циклическим полуполям и конечным циклическим полукольцам с полурешеточным сложением [7].

Начало исследований конечных циклических полуколец с полурешеточным сложением положено А. С. Бестужевым в работе [1]. В этой работе установлено, что свойства операции сложения в конечном циклическом полукольце с полурешеточным сложением определяются элементами, непосредственно большими 1, и в терминах полурешеток описаны идемпотентные конечные циклические полукольца, представимые полурешетками ширины $m \leqslant 3$.

Дальнейшее исследование ведется Е. М. Вечтомовым, Д. В. Чупраковым и А. В. Ведерниковой [4, 21, 23]. В статье [4] задача описания конечных циклических полуколец с полурешеточным сложением сведена к исследованию свойств идеалов полукольца целых неотрицательных чисел. В докладе [23] изложен алгоритм построения конечных циклических полуколец с полурешеточным сложением по числу элементов и базису идеала показателей элементов верхнего конуса единицы полукольца. В работе [21] описаны конечные циклические полукольца с полурешеточным сложением, заданные идеалом полукольца целых неотрицательных чисел с двумя взаимно простыми образующими. Наконец, основные результаты данной работы анонсированы в докладах [11, 20].

Ниже в работе мы будем рассматривать циклические полукольца $S = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ с полурешеточным сложением.

2. Представление конечных мультипликативных циклических полуколец с полурешеточным сложением

Через $\mathbb{N}_0$ обозначим полукольцо целых неотрицательных чисел с арифметическими операциями сложения и умножения. Рассмотрим отрезок первых $n+1$ целых неотрицательных чисел $\{0, 1, \ldots, n\}$ и введем на нем аддитивную $(+)$ и мультипликативную $(\cdot)$ операции, заданные для всех $x, y \in \{0, 1, \ldots, n\}$ формулами

$$x + y = \min_{x,y,n \in \mathbb{N}_0} \{x + y, n\}, \qquad x \cdot y = \min_{x,y,n \in \mathbb{N}_0} \{xy, n\}.$$

Построенная алгебра $\mathbb{N}_n = \langle\, \{0, 1, \ldots, n\}, +, \cdot \,\rangle$ является полукольцом.

Пусть $S = \{1, \alpha, \ldots, \alpha^n\}$ — $(n+1)$-элементное циклическое полукольцо с единицей и полурешеточным сложением. На полукольце $\mathbb{N}_n$ зададим порядок $\preccurlyeq$ правилом

$$x \preccurlyeq y \Longleftrightarrow \alpha^x \leqslant \alpha^y \tag{2}$$

для всевозможных $x, y \in \mathbb{N}_n$.

Порядок $\preccurlyeq$ будем называть *порядком, индуцированным конечным циклическим полукольцом* S, а упорядоченное полукольцо $\langle \mathbb{N}_n, \preccurlyeq \rangle$ — *полукольцом показателей* S.

Отображение $\alpha^i \to i$ устанавливает порядковый изоморфизм

$$\langle S, \leqslant \rangle \cong \langle \mathbb{N}_n, \preccurlyeq \rangle \tag{3}$$

между полукольцом S с разностным порядком, заданным правилом (1), и полукольцом $\mathbb{N}_n$ с порядком $\preccurlyeq$.

Естественный линейный порядок на множестве $\mathbb{N}_n$ обозначим через $\leqslant$.

Вводя на верхней полурешетке $\langle \mathbb{N}_n, \preccurlyeq \rangle$ аддитивную операцию $\vee_{\preccurlyeq}$ правилом

$$b \vee_{\preccurlyeq} c = \sup\{b, c\}, \qquad b, c \in \mathbb{N}_n,$$

получаем полукольцо

$$\check{\mathbb{N}}_n = \langle \mathbb{N}_n, \vee_{\preccurlyeq}, + \rangle,$$

изоморфное полукольцу S.

Таким образом, $(n+1)$-элементное циклическое полукольцо S с полурешеточным сложением однозначно определяется своей аддитивной полугруппой $\langle S, + \rangle$.

На полукольце $\mathbb{N}_n$ имеет место аналог сократимости [4, лемма 1]. Если $x + d = y + d < n$ для некоторого $d \in \mathbb{N}_n$, то $x = y$.

Определим в $\mathbb{N}_n$ разность $y - x$ как наименьший элемент d, относительно естественного порядка $\leqslant$ такой, что $x + d = y$. Тогда для любых $x, y \in \mathbb{N}$, если $n - y = n - x$, то $x = y$.

Значит, в силу дистрибутивности в конечном циклическом полукольце S операция полурешеточного сложения однозначно задается суммами единицы со всеми его элементами $\alpha^{p_k} = 1 + \alpha^k, k \in \{0, 1, \ldots, n\}$. Иными словами, каждое $(n+1)$-элементное циклическое полукольцо S с полурешеточным сложением однозначно задается $(n+1)$-элементным кортежем:

$$(p_0, p_1, \ldots, p_n) \in \{0, 1, \ldots, n\}^{n+1}, \text{ где } 1 + \alpha^i = \alpha^{p_i}. \tag{4}$$

Операции $\vee_{\preccurlyeq}$ и $+$ на полукольце $\check{\mathbb{N}}_n$ связаны следующим соотношением:

$$b \vee_{\preccurlyeq} c = \min\{b, c\} + p_{|b-c|}.$$

Обозначим через I множество всех компонент кортежа (4) конечного полукольца S:

$$I = \big\{p_i : i \in \{0, 1, \ldots, n\}\big\}. \tag{5}$$

Множество I обладает следующими свойствами:

1. Множество $I \subseteq \mathbb{N}_n$ является верхним конусом нуля $0 \in \mathbb{N}_n$ относительно порядка $\preccurlyeq$.
2. Множество I является множеством показателей элементов S, выдерживающих прибавление единицы:
$$I = \big\{k \in \{0, 1, \ldots, n\} : k = p_k\big\}.$$
3. Множество I является идеалом полукольца $\mathbb{N}_n$ [4, Теорема 2].

Лемма 1. *Для любых элементов a и b полукольца $\mathbb{N}_n$ с отношением $\preccurlyeq$, индуцированным полукольцом S, справедливо свойство:*

$$a \preccurlyeq b \Longleftrightarrow b = a + j, \text{ для некотого } j \in I, \tag{6}$$

где I — множество элементов кортежа (4)*, задающего полукольцо S.*

Доказательство. Для любых двух элементов a и b полукольца $\mathbb{N}_n$, отношение $a \preccurlyeq b$ по определению (2) равносильно отношению $\alpha^a \leqslant \alpha^b$ в S, что, в свою очередь, по (1) равносильно $\alpha^b = \alpha^a + \alpha^b = \alpha^a(1 + \alpha^c) = \alpha^{a+p_c}$. Иными словами, $b = a + j$ для $j = p_c \in I$.

Обратно, пусть $b = a + j$ и $j \in I$. По свойству 2 справедливо равенство $j = p_j$ и, следовательно, $\alpha^b = \alpha^a(1 + \alpha^j) = \alpha^a + \alpha^{(a+j)} = \alpha^a + \alpha^b$, что равносильно $a \preccurlyeq b$. Лемма доказана.

Обозначим через I_k множество показателей элементов верхнего конуса $\{\alpha^k\}^{\triangle}$ конечного циклического полукольца S. В силу леммы 1 выполняется равенство $I_k = I + k$.

Так как полукольцо S является верхней полурешеткой, то и для каждого индекса $k \in \{0, 1, 2, \ldots, n\}$ справедливо равенство

$$p_k = \min(I \cap I_k). \tag{7}$$

Отсюда вытекает справедливость следующих утверждений, характеризующих взаимосвязь порядков:

Следствие 1 ([21, лемма 3]). *Для любых элементов $k, l \in \mathbb{N}_n$ и порядка $\preccurlyeq$, индуцированного конечным циклическим полукольцом S, из справедливости неравенства $k \preccurlyeq l$ следует $k \leqslant l$, а если $k \leqslant l$, то либо $k \preccurlyeq l$, либо k и l несравнимы.*

Следствие 2 ([4, предложение 2]). *Для каждого элемента p_k кортежа (4), задающего некоторое конечное циклическое полукольцо с полурешеточным сложением, справедливо неравенство $p_k \geqslant k$.*

Идеал I полукольца $\mathbb{N}_n$ конечен и, значит, порожден конечным базисом $G = \{g_1, \ldots, g_l\}$, то есть каждый элемент $b \in I$ представим в виде линейной комбинации $b = \sum_{i=1}^{l} k_i g_i$, где $k_1, \ldots, k_l \in \mathbb{N}_n$ и никакой элемент множества G нельзя представить в виде комбинации остальных элементов G с коэффициентами из $\mathbb{N}_n$. Ясно, что поглощающий элемент n полукольца $\mathbb{N}_n$ может быть базисным только в случае, когда $I = \{0, n\}$.

Так как построение базиса идеала I сводится к последовательному выбору наименьшего элемента $i_j \in I$, не представимого в виде комбинации $i_1, \ldots, i_{j-1}$, то базис идеала I определен однозначно.

Идеал I, порожденный базисом $G = \{g_1, \ldots, g_l\}$, будем обозначать $I = \langle g_1, g_2, \ldots, g_l \rangle$.

Заметим, что имеют место следующие предложения:

Предложение 1 ([21, предложение 3]). *Каждое упорядоченное множество $\langle I_k, \preccurlyeq \rangle$ относительно порядка $\preccurlyeq$, индуцированного конечным циклическим полукольцом S с полурешеточным сложением по правилу (2), является решеткой с наименьшим элементом k и наибольшим — n. Атомами решетки $\langle I_k, \preccurlyeq \rangle$ являются в точности элементы вида $k + g_i$ для всевозможных базисных элементов g_i идеала I.*

Предложение 2 ([4, теорема 3]). *Кортеж (4), определяющий полурешеточную операцию сложения $(n+1)$-элементного циклического полукольца S, однозначно восстанавливается по множеству G базисных элементов идеала его компонентов.*

Идеал полукольца целых неотрицательных чисел $J = \langle g_1, g_2, \ldots, g_l \rangle$ с базисом $G = (g_1, g_2, \ldots, g_l)$ будем называть идеалом, *ассоциированным с полукольцом S*. Полукольцо S, в свою очередь, назовем *ассоциированным с идеалом J*.

Ясно, что для каждого $(n+1)$-элементного циклического полукольца S, ассоциированного с идеалом натуральных чисел J, множество элементов $I = \{p_i : i \in \{0, 1, \ldots, n\}\}$ кортежа (4) выражается через идеал J следующим образом:

$$I = \{\min\{j, n\} : j \in J\} \cup \{n\} \tag{8}$$

3. Общие свойства конечных циклических полуколец с полурешеточным сложением

Лемма 2 ([21, лемма 2]). *Если элемент $p_j \neq n$ идеала $I \subseteq \mathbb{N}_n$ с базисом $G = \{g_1, \ldots, g_l\}$ представлен в виде*

$$p_j = \sum_{i=1}^{l} c_i g_i = k + \sum_{i=1}^{l} d_j g_j, \qquad c_i, d_i \in \mathbb{N}_n,$$

то $\min\{c_i, d_i\} = 0$ для каждого $i \in \{1, 2, \ldots, l\}$.

Теорема 1 (критерий существования конечного циклического полукольца с полурешеточным сложением [21, теорема 1]). *Пусть I — идеал полукольца $\mathbb{N}_n$, порожденный базисом $G = \{g_1, g_2, \dots, g_l\}$, и на полукольце $\mathbb{N}_n$ определен порядок $\preccurlyeq$ свойством:*

$$b \preccurlyeq c \Longleftrightarrow c = b + j, \text{ для некоторого } j \in I.$$

Тогда следующие условия равносильны:

1) *существует единственное $(n+1)$-элементное циклическое полукольцо S с образующим α и полурешеточным сложением, заданным кортежем:*

$$(p_0, p_1, \dots, p_n), \qquad 1 + \alpha^i = \alpha^{p_i}, \qquad p_i \in I,$$

причем, каждый элемент идеала I входит в кортеж;

2) *идеал I является решеткой относительно порядка $\preccurlyeq$;*

3) *для каждого элемента k полукольца $\mathbb{N}_n$ найдется элемент $p_k \in I$ такой, что $I \cap I_k = I_{p_k}$;*

4) *для каждого элемента $k < \min G$ полукольца $\mathbb{N}_n$ найдется элемент $p_k \in I$ такой, что $I \cap I_k = I_{p_k}$.*

Лемма 3. *Пусть $(n+1)$-элементное циклическое полукольцо S с полурешеточной аддитивной операцией, заданной кортежем*

$$(p_0, p_1, \dots, p_n,) \in \{0, 1, \dots, n\}^{n+1}$$

ассоциировано с идеалом полукольца целых неотрицательных чисел $J = \langle g_1, g_2, \dots, g_l \rangle$, где наибольший общий делитель базисных элементов $g_1, g_2, \dots, g_l$ равен d. Тогда для каждого $k \in \{0, 1, 2, \dots, n\}$ элемент p_k делится на d в полукольце $\mathbb{N}_n$. При этом, если k не делится на d, то $p_k = n$.

Действительно, $n \in \mathbb{N}_n$ делится на d как поглощающий элемент, а если $p_k \neq n$, то p_k лежит в идеале J, все элементы которого кратны d. Теперь, если k не делится на d, то все элементы $J_k = J + k$ не кратны d, значит, $J \cap J_k = \varnothing$ и, следовательно, $I \cap I_k = \{n\}$, откуда $p_k = n$.

Предложение 3. *Пусть S — $(n+1)$-элементное циклическое полукольцо с полурешеточной аддитивной операцией, заданной кортежем*

$$(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}.$$

Тогда кортеж

$$(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, dn\}^{dn+1},$$

где $q_k = dn$ для всех индексов $k \in \{0, 1, \dots, dn\}$, не кратных d, и $q_{dt} = dp_t$ для всех $t \in \{0, 1, \dots, n\}$, определяет $(dn+1)$-элементное циклическое полукольцо.

Доказательство. Пусть полукольцо S задано кортежем $(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}$ и I — множество элементов этого кортежа. Рассмотрим множество $S' = \{0, 1, \dots, n\}$ и кортеж $(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, dn\}^{dn+1}$. Согласно теореме 1, этот кортеж определяет $(dn+1)$-элементное полукольцо, если справедливы условия $I' \cap I'_k = I'_{q_k}$, где $I' = \{q_0, q_1, \dots, q_{dn}\}$, $I'_k = I' + k$ для каждого $k \in \{0, 1, \dots, dn\}$. Ясно, что $I' = dI$.

Для каждого $k \in \{0, 1, \dots, dn\}$, не кратного d, множество I'_k не содержит элементов кратных d, отличных от dn — показателя поглощающего элемента. Значит, $I \cap I'_k = I'_{q_k} = \{dn\}$.

Рассмотрим теперь $k = dt$, где $t \in \{0, 1, \dots, n\}$. Имеем

$$I'_k = I' + dt = dI + dt = d\,(I + t) = dI_t,$$
$$I' \cap I'_k = d(I \cap I_t) = dI_{p_t} = I_{q_{dt}} = I_{q_k}.$$

Таким образом, по теореме 1, кортеж $(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, d\}^{dn+1}$ определяет $(dn+1)$-элементное циклическое полукольцо. Предложение доказано.

Предложение 4. *Пусть существует $(N+1)$-элементное циклическое полукольцо, ассоциированное с идеалом J полукольца целых неотрицательных чисел, порожденным базисом G. Тогда для каждого n, удовлетворяющего неравенству $M < n \leqslant N$, где $M = \min G$, найдется единственное $(n+1)$-элементное циклическое полукольцо S, ассоциированное с идеалом J полукольца целых неотрицательных чисел.*

Доказательство. Рассмотрим конечное циклическое полукольцо S с полурешеточным сложением, заданным $(N+1)$-элементным кортежем $(p_0, p_1, \ldots, p_N) \in \{0, 1, \ldots, N\}^{N+1}$. Множество I элементов этого кортежа является идеалом.

Для каждого n, удовлетворяющего неравенству $M < n \leqslant N$, рассмотрим кортеж

$$(q_0, p_1, \ldots, q_n) \in \{0, 1, \ldots, n\}^{n+1}, \qquad q_k = \min\{p_k, n\} \in \{0, 1, \ldots, n\}$$

и идеал

$$I^{'} = \{q_k : k \in \{0, 1, \ldots, n\}\}.$$

По теореме 1 достаточно показать, что для каждого $k \in \{0, 1, \ldots, n\}$ справедливо равенство $I'_{p_k} = I' \cap I'_k$.

С учетом неравенства $p_i \geqslant i$ для каждого $i \in \{0, 1, \ldots, N\}$ имеем

$$I' = \{\min\{p_i, n\} : i \in \{0, 1, \ldots, N\}\} = \{\min\{p_i, n\} : p_i \in I\};$$
$$I'_k = I' + k = \{\min\{p_i, n\} + k : p_i \in I\} = \{\min\{p_i + k, n\} : p_i \in I\} = \{\min\{p_i, n\} : p_i \in I_k\};$$
$$I' \cap I'_k = \{\min\{p_i, n\} : p_i \in I \cap I_k\} = \{\min\{p_i, n\} : p_i \in I_{p_k}\} = I'_{p_k}.$$

Предложение доказано.

Из равносильности 1) $\Longleftrightarrow$ 4) теоремы 1, равенства (8) и предложения 4 вытекает следующее утверждение.

Следствие 3. *Для каждого идеала J полукольца целых неотрицательных чисел, заданного неодноэлементным базисом $G = \{g_1, g_2, \ldots, g_l\}$, и каждого числа n, удовлетворяющего двойному неравенству*

$$\max G < n \leqslant \min \bigcup_{j=1}^{\min G - 1} \big((J \cap J_j) \setminus J_{p_j}\big),$$

существует единственное $(n+1)$-элементное циклическое полукольцо с полурешеточным сложением, ассоциированное с идеалом J, причем других полуколец с полурешеточным сложением, ассоциированных с идеалом J, нет.

Замечание 1. *Отметим, что для любого неодноэлементного главного идеала $J = (m)$, полукольца целых неотрицательных чисел каждому числу $n \geqslant m$ соответствует единственное $(n+1)$-элементное циклическое полукольцо с полурешеточным сложением, заданным кортежем $(p_0, p_1, \ldots, p_n)$, где $p_k = k$, если k кратно m, и $p_k = n$ — в противном случае.*

Предложение 5. *Пусть J' — идеал полукольца натуральных чисел и полукольцо S, ассоциировано с идеалом $J = dJ' = \{dj : j \in J'\}$ полукольца целых неотрицательных чисел, тогда S содержит подполукольцо, изоморфное полукольцу S', ассоциированному с идеалом J'.*

Доказательство. Пусть J' — идеал полукольца натуральных чисел, $J = dJ'$ и циклическое полукольцо S, ассоциированное с идеалом J, задано кортежем $(p_0, p_1, \ldots, p_n) \in \{0, 1, \ldots, n\}^{n+1}$. Обозначим через α образующий элемент S.

Рассмотрим натуральное число m, удовлетворяющее условию

$$(m-1)\, d < n \leqslant md,$$

и $(m+1)$-элементное циклическое полукольцо S', ассоциированное с идеалом J', имеющее образующий элемент $\beta \in S'$.

Пусть S' задано кортежем $(q_0, q_1, \ldots, q_m) \in \{0, 1, \ldots, m\}^{m+1}$. По предложениям 3 и 4 имеет место свойство $p_{dt} = dq_t$ для всех $t < m$.

Рассмотрим отображение $\varphi\colon S' \to S$, заданное правилом $\varphi(b^i) = \alpha^{di}$ для всех $i < m$ и $\varphi(\beta^m) = \alpha^n$.

Тогда для произвольных $i, j \leqslant m$ справедливы равенства

$$\varphi(\beta^i\beta^j) = \varphi(\beta^{\min\{i+j,m\}}) = \alpha^{\min\{d(i+j),n\}} = \alpha^{di}\alpha^{dj} = \varphi(\beta^i)\varphi(\beta^j);$$
$$\varphi(\beta^i + \beta^m) = \varphi(\beta^m) = \alpha^n = \alpha^{di} + \alpha^m = \varphi(\beta^i) + \varphi(\beta^m).$$

Для всех $i \leqslant j < m$, $i + j < m$ имеем

$$\varphi(\beta^i + \beta^j) = \varphi(\beta^i(1 + \beta^{j-i})) = \varphi(\beta^i\beta^{q_{j-i}}) = \alpha^{di}\alpha_{j-i}^{dq} = \alpha^{di}\alpha^{p_{dj-di}} =$$
$$= \alpha^{di}(1 + \alpha^{dj-di}) = \alpha^{di} + a^{dj} = \varphi(\beta^i) + \varphi(\beta^j).$$

Наконец, для всех $i \leqslant j < m$, $i + j \geqslant m$ имеем $di + dj \geqslant dm \geqslant n$ и

$$\varphi(\beta^i + \beta^j) = \varphi(\beta^m) = \alpha^n = \alpha^{di} + \alpha^{dj} = \varphi(\beta^i) + \varphi(\beta^j) =$$
$$= \alpha^{di}(1 + \alpha^{dj-di}) = \alpha^{di} + \alpha^{dj} = \varphi(\beta^i) + \varphi(\beta^j)$$

Итак, $\varphi\colon S' \to S$ — полукольцевой гомоморфизм и, следовательно, осуществляет требуемое вложение. Предложение доказано.

Следующие диаграммы Хассе (рис. 1) иллюстрируют применение предложения 5.

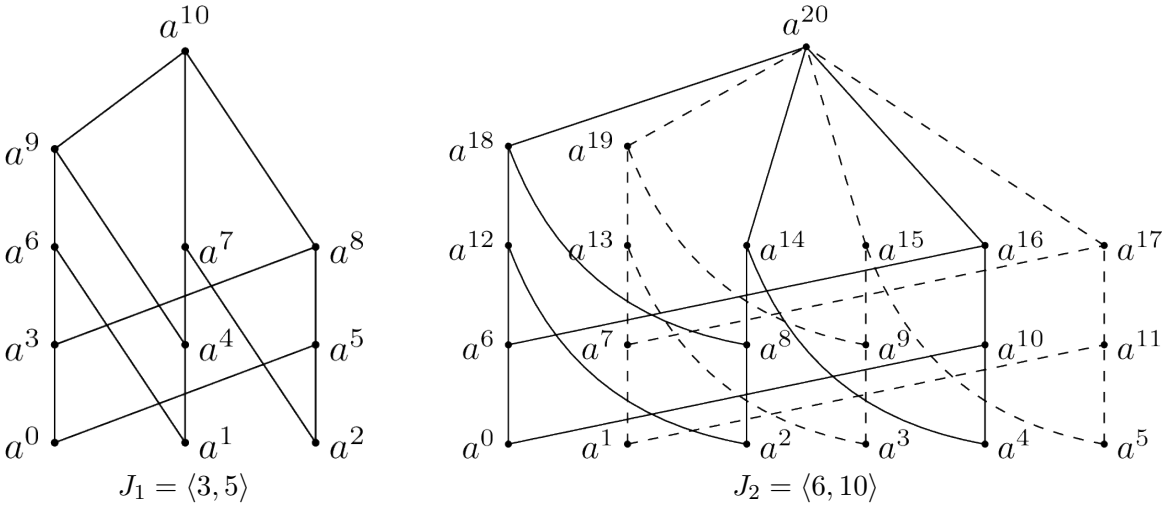

Рис. 1: Диаграммы Хассе полуколец с полурешеточным сложением

В полукольце с операцией сложения, заданной идеалом $J_2 = \langle 6, 10\rangle$, выделено подполукольцо, изоморфное полукольцу с операцией сложения, заданной идеалом $J_1 = \langle 3, 5\rangle$.

Заметим также, что для построения циклических полуколец с полурешеточным сложением полезно следующее свойство базисных элементов идеала полукольца целых неотрицательных чисел, ассоциированного с полукольцом S:

Предложение 6 ([21]). *Пусть $G = \{g_1, \ldots, g_k\}$ — базис идеала полукольца целых неотрицательных чисел, ассоциированного с полукольцом S с полурешеточным сложением. Тогда все попарные разности элементов множества G различны.*

Доказательство. Допустим, что нашлись элементы $g_{i_1}, g_{i_2}, g_{i_3}, g_{i_4} \in G$ и целое неотрицательное число Δ такие, что $g_{i_1} + \Delta = g_{i_2}$, $g_{i_3} + \Delta = g_{i_4}$.

1) Если $g_{i_2} \leqslant g_{i_3}$, то найдется неотрицательное целое число l, что $g_{i_3} = g_{i_2} + l$.

В полукольце S $\alpha^{g_{i_1}} = \alpha^{g_{i_1}} + \alpha^0$, следовательно $\alpha^{g_{i_3}} = \alpha^{g_{i_1}+l+\Delta} = \alpha^{g_{i_1}+l+\Delta} + \alpha^{l+\Delta}$. Иными словами, $\alpha^{g_{i_3}} > \alpha^{l+\Delta}$. В то же время $\alpha^{g_{i_3}} > \alpha^0$. Значит, $\alpha^{g_{i_3}} \geqslant \alpha^{p(l+\Delta)}$. Аналогично $\alpha^{g_{i_4}} \geqslant \alpha^{p(l+\Delta)}$. Так как $\alpha^{g_{i_3}}$ и $\alpha^{g_{i_4}}$ несравнимы, то $\alpha^{g_{i_3}} > \alpha^{p(l+\Delta)}$ и $\alpha^{g_{i_4}} > \alpha^{p(l+\Delta)}$, что противоречит атомарности элементов $\alpha^{g_{i_3}}$ и $\alpha^{g_{i_4}}$.

2) Если $g_{i_2} \geqslant g_{i_3}$, то существует неотрицательное целое число l, такое, что $g_{i_2} = g_{i_3} + l$. При этом $g_{i_2} = g_{i_1} + \Delta$. Если $g_{i_1} < g_{i_3}$, то $g_{i_3} = g_{i_1} + \Delta'$ и $g_{i_4} = g_{i_2} + \Delta'$, где $\Delta' + l = \Delta$. Дальнейшие рассуждения аналогичны случаю 1.

Результаты параграфа 3 позволяют свести вопрос описания структуры конечных циклических полуколец с полурешеточным сложением к задаче определения наибольшего числа элементов полукольца, ассоциированного с идеалом полукольца целых неотрицательных чисел, базисные элементы которого взаимно просты в совокупности.

4. Строение конечных циклических полуколец с полурешеточным сложением, заданным двухпорожденным идеалом полукольца целых неотрицательных чисел

В начале параграфа (леммы 4, 5, предложение 7) установим свойства идеалов полукольца целых неотрицательных чисел, полезные для исследования конечных циклических полуколец с полурешеточным сложением.

Лемма 4. *Для произвольных взаимно простых натуральных чисел g_1 и g_2, и каждого натурального числа $k \leqslant \min\{g_1, g_2\}$ существует единственная пара целых чисел v_1 и v_2 таких, что*

$$k = v_1 g_1 + v_2 g_2, \quad |v_1| \leqslant \frac{g_2}{2}, \quad |v_2| \leqslant \frac{g_1}{2}, \tag{9}$$

причем, хотя бы одно из неравенств строгое.

Доказательство. Пусть НОД$(g_1, g_2) = 1$. Для них найдется единственная пара (см. [17, предложение 61]) целых чисел u_1 и u_2, что

$$1 = u_1 g_1 + u_2 g_2, \quad |u_1| \leqslant \frac{g_2}{2}, \quad |u_2| \leqslant \frac{g_1}{2}. \tag{10}$$

Пусть $u_1 > 0$ и $u_2 < 0$. Если это не так, то изменим нумерацию чисел g_1 и g_2 и соответствующих коэффициентов u_1, u_2.

Возьмем произвольное натуральное число $k < \min\{g_1, g_2\}$, рассмотрим $k = ku_1 g_1 + ku_2 g_2$ и представим $ku_1 = q_1 g_2 + r_1$ и $-ku_2 = q_2 g_1 + r_2$. Ясно, что $r_1 \neq 0$ и $r_2 \neq 0$. Имеем

$$k = (q_1 - q_2) g_1 g_2 + r_1 g_1 - r_2 g_2.$$

Так как $k < \min\{g_1, g_2\}$, то $k + r_2 g_2 - r_1 g_1 < (r_2 + 1) g_2 - r_1 g_1 < g_1 g_2$. Следовательно, $q_1 - q_2 = 0$. Иными словами, нашлись коэффициенты $r_1 < g_2$, $r_2 < g_1$, что

$$k = r_1 g_1 - r_2 g_2.$$

Покажем, что либо $r_1 \leqslant \frac{g_2}{2}$ и $r_2 \leqslant \frac{g_1}{2}$, либо $r_1 \geqslant \frac{g_2}{2}$ и $r_2 \geqslant \frac{g_1}{2}$.

Действительно, если $r_1 > \frac{g_2}{2}$, $r_2 < \frac{g_1}{2}$, то $2r_1 = g_2 + t_1$, $2r_2 = g_1 - t_2$ для некоторых натуральных t_1 и t_2. Значит,

$$2k = 2r_1 g_1 - 2r_2 g_2 = g_1 g_2 + g_1 t_1 - g_1 g_2 + g_2 t_2 = g_1 t_1 + g_2 t_2 > g_1 + g_2.$$

Однако, $2k = 2\min\{g_1, g_2\} < g_1 + g_2$.

Аналогично, если $r_1 < \frac{g_2}{2}$, $r_2 > \frac{g_1}{2}$, то для некоторых натуральных чисел t_1, t_2 имеем $2r_1 = g_2 - t_1$, $2r_2 = g_1 + t_2$,

$$2k = g_1g_2 - g_1t_1 - g_1g_2 - g_2t_2 = -(g_1t_1 + g_2t_2) < 0,$$

что невозможно.

Итак, если $r_1 \leqslant \frac{g_2}{2}$, $r_2 \leqslant \frac{g_1}{2}$, то $v_1 = r_1$ и $v_2 = -r_2$. Если же $r_1 \geqslant \frac{g_2}{2}$, $r_2 \geqslant \frac{g_1}{2}$, то $v_1 = g_1 - r_2$ и $v_2 = r_1 - g_2$. При этом хотя бы одно из неравенств (9) строгое, так как $k \neq 0$.

Докажем единственность коэффициентов v_1 и v_2. Ясно, что если $k = v_1'g_1 + v_2'g_2$ для $v_1' \neq v_1$, $v_2' \neq v_2$, то $(v_1' - v_1)g_1 + (v_2' - v_2)g_2 = 0$ и $v_1' = v_1 + q_1g_2$, $v_2' = v_2 + q_2g_1$ для некоторых целых ненулевых q_1, q_2. Следовательно, $|v_1'| \geqslant \frac{g_2}{2}$ и $|v_2| \geqslant \frac{g_1}{2}$, причем хотя бы одно из неравенств строгое. Лемма доказана.

Непосредственно из леммы 4 вытекает

Следствие 4. *Для произвольных натуральных чисел g_1 и g_2, таких, что $d = (g_1, g_2) \neq \min\{g_1, g_2\}$, и каждого натурального числа $k \leqslant \min\{g_1, g_2\}$, кратного d, существует единственная пара целых чисел v_1 и v_2 таких, что*

$$k = v_1g_1 + v_2g_2, \quad |v_1| \leqslant \frac{g_2}{2d}, \quad |v_2| \leqslant \frac{g_1}{2d}, \tag{11}$$

причем хотя бы одно из неравенств строгое.

В линейном представлении (11) числа $k \leqslant \min\{g_1, g_2\}$ положительное слагаемое обозначим символом $k^+_{g_1,g_2}$, а отрицательное — $k^-_{g_1,g_2}$.

Лемма 5. *Для произвольных взаимно простых натуральных чисел g_1, g_2, и каждого представления натурального числа $k \leqslant \min\{g_1, g_2\}$ в виде сумм*

$$k = \alpha_1g_1 - \alpha_2g_2 = \beta_2g_2 - \beta_1g_1, \qquad \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$$

справедливы неравенства

$$\alpha_1g_1 \geqslant k^+_{g_1,g_2}, \qquad \alpha_2g_2 \geqslant -k^-_{g_1,g_2}, \qquad \beta_2g_2 \geqslant k^+_{g_1,g_2}, \qquad \beta_1g_1 \geqslant -k^-_{g_1,g_2}.$$

Доказательство. Рассмотрим взаимно простые натуральные числа g_1 и g_2 и число $k \leqslant \min\{g_1, g_2\}$. По лемме 4 найдутся целые числа v_1, v_2, что $k = v_1g_1 + v_2g_2$, $|v_1| \leqslant \frac{g_2}{2}$, $|v_2| \leqslant \frac{g_1}{2}$, причем хотя бы одно из неравенств строгое. Не умаляя общности будем считать, что

$$k^+_{g_1,g_2} = v_1g_1, \qquad k^-_{g_1,g_2} = v_2g_2.$$

Предположим, что нашлась пара натуральных чисел α_1 и α_2, для которых $k = \alpha_1g_1 - \alpha_2g_2$ и $0 < \alpha_1g_1 < k^+_{g_1,g_2}$. Тогда $\alpha_1g_1 - \alpha_2g_2 = v_1g_1 - |v_2|g_2 = k$. Так как $\alpha_1g_1 < v_1g_1$ и числа g_1 и g_2 взаимно просты, то $v_1 - \alpha_1 = \delta g_2$, для некоторого $\delta \in \mathbb{N}$.

Однако, в этом случае,

$$\alpha_1g_1 = v_1g_1 - \delta g_2g_1 \leqslant \frac{g_1g_2}{2} - \delta g_1g_2 = g_1g_2\left(\frac{1}{2} - \delta\right) < 0.$$

Получаем противоречие предположению.

Пусть натуральные числа α_1 и α_2 таковы, что $k = \alpha_1g_1 - \alpha_2g_2$ и $0 < \alpha_2g_1 < -k^-_{g_1,g_2}$. Тогда $0 < \alpha_2g_1 + k^-_{g_1,g_2} < 0$ и $0 < \alpha_1g_1 = (\alpha_2g_2 + k^-_{g_1,g_2}) + v_1g_1 < v_1g_1$. Что невозможно по доказанному выше.

Рассмотрим теперь произвольные натуральные числа β_1 и β_2, для которых выполняется условие $k = \beta_2 g_2 - \beta_1 g_1$. Имеем $\beta_2 g_2 - \beta_1 g_1 = v_1 g_1 - |v_2| g_2 = k$. В силу взаимной простоты чисел g_1 и g_2 имеет место равенство $\beta_2 + |v_2| = \delta g_1$ для некоторого натурального числа δ.

$$\beta_2 g_2 = \delta g_1 g_2 - |v_2| g_2 \geqslant \delta g_1 g_2 - \frac{g_1 g_2}{2} = g_1 g_2 \left(\delta - \frac{1}{2}\right) > \frac{g_1 g_2}{2} \geqslant |v_1| g_1 = k^+_{g_1,g_2}.$$

Итак, установлено неравенство $\beta_2 g_2 \geqslant k^+_{g_1,g_2}$.

Справедливость неравенства $\beta_1 g_1 \geqslant -k^-_{g_1,g_2}$ проверяется аналогично неравенству $\alpha_2 g_2 \geqslant \geqslant -k^-_{g_1,g_2}$. Лемма доказана.

Предложение 7. *Для каждого двупорожденного идеала целых неотрицательных чисел* $J = \langle g_1, g_2 \rangle$, НОД$(g_1, g_2) = 1$, *справедливы следующие утверждения:*

1) *наименьшим элементом множества* $J \cap J_k$ *является число* $k^+_{g_1,g_2}$;

2) *наименьшим элементом множества* $J \cap J_k$, *не лежащим во множестве* $J_{k^+_{g_1,g_2}}$, *является число* $g_1 g_2 + k^-_{g_1,g_2}$.

Доказательство. Первое утверждение непосредственно следует из лемм 4 и 5.

Докажем второе утверждение. Пусть g_1, g_2 взаимно простые базисные элементы двупорожденного идеала J. По лемме 4 для каждого $k \leqslant \min\{g_1, g_2\}$ найдется единственная пара целых чисел v_1 и v_2, удовлетворяющих условию (9). Причем хотя бы одно из неравенств $|v_1| \leqslant \frac{g_2}{2}$ или $|v_2| \leqslant \frac{g_1}{2}$ строгое.

Будем считать, что $v_1 > 0$, $v_2 < 0$. Тогда

$$k^+_{g_1,g_2} = v_1 g_1, \qquad k^-_{g_1,g_2} = v_2 g_2.$$

Обозначим

$$u_1 = (g_2 - v_1) > 0, \quad u_2 = (g_1 + v_2) > 0.$$

Ясно, что

$$k = u_2 g_2 - u_1 g_1, \qquad \frac{g_2}{2} \leqslant u_1 < g_2, \qquad \frac{g_1}{2} \leqslant u_2 < g_1. \tag{12}$$

Рассмотрим элемент $z \in J \cap J_k$, заданный равенством

$$z = u_2 g_2 = k + u_1 g_1. \tag{13}$$

Заметим, что $k^+_{g_1,g_2} \leqslant \frac{g_1 g_2}{2} \leqslant z$, причем хотя бы одно из двух неравенств строгое.

Нам нужно доказать, что $z = \min\big((J \cap J_k) \setminus J_{k^+_{g_1,g_2}}\big)$.

Сначала установим, что $z \notin J_{k^+_{g_1,g_2}}$. Действительно, предположим, что $z \in J_{k^+_{g_1,g_2}}$, тогда найдутся целые неотрицательные числа c_1, c_2:

$$z = c_1 g_1 + c_2 g_2 + k^+_{g_1,g_2}.$$

Подставляя в данное равенство линейные представления чисел $k^+_{g_1,g_2}$ и z в базисе G, получаем:

$$u_2 g_2 = (c_1 + v_1) g_1 + c_2 g_2.$$

Значит, $u_2 > c_2$ и $(u_2 - c_2) g_2 = (c_1 + u_1) g_1$. В силу взаимной простоты чисел g_1 и g_2 разность $u_2 - c_2$ делится на g_1. Откуда $u_2 - c_2 \geqslant g_1$, однако, $0 < u_2 - c_2 < u_2 < g_1$. Полученное противоречие доказывает, что $z \in (J \cap J_k) \setminus J_{k^+_{g_1,g_2}}$.

Покажем, что z — наименьший элемент множества $(J \cap J_k) \setminus J_{k^+_{g_1,g_2}}$.

Действительно, пусть $z^* \in (J \cap J_k) \setminus J_{k^+_{g_1,g_2}}$ и $z^* < z$. Ясно, что

$$k^+_{g_1,g_2} < z^* < z.$$

Так как $z^* \in J \cap J_k$, то $z^* < z$. Найдутся целые неотрицательные числа d_1, d_2, для которых выполняется равенство $z^* = d_1 g_1 + d_2 g_2$.

Используя равенства (13), получаем

$$g_1 v_1 < d_1 g_1 + d_2 g_2 < u_2 g_2.$$

Заметим, что $d_2 < u_2$ и $d_1 < v_1$. Так как, если $d_2 \geqslant u_2$, то $z^* = d_1 g_1 + (d_2 - u_2) g_2 + z \in J_{k^+_{g_1,g_2}}$, что невозможно в силу выбора z^*. Противоречие также получается, если допустить, что $d_1 \geqslant u_1$. В этом случае $z^* = (d_1 - v_1) g_1 + d_2 g_2 + z_0 \in J_{z_0}$

Так как $z^* \in J_k$, то найдутся целые неотрицательные числа e_1 и e_2 такие, что $z^* = e_1 g_1 + e_2 g_2 + k$.

Пусть $l_1 = \min\{d_1, e_1\}$, $l_2 = \min\{d_2, e_2\}$. Рассмотрим элемент

$$z' = (d_1 - l_1) g_1 + (d_2 - l_2) g_2 = (e_1 - l_1) g_1 + (e_2 - l_2) g_2 + 1 \in J \cap J_1.$$

Ясно, что $z^* = z' + l_1 g_1 + l_2 g_2$. Иными словами, $z' \leqslant z^*$.

По лемме 2 либо $d_1 - l_1 = 0$, либо $e_1 - l_1 = 0$.

Пусть $d_1 - l_1 = 0$. Обозначим $y_1 = e_1 - l_1 \neq 0$ и $y_2 = d_2 - l_2 \neq 0$. Значит, по лемме 2 $(e_2 - l_2) g_2 = 0$ и $z' = y_2 g_2 = y_1 g_1 + k$.

Имеем, $y_2 g_2 - y_1 g_1 = k$, $y_2 < g_1$ и $y_1 < g_2$.

Из доказательства леммы 4 следует, что возможно два случая:

а) $y_2 \leqslant \frac{g_1}{2}$ и $y_1 \leqslant \frac{g_2}{2}$, причем равенства не достигаются одновременно.

б) $\frac{g_1}{2} \leqslant y_2 < g_1$ и $\frac{g_2}{2} \leqslant y_1 < g_2$, причем хотя бы одно из неравенств строгое.

В случае а) $z' = z_0$ в силу (13) и леммы 4. При этом, $z^* = z_0 + l_1 g_1 + l_2 g_2 \in J_{k^+_{g_1,g_2}}$, что противоречит доказанному выше.

В случае б) $z' = z$, $z^* \geqslant z$ и, в силу произвольности выбора элемента $z^* \in (J \cap J_k) \setminus J_{z_0}$, число z — наименьший элемент множества $(J \cap J_k) \setminus J_{z_0}$.

Ситуация $(e_1 - l_1) = 0$ аналогична рассмотренной. Предложение доказано.

Непосредственно из предложения 7 вытекает

Предложение 8. *Пусть I идеал показателей элементов верхнего конуса $\{\alpha^0\}^\triangle$ конечного циклического полукольца S с полурешеточным сложением, заданный условием (5) и $G = \{g_1, g_2\}$ — его базис, причем* НОД$(g_1, g_2) = 1$. *Тогда для каждого элемента $k < \min\{g_1, g_2\}$ полукольца $\mathbb{N}_n$ элемент $p_k = k^+_{g_1,g_2}$.*

Сформулируем центральный результат работы.

Теорема 2 (о строении конечного циклического полукольца с полурешеточным сложением, заданным двухпорожденным идеалом). *Пусть натуральные числа g_1, g_2 таковы, что $d = (g_1, g_2)$ и $d < g_1 < g_2$. Каждому натуральному числу n, удовлетворяющему неравенствам*

$$g_2 < n \leqslant \frac{g_1 g_2}{d} + \min\{k^-_{g_1,g_2} : k = dt < g_1,\ t \in \mathbb{N}\}, \tag{14}$$

$$k = k^+_{g_1,g_2} + k^-_{g_1,g_2}, \qquad -\frac{g_1 g_2}{2d} \leqslant k^-_{g_1,g_2} < 0 < k^+_{g_1,g_2} \leqslant \frac{g_1 g_2}{2d}, \qquad k^+_{g_1,g_2}, k^-_{g_1,g_2} \in \mathbb{N},$$

соответствует единственное $(n+1)$-элементное циклическое полукольцо $S = \{1, \alpha, \ldots, \alpha^n\}$ с полурешеточным сложением, заданным двухпорожденным идеалом $\langle g_1, g_2\rangle$. Операция сложения на S определяется свойством $\alpha^{p_i} = 1 + \alpha^i$, где

$$p_i = \begin{cases} k^+_{g_1,g_2}, & k \text{ делится на } d, \\ n, & k \text{ не делится на } d, \end{cases} \qquad i \in \{0, 1, \ldots, n\}.$$

При этом построенными полукольцами с точностью до изоморфизма исчерпываются все конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом $\langle g_1, g_2\rangle$ полукольца $\mathbb{N}_0$.

Доказательство. Пусть $J = \langle g_1, g_2 \rangle$ — двухпорожденный идеал целых неотрицательных чисел и $d = (g_1, g_2)$ — наибольший общий делитель базисных элементов. Будем считать, что $g_1 < g_2$. В силу того, что базис идеала J содержит два элемента, их наибольший общий делитель не совпадает ни с одним из них. Следовательно, $g_1 \geqslant 2$.

Сначала рассмотрим случай взаимно простых базисных элементов g_1 и g_2.

По лемме 4 каждое число $k \leqslant g_1$ может быть единственным образом представлено в виде линейной комбинации $k = k^+_{g_1,g_2} + k^-_{g_1,g_2}$. Рассмотрим идеалы

$$J \subset \mathbb{N}_0, \quad I = \big(J \cup \{n\}\big) \cap \{0, 1, \ldots, n\} \subset \mathbb{N}_n$$

и множества

$$J_k = J + k \subset \mathbb{N}_0, \quad I_k = \big(J_k \cup \{n\}\big) \cap \{0, 1, \ldots, n\} \subset \mathbb{N}_n.$$

По предложению 7 для каждого числа n, удовлетворяющего условию (14), и каждого натурального $k \leqslant g_1$ справедливо неравенство $\min\Big((J \cap J_k) \setminus J_{k^+_{g_1,g_2}}\Big) \geqslant n$. Следовательно, выполняется равенство $I_{k^+_{g_1,g_2}} = I \cap I_k$. По теореме 1 существует единственное $(n+1)$-элементное полукольцо S с множеством показателей элементов верхнего конуса $\{\alpha^0\}^\triangle$.

Пусть теперь $d = (g_1, g_2) \neq 1$. Обозначим $g'_1 = \frac{g_1}{d}$, $g'_2 = \frac{g_2}{d}$ и рассмотрим идеал $J' = \langle g'_1, g'_2 \rangle$, где $g'_1 < g_2$, $(g'_1, g'_2) = 1$.

Найдется $N'+1$-элементное полукольцо S', ассоциированное с идеалом J', где $N' = g'_1 g'_2 + {} + \min\big\{k^-_{g'_1 g'_2} : k \in \mathbb{N},\ k < g'_1\big\}$ — максимально возможный показатель поглощающего элемента полукольца S'.

Так как полукольцо S' однозначно задается кортежем

$$(p_0, p_1, \ldots, p_{N'}) \in \{0, 1, \ldots, N'\}^{N'+1},$$

то в силу предложения 3 существует $(dN'+1)$-элементное циклическое полукольцо S с полурешеточной операцией сложения, определенной кортежем $(q_0, q_1, \ldots, q_{dN}) \in \{0, 1, \ldots, dN'\}^{dN'+1}$, где $q_k = dN'$ для всех индексов $k \in \{0, 1, \ldots, dN\}$, некратных d, и $q_{dt} = dp_t$ для всех $t \in \{0, 1, \ldots, N\}$, причем S' вкладывается в S по предложению 5. Ясно, что полукольцо S ассоциировано с идеалом $J = \langle g_1, g_2 \rangle$.

По предложению 4 для каждого n, удовлетворяющего неравенству $dM < n \leqslant dN$, существует единственное полукольцо, ассоциированное с идеалом J.

Наконец, по следствию 3 других циклических полуколец с полурешеточным сложением, заданным идеалом J, нет. Теорема доказана.

5. Число конечных циклических полуколец с полурешеточным сложением и небольшим числом элементов

Опираясь на теоремы 1, 2, предложения 3, 5, 6, следствие 3 и замечание 1 в системе компьютерной алгебры SageMath нами была составлена программа, подсчитывающая число полуколец и формирующая кортежи (4) для каждого полукольца. С помощью неё найдены, с точностью до изоморфизма, все циклические полукольца с полурешеточным сложением, заданные идеалами полукольца $\mathbb{N}_0$ с базисом G мощности l и содержащие не более 31 элемента. Их число приведено в табл. 1.

Отметим, что все полукольца, найденные программно, обладают свойством, которое мы сформулируем в качестве гипотезы:

Гипотеза. *Число элементов конечного циклического полукольца с полурешеточным сложением, заданным идеалом $\langle g_1, g_2, \ldots, g_m \rangle$, где $g_1 < g_2 < \ldots < g_m$ и $m > 2$, не превосходит максимального числа элементов полукольца, ассоциированного с идеалом $\langle g_1, g_2 \rangle$.*

Таблица 1: Число циклических полуколец с полурешеточным сложением

$\|G\| = l$	Порядок полукольца														
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	0	0	1	1	4	5	10	11	17	21	30	32	43	51
3	0	0	0	0	0	0	0	2	2	6	6	17	17	32	39
4	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Число полуколец	1	2	3	5	6	10	12	20	22	33	38	59	62	91	107

$\|G\| = l$	Порядок полукольца														
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	62	67	82	91	108	116	132	148	169	175	197	217	239	255	282
3	62	69	105	115	169	182	241	275	369	379	482	540	662	726	890
4	10	10	26	26	60	63	116	122	214	222	355	395	565	614	879
5	0	0	0	0	0	0	0	0	4	4	22	22	68	68	156
Число полуколец	150	163	231	251	357	382	511	568	780	805	1082	1201	1562	1692	2237

Данное предположение продиктовано его справедливостью для рассмотренных полуколец малых порядков и тем фактом, что добавление нового элемента к базису идеала J полукольца целых неотрицательных чисел не увеличивает отличные от n значения элементов кортежа (4), задающего полукольцо S, ассоциированное с идеалом J, где n — степень поглощающего элемента полукольца S.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бестужев А. С. Конечные идемпотентные циклические полукольца // Математический вестник педвузов и университетов Волго-Вятского региона. 2011. Вып. 13. С. 71–78.

2. Бестужев А. С. Вечтомов Е. М. Циклические полукольца с коммутативным сложением // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2015. Вып. 20. С. 8–39.

3. Бестужев А. С., Вечтомов Е. М., Лубягина И. В. Полукольца с циклическим умножением // Международная конференция «Алгебра и математическая логика», посвященная 100-летию В. В. Морозова. Казань: КФУ, 2011. С. 51–52.

4. Ведерникова А. В., Чупраков Д. В. О представлении конечных идемпотентных циклических полуколец кортежами целых чисел // Математический вестник педвузов и университетов Волго-Вятского региона. 2017. Вып. 19. С. 70–76.

5. Вечтомов Е. М. Введение в полукольца. Киров: ВГПУ, 2000. 44 с.

6. Вечтомов Е. М. Мультипликативно циклические полукольца // Технологии продуктивного обучения математике: традиции и новации. Арзамас: Арзамасский филиал ННГУ, 2016. С. 130–140.

7. Вечтомов Е. М., Лубягина (Орлова) И. В. Циклические полукольца с идемпотентным некоммутативным сложением // Фундаментальная и прикладная математика. 2012. Т. 17. Вып. 1. С. 33–52.

8. Вечтомов Е. М., Орлова И. В. Циклические полукольца с неидемпотентным некоммутативным сложением // Фундаментальная и прикладная математика, 2015, Т. 20, № 6, С. 17–41.

9. Вечтомов Е. М., Орлова И. В. Идеалы и конгруэнции циклических полуколец // Вестник Сыктывкарского университета. Сер.1: Математика. Механика. Информатика. 2017. Вып. 1(22). С. 29–40.

10. Вечтомов Е. М., Орлова И. В. Конечные циклические полукольца без единицы // Алгебра и теория алгоритмов [Электронный ресурс]: Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета: сборник материалов. — Иваново: Иван. гос. ун-т, 2018. С. 113–115. Режим доступа: http://math.ivanovo.ac.ru/math-ivsu-100/materials.html

11. Вечтомов Е. М., Орлова И. В., Чупраков Д. В. К теории мультипликативно циклических полуколец // XV Международная конференция «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения», посвященная столетию со дня рождения профессора Николая Михайловича Коробова 29 мая 2018 г. Тула: ТГПУ им. Л. Н. Толстого, 2018 С. 136–138.

12. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. 3-е изд., перераб. и доп. М.: Наука, 1982. 288 с.

13. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. В 2-х т. Т. 1. М.: Мир, 1972. 286 с.

14. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Т. 1. М.: Мир, 1988. 430 с.

15. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Т. 2. М.: Мир, 1988. 822 с.

16. Лубягина И. В. О циклических полукольцах с некоммутативным сложением // Труды Математического центра им. Н. И. Лобачевского. Казань: Издательство Казанского математического общества, 2010. Т. 40. С. 212–215.

17. Ноден П., Китте К. Алгебраическая алгоритмика с упражнениями и решениями. М.: Мир, 1999. 720 с.

18. Перевощикова Т. Н. О конечных полукольцах // Вестник ВятГГУ. 2003. № 8. С. 135–137.

19. Чермных В. В., Николаева О. В. Об идеалах полукольца натуральных чисел // Математический вестник педвузов и университетов Волго-Вятского региона. 2009. Вып. 11. С. 118–121.

20. Чупраков Д. В. Конечные циклические полукольца с коммутативным идемпотентным сложением, ассоциированные с двухпорожденными идеалами полукольца натуральных чисел // Математическое моделирование и информационные технологии : сборник статей Международной научной конференции (10–11 ноября 2017 г., г. Сыктывкар). Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2017. с. 148–152.

21. Чупраков Д. В., Ведерникова А. В. О структуре конечных циклических полуколец с идемпотентным коммутативным сложением // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2017. № 2 (23). С. 92–109.

22. Bestugev A. S., Vechtomov E. M. Multiplicatively cyclic semirings // XIII Международная научная конференция им. Академика М. Кравчука. Киев: Национальный технический университет Украины, 2010. С. 39.

23. Chuprakov D. V. Algorithm for constructing finite idempotent cyclic semirings with commutative addition // Proceedings of the 4th Conference of Mathematical Society of Moldova CMSM4'2017 , June 28-July 2, 2017, Chisinau, Republic of Moldova. p. 59–62.

24. Durcheva M. I., Trendafilov I. D. Public key cryptosystem based on max-semirings // AIP Conference Proceedings. AIP, 2012. Т. 1497. №. 1. P. 357–364.

25. He M., Fan P. A multi-level secret sharing scheme based on semigroup structures // Journal of Software. 2002 V. 13, №. 2 P. 168–175

26. Kumar G., Saini H. Novel Noncommutative Cryptography Scheme Using Extra Special Group //Security and communication networks. 2017. V. 2017.

27. Vandiver H. S. Note on a simple type of algebra in which cancellation law of addition does not hold // Bull. Amer. Math. Soc. 1934. V. 40. № 12. P. 914–920.

REFERENCES

1. Bestuzhev A. S. 2011, "Konechnye idempotentnye ciklicheskie polukolca", *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 13, pp. 71–78.

2. Bestuzhev A. S. & Vechtomov E. M. 2015, "Cyclic semirings with commutative addition" *Vestnik Syktyvkarskogo universiteta. Seriya 1: Matematika. Mekhanika. Informatika*, no. 20, pp. 8–39.

3. Bestuzhev A. S., Vechtomov E. M. & Lubyagina I. V. 2011, "Polukolca s ciklicheskim umnozheniem", *Mezhdunarodnaya konferenciya "Algebra i matematicheskaya logika", posvyashchennaya 100-letiyu V. V. Morozova*, KFU, Kazan, pp. 51–52.

4. Vedernikova A. V. &, Chuprakov D. V. 2017, "O predstavlenii konechnyh idempotentnyh ciklicheskih polukolec kortezhami celyh chisel" *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 19. pp. 70–76.

5. Vechtomov E. M. 2000, "Vvedenie v polukolca", VGPU, Kirov, 44 p.

6. Vechtomov E. M. 2016, "Multiplicativity idempotent semirings" *Tekhnologii produktivnogo obucheniya matematike: tradicii i novacii.* Arzamasskij filial NNGU, Arzamas: . pp. 130–140.

7. Vechtomov, E.M. & Orlova, I.V. 2011, "Cyclic semirings with idempotent noncommutative addition" *Fundamentalnaya i Prikladnaya Matematika*, vol. 17, no. 1, pp. 33–52.

8. Vechtomov, E.M. & Orlova, I.V. 2015, "Cyclic Semirings with Nonidempotent Noncommutative Addition" *Fundamentalnaya i Prikladnaya Matematika*, vol. 20, no. 6, pp.17–41,

   doi: `https://doi.org/10.1007/s10958-018-3922-x`

9. Vechtomov E. M., & Orlova I. V. 2017, "Idealy i kongruehncii ciklicheskih polukolec", *Vestnik Syktyvkarskogo universiteta. Seria 1: Matematika. Mekhanika. Informatika*, no. 1(22). pp. 29–40.

10. Vechtomov E. M. &, Orlova I. V. 2018, "Konechnye ciklicheskie polukolca bez edinicy" *Algebra i teoriya algoritmov: Vserossijskaya konferenciya, posvyashchennaya 100-letiyu fakul'teta matematiki i komp'yuternyh nauk Ivanovskogo gosudarstvennogo universiteta: sbornik materialov.* — Ivanovo state university, Ivanovo, pp. 113–115. `http://math.ivanovo.ac.ru/math-ivsu-100/materials.html`

11. Vechtomov E. M., Orlova I. V. & CHuprakov D. V. 2018, "K teorii mul'tiplikativno ciklicheskih polukolec" *XV Mezhdunarodnaya konferenciya «Algebra, teoriya chisel i diskretnaya geometriya: sovremennye problemy i prilozheniya», posvyashchennaya stoletiyu so dnya rozhdeniya professora Nikolaya Mihajlovicha Korobova 29 may 2018*, TGPU im. L. N. Tolstogo, Tula, pp. 136–138.

12. Kargapolov M. I. &, Merzlyakov Y. I. 1982, "Osnovy teorii grupp". Nauka, Moscow, 288 p.

13. Klifford A. & Preston G. 1972, "Algebraicheskaya teoriya polugrupp", vol. 1, Mir, Moscow, 286 p.

14. Lidl R., & Niderrajter G. 1988, "Konechnye polya", vol. v. Mir, Moscow, 430 p.

15. Lidl R., & Niderrajter G. 1988, "Konechnye polya", vol. 2. Mir, Moscow, 822 p.

16. Lubyagina I. V. 2010, "O ciklicheskih polukolcah s nekommutativnym slozheniem" *Trudy Matematicheskogo centra im. N. I. Lobachevskogo*, Izdatel'stvo Kazanskogo matematicheskogo obshchestva, Kazan, vol. 40. pp. 212–215.

17. Noden P. & Kitte K. 1999, "Algebraicheskaya algoritmika s uprazhneniyami i resheniyami", Mir, Moscow, 720 p.

18. Perevoshchikova T. N. 2003, "O konechnyh polukolcah", no. 8, *Vestnik VyatGGU*, pp. 135–137.

19. Chermnyh V. V. & Nikolaeva O. V. 2009, "Ob idealah polukoltca naturalnih chisel" *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 11. pp. 118–121.

20. Chuprakov D. V. 2017, "Konechnye ciklicheskie polukolca s kommutativnym idempotentnym slozheniem, associirovannye s dvuxporozhdennymi idealami polukol'ca naturalnyh chisel" *Mathematical modeling and information technologies (10–11 november 2017, Syktyvkar).* Publisher Pitirim Sorokin Syktyvkar State University, Syktyvkar, pp. 148–152.

21. Chuprakov D. V. & Vedernikova A. V. 2017, "About structure of finite cyclic semirings vith idempotent commutative addition" *Vestnik Syktyvkarskogo universiteta. Seria 1: Mathematika. Mechanika. Informatika.*, no. 2 (23), pp. 92–109.

22. Bestugev A. S. &, Vechtomov E. M. 2010, "Multiplicatively cyclic semirings" *XIII Myhaylo Kravchuk's conference*, Kiev, p. 39.

23. Chuprakov D. V. 2017, "Algorithm for constructing finite idempotent cyclic semirings with commutative addition" *Proceedings of the 4th Conference of Mathematical Society of Moldova CMSM4'2017, June 28–July 2*, Chisinau, Republic of Moldova, pp. 59–62.

24. Durcheva M. I. & 2012, "Trendafilov I. D. Public key cryptosystem based on max-semirings", *AIP Conference Proceedings.* vol. 1497. no. 1. pp. 357–364.

25. He M. & Fan P. 2002, "A multi-level secret sharing scheme based on semigroup structures" *Journal of Software*, vol. 13, no. 2 pp. 168–175.

26. Kumar G. & Saini H. 2017, “Novel Noncommutative Cryptography Scheme Using Extra Special Group“, *Security and communication networks*, vol. 2017.

27. Vandiver H. S. 1934, “Note on a simple type of algebra in which cancellation law of addition does not hold “,*Bull. Amer. Math. Soc.*, vol. 40. no. 12. pp. 914–920.

Получено 24.11.2018 г.
Принято в печать 20.03.2020 г.