

Циклические полукольца с идемпотентным некоммутативным сложением

Е. М. ВЕЧТОМОВ

Вятский государственный гуманитарный университет
e-mail: vecht@mail.ru

И. В. ЛУБЯГИНА

Вятский государственный университет
e-mail: lubyagina@yandex.ru

УДК 512.55

Ключевые слова: циклическое полукольцо, некоммутативное сложение, идемпотентное полукольцо, конечное полутело.

Аннотация

В статье рассматривается строение циклических полуколец с некоммутативным сложением. В бесконечном случае сложение идемпотентно и является либо левым, либо правым. Сложение в конечных циклических полукольцах может быть как идемпотентным, так и неидемпотентным. В конечном аддитивно идемпотентном циклическом полукольце сложение сводится к сложению в циклическом подполукольце с коммутативным сложением и поглощающим элементом по умножению и сложению в цикле, являющимся циклическим полутелом.

Abstract

E. M. Vechtomov, I. V. Lubyagina, Cyclic semirings with idempotent noncommutative addition, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 1, pp. 33–52.

The article discusses the structure of cyclic semirings with noncommutative addition. In the infinite case, the addition is idempotent and is either left or right. Addition of a finite cyclic semirings can be either idempotent or nonidempotent. In the finite additively idempotent cyclic semiring, addition is reduced to the addition of cyclic subsemiring with commutative addition and absorbing element for multiplication and the addition of a cycle that is a finite semifield.

Введение

Данная работа посвящена изучению строения циклических полуколец с некоммутативным сложением. Строение бесконечных циклических полуколец S с коммутативным сложением известно [2]. Именно, S изоморфно одному из двух аддитивно идемпотентных числовых полуколец со сложением $\max$ и обычным умножением $\cdot$: полукольцу $\{2^n: n \in \mathbb{N}_0\} \cup \{0\}$ или полукольцу $\{1/2^n: n \in \mathbb{N}_0\} \cup \{0\}$. Конечные циклические полукольца с коммутативным

Фундаментальная и прикладная математика, 2011/2012, том 17, № 1, с. 33–52.

© 2011/2012 Центр новых информационных технологий МГУ,
Издательский дом «Открытые системы»

сложением изучал А. С. Бестужев [1]. Мы отказываемся от требования коммутативности сложения в циклическом полукольце. В бесконечном случае такие полукольца имеют идемпотентное сложение, а в конечном случае сложение может быть как идемпотентным, так и неидемпотентным.

В разделе 1 даются предварительные сведения о циклических полукольцах. В разделе 2 описывается строение бесконечных циклических полуколец с некоммутативным сложением. В разделе 3 выясняется строение конечных циклических полутел. В разделе 4 приводятся общие результаты о конечных циклических полукольцах с некоммутативным сложением. В разделе 5 изучаются конечные циклические полукольца с идемпотентным некоммутативным сложением.

1. Основные понятия. Предварительные результаты

Определение 1. *Полукольцом* будем называть алгебраическую структуру S с операциями сложения $+$ и умножения $\cdot$, такими что $\langle S, + \rangle$ — полугруппа, $\langle S, \cdot \rangle$ — полугруппа и умножение дистрибутивно относительно сложения с обеих сторон.

Если в полукольце S существует нейтральный по сложению элемент 0 , обладающий свойством мультипликативности (т. е. $x \cdot 0 = 0 \cdot x = 0$ для любого $x \in S$), то полукольцо S будем называть *полукольцом с нулём*.

Если в полукольце существует нейтральный по умножению элемент 1 , то полукольцо будем называть *полукольцом с единицей*.

Определение 2. *Полутелом* называется полукольцо, являющееся группой по умножению.

Определение 3. Полукольцо S с единицей 1 назовём *циклическим*, если в S существует образующий элемент $a \neq 1$, такой что каждый ненулевой элемент из S является его неотрицательной целой степенью. Циклическое полукольцо S с образующим a обозначим $S = (a)$.

Отметим, что в циклическом полукольце $S = (a)$ с нулём образующий элемент может быть *нильпотентным*, т. е. $a^n = 0$ для некоторого натурального n .

Полукольцо с тождеством $x + x = x$ называется *идемпотентным*.

На идемпотентом полукольце S с коммутативным сложением вводится естественный порядок $\leq$,

$$x \leq y \iff x + y = x,$$

превращающий $\langle S, + \rangle$ в верхнюю полурешётку [3, с. 151, 152].

Полукольцо с нулём называется *антикольцом*, если в нём верно квазитожество

$$x + y = 0 \implies x = 0.$$

Сложение в полукольце назовём *левым сложением* (*правым сложением*), если в нём тождественно выполнено $x + y = x$ ($x + y = y$).

Предложение 1. *Всякое конечное циклическое полукольцо S с нулём и с нильпотентным образующим a является цепью по сложению.*

Доказательство. Пусть n — наименьшее натуральное число, такое что $a^n = 0$. Рассмотрим сумму произвольных элементов a^r и a^s ($r, s \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, r и s не равны 0 одновременно) полукольца S . Покажем, что $a^r + a^s = a^{\min(r,s)}$. Положим сначала $r < s$.

Если $s = n$, то $a^s = 0$ и $a^r + a^s = a^r$.

Пусть $s < n$ и $a^r + a^s = a^t$. Домножив равенство на a^{n-s} , получим

$$a^{r+n-s} + a^n = a^{t+n-s}, \quad a^{r+n-s} = a^{t+n-s}.$$

Так как $r + n - s < n$, то $a^{r+n-s} \neq 0$. Следовательно, $a^{t+n-s} \neq 0$. Тогда $r + n - s = t + n - s$ и $r = t$, откуда следует, что $a^r + a^s = a^r$.

Аналогично $a^s + a^r = a^r$.

Пусть $1 + 1 = 0$. Тогда $1 + (1 + a) = a$. По доказанному выше $1 + a = 1$, следовательно, $0 = a$; противоречие.

Поэтому $1 + 1 = a^m$, где $0 < m < n$. Так как $1 + a^m = 1$, имеем $a^m = 1 + 1 = 1 + 1 + a^m = a^m(1 + 1) = a^{2m}$. Так как $a^m \neq 0$, то $m = 2m$, откуда следует, что $m = 0$; противоречие.

Таким образом, $1 + 1 = 1$, т. е. S идемпотентно.

Пусть $r = s$. Тогда $a^r + a^s = a^r + a^r = a^r$.

Таким образом, в S тождественно выполняется $a^r + a^s = a^{\min(r,s)}$ и сложение коммутативно. Для любых x и y выполняется $x + y = x$ или $x + y = y$.

Получили, что $\langle S, + \rangle$ является верхней полурешёткой с линейным порядком $\leq$, т. е. цепью. $\square$

Предложение 2. *Всякое циклическое полукольцо S с нулём и с некоммутативным сложением является антикольцом.*

Доказательство. Предположим от противного, что $a^r + a^s = 0$ для некоторых элементов a^r и a^s полукольца S . Пусть сначала $a^r = a^s$. Тогда $a^r(1 + 1) = 0$. Отсюда следует, что либо $a^r = 0$, либо $1 + 1 = 0$. В первом случае по предположению 1 получаем полукольцо с коммутативным сложением. Если $1 + 1 = 0$, то $\langle S, + \rangle$ — группа с тождеством $x + x = 0$; в такой группе сложение коммутативно.

Имеем $a^r \neq a^s$, для определённости положим $r < s$. Тогда $a^r(1 + a^{s-r}) = 0$. Если $1 + a^{s-r} \neq 0$, то $a^q = 0$ для некоторого q . В этом случае сложение коммутативно по предположению 1. Пусть теперь $1 + a^{s-r} = 0$. Тогда любой элемент полугруппы $\langle S, + \rangle$ имеет правый противоположный элемент относительно нейтрального элемента 0. Такая полугруппа $\langle S, + \rangle$ будет группой, а полукольцо S с 1 будет кольцом (сложение коммутативно). $\square$

Принимая во внимание предложения 1 и 2, в дальнейшем будем рассматривать только циклические полукольца без нуля.

Лемма 1. *В любом идемпотентном полукольце справедливы тождества $(1 + x)^i = 1 + x + \dots + x^i$ и $(x + 1)^i = x^i + x^{i-1} + \dots + x + 1$ для любого $i \in \mathbb{N}$.*

Доказательство. Для $i = 1$ равенство верно. Пусть оно верно для любого i . Тогда для $i + 1$ имеем

$$\begin{aligned}(1+x)^{i+1} &= (1+x)(1+x)^i = (1+x)(1+x+\dots+x^i) = \\ &= 1+x+x+x^2+\dots+x^i+x^{i+1} = 1+x+x^2+\dots+x^{i+1}.\end{aligned}$$

Аналогично для любого $i \in \mathbb{N}$ $(x+1)^i = x^i + x^{i-1} + \dots + x + 1$. $\square$

Лемма 2. Если в произвольном циклическом полукольце $S = (a)$ выполняется $1+a^s = 1$ ($a^s+1=1$) для некоторого $s \in \mathbb{N}$, то верно $1+a^{si} = 1$ ($a^{si}+1=1$) для любого $i \in \mathbb{N}$.

Доказательство. Равенство $1+a^s = 1$ верно по условию. Пусть $1+a^{si} = 1$ верно для любого i . Для $i+1$ имеем

$$1+a^{s(i+1)} = 1+a^{si} + a^{s(i+1)} = 1+a^{si}(1+a^s) = 1+a^{si} = 1.$$

Аналогично из соотношения $a^s+1=1$ для некоторого $s \in \mathbb{N}$ следует, что $a^{si}+1=1$ для любого $i \in \mathbb{N}$. $\square$

Лемма 3. Если в идемпотентном циклическом полукольце $S = (a)$ с некоммутативным сложением справедливо $1+a=1$ ($a+1=1$), то сложение в полукольце S левое (правое).

Доказательство. Пусть $1+a=1$. По лемме 2 имеем $1+a^i = 1$ для любого $i \in \mathbb{N}$.

Пусть $a+1=a^q$, $q \geq 0$. Если $q=0$, т. е. $a+1=1$, то по лемме 2 имеем $a^i+1=1$ для любого $i \in \mathbb{N}$, откуда следует, что $1+a^i = a^i+1$ для любого $i \in \mathbb{N}$, что влечёт коммутативность сложения. Поэтому $q \geq 1$. Тогда, прибавляя слева элемент a к равенству $a+1=a^q$ и пользуясь идемпотентностью, получаем, что $a+a^q = a^q$. Поэтому

$$a = a(1+a^{q-1}) = a+a^q = a^q = a+1.$$

Докажем, что $a^i+1 = a^i$ выполняется для любого $i \in \mathbb{N}$. Для $i=1$ равенство доказано. Пусть оно верно для i . Для $i+1$ имеем

$$a^{i+1}+1 = a \cdot a^i+1 = a(a^i+1)+1 = a^{i+1}+a+1 = a^{i+1}+a = a(a^i+1) = a \cdot a^i = a^{i+1}.$$

Рассмотрим теперь произвольные элементы $a^r, a^s \in S$. Если $r \leq s$, то $a^r+a^s = a^r(1+a^{s-r}) = a^r$. Если $r \geq s$, то $a^r+a^s = a^s(a^{r-s}+1) = a^s \cdot a^{r-s} = a^r$. Значит, сложение в S левое.

Аналогично если $a+1=1$, то сложение в S будет правое. $\square$

2. Бесконечные циклические полукольца с некоммутативным сложением

Выясним строение бесконечных циклических полуколец с некоммутативным сложением.

Теорема 1. *Бесконечные циклические полукольца с некоммутативным сложением имеют левое или правое сложение.*

Доказательство. Покажем, что бесконечные циклические полукольца имеют идемпотентное сложение. Пусть $S = (a)$ — бесконечное циклическое полукольцо, т. е. $S = \{1, a, a^2, \dots, a^n, \dots\}$. В силу бесконечности полукольца степени образующего a попарно различны.

Пусть $1+1 = a^r$, где $r \neq 0$. Рассмотрим множество $S' = \{1, 1+1, 1+1+1, \dots\}$, которое является подполукольцом в S . Поскольку $\{a^r, a^{2r}, a^{3r}, \dots\} \subseteq \{1, 1+1, 1+1+1, \dots\}$ и все степени элемента a различны, подполукольцо S' является бесконечным. Тогда подполугруппа S' мультипликативной полугруппы S изоморфна мультипликативной полугруппе $\mathbb{N}$, которая не является конечно порождённой. С другой стороны, полугруппа $\langle S, \cdot \rangle$ изоморфна аддитивной полугруппе $\mathbb{N}_0$, все подполугруппы которой конечно порождённые [4, с. 45]. Противоречие. Таким образом, $1+1 = 1$, т. е. S идемпотентно.

Покажем, что $1+a = 1$ или $1+a = a$. Пусть $1+a = a^r$, где $r \in \mathbb{N}_0$. Если $r = 0$, то $1+a = 1$. Пусть теперь $r \neq 0$. Учитывая лемму 1, имеем для любого $i \in \mathbb{N}$

$$\begin{aligned} (1+a)^{2i-1} &= 1+a+a^2+\dots+a^{2i-2}+a^{2i-1}= \\ &= (1+a+\dots+a^{i-1})+(a^i+\dots+a^{2i-1})= \\ &= (1+a)^{i-1}+a^i(1+a)^{i-1}=(1+a^i)(1+a)^{i-1}. \end{aligned}$$

Тогда $a^{r(2i-1)} = (1+a^i)a^{r(i-1)}$ и $1+a^i = a^{ri}$.

При $i = r$ имеем $1+a^r = a^{r \cdot r}$. Добавляя к равенству $1+a = a^r$ единицу 1 слева и пользуясь идемпотентностью, получаем $1+a^r = a^r$. Тогда $a^{r^2} = a^r$ и $r^2 = r$. Отсюда следует, что $r = 1$. Тогда для любого $i \in \mathbb{N}$ справедливо $1+a^i = 1$ или $1+a^i = a^i$.

Аналогично для любого $i \in \mathbb{N}$ справедливо $a^i+1 = 1$ или $a^i+1 = a^i$.

Таким образом, возможны четыре случая (для всех $i \in \mathbb{N}_0$):

- 1) $1+a^i = a^i+1 = 1$;
- 2) $1+a^i = a^i+1 = a^i$;
- 3) $1+a^i = 1$ и $a^i+1 = a^i$;
- 4) $1+a^i = a^i$ и $a^i+1 = 1$.

Случаи 1) и 2) дают коммутативное сложение. В случае 3) получаем левое сложение, в случае 4) — правое (как в лемме 3). $\square$

Замечание 1. Любая мультипликативно записанная группа становится полутелом, если на ней задать левое (или правое) сложение. На бесконечной мультипликативной циклической группе $C = \{a^i : i \in \mathbb{Z}\}$ можно задать сложение, превращающее её в полутело, четырьмя способами: левое сложение; правое сложение; $a^r + a^s = a^{\min\{r,s\}}$ для любых элементов a^r и a^s из C ; $a^r + a^s = a^{\max\{r,s\}}$ для любых элементов a^r и a^s из C (в последних двух случаях получаем изоморфные полутела).

3. Конечные циклические полутела

Строение конечных полутел было изучено Х. Вайнертом [5]. Он показал, что описание конечных полутел сводится к конечным группам: любое конечное полутело C изоморфно $(C + 1) \times (1 + C)$, где $C + 1$ — подполутело в C с левым сложением, $1 + C$ — подполутело в C с правым сложением.

Приведём прямое доказательство теоремы Вайнерта.

Теорема А. *Всякое конечное полутело изоморфно прямому произведению двух полутел, одно из которых с левым сложением, а другое с правым сложением.*

Докажем эту теорему в виде последовательности лемм.

Лемма 4. *Любое конечное полутело C идемпотентно.*

Доказательство. Сумму k единиц $\underbrace{1 + 1 + \dots + 1}_k$ будем обозначать через k .

Из того что $\langle C, \cdot \rangle$ — конечная группа порядка n , следует, что $k^n = 1$ для любого $k \in C$, т. е. $\underbrace{(1 + 1 + \dots + 1)}_k^n = 1$. Поэтому $k + s = 1$ для некоторого элемента

$s \in C$. Добавляя к предыдущему равенству $k - 1$, получаем $k + l = k$ для некоторого элемента $l \in C$. Добавляя $k(l - 1)$, получаем $kl + l = kl$. Добавляя $l(k - 1)$, получаем $kl + kl = kl$.

Домножая равенство на элемент $(kl)^{-1}$, получаем $1 + 1 = 1$, поэтому $x + x = x$ для любого $x \in C$. $\square$

Лемма 5. *В любом конечном полутеле C выполняются следующие тождества:*

- 1) $x + y + x = x$;
- 2) $x + y + z = x + z$;
- 3) $(x + 1)(1 + y) = (x + 1) + (1 + y) = x + y = (1 + y)(x + 1)$;
- 4) $(x + 1)(y + 1) = xy + 1$, $(1 + x)(1 + y) = 1 + xy$.

Доказательство. 1. Пусть x, y и z — произвольные элементы конечного полутела C . Обозначим $1 + x + 1 = a$. Тогда $1 + a = a + 1 = a$.

Используя лемму 1, получаем

$$(1 + a)^k = 1 + a + \dots + a^k, \quad (a + 1)^k = a^k + \dots + a + 1.$$

Тогда

$$a^k = (1 + a)^k = 1 + a + \dots + a^k, \quad a^k = (a + 1)^k = a^k + \dots + a + 1.$$

Добавляя к первому равенству элемент 1 слева, а ко второму равенству элемент 1 справа, получаем, что $1 + a^k = a^k = a^k + 1$ для любого $k \in \mathbb{N}$.

Рассмотрим сумму $a^n + a^{n-1} + \dots + a$:

$$a^n + a^{n-1} + \dots + a = a(a^{n-1} + \dots + 1) = a(a + 1)^{n-1}.$$

С другой стороны,

$$\begin{aligned} a^n + a^{n-1} + \dots + a &= 1 + a^{n-1} + \dots + a = a^{n-1} + 1 + \dots + a = \dots = \\ &= a^{n-1} + \dots + a + 1 = (a + 1)^{n-1}. \end{aligned}$$

Отсюда выводим, что $a(a + 1)^{n-1} = (a + 1)^{n-1}$. Домножая равенство справа на элемент, обратный к $(a + 1)^{n-1}$, получаем $a = 1$.

По уже доказанному $1 + yx^{-1} + 1 = 1$. Домножая это равенство на x и используя закон дистрибутивности, получаем $x + y + x = x$.

2. Воспользовавшись тождеством 1) и идемпотентностью сложения, получаем

$$\begin{aligned} x + y + 1 &= (x + 1 + x) + y + 1 = x + (1 + x + y + 1) = x + 1, \\ x + y + z &= (xz^{-1} + yz^{-1} + 1)z = (xz^{-1} + 1)z = x + z. \end{aligned}$$

3. Используя тождества 1) и 2), получаем

$$\begin{aligned} (x + 1)(1 + y) &= x + (1 + xy) + y = x + (1 + y + 1 + xy) + y = \\ &= x + 1 + (y + 1 + xy + y) = x + 1 + y = (x + 1) + (1 + y) = x + y = \\ &= x + (1 + yx) + y = (x + 1) + y(x + 1) = (1 + y)(x + 1). \end{aligned}$$

4. Используя тождество 2), получаем

$$\begin{aligned} (x + 1)(y + 1) &= x(y + 1) + (y + 1) = xy + (x + y) + 1 = xy + 1, \\ (1 + x)(1 + y) &= (1 + y) + x(1 + y) = 1 + (y + x) + xy = 1 + xy. \end{aligned}$$

□

Для полутела C введём следующие обозначения:

$$C + 1 = \{x + 1 \mid x \in C\}, \quad 1 + C = \{1 + x \mid x \in C\}.$$

Лемма 6. В любом конечном полутеле C $C + 1$ является подполутелом с левым сложением, $1 + C$ — подполутелом с правым сложением.

Доказательство. Имеем, что

$$\begin{aligned} (x + 1) + (y + 1) &= (x + 1 + y) + 1 \in C + 1, \\ (x + 1)(y + 1) &= (x(y + 1) + y) + 1 \in C + 1. \end{aligned}$$

Следовательно, $C + 1$ замкнуто относительно операций сложения и умножения. Учитывая замкнутость умножения и равенство

$$1 = (x + 1)^n = (x + 1)(x + 1)^{n-1} \quad \text{для любого } x \in C,$$

получаем, что $C + 1$ замкнуто относительно взятия обратного элемента. Также имеем

$$(x + 1) + (y + 1) = x + (1 + y + 1) = x + 1.$$

Следовательно, $C + 1$ — подполутело в C с левым сложением.

Аналогично показывается, что $1 + C$ — подполутело в C с правым сложением.

□

Доказательство теоремы А. Для произвольного конечного полутела C определим отображение

$$\alpha: C \rightarrow (C + 1) \times (1 + C)$$

по формуле

$$\alpha(x) = (x + 1, 1 + x) \text{ для любого } x \in C.$$

Покажем, что α — искомый изоморфизм.

Пусть $(x + 1, 1 + x) = (y + 1, 1 + y)$ для произвольных $x, y \in C$, т. е.

$$x + 1 = y + 1, \quad 1 + x = 1 + y.$$

Тогда по леммам 4 и 5 (пункт 1))

$$x = x + 1 + x = (x + 1) + (1 + x) = (y + 1) + (1 + y) = y + 1 + y = y.$$

Значит, α — инъекция.

Рассмотрим образ элемента $x + 1 + y$ для произвольных элементов $x, y \in C$:

$$\alpha: x + 1 + y \rightarrow (x + 1 + y + 1, 1 + x + 1 + y) = (x + 1, 1 + y).$$

Получаем, что α — сюръекция. Доказано, что α — биекция.

Проверим сохранение операций сложения и умножения при отображении α . Используя лемму 5 (пункты 2) и 4)), получаем

$$\begin{aligned} \alpha(x + y) &= (x + y + 1, 1 + x + y) = (x + 1, 1 + y) = \\ &= (x + 1 + y + 1, 1 + x + 1 + y) = \\ &= (x + 1, 1 + x) + (y + 1, 1 + y) = \alpha(x) + \alpha(y), \\ \alpha(xy) &= (xy + 1, 1 + xy) = ((x + 1)(y + 1), (1 + x)(1 + y)) = \\ &= (x + 1, 1 + x)(y + 1, 1 + y) = \alpha(x)\alpha(y). \end{aligned} \quad \square$$

Замечание 2. Известно, что если циклическая группа G порядка n с образующим c изоморфна прямому произведению двух групп G_1 и G_2 порядков m и h соответственно, то они являются циклическими и их порядки взаимно просты: $(m, h) = 1$, $G_1 = \langle c^h \rangle$ и $G_2 = \langle c^m \rangle$.

Рассмотрим циклическое полутело C порядка n с образующим элементом c . Пусть порядок $C + 1$ равен m , а порядок $1 + C$ равен h . Тогда $C + 1 = \langle c^h \rangle$, $1 + C = \langle c^m \rangle$. Из того что $(m, h) = 1$, следует, что $1 = hx + my$ для некоторых целых чисел x, y . Тогда любой элемент c^r полутела C представим в виде $c^r = c^{hrx+my} = c^{hi+mj}$. Можно считать, что $i, j \in \mathbb{N}$, так как в противном случае положительные i, j можно получить прибавлением к показателю степени элемента c числа, кратного n .

Циклическое полутело C порядка n имеет $\varphi(n)$ образующих, где φ — функция Эйлера. Следовательно, существует $\varphi(n)$ мультипликативных автоморфизмов полутела C . Число сложений на полутеле C равно удвоенному числу разложений числа n в произведение двух взаимно простых сомножителей. Любой мультипликативный автоморфизм C отображает подполутела $C + 1$ и $1 + C$

сами на себя и сохраняет сложение на каждом из них (в силу леммы 6), следовательно, и на полутеле C . Таким образом, мультипликативные автоморфизмы полутела C являются его полукольцевыми автоморфизмами.

Предложение 3. Сложение в конечном циклическом полутеле C осуществляется следующим образом:

$$c^{hi_1+mj_1} + c^{hi_2+mj_2} = c^{hi_1+mj_2} \quad \text{для любых } i_1, j_1, i_2, j_2 \in \mathbb{N}.$$

Доказательство. Учитывая, что $c^{hi_1}, c^{hi_2} \in C + 1$, $c^{mj_1}, c^{mj_2} \in 1 + C$, и используя лемму 5 (пункты 2) и 3)), имеем

$$\begin{aligned} c^{hi_1+mj_1} + c^{hi_2+mj_2} &= c^{hi_1} c^{mj_1} + c^{hi_2} c^{mj_2} = \\ &= c^{hi_1} + c^{mj_1} + c^{hi_2} + c^{mj_2} = c^{hi_1} + c^{mj_2} = c^{hi_1} c^{mj_2} = c^{hi_1+mj_2}. \quad \square \end{aligned}$$

4. Общие результаты о конечных циклических полукольцах с некоммутативным сложением

Мультипликативная полугруппа циклического полукольца S является циклической. Любая циклическая (моногоенная) полугруппа с единицей 1 изоморфна или аддитивной полугруппе чисел $\mathbb{N}_0$, или некоторому циклу с хвостом (возможно, пустым) [3, с. 65].

Рассмотрим циклическое полукольцо $S = \{1, a, a^2, \dots, a^k, \dots, a^{k+n-1}\}$, в котором $a^{k+n} = a^k$, где $k \in \mathbb{N}_0$, $n \in \mathbb{N}$ ($|S| = k + n \geq 2$). Полукольцо с такой мультипликативной циклической полугруппой будем называть *полукольцом типа (k, n)* . В дальнейшем множество $\{1, a, a^2, \dots, a^{k-1}\}$ будем называть *хвостом* полукольца S в случае $k \geq 1$, множество $C = \{a^k, a^{k+1}, \dots, a^{k+n-1}\}$ — его *циклом*.

Теорема 2. Цикл C конечного циклического полукольца $S = (a)$ типа (k, n) с некоммутативным сложением является циклическим полутелом с образующим элементом a^{nl+1} и единицей a^{nl} для некоторого $l \in \mathbb{N}_0$, такого что $nl \geq k > n(l-1)$.

Доказательство. В силу того что $a^{k+n} = a^k$, множество C замкнуто по умножению. Нейтральным по умножению элементом служит a^{nl} , где l — наименьшее неотрицательное целое число, для которого $nl \geq k$. Действительно, $a^s \cdot a^{nl} = a^{nl} \cdot a^s = a^s$ для любого элемента $a^s \in C$. Элемент a^{nl+1} является образующим мультипликативной группы C .

Рассмотрим сумму $a^r + a^s = a^t$ произвольных элементов a^r, a^s из цикла C , где $k \leq r, s \leq k+n-1$ и $t \in \mathbb{N}_0$. Домножив это равенство на единицу цикла a^{nl} , получим $a^r + a^s = a^{t+nl}$. Тогда $a^t = a^{t+nl} \in C$, так как $t + nl \geq k$.

Следовательно, цикл C циклического полукольца S является циклическим полутелом. $\square$

Поскольку строение конечных циклических полутел изучено, то до конца статьи будем рассматривать конечные циклические полукольца, не являющиеся полутелами, т. е. полагаем, что $k \geq 1$.

Учитывая замечание 2, имеем

$$C + a^{nl} = (a^{(nl+1)h}), \quad a^{nl} + C = (a^{(nl+1)m}).$$

Тогда для любого $i \in \mathbb{N}$ справедливо, что $a^{(nl+1)hi} \in C + a^{nl}$. Аналогично для любого $j \in \mathbb{N}$ справедливо, что $a^{(nl+1)mj} \in a^{nl} + C$.

По лемме 6 имеем, что $a^{nl} \in C + a^{nl}$ и выполняется

$$a^{nl} + a^{(nl+1)hi} = a^{nl}, \quad a^{(nl+1)hi} + a^{nl} = a^{(nl+1)hi}. \quad (1)$$

Аналогично $a^{nl} \in a^{nl} + C$ и выполняется

$$a^{nl} + a^{(nl+1)mj} = a^{(nl+1)mj}, \quad a^{(nl+1)mj} + a^{nl} = a^{nl}. \quad (2)$$

Учитывая предложение 3, получаем, что сложение в цикле C полукольца S осуществляется следующим образом (для любых $i_1, j_1, i_2, j_2 \in \mathbb{N}$):

$$a^{(nl+1)(hi_1+mj_1)} + a^{(nl+1)(hi_2+mj_2)} = a^{(nl+1)(hi_1+mj_2)}. \quad (3)$$

Лемма 7. В конечном циклическом полукольце $S = (a) \neq C$ типа (k, n) эквивалентны следующие условия:

- 1) $1 + a^s = 1$ ($a^s + 1 = 1$) для некоторого натурального s ;
- 2) $1 + a^{nl} = 1$ ($a^{nl} + 1 = 1$);
- 3) $a^r + a^s = a^r$ ($a^s + a^r = a^r$) для любых $a^r \in S$ и $a^s \in C$;
- 4) $1 + a^i = 1$ ($a^i + 1 = 1$) для любого натурального i .

Доказательство. Доказательство проведём по циклу

$$1) \implies 2) \implies 3) \implies 4) \implies 1).$$

Докажем импликацию $1) \implies 2)$. По лемме 2 из того что $1 + a^s = 1$ для некоторого $s \in \mathbb{N}$, вытекает $1 + a^{si} = 1$ для любого $i \in \mathbb{N}$. В частности, для $i = nl$ имеем $1 + a^{s(nl)} = 1 + a^{nl} = 1$.

Докажем импликацию $2) \implies 3)$. Пусть $1 + a^{nl} = 1$. Тогда, используя (1), для любого $i \in \mathbb{N}$ получаем

$$1 = 1 + a^{nl} = 1 + a^{nl} + a^{(nl+1)hi} = 1 + a^{(nl+1)hi}.$$

Используя (2), для любого $j \in \mathbb{N}$ получаем

$$1 = 1 + a^{nl} = 1 + a^{(nl+1)mj} + a^{nl},$$

откуда следует, что $1 + a^{(nl+1)mj} = 1$. (Если $1 + a^{(nl+1)mj} = a^t$, где $t > 0$, то $a^t + a^{nl} = 1$. Из $t \leq nl$ следует, что $a^t(1 + a^{nl-t}) = 1$, поэтому $a^q = 1$ для некоторого $q \geq t > 0$, откуда получаем, что S — полутело. Из $t \geq nl$ также вытекает, что S — полутело.)

Учитывая замечание 2, получаем, что произвольный элемент цикла C имеет вид $a^{(nl+1)(hi+mj)}$ для некоторых $i, j \in \mathbb{N}$. Найдём сумму 1 и произвольного элемента из цикла C . Для любых $i, j \in \mathbb{N}$ имеем

$$\begin{aligned} 1 &= (1 + a^{(nl+1)hi})(1 + a^{(nl+1)mj}) = \\ &= (1 + a^{(nl+1)mj}) + a^{(nl+1)hi} + a^{(nl+1)(hi+mj)} = \\ &= (1 + a^{(nl+1)hi}) + a^{(nl+1)(hi+mj)} = 1 + a^{(nl+1)(hi+mj)}. \end{aligned}$$

Таким образом, выполняется $1 + a^t = 1$ для любого $a^t \in C$.

Рассмотрим теперь произвольные элементы $a^r \in S$ и $a^s \in C$. Имеем

$$a^r + a^s = a^r + a^{s+nl+nl} = a^r(1 + a^{s+nl+nl-r}) = a^r.$$

Докажем импликацию 3) $\implies$ 4). Пусть $a^r + a^s = a^r$ для любых $a^r \in S$ и $a^s \in C$. В частности, для $a^r = a^{k-1}$ и $a^s = a^k$ имеем

$$a^{k-1} + a^k = a^{k-1}, \quad a^{k-1}(1 + a) = a^{k-1},$$

откуда следует, что $1 + a = 1$. По лемме 2 имеем $1 + a^i = 1$ для любого $i \in \mathbb{N}$.

Импликация 4) $\implies$ 1) очевидна.

Аналогично доказывается эквивалентность утверждений в скобках. $\square$

Замечание 3. Если в конечном циклическом полукольце S выполняется $1 + a^s = 1$ ($a^s + 1 = 1$) для некоторого $s \in \mathbb{N}$, то сложение в цикле C полукольца S левое (правое).

Предложение 4. В конечном циклическом полукольце $S = (a) \neq C$ типа (k, n) с некоммутативным сложением возможен один из следующих случаев:

- 1) $1 + a^{nl} = 1$, $a^{nl} + 1 = a^{nl}$;
- 2) $1 + a^{nl} = a^{nl}$, $a^{nl} + 1 = 1$;
- 3) $1 + a^{nl} = a^{nl}$, $a^{nl} + 1 = a^{nl}$.

Доказательство. Используя лемму 4 и теорему 2, имеем

$$(1 + a^{nl})(1 + a^{nl}) = 1 + a^{nl} + a^{nl} + a^{nl} \cdot a^{nl} = 1 + a^{nl} + a^{nl} + a^{nl} = 1 + a^{nl}.$$

Значит, $1 + a^{nl} = 1$ или $1 + a^{nl} = a^{nl}$.

Аналогично $a^{nl} + 1 = 1$ или $a^{nl} + 1 = a^{nl}$.

Тем самым формально возможны четыре случая: 1)–3) и $1 + a^{nl} = a^{nl} + 1 = 1$. Но в последнем случае по лемме 7 получаем, что $1 + a^i = a^i + 1 = 1$ для любого $i \in \mathbb{N}$, откуда вытекает коммутативность сложения в S , что невозможно. $\square$

Следствие 1. В конечном циклическом полукольце $S = (a) \neq C$ типа (k, n) с некоммутативным сложением и с поглощающим элементом a^k выполняется один из следующих случаев:

- 1) $1 + a^k = 1$, $a^k + 1 = a^k$;
- 2) $1 + a^k = a^k$, $a^k + 1 = 1$;
- 3) $1 + a^k = a^k$, $a^k + 1 = a^k$.

Доказательство. Достаточно заметить, что в конечном циклическом полукольце S с поглощающим элементом a^k цикл C состоит из одного элемента $C = \{a^k\}$, и воспользоваться предложением 4. $\square$

Лемма 8. Если в конечном циклическом полукольце $S \neq C$ выполняется $1 + a^{nl} = a^{nl}$ ($a^{nl} + 1 = a^{nl}$), где a^{nl} — единица цикла C , то $a^r + a^s = a^{r+nl} + a^s$ ($a^s + a^r = a^s + a^{r+nl}$) для любых $a^r \in S$ и $a^s \in C$.

Доказательство. Имеем $1 + a^{nl} = a^{nl}$. Пусть i и j — произвольные натуральные числа. Обозначим $1 + a^{(nl+1)hi} = a^s$ для некоторого s . Добавляя справа элемент a^{nl} и учитывая (1), получаем

$$1 + a^{(nl+1)hi} + a^{nl} = a^s + a^{nl}, \quad 1 + a^{(nl+1)hi} = a^s + a^{nl}, \quad a^s = a^s + a^{nl}.$$

Пусть $a^s \notin C$. Тогда $a^s(1 + a^{nl-s}) = a^s$, $1 + a^{nl-s} = 1$, и по лемме 7 получаем $1 + a^{nl} = 1$. Противоречие. Следовательно, $a^s \in C$. Тогда

$$a^s = a^{nl} \cdot a^s = a^{nl}(1 + a^{(nl+1)hi}) = a^{nl} + a^{(nl+1)hi} = a^{nl},$$

т. е.

$$1 + a^{(nl+1)hi} = a^{nl}.$$

Отсюда, учитывая (2) и (3), получаем

$$1 + a^{(nl+1)(hi+mj)} = 1 + a^{(nl+1)hi} + a^{(nl+1)mj} = a^{nl} + a^{(nl+1)mj} = a^{(nl+1)mj}.$$

Используя (1)–(3), имеем

$$a^{nl} + a^{(nl+1)(hi+mj)} = a^{nl} + a^{(nl+1)hi} + a^{(nl+1)mj} = a^{nl} + a^{(nl+1)mj} = a^{(nl+1)mj}.$$

Таким образом, выполняется $1 + a^t = a^{nl} + a^t$ для любого $a^t \in C$.

Рассмотрим теперь произвольные элементы $a^r \in S$ и $a^s \in C$. Имеем

$$\begin{aligned} a^r + a^s &= a^r + a^{s+nl+nl} = a^r(1 + a^{s+nl+nl-r}) = \\ &= a^r(a^{nl} + a^{s+nl+nl-r}) = a^{r+nl} + a^{s+nl+nl} = a^{r+nl} + a^s. \end{aligned}$$

Аналогично из равенства $a^{nl} + 1 = a^{nl}$ вытекает (для любых $a^r \in S$ и $a^s \in C$), что $a^s + a^r = a^s + a^{r+nl}$. $\square$

Из леммы 8 вытекает следующая лемма.

Лемма 9. Если в конечном циклическом полукольце $S \neq C$ с некоммутативным сложением выполняется $1 + a^{nl} = a^{nl} + 1 = a^{nl}$, то для любых $x, y \in S$ выполнено, что если $x \in C$ или $y \in C$, то $x + y, y + x \in C$. $\square$

5. Конечные идемпотентные циклические полукольца с некоммутативным сложением

В этом разделе мы выясняем строение конечных идемпотентных циклических полуколец $S = (a)$ типа (k, n) с некоммутативным сложением.

Лемма 10. Если в конечном идемпотентном циклическом полукольце $S \neq C$ с некоммутативным сложением справедливо $1 + a^{nl} = 1$ ($a^{nl} + 1 = 1$), то сложение в полукольце S левое (правое).

Доказательство. Пусть $1 + a^{nl} = 1$. Тогда по леммам 3 и 7 сложение в полукольце S левое.

Аналогично если $a^{nl} + 1 = 1$, то сложение в полукольце S правое. $\square$

5.1. Конечные идемпотентные циклические полукольца с поглощающим элементом

Теорема 3. Всякое конечное идемпотентное циклическое полукольцо $S = (a)$ типа (k, n) с некоммутативным сложением и с поглощающим элементом a^k имеет либо левое сложение, либо правое сложение.

Доказательство. В конечном циклическом полукольце S с поглощающим элементом a^k цикл C состоит из одного элемента a^k . По теореме 2 имеем $a^{nl} = a^k$. По следствию 1 и лемме 10 остаётся показать, что случай $1 + a^k = a^k + 1 = a^k$ невозможен.

Пусть l и r — произвольные натуральные числа, такие что $l \leq k$ и $r \leq k$.

Домножая равенства $1 + a^k = a^k$ и $a^k + 1 = a^k$ на элемент a^r , получаем

$$a^r + a^k = a^k = a^k + a^r. \quad (4)$$

Домножая равенства $1 + a^k = a^k$ и $a^k + 1 = a^k$ на элемент a^{k-l} , получаем

$$\begin{aligned} a^{k-l} + a^k &= a^k + a^{k-l} = a^k, \\ a^{k-l}(1 + a^l) &= a^{k-l}(a^l + 1) = a^k. \end{aligned}$$

Тогда $1 + a^l = a^t$ для некоторого $t \geq l$ и $a^l + 1 = a^s$ для некоторого $s \geq l$.

Возможны два случая:

- 1) $t = l$ или $s = l$;
- 2) $t > l$ и $s > l$.

Рассмотрим первый случай. Пусть $t = l$, т. е. выполняется равенство $1 + a^l = a^l$. Рассмотрим сумму $a^l + 1 + a^l$:

$$(a^l + 1) + a^l = a^l + (1 + a^l), \quad a^s + a^l = a^l.$$

Домножая последнее равенство на a^{k-s} , получаем

$$a^k + a^{k+(l-s)} = a^{k+(l-s)}.$$

Учитывая равенство (4), выводим, что

$$a^k = a^{k+(l-s)},$$

откуда следует, что $k + (l - s) \geq k$, следовательно $l \geq s$. Учитывая, что $l \leq s$, имеем $s = l$, т. е. $a^l + 1 = a^l = 1 + a^l$.

Аналогично из равенства $s = l$ ($a^l + 1 = a^l$) вытекает $1 + a^l = a^l = a^l + 1$.

Рассмотрим второй случай. Пусть теперь $t > l$ и $s > l$. Добавляя к равенству $1 + a^l = a^t$ элемент 1 слева и к равенству $a^l + 1 = a^s$ элемент 1 справа, получаем

$$1 + a^t = a^t, \quad a^s + 1 = a^s.$$

Применяя рассуждения, приведённые выше, имеем

$$1 + a^t = a^t + 1 = a^t, \quad 1 + a^s = a^s + 1 = a^s.$$

Наконец,

$$1 + a^l = a^t = a^t + 1 = 1 + a^l + 1 = 1 + a^s = a^s = a^l + 1.$$

Таким образом, имеем коммутативное сложение в S , что противоречит условию. $\square$

5.2. Конечные идемпотентные циклические полукольца с циклом

В этом разделе мы изучим строение конечных идемпотентных циклических полуколец $S = (a)$ типа (k, n) с некоммутативным сложением, имеющих нетривиальный цикл C ($n \geq 2$).

В силу предложения 4 и леммы 10 остаётся рассмотреть случай

$$1 + a^{nl} = a^{nl} + 1 = a^{nl}.$$

На таком полукольце S зададим бинарное отношение $\sim$ формулой

$$x \sim y \iff x, y \in C \text{ или } x = y.$$

Лемма 11. *Отношение $\sim$ является конгруэнцией.*

Доказательство. Достаточно воспользоваться леммой 9. $\square$

Отношение $\sim$ «склеивает» элементы цикла C в один класс, а каждый из оставшихся элементов полукольца S образует одноэлементный класс.

Рассмотрим канонический гомоморфизм $\pi: S \rightarrow S/\sim$, такой что $\pi(x) = [x]_\sim$ для всех $x \in S$. Фактор-полукольцо $S/\sim$ также является конечным идемпотентным циклическим полукольцом, но с поглощающим элементом $[a^k]_\sim$. По теореме 3 сложение в фактор-полукольце $S/\sim$ либо левое, либо правое, либо коммутативное.

Лемма 12. *Если в фактор-полукольце $S/\sim$ сложение левое (правое), то и в самом полукольце S сложение левое (правое).*

Доказательство. Пусть в фактор-полукольце $S/\sim$ сложение левое. Имеем

$$\pi(1 + a) = \pi(1) + \pi(a) = \pi(1) = 1.$$

Отсюда следует, что $1 + a = 1$, и по лемме 3 в полукольце S сложение левое.

Аналогично показывается, что если в фактор-полукольце $S/\sim$ сложение правое, то и в полукольце S сложение правое. $\square$

Следствие 2. Если в конечном идемпотентном циклическом полукольце S сложение не является ни левым, ни правым, то в фактор-полукольце $S/\sim$ сложение коммутативное. $\square$

Лемма 13. Если в фактор-полукольце $S/\sim$ коммутативное сложение, то

- 1) $1 + a^{nl} = a^{nl} = a^{nl} + 1$, где a^{nl} — единица цикла C полукольца S для такого натурального l , что $n(l-1) < k \leq nl$;
- 2) для любых элементов a^r и a^s полукольца S , $r-s \not\equiv 0 \pmod{n}$, выполняется равенство

$$a^r + a^s = a^{r+nl} + a^{s+nl}. \quad (5)$$

Доказательство. Первое утверждение следует из предложения 4 и леммы 10.

Докажем второе утверждение. Пусть t — произвольное натуральное число, такое что $t \not\equiv 0 \pmod{n}$.

Так как сложение в фактор-полукольце $S/\sim$ коммутативно, имеем

$$\pi(1 + a^t) = \pi(1) + \pi(a^t) = \pi(a^t) + \pi(1) = \pi(a^t + 1).$$

Пусть $1 + a^t \notin C$. Тогда $\pi(1 + a^t) \notin C$, $\pi(a^t + 1) \notin C$, откуда следует, что $1 + a^t = a^t + 1$. Домножая это равенство на элемент a^{nl} , получаем

$$a^{nl} + a^{nl+t} = a^{nl+t} + a^{nl}.$$

Так как сложение в цикле C некоммутативно, имеем

$$a^{nl} = a^{nl+t}, \quad nl \equiv nl + t \pmod{n}, \quad 0 \equiv t \pmod{n}.$$

Противоречие. Следовательно, $1 + a^t \in C$, и поэтому выполняется

$$1 + a^t = a^{nl}(1 + a^t) = a^{nl} + a^{t+nl}.$$

Аналогично показывается, что выполняется равенство $a^t + 1 = a^{t+nl} + a^{nl}$.

Рассмотрим теперь произвольные элементы a^r и a^s полукольца S , такие что $r-s \not\equiv 0 \pmod{n}$. Если $r < s$, то

$$a^r + a^s = a^r(1 + a^{s-r}) = a^r(a^{nl} + a^{s-r+nl}) = a^{r+nl} + a^{s+nl}.$$

Если $r > s$, то снова получим равенство (5). $\square$

Лемма 14. Если в фактор-полукольце $S/\sim$ сложение коммутативное, то множество $T = \{1, a^n, a^{2n}, \dots, a^{nl}\}$ является циклическим подполукольцом в полукольце S , имеющим коммутативное сложение и поглощающий элемент a^{nl} .

Доказательство. Пусть a^{ni} и a^{nj} — произвольные элементы из множества T . Имеем

$$a^{ni} \cdot a^{nj} = a^{n(i+j)} \in T.$$

Значит, множество T замкнуто по умножению.

Так как сложение в фактор-полукольце $S/\sim$ коммутативно, имеем

$$\pi(1 + a^{ni}) = \pi(1) + \pi(a^{ni}) = \pi(a^{ni}) + \pi(1) = \pi(a^{ni} + 1).$$

Пусть $1 + a^{ni} \notin C$. Тогда $a^{ni} \notin C$ (по леммам 13 и 9), $\pi(1 + a^{ni}) \notin C$, $\pi(a^{ni} + 1) \notin C$, откуда следует, что $1 + a^{ni} = a^{ni} + 1$. Тогда если $1 + a^{ni} = a^{nq+r}$ для некоторых $q, r \in \mathbb{N}$, $0 \leq r < n$, то $a^{ni} + 1 = a^{nq+r}$. Добавляя к первому равенству 1 слева, а ко второму равенству 1 справа и учитывая, что $1 + a^{ni} = a^{ni} + 1$, получаем

$$1 + a^{nq+r} = a^{nq+r} = a^{nq+r} + 1.$$

Домножая это равенство на элемент a^{nl} , получаем

$$a^{nl} + a^{nl+nq+r} = a^{nl+nq+r} + a^{nl}.$$

Так как сложение в цикле C некоммукативно, имеем

$$a^{nl} = a^{nl+nq+r}, \quad nl \equiv nl + nq + r \pmod{n}, \quad 0 \equiv r \pmod{n}, \quad r = 0,$$

откуда следует, что

$$1 + a^{ni} = a^{nq} = a^{ni} + 1.$$

Пусть $1 + a^{ni} \in C$. Тогда и $a^{ni} + 1 \in C$ по леммам 13 и 9. Имеем

$$\begin{aligned} 1 + a^{ni} &= a^{nl}(1 + a^{ni}) = a^{nl} + a^{nl} \cdot a^{ni} = a^{nl} + a^{nl} = a^{nl}, \\ a^{ni} + 1 &= a^{nl}(a^{ni} + 1) = a^{nl} \cdot a^{ni} + a^{nl} = a^{nl} + a^{nl} = a^{nl}, \end{aligned}$$

откуда следует, что

$$1 + a^{ni} = a^{nl} = a^{ni} + 1.$$

Итак, для произвольного элемента $a^{ni} \in T$ верно $1 + a^{ni} = a^{nq} = a^{ni} + 1$ для некоторого $q \in \mathbb{N}$.

Рассмотрим сумму $a^{ni} + a^{nj}$ произвольных элементов a^{ni} и $a^{nj} \in T$. Если $ni \leq nj$ (аналогично при $ni \geq nj$), то

$$a^{ni} + a^{nj} = a^{ni}(1 + a^{n(j-i)}) = a^{ni} \cdot a^{nq} = a^{n(i+q)} = a^{ni}(a^{n(j-i)} + 1) = a^{nj} + a^{ni}$$

для некоторого $q \in \mathbb{N}$. Из последних равенств вытекает замкнутость и коммутативность сложения в множестве T .

Образующим элементом в подполукольце T является элемент a^n .

Элемент a^{nl} является поглощающим элементом в полукольце T , так как $a^{nl} \cdot a^n = a^{nl}$. $\square$

Суммируя следствие 2 и леммы 13 и 14, получаем следующий результат.

Теорема 4. Пусть в конечном идемпотентном циклическом полукольце $S = (a)$ типа (k, n) , $k \geq 1$, $n \geq 2$, сложение не является ни коммутативным, ни левым, ни правым. Тогда

- 1) $1 + a^{nl} = a^{nl} + 1 = a^{nl}$, где a^{nl} — единица цикла C полукольца S для такого натурального l , что $n(l-1) < k \leq nl$;
- 2) множество $T = \{1, a^n, a^{2n}, \dots, a^{nl}\}$ является циклическим подполукольцом в полукольце S , имеющим коммутативное сложение и поглощающий элемент a^{nl} ;

3) для любых $r, s \in \mathbb{N}_0$, где $r - s \not\equiv 0 \pmod{n}$, выполняется

$$a^r + a^s = a^{r+nl} + a^{s+nl}.$$

□

В следующей теореме доказывается существование и единственность полукольца со структурой, описанной в теореме 4.

Теорема 5. Пусть даны натуральные числа k, n, l , такие что $n \geq 2$ и $n(l-1) < k \leq nl$, произвольное идемпотентное циклическое полукольцо $T = \{1, b, b^2, \dots, b^l\}$ с коммутативным сложением и с поглощающим элементом b^l с условием $1 + b^l = b^l$ и некоторое циклическое полутело $C = \{1, c, c^2, \dots, c^{n-1}\}$. Тогда существует единственное с точностью до изоморфизма конечное идемпотентное циклическое полукольцо $S = (a)$ типа (k, n) с некоммутативным сложением, не являющимся ни левым, ни правым, такое что его подполукольцо $\{1, a^n, a^{2n}, \dots, a^{ln}\}$ изоморфно T , а его цикл $\{a^k, a^{k+1}, \dots, a^{k+n-1}\}$ изоморфен C .

Доказательство. Определим на циклической полугруппе $S = \{1, a, a^2, \dots, a^k, \dots, a^{k+n-1}\}$ операцию сложения $+$, превращающую эту группу в циклическое полукольцо S типа (k, n) . Установим сначала изоморфизмы мультипликативных полугрупп:

$$\begin{aligned} \alpha: \{1, b, b^2, \dots, b^l\} &\rightarrow \{1, a^n, a^{2n}, \dots, a^{ln}\}, \\ \alpha(b^i) &= a^{ni} \text{ для каждого } i = 0, 1, \dots, l, \\ \beta: \{1, c, c^2, \dots, c^{n-1}\} &\rightarrow \{a^{nl}, a^{nl+1}, \dots, a^{nl+n-1}\}, \\ \beta(c^i) &= a^{nl+i} \text{ для каждого } i = 0, 1, \dots, n-1. \end{aligned}$$

На циклической подполугруппе $\{1, a^n, a^{2n}, \dots, a^{ln}\}$ циклической полугруппы S зададим операцию сложения $+$ по формуле

$$a^{ni} + a^{nj} = \alpha(b^i + b^j) \text{ для всех } i, j = 0, 1, \dots, l,$$

а на циклической подполугруппе $\{a^{nl}, a^{nl+1}, \dots, a^{nl+n-1}\}$ по правилу

$$a^{nl+i} + a^{nl+j} = \beta(c^i + c^j) \text{ для всех } i, j = 0, 1, \dots, n-1.$$

Относительно введённых операций сложения и имеющегося умножения получаем алгебры $\{1, a^n, a^{2n}, \dots, a^{ln}\}$ и $\{a^{nl}, a^{nl+1}, \dots, a^{nl+n-1}\}$, первая из которых изоморфна T , а вторая C . Поэтому $\{1, a^n, a^{2n}, \dots, a^{ln}\}$ — циклическое полукольцо с коммутативным сложением и поглощающим элементом a^{ln} , а $\{a^{nl}, a^{nl+1}, \dots, a^{nl+n-1}\}$ — циклическое полутело.

Зададим сложение остальных элементов полугруппы S по следующему правилу:

- а) $a^r + a^s = a^{r+nl} + a^{s+nl}$ для любых $r, s \in \mathbb{N}_0$, таких что $r - s \not\equiv 0 \pmod{n}$;
- б) $a^r + a^s = a^{\min\{r,s\}}(1 + a^{|r-s|})$ для любых $r, s \in \mathbb{N}_0$, таких что $r - s \equiv 0 \pmod{n}$.

Проверим дистрибутивность умножения относительно сложения и ассоциативность сложения в полугруппе S . Проверим закон дистрибутивности:

$$a^r(a^s + a^t) = a^{r+s} + a^{r+t}.$$

Возможны два случая:

- 1) $t - s \not\equiv 0 \pmod{n}$; при этом

$$\begin{aligned} a^r(a^s + a^t) &= a^r(a^{s+nl} + a^{t+nl}) = \\ &= a^{r+nl}(a^{s+nl} + a^{t+nl}) = a^{r+s+nl} + a^{r+t+nl} = a^{r+s} + a^{r+t}; \end{aligned}$$

- 2) $t - s \equiv 0 \pmod{n}$; если $s \leq t$ (аналогично при $s > t$), то

$$a^r(a^s + a^t) = a^r(a^s(1 + a^{t-s})) = a^{r+s}(1 + a^{t-s}) = a^{r+s} + a^{r+t}.$$

Таким образом, дистрибутивность в S выполняется.

Проверим ассоциативность сложения:

$$(a^r + a^s) + a^t = a^r + (a^s + a^t).$$

Вынося за скобки наименьшую степень элемента a , в скобках получим сумму 1 и двух степеней элемента a . Поэтому достаточно показать, что для любых $i, j \in \mathbb{N}_0$ выполняется

$$(1 + a^i) + a^j = 1 + (a^i + a^j), \quad (a^i + 1) + a^j = a^i + (1 + a^j), \quad (a^i + a^j) + 1 = a^i + (a^j + 1).$$

Проверим первое равенство. Остальные равенства проверяются точно так же.

Сначала отметим, что для любого натурального $t \geq k$ справедливы равенства

$$1 + a^t = a^{nl} + a^{t+nl}, \quad a^t + 1 = a^{t+nl} + a^{nl}. \quad (6)$$

Действительно, если $t \not\equiv 0 \pmod{n}$, то по определению сложения $1 + a^t = a^{nl} + a^{t+nl}$. Если $t \equiv 0 \pmod{n}$, то $a^t = a^{nl}$ и $1 + a^t = 1 + a^{nl} = a^{nl} = a^{nl} + a^{nl} = a^{nl} + a^{t+nl}$. Аналогично $a^t + 1 = a^{t+nl} + a^{nl}$ для любого $a^t \in C$.

При рассмотрении следующих случаев без специальных оговорок используются равенства (6) и доказанная дистрибутивность.

Возможны четыре случая.

1. $i \equiv 0 \pmod{n}$, $j \equiv 0 \pmod{n}$. Ассоциативность выполняется, поскольку она выполняется для этих элементов в заданном полукольце T .
2. $i \equiv 0 \pmod{n}$, $j \not\equiv 0 \pmod{n}$. Имеем $1 + a^i = a^{nt}$ для некоторого $t \in \mathbb{N}_0$. Так как $nt - j \not\equiv 0 \pmod{n}$, то

$$\begin{aligned} (1 + a^i) + a^j &= a^{nt}(1 + a^i) + a^{j+nl} = (a^{nt} + a^{i+nt}) + a^{j+nl}, \\ 1 + (a^i + a^j) &= 1 + (a^{i+nl} + a^{j+nl}) = a^{nl} + (a^{i+nl} + a^{j+nl}). \end{aligned}$$

Правые части полученных равенств равны, поскольку $a^{nl}, a^{i+nl}, a^{j+nl} \in C$, а сложение в C ассоциативно (соответствующее заключение верно и в случаях 3 и 4 а)).

3. $i \not\equiv 0 \pmod{n}$, $j \equiv 0 \pmod{n}$. Имеем $i - j \not\equiv 0 \pmod{n}$. Тогда

$$\begin{aligned}(1 + a^i) + a^j &= (a^{nl} + a^{i+nl}) + a^j = a^j((a^{nl} + a^{i+nl}) + 1) = \\ &= a^j(a^{nl}(a^{nl} + a^{i+nl}) + a^{nl}) = a^j((a^{nl} + a^{i+nl}) + a^{nl}) = \\ &= (a^{nl} + a^{i+nl}) + a^{nl}, \\ 1 + (a^i + a^j) &= 1 + (a^{i+nl} + a^{j+nl}) = a^{nl} + (a^{i+nl} + a^{nl}).\end{aligned}$$

4. $i \not\equiv 0 \pmod{n}$, $j \not\equiv 0 \pmod{n}$.

а) $i - j \not\equiv 0 \pmod{n}$.

$$\begin{aligned}(1 + a^i) + a^j &= (a^{nl} + a^{i+nl}) + a^j = a^j((a^{nl+nl-j} + a^{i+nl+nl-j}) + 1) = \\ &= a^j((a^{nl+nl-j} + a^{i+nl+nl-j}) + a^{nl}) = (a^{nl} + a^{i+nl}) + a^{j+nl}, \\ 1 + (a^i + a^j) &= 1 + (a^{i+nl} + a^{j+nl}) = a^{nl} + (a^{i+nl} + a^{j+nl}).\end{aligned}$$

б) $i - j \equiv 0 \pmod{n}$. Если $i \leq j$ (аналогично при $i > j$), то

$$\begin{aligned}(1 + a^i) + a^j &= (a^{nl} + a^{i+nl}) + a^j = a^j((a^{nl+nl-j} + a^{i+nl+nl-j}) + 1) = \\ &= a^j((a^{nl+nl-j} + a^{i+nl+nl-j}) + a^{nl}) = (a^{nl} + a^{i+nl}) + a^{j+nl} = \\ &= a^{nl} + (a^{i+nl} + a^{j+nl}) = a^{nl} + a^{i+nl}(1 + a^{j-i}) = a^{nl} + a^{i+nl}, \\ 1 + (a^i + a^j) &= 1 + a^i(1 + a^{j-i}) = a^{nl} + a^{i+nl}(1 + a^{j-i}) = a^{nl} + a^{i+nl}.\end{aligned}$$

Итак, циклическая полугруппа $S = (a)$ с определённым выше сложением является конечным идемпотентным циклическим полукольцом типа (k, n) с некоммутативным сложением и соответствующими изоморфизмами α и β . Единственность такого полукольца S обеспечивается однозначностью задания сложения в S , вытекающего из свойства 3) теоремы 4. $\square$

Замечание 4. Теоремы 3—5 дают описание конечных идемпотентных циклических полуколец с некоммутативным сложением «по модулю» конечных идемпотентных циклических полуколец с коммутативным сложением, которые имеют свою специфику и требуют отдельного рассмотрения.

С помощью системы Maple для математических вычислений были найдены конечные неидемпотентные циклические полукольца с некоммутативным сложением небольшого порядка. Они достаточно многочисленны и разнообразны. Например, таких полуколец с поглощающим элементом с точностью до изоморфизма имеется 4 порядка 4, 28 порядка 5, 194 порядка 6. Строение неидемпотентных циклических полуколец с некоммутативным сложением предполагается изложить в следующей статье.

Литература

- [1] Бестужев А. С. О строении конечных циклических полуколец // Вестник ВятГГУ. Информатика. Математика. Язык. — 2010. — Вып. 6. — С. 143—148.
- [2] Вечтомов Е. М. Введение в полукольца. — Киров: Вятский гос. пед. ун-т, 2000.

- [3] Скорняков Л. А. Элементы алгебры. — М.: Наука, 1986.
- [4] Чермных В. В. Полукольца. — Киров: Вятский гос. пед. ун-т, 1997.
- [5] Weinert H. J. Zur Theorie der HalbFastkörper // Studia Sci. Math. Hungar. — 1981. — Vol. 16. — P. 201—218.