*Вестник Сыктывкарского университета.
Сер.1. Вып.16.2012*

УДК 512.55

О КОНЕЧНЫХ ЦИКЛИЧЕСКИХ ПОЛУКОЛЬЦАХ С НЕИДЕМПОТЕНТНЫМ НЕКОММУТАТИВНЫМ СЛОЖЕНИЕМ

И. В. Орлова (Лубягина)

В работе конечные циклические полукольца с неидемпотентным некоммутативным сложением сведены к таким полукольцам с поглощающим элементом и конечным циклическим полутелам (теорема 1). Изучаются конечные циклические полукольца с неидемпотентным некоммутативным сложением и коротким хвостом. Теоремы 2 и 4 дают необходимые условия на сложение в изучаемых полукольцах, а теорема 3 дает достаточное условие на сложение в мультипликативной циклической полугруппе, превращающее ее в циклическое полукольцо с неидемпотентным некоммутативным сложением. Теорема 5 является критерием для определения того, является ли конечная мультипликативная циклическая полугруппа с коротким хвостом и с заданным на ней сложением полукольцом.
Ключевые слова: полукольцо, полутело, циклическое полукольцо, неидемпотентное сложение, некоммутативное сложение.

1. Введение

Данная работа посвящена изучению строения конечных циклических полуколец с неидемпотентным некоммутативным сложением. Строение бесконечных циклических полуколец с коммутативным сложением получено Е. М. Вечтомовым [1]. Бесконечные циклические полукольца с некоммутативным сложением имеют идемпотентное сложение: левое или правое [2]. Изучение конечных циклических полуколец с коммутативным сложением ведется А. С. Бестужевым [3]. Конечные циклические полукольца с идемпотентным некоммутативным сложением описаны в работе [2]. В нашей статье рассматриваются конечные циклические полукольца с неидемпотентным некоммутативным сложением. Большое внимание уделяется конечным циклическим полукольцам с неидемпотентным некоммутативным сложением и коротким хвостом (типа (k, n) при $k \leqslant n$). Для нахождения подобных полуколец небольшого порядка ($n \leqslant 12$) написана программа на языке Си.

2. Предварительные сведения

Полукольцом называется алгебра $\langle S, +, \cdot \rangle$ с операциями сложения $+$ и умножения $\cdot$, такими, что $\langle S, + \rangle$ и $\langle S, \cdot \rangle$ — полугруппы и умножение дистрибутивно относительно сложения с обеих сторон. В полукольце S может существовать нейтральный по сложению элемент 0, обладающий свойством мультипликативности (то есть $x \cdot 0 = 0 \cdot x = 0$ для любого $x \in S$), называемый *нулем*. Полукольцо S с тождеством $x + x = x$ называется *идемпотентным*, в противном случае — *неидемпотентным*.

Циклическим полукольцом называется полукольцо S с единицей 1, если в S существует *образующий* элемент $a \neq 1$, такой, что каждый элемент из S является его неотрицательной целой степенью. Заметим, что бесконечные циклические полукольца идемпотентны [1, теорема 4], [2, теорема 1]. Учитывая предложения 1 и 2 [2], будем рассматривать циклические полукольца без нуля.

Циклическая (мультипликативная) полугруппа $\{1, a, a^2, \ldots, a^k, \ldots, a^{k+n-1}\}$, в которой $a^{k+n} = a^k$, где $k \in \mathbb{N}_0$, $n \in N$ (мощность полугруппы $|S| = k + n \geqslant 2$), называется *полугруппой типа* (k, n). Полукольцо с мультипликативной полугруппой типа (k, n) называется *полукольцом типа* (k, n). В дальнейшем множество $\{1, a, a^2, \ldots, a^{k-1}\}$ называется *хвостом* полукольца S в случае $k \geqslant 1$, множество $C = \{a^k, a^{k+1}, \ldots, a^{k+n-1}\}$ — его *циклом*. По теореме 2 [2] цикл C полукольца S является циклическим полутелом с единицей $e = a^{nl}$ и образующим элементом $c = a^{nl+1}$ для некоторого $l \in \mathbb{N}_0$ такого, что $nl \geqslant k > n(l-1)$.

По теореме Вейнерта любое конечное полутело $C \cong (C+e) \times (e+C)$, где $C + e$ — подполутело в C с левым сложением, $e + C$ — подполутело в C с правым сложением. Поскольку циклическая группа C порядка n раскладывается в прямое произведение двух групп $C + e$ и $e + C$ порядков m и h соответственно, то эти группы являются циклическими, их порядки взаимно просты $(m, h) = 1$, $m \cdot h = n$, $C + e = (c^h)$, $e + C = (c^m)$.

По предложению 3 [2] сложение в конечном циклическом полутеле $C = (c)$ осуществляется по формуле (для любых $hi_1, mj_1, hi_2, mj_2 \in \mathbb{N}$):

$$c^{hi_1+mj_1} + c^{hi_2+mj_2} = c^{hi_1+mj_2}.$$

Пусть произвольные числа $r, s \in \mathbb{N}_0$ имеют разложения:

$$r = hi_1 + mj_1, \quad s = hi_2 + mj_2. \tag{1}$$

для некоторых $i_1, j_1, i_2, j_2 \in \mathbb{Z}$.

Обобщим правило сложения в конечном циклическом полутеле $C = (c)$: для любых $r, s \in \mathbb{N}_0$ выполняется

$$c^r + c^s = c^t, \text{ где } t \equiv hi_1 + mj_2 (\operatorname{mod} n). \tag{2}$$

В циклических полукольцах типа (k, n) с неидемпотентным некоммутативным сложением $k \geqslant 1$, поскольку в случае $k = 0$ получаем полутело, которое всегда идемпотентно [2, лемма 4].

Ранее с помощью системы Maple для математических вычислений нами были найдены конечные циклические полукольца с неидемпотентным некоммутативным сложением небольшого порядка [2]. Они достаточно многочисленны и разнообразны. Например, таких полуколец с поглощающим элементом с точностью до изоморфизма: 4 порядка 4, 28 порядка 5, 194 порядка 6.

3. Общие свойства конечных циклических полуколец с неидемпотентным некоммутативным сложением

Пусть $S = (a)$ — циклическое полукольцо типа (k, n) с неидемпотентным сложением (если не оговорено противное).

Лемма 1. *В $S = (a)$ выполняется $1 + 1 = a^{ni}$ для некоторого натурального числа i. В частности, если $k \leqslant n$, то $1 + 1 = a^n \in C$.*

Доказательство. В силу идемпотентности сложения в конечных полутелах [2] имеем $a^{nl} + a^{nl} = a^{nl}$, где $nl \geqslant k > n(l-1)$. Тогда $a^{nl}(1+1) = a^{nl}$, откуда $1 + 1 = a^{ni}$ для некоторого натурального i. □

Замечание 1. Если в $S = (a)$ выполняется $1 + 1 = a$, то сложение в S коммутативно. Действительно, если $1 + 1 = a$, то для любого натурального i элемент $a^i = (1 + 1)^i = \underbrace{1 + \ldots + 1}_{2^i}$, откуда $1 + a^i = \underbrace{1 + \ldots + 1}_{2^i + 1} = a^i + 1$, то есть сложение в S коммутативно.

Лемма 2. *В $S = (a)$ с некоммутативным сложением не выполняется ни одно из равенств $1 + a^{nl} = 1$, $a^{nl} + 1 = 1$, где $nl \geqslant k > n(l-1)$.*

Доказательство. Пусть $1 + a^{nl} = 1$ в S. Имеем $1 + 1 = a^r$ для некоторого натурального r. Тогда по лемме 7 [2] выполняется $a^{nl} + 1 = 1$.

По предложению 4 [2] случай $1+a^{nl}=a^{nl}+1=1$ невозможен (приводит к коммутативности сложения). □

Лемма 3. *В $S=(a)$ с некоммутативным сложением выполняется $1+a^{nl}=a^{nl}+1=a^{nl}$, где $nl\geqslant k>n(l-1)$.*

Доказательство. Утверждение леммы следует из предложения 4 [2] и леммы 2. □

Лемма 4. *В $S=(a)$ с некоммутативным сложением для любых $r<k$ и $s<k$ выполняется*

$$a^r+a^s=a^t,\ \textit{где}\ t>\max\{r,s\}. \tag{3}$$

Доказательство. Пусть $r<k$, $s<k$ и $a^r+a^s=a^t$.

В случае $r=s=0$ получаем $t>\max\{r,s\}$ в силу неидемпотентности сложения в S.

Рассмотрим случай $r=0$ и $0\neq s<k$. Пусть $t<s$, тогда, домножая равенство $1+a^s=a^t$ на a^{k-s}, получаем $a^{k-s}+a^k=a^{k+t-s}\notin C$. С другой стороны, по лемме 3 и лемме 9 [2] имеем $a^{k-s}+a^k\in C$. Противоречие. Таким образом, $t\geqslant s$.

Пусть s – наименьшее натуральное число такое, что $1+a^s=a^s$. Добавляя слева к последнему равенству элемент 1 и используя лемму 1, получаем $a^{ni}+a^s=a^s$ для некоторого натурального i. В случае $ni=s$ противоречие с неидемпотентностью сложения. Если $ni<s$, то $a^{ni}(1+a^{s-ni})=a^s$, откуда $1+a^{s-ni}=a^{s-ni}$ и получаем противоречие с наименьшестью s. Если $ni>s$, то $a^s(a^{ni-s}+1)=a^s$, откуда $a^{ni-s}+1=1$ и по лемме 7 [2] выполняется $a^{nl}+1=1$, противоречие с леммой 3. Следовательно, $1+a^s\neq a^s$ ни для какого $s<k$, то есть $t\neq s$.

Таким образом, для $r=0$ и $s\neq 0$ выполняется $t>s$ и утверждение леммы верно.

Аналогично, оно верно и для $r\neq 0$ и $s=0$.

Пусть $r\neq 0$ и $s\neq 0$. Тогда, учитывая вышеприведенные доказательства, в случае $r\leqslant s$ верно $a^r+a^s=a^r(1+a^{s-r})=a^t$, где $t>s$; в случае $r>s$ выполняется $a^r+a^s=a^s(a^{r-s}+1)=a^t$, где $t>r$.

Итак, для любых $r<k$ и $s<k$ имеем $a^r+a^s=a^t$, где $t>\max\{r,s\}$. □

Замечание 2. Утверждение леммы 4 верно и в случас, когда $r\geqslant k$ или $s\geqslant k$. Действительно, по лемме 3 и лемме 9 [2] имеем $t\geqslant k$. Поскольку t можно сделать сколь угодно большим, добавляя к нему число n до тех пор, пока оно не превысит r и s, можно считать, что $t>\max\{r,s\}$.

Лемма 5. *В* $S = (a)$ *с некоммутативным сложением для любых* $r, s \in \mathbb{N}_0$ *выполняется:*

$$a^r + a^s = a^t, \text{ где } t \equiv hi_1 + mj_2 (\operatorname{mod} n). \tag{4}$$

Доказательство. Пусть $r, s \in \mathbb{N}_0$ — произвольные числа, имеющие разложения (1). По правилу сложения (2) в цикле C имеем:

$$a^{nl}(a^r + a^s) = a^{(nl+1)(hi_1+mj_1)} + a^{(nl+1)(hi_2+mj_2)} = a^{(nl+1)(hi_1+mj_2)},$$

откуда получаем утверждение леммы. □

Лемма 6. *В циклической полугруппе* $S = (a)$ *типа* (k, n) *со сложением, заданным правилами* (3) *и* (4) *и удовлетворяющим правилу* (*для любых* r *и* s*:* $0 \leqslant r \leqslant k+n-1$, $0 \leqslant s \leqslant k+n-1$)*:*

$$a^r + a^s = \begin{cases} a^r(1 + a^{s-r}), & \text{при } r \leqslant s, \\ a^s(a^{r-s} + 1), & \text{иначе,} \end{cases} \tag{5}$$

умножение дистрибутивно относительно сложения.

Доказательство. Докажем, что для любых $r, s, t \in \mathbb{N}_0$ выполняется

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

Это равенство достаточно доказать для $s \leqslant k+n-1$ и $t \leqslant k+n-1$.

Обозначим $a^p = a^r(a^s + a^t)$, $a^q = a^{r+s} + a^{r+t}$. По правилу сложения (4) имеем $p \equiv q \pmod n$.

Пусть $s \leqslant t$.

Если $r + s \geqslant k$, то $r + t \geqslant k$. Тогда $a^p = a^{r+s}(1 + a^{t-s}) \in C$, $a^q \in C$ по правилу (3) и $a^p = a^q$.

В случае $r+s < k$ и $r+t \leqslant k+n-1$ равенство $a^r(a^s+a^t) = a^{r+s}+a^{r+t}$ следует из правила сложения (5).

Если $r + s < k$ и $r + t > k + n - 1$, то $p > r + t > k + n - 1$ и $a^p \in C$. Элемент $a^q \in C$ по правилу (3). Таким образом, $a^p = a^q$.

Аналогично, для $s > t$ закон дистрибутивности выполняется. □

Лемма 7. *В циклической полугруппе* $S = (a)$ *типа* (k, n) *со сложением, заданным правилами* (3) *и* (4)*, выполняется:*

$$(r \geqslant k \text{ или } s \geqslant k \text{ или } t \geqslant k) \Rightarrow (a^r + a^s) + a^t = a^r + (a^s + a^t). \ \square$$

Лемма 8. *Сложение, заданное на циклической полугруппе $S = (a)$ типа (k, n) правилами (3) и (4) и удовлетворяющее правилу (5), превращает цикл C в полутело.*

Доказательство. Замкнутость сложения в цикле C следует из правила сложения в S, дистрибутивность умножения относительно сложения - из леммы 6, ассоциативность сложения – из леммы 7. □

Аналогично рассмотренному в работе [2] отношению $\sim$, зададим бинарное отношение $\sim$ на S формулой:

$$x \sim y \Leftrightarrow (x \in C \text{ и } y \in C) \text{ или } x = y.$$

Аналогично идемпотентному случаю выполняется

Лемма 9. *Отношение $\sim$ является конгруэнцией.*

Достаточно воспользоваться леммой 3 и леммой 9 [2].

Отношение $\sim$ «склеивает» элементы цикла C в один класс, а каждый из остальных элементов полукольца S образует одноэлементный класс. Факторполукольцо $S/\sim$ является циклическим полукольцом с неидемпотентным некоммутативным сложением и поглощающим элементом $[a^k]_\sim$.

Выясним условия, при которых из циклического полукольца $S' = (a)$ с неидемпотентным некоммутативным сложением и поглощающим элементом a^k и циклического полутела C' порядка n можно построить циклическое полукольцо S типа (k, n) с неидемпотентным некоммутативным сложением так, чтобы $S/\sim = S'$ и $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$.

Теорема 1. *Пусть даны произвольные натуральные числа k и n, произвольное циклическое полукольцо $S' = \{1, a, a^2, \ldots, a^k\}$ с неидемпотентным некоммутативным сложением и поглощающим элементом a^k, некоторое циклическое полутело $C' = \{e = c^n, c, c^2, \ldots, c^{n-1}\}$ порядка n, где $|C' + e| = m$, $|e + C'| = h$. Циклическое полукольцо $S = (a)$ типа (k, n), факторполукольцо которого по конгруэнции $\sim$ совпадает с полукольцом S', то есть $S/\sim = S'$, а цикл C полукольца S изоморфен полутелу C', то есть $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$, существует тогда и только тогда, когда в S' для любых $r, s \in \mathbb{N}_0$ выполняется условие:*

$$a^r + a^s = a^t, \text{ где } t \equiv hi_1 + mj_2 (\operatorname{mod} n), t > \max\{r, s\}. \tag{6}$$

Доказательство. Пусть $S = (a)$ – циклическое полукольцо типа (k, n) с неидемпотентным некоммутативным сложением, в котором $S/\sim = S'$ и $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$. По лемме 4, замечанию 2 и лемме 5 сложение в S удовлетворяет условию (6). Из $S/\sim = S'$ следует, что условие (6) выполняется и в S'.

В обратную сторону. Пусть в S' выполняется условие (6). Построим циклическое полукольцо типа (k, n) с неидемпотентным некоммутативным сложением, определив сложение в циклической полугруппе $S = (a)$ типа (k, n) следующим образом. Суммы вида $1 + a^z$ и $a^z + 1$, где $z < k$, положим равными соответствующим суммам в S', если те не равны a^k. Остальные суммы того же вида определим по формулам ($z = hi + mj$):

$$1 + a^z = a^p, \text{ где } p \equiv mj (\operatorname{mod} n), p > z,$$
$$a^z + 1 = a^q, \text{ где } q \equiv hi (\operatorname{mod} n), q > z.$$

Суммы остальных элементов полугруппы S зададим по правилу (5). Учитывая введенное на S сложение, условие (6) в S выполняется.

По лемме 6 умножение дистрибутивно относительно сложения.

Докажем ассоциативность сложения в S, то есть для любых натуральных r, s и t верно:

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

Обозначим $a^p = (a^r + a^s) + a^t$, $a^q = a^r + (a^s + a^t)$. По условию (6) имеем $p \equiv q (\operatorname{mod} n)$.

Если $r \geqslant k$ или $s \geqslant k$ или $t \geqslant k$, то по лемме 7 имеем $a^p = a^q$.

Пусть одновременно $r < k$, $s < k$, $t < k$. Если в S сумма $(a^r + a^s) + a^t \notin C$, то в S' аналогичная сумма $(a^r + a^s) + a^t \neq a^k$. В силу ассоциативности сложения в полукольце S' имеем $a^r + (a^s + a^t) = (a^r + a^s) + a^t \neq a^k$, следовательно, в S элемент $a^r + (a^s + a^t) \notin C$ и в S также верно $(a^r + a^s) + a^t = a^r + (a^s + a^t)$.

Если в S сумма $(a^r + a^s) + a^t \in C$, то в S' имеем $(a^r + a^s) + a^t = a^k$. В силу ассоциативности сложения в S' выполняется $a^r + (a^s + a^t) = (a^r + a^s) + a^t = a^k$, следовательно, в S элемент $a^r + (a^s + a^t) \in C$, и в S верно $(a^r + a^s) + a^t = a^r + (a^s + a^t)$.

Таким образом, S – циклическое полукольцо типа (k, n). По построению полукольца S имеем $S/\sim = S'$.

Установим изоморфизм мультипликативных полугрупп:

$$\alpha : \{e = c^n, c, c^2, \ldots, c^{n-1}\} \to \{a^k, a^{k+1}, a^{k+2}, \ldots, a^{k+n-1}\},$$
$$\alpha(c^i) = a^{(nl+1)i} \ \forall i = 1, 2, \ldots, n.$$

Учитывая правило сложения (2) в полутеле C' и условие (6) в полукольце S, получаем, что для любых $r, s \in \mathbb{N}_0$:

$$\alpha(c^r + c^s) = \alpha(c^{hi_1+mj_2}) = a^{(nl+1)(hi_1+mj_2)} = a^{(nl+1)(hi_1+mj_1)} + a^{(nl+1)(hi_2+mj_2)} = \\ = \alpha(c^r) + \alpha(c^s).$$

Таким образом, α – аддитивный изоморфизм и $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$. □

Замечание 3. Из лемм 4, 5 и замечания 2 следует, что полукольцо S из теоремы 1 единственно (если оно существует).

Предложение 1. *Хвост T полукольца S из теоремы 1 совпадает с $S' \setminus \{a^k\}$, то есть $\langle T, +, \cdot\rangle = \langle S' \setminus \{a^k\}, +, \cdot\rangle$, только в случае $|C'| = 1$.*

Доказательство. В случае $|C'| = 1$ очевидно, что $\langle S, +, \cdot\rangle = \langle S', +, \cdot\rangle$, следовательно, $\langle T, +, \cdot\rangle = \langle S' \setminus \{a^k\}, +, \cdot\rangle$.

Пусть $|C'| \neq 1$. В силу идемпотентности сложения в цикле C полукольца S имеем $a^k + a^k = a^k$, откуда, учитывая неидемпотентность сложения в S, получаем $a^{k-1} + a^{k-1} = a^{k+n-1}$. Отсюда, принимая во внимание $a^k \neq a^{k+n-1}$, следует $\langle T, +\rangle \neq \langle S' \setminus \{a^k\}, +\rangle$. Таким образом, $\langle T, +, \cdot\rangle \neq \langle S' \setminus \{a^k\}, +, \cdot\rangle$. □

4. Необходимые условия для сложения в конечных циклических полукольцах с неидемпотентным некоммутативным сложением и коротким хвостом

Пусть $S = (a)$ — циклическое полукольцо типа (k, n) с неидемпотентным сложением и условием $k \leqslant n$.

Задача заключается в нахождении правила сложения в полукольце S.

Рассмотрим разложения натурального числа z, где $0 \leqslant z \leqslant k+n-1$:

$$z = hi_1 + mj_1, \quad \text{где} \quad 1 \leqslant mj_1 \leqslant n, \tag{7}$$

$$z = hi_2 + mj_2, \quad \text{где} \quad 1 \leqslant hi_2 \leqslant n \tag{8}$$

для $i_1, i_2, j_1, j_2 \in \mathbb{Z}$. Такие разложения всегда можно получить из произвольного разложения $z = hi + mj$, одновременно добавляя к hi число n и вычитая из mj число n, или наоборот.

Теорема 2. *Если полукольцо $S = (a)$ типа (k, n), где $k \leqslant n$, имеет некоммутативное сложение, цикл C изоморфен прямому произведению подполутел $C + e$ и $e + C$ порядков m и h соответственно, то выполняются равенства:*

$$\text{(a) } 1 + a^z = \begin{cases} a^{mj_1+n}, \text{ если } mj_1 - hi_1 < k, \\ a^{mj_1}(\text{I}) \text{ или } a^{mj_1+n}(\text{II}), \text{ в иных случаях,} \end{cases}$$

где z удовлетворяет (7).

(б) $a^z+1=\begin{cases} a^{hi_2+n}, \text{ если } hi_2-mj_2<k, \\ a^{hi_2}(\mathrm{I}) \text{ или } a^{hi_2+n}(\mathrm{II}), \text{ в иных случаях,} \end{cases}$

где z удовлетворяет (8).

Доказательство. Пусть $z=hi_1+mj_1$ — натуральное число, удовлетворяющее (7). Заметим, что если $k\leqslant mj_1\leqslant n$, то по лемме 5 верно $1+a^z=a^{mj_1}=a^{mj_1+n}$.

Возможны следующие случаи.

1. Если $z=0$, то $mj_1\equiv 0(\operatorname{mod} h)$, откуда $mj_1=n\geqslant k$.

2. Пусть $z\geqslant k$. Тогда по леммам 4 и 5 получаем $1+a^z=a^{mj_1+n}$.

В случае $mj_1-hi_1\geqslant k$ верно $mj_1\geqslant k$ и, как отмечено выше, $1+a^z=a^{mj_1}=a^{mj_1+n}$.

3. Пусть $1\leqslant z<k$ и $1\leqslant mj_1<k$. По леммам 4 и 5:

$$a^{hi_1+mj_1+n-k}(a^{k-hi_1-mj_1}+a^k)=a^{mj_1+n},$$

откуда, учитывая $a^{k-hi_1-mj_1}+a^k\in C$ (по леммам 3 и 9 [2]), имеем:

$$a^{k-hi_1-mj_1}(1+a^{hi_1+mj_1})=a^{k-hi_1+n} \quad \text{при } hi_1>0,$$
$$a^{k-hi_1-mj_1}(1+a^{hi_1+mj_1})=a^{k-hi_1} \quad \text{при } hi_1\leqslant 0.$$

Если $hi_1>0$, то $1+a^{hi_1+mj_1}=a^{mj_1+n}$. Заметим, что в этом случае $mj_1-hi_1<k$.

Если $hi_1\leqslant 0$, то $1+a^{hi_1+mj_1}=a^{mj_1}$ или $1+a^{hi_1+mj_1}=a^{mj_1+n}$.

Пусть в случае $hi_1\leqslant 0$ одновременно $mj_1-hi_1<k$ и $1+a^{hi_1+mj_1}=a^{mj_1}$. По леммам 4 и 5 имеем $a^{-hi_1}+1=a^{-hi_1+n}\in C$ и по лемме 9 [2] $(a^{-hi_1}+1)+a^{hi_1+mj_1}\in C$. Тогда:

$$(a^{-hi_1}+1)+a^{hi_1+mj_1}=a^{-hi_1}+(1+a^{hi_1+mj_1})=a^{-hi_1}+a^{mj_1}=$$
$$=a^{-hi_1}(1+a^{hi_1+mj_1})=a^{-hi_1}\cdot a^{mj_1}=a^{mj_1-hi_1}\notin C, \text{ противоречие.}$$

Следовательно, если $mj_1-hi_1<k$, то $1+a^{hi_1+mj_1}=a^{mj_1}$ не выполняется, поэтому имеем $1+a^{hi_1+mj_1}=a^{mj_1+n}$.

Если же $mj_1-hi_1\geqslant k$, то $1+a^{hi_1+mj_1}=a^{mj_1}$ или $1+a^{hi_1+mj_1}=a^{mj_1+n}$.

Вторая часть теоремы доказывается аналогично. □

Следствие 1. *В $S=(a)$ с некоммутативным сложением и $k\leqslant n$ для произвольных чисел $i,j\in\mathbb{N}_0$ выполняются равенства:*

$$1+a^{hi}=a^{mj}+1=a^n\in C,$$
$$1+a^{mj}=a^{mj+n}\in C,$$
$$a^{hi}+1=a^{hi+n}\in C.$$

(k,n)	1	2	3	4	5	6	7	8	9	10	11	12
1	0	2	2	2	2	4	2	2	2	4	2	4
2		2	2	2	2	4	2	2	2	4	2	4
3			2	2	2	4	2	2	2	4	2	4
4				2	2	6	2	2	2	4	2	4
5					2	10	2	2	2	4	2	6
6						6	2	2	2	10	2	6
7							2	2	2	18	2	10
8								2	2	10	2	6
9									2	18	2	18
10										10	2	50
11											2	34
12												18

Рис. 1: Количество полуколец типа (k,n) с неидемпотентным некоммутативным сложением при $k \leqslant n$

Следствие 2. *Если в условиях теоремы 2 $m = 1$ или $h = 1$, то сложение в полукольце S сводится к сложению в цикле C следующим образом: $a^r + a^s = a^{r_1} + a^{s_1}$, где $r_1 \geqslant k$, $s_1 \geqslant k$, $r_1 \equiv r \pmod{n}$, $s_1 \equiv s \pmod{n}$.*

Предложение 2. *Для любого натурального $n = p^s$, где p – простое число ($p \geqslant 2$) и для любого натурального числа k ($k \leqslant n$) существует ровно два полукольца $S = (a)$ типа (k,n) с неидемпотентным некоммутативным сложением. По следствию 2 это сложение является «намоткой».*

Замечание 4. Для нахождения циклических полуколец с неидемпотентным некоммутативным сложением и коротким хвостом написана программа на языке Си. Она позволяет по заданным числам m, h и k находить все полукольца $S = (a)$ типа (k,n), где $n = m \cdot h$, $|C+e| = m$, $|e+C| = h$. В программе учтены необходимые условия для циклических полуколец, сформулированные в теореме 2. В таблице (рис.1) приведено количество полуколец $S = (a)$ с некоммутативным сложением для $n \leqslant 12$.

Найденные с помощью программы полукольца иллюстрируют существование циклических полуколец со сложением, отличным от сложения «намотка». «Первые» подобные полукольца $S = (a)$ с некоммутативным сложением имеют тип $(4,6)$. Их всего 2. Остальные 4 полукольца типа $(4,6)$ имеют сложение «намотка».

Теорема 2 дает необходимые условия существования циклических полуколец с неидемпотентным некоммутативным сложением и коротким хвостом.

Примеры показывают, что не любое сложение, заданное на циклической полугруппе по правилу, описанному в теореме 2, превращает его в полукольцо. «Первые» такие полугруппы имеют тип $(10,12)$. Существуют аналогичные полугруппы и большего порядка. Например, возьмем полугруппу $S=(a)$ типа $(70,88)$ и числа $m=8$, $h=11$. Зададим на S сложение по правилу $(1.I)$ из теоремы 2. Это сложение не ассоциативно.

5. Достаточные условия для сложения в конечных циклических полукольцах с неидемпотентным некоммутативным сложением и коротким хвостом

Покажем, что произвольную циклическую полугруппу можно превратить в полукольцо с неидемпотентным некоммутативным сложением.

Теорема 3. *Пусть дана циклическая полугруппа $S=(a)$ типа (k,n), $n\geqslant 2$. Тогда для любых натуральных чисел m, h и l, таких, что $m\cdot h=n$, $(m,h)=1$ и $nl\geqslant k>n(l-1)$, на S существует неидемпотентное некоммутативное сложение, определяемое равенствами:*

(а) $1+a^z=a^{mj_1+nl}$, *где z удовлетворяет* (7),

(б) $a^z+1=a^{hi_2+nl}$, *где z удовлетворяет* (8),

превращающее S в циклическое полукольцо.

Доказательство. Зададим операцию сложения $+$ на цикле $C=\{a^k,\dots,a^{k+n-1}\}$ по формуле $(\forall i_1,i_2,j_1,j_2\in\mathbb{N})$:

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

Непосредственно проверяется, что в C выполняются законы ассоциативности сложения и дистрибутивности умножения относительно сложения.

Определим сложение остальных элементов циклической полугруппы S по следующему правилу: $a^r+a^s=a^{r+nl}+a^{s+nl}$ для любых $r,s\in\mathbb{N}_0$.

Проверим ассоциативность такого сложения, учитывая ассоциативность сложения в C:

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

Проверим дистрибутивность умножения относительно сложения:

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

Для z, удовлетворяющего (7), выполняется:

$$1+a^z=a^{nl}+a^{hi_1+mj_1+nl}=a^{(nl+1)nl}+a^{(nl+1)(hi_1+mj_1+nl)}$$

$$=a^{(nl+1)(mj_1+nl)}=a^{mj_1+nl}.$$

Аналогично для z, удовлетворяющего (8), имеем:

$$a^z+1=a^{hi_2+nl}.\square$$

Сложение в S действительно определяется равенствами (а) и (б) из теоремы 3, поскольку суммы остальных элементов полукольца находятся по дистрибутивности.

Замечание 5. Если в условиях теоремы 3 полукольцо $S=(a)$ имеет тип $(k,1)$, то сложение, определяемое указанными в теореме равенствами, превращает S в полукольцо с коммутативным сложением, в котором $a^r+a^s=a^k$ для любых $r,s\in\mathbb{N}_0$.

Замечание 6. На циклической полугруппе $S=(a)$ типа (k,n), где $n\geqslant 2$ и $k\leqslant n$, кроме сложения «намотка», указанного в теореме 3, иногда можно ввести другое сложение. Пусть существует целое число $0<z<k$, удовлетворяющее (7) и $mj_1-hi_1\geqslant k$. Тогда сложение на S можно задать следующим образом: $1+a^z=a^{mj_1}$, остальные суммы элементов определяются как в теореме 3. Заметим, что, если $k\leqslant mj_1<n$, то $a^{mj_1}=a^{mj_1+n}$ и «новое» сложение совпадает со сложением из теоремы 3.

Теперь рассмотрим циклическую полугруппу с коротким хвостом. Зададим на ней сложение и выясним, при каких условиях заданное сложение превратит данную полугруппу в полукольцо.

Пусть $S=(a)$ — циклическая полугруппа типа (k,n), где $k\leqslant n$, m и h — произвольные натуральные числа такие, что $m\cdot h=n$, $(m,h)=1$. Для того, чтобы превратить полугруппу S в полукольцо, зададим на ней сложение по правилам (а) и (б) из теоремы 2, а для выполнения дистрибутивности умножения относительно сложения суммы остальных элементов полугруппы S определим по правилу (5)

Лемма 10. *В циклической полугруппе $S = (a)$ типа (k, n), где $k \leqslant n$, со сложением, последовательно заданным правилами* (а) *и* (б) *из теоремы* 2 *и правилом* (5), *для любых $r < k$, $s < k$ выполняется*

$$a^r + a^s = a^t, \text{ где } t > \max\{r, s\}.$$

Доказательство. Достаточно доказать, что для любого $z \in \mathbb{N}_0$:

$$1 + a^z = a^p, \text{ где } p > z,$$
$$a^z + 1 = a^q, \text{ где } q > z.$$

Докажем первое равенство. Пусть $z = hi + mj \in \mathbb{N}_0$, удовлетворяет (7) и $1 + a^z = a^p$. Если $p \geqslant k$, то, поскольку p можно сделать сколь угодно большим, добавляя к нему n, можно считать, что $p > z$. Пусть теперь $p < k$, тогда по правилу сложения (а) из теоремы 2 верно $p = mj < k$, $mj - hi \geqslant k$, откуда $hi < 0$, следовательно, $hi + mj < mj$, то есть $p > z$.

Второе равенство доказывается аналогично. □

Лемма 11. *В циклической полугруппе $S = (a)$ типа (k, n), где $k \leqslant n$, со сложением, последовательно заданным правилами* (а) *и* (б) *из теоремы* 2 *и правилом* (5), *для любых $r, s \in \mathbb{N}_0$ выполняется*

$$a^r + a^s = a^t, \quad \text{где} \quad t \equiv hi_1 + mj_2 \pmod n,$$

$r = hi_1 + mj_1$, $s = hi_2 + mj_2$.

Доказательство. По правилам сложения (а) и (б) из теоремы 2 для любого $z \in \mathbb{N}_0$ верно:

$$1 + a^z = a^p, \text{ где } p \equiv mj (\operatorname{mod} n),$$
$$a^z + 1 = a^q, \text{ где } q \equiv hi (\operatorname{mod} n),$$

откуда, используя дистрибутивность умножения (5), следует утверждение леммы. □

Лемма 12. *В циклической полугруппе $S = (a)$ типа (k, n), где $k \leqslant n$, со сложением, последовательно заданным правилами* (а) *и* (б) *из теоремы* 2 *и правилом* (5), *выполняется*

$$(a^r + 1) + a^s \in C \quad \text{или} \quad a^r + (1 + a^s) \in C,$$
$$1 + (a^r + a^s) \in C \quad \text{или} \quad (1 + a^r) + a^s \in C,$$
$$(a^r + a^s) + 1 \in C \quad \text{или} \quad a^r + (a^s + 1) \in C.$$

Доказательство. I. Рассмотрим суммы $(a^r+1)+a^s$ и $a^r+(1+a^s)$, где r и s имеют разложения (8) и (7) соответственно.

1. Если $a^r+1 \in C$ или $1+a^s \in C$, то по лемме 10 имеем $(a^r+1)+a^s \in C$ или $a^r+(1+a^s) \in C$.

2. Пусть $a^r+1 \notin C$ и $1+a^s \notin C$. Тогда $a^r+1 = a^{hi_1}$, $1+a^s = a^{mj_2}$. Учитывая правила (а) и (б) из теоремы 2 и лемму 10, получаем систему:

$$\begin{cases} 1 \leqslant r = hi_1 + mj_1 < k, \\ 1 \leqslant s = hi_2 + mj_2 < k, \\ 1 \leqslant hi_1 < k, \\ 1 \leqslant mj_2 < k, \\ hi_1 - mj_1 \geqslant k, \\ mj_2 - hi_2 \geqslant k. \end{cases} \tag{9}$$

Имеем $(a^r+1)+a^s = a^{hi_1} + a^{hi_2+mj_2}$.

а) Если $hi_1 = hi_2 + mj_2$, то $mj_2 \equiv 0 \pmod h$ и, учитывая четвертое неравенство системы (9), таких mj_2 не существует.

б) Если $hi_1 < hi_2 + mj_2$, то по правилу сложения (а) из теоремы 2 имеем:

$$a^{hi_1} + a^{hi_2+mj_2} = \begin{cases} a^{hi_1+mj_2+n}, \text{ если } mj_2 + hi_1 - hi_2 < k, \\ a^{hi_1+mj_2} \text{ или } a^{hi_1+mj_2+n}, \text{ в иных случаях.} \end{cases} \tag{10}$$

в) Если $hi_1 > hi_2 + mj_2$, то $hi_1 - hi_2 > mj_2 \geqslant 1$. Учитывая второе, третье и четвертое неравенства системы (9), выполняется:

$$1-k < 1-mj_2 \leqslant hi_2 < k - mj_2 \leqslant k-1,$$
$$-k+2 < hi_1 - hi_2 < 2k-1 \leqslant k+n-1.$$

Тогда

$$1 < hi_1 - hi_2 < k+n-1.$$

В случае $1 < hi_1 - hi_2 \leqslant n$ также получаем систему (10).

Пусть теперь $n < hi_1 - hi_2 < k+n-1$, откуда $0 < hi_1 - hi_2 - n < k-1$ и, учитывая неравенство $-mj_2+n > 0$, имеем $(hi_1-hi_2-n)-(-mj_2+n) < k$. Тогда по правилу сложения (б) из теоремы 2 получаем

$$a^{hi_1} + a^{hi_2+mj_2} = a^{hi_2+mj_2}(a^{(hi_1-hi_2-n)+(-mj_2+n)}+1) =$$
$$= a^{hi_2+mj_2} \cdot a^{hi_1-hi_2} = a^{hi_1+mj_2+n} \in C.$$

Заметим, что $hi_1 - hi_2 + mj_2 > n + mj_2 > k$.

Таким образом,

$$a^{hi_1} + a^{hi_2+mj_2} = \begin{cases} a^{hi_1+mj_2+n} \in C, \text{ если } hi_1 - hi_2 + mj_2 < k, \\ a^{hi_1+mj_2} \text{ или } a^{hi_1+mj_2+n} \in C, \text{ если } hi_1 - hi_2 + mj_2 \geqslant k. \end{cases}$$

Пусть $a^{hi_1} + a^{hi_2+mj_2} \notin C$. Тогда числа hi_1, mj_1, hi_2, mj_2 удовлетворяют системе:

$$\begin{cases} 1 \leqslant hi_1 < k, \\ 1 \leqslant mj_2 < k, \\ 1 \leqslant hi_1 + mj_1 < k, \\ 1 \leqslant hi_2 + mj_2 < k, \\ hi_1 - mj_1 \geqslant k, \\ mj_2 - hi_2 \geqslant k, \\ hi_1 - hi_2 + mj_2 \geqslant k, \\ hi_1 + mj_2 < k. \end{cases}$$

Обозначим числа: $f = hi_1$, $b = mj_1$, $c = hi_2$, $d = mj_2$.

Из третьего и пятого уравнений системы следует $1 - f \leqslant f - k$, $f \geqslant \frac{k+1}{2}$. Из четвертого и шестого — $1 - d \leqslant d - k$, откуда $d \geqslant \frac{k+1}{2}$. Тогда из последнего неравенства системы вытекает $\frac{k+1}{2} + \frac{k+1}{2} \leqslant f + d < k$, откуда $k + 1 < k$. Противоречие.

Таким образом, $(a^r + 1) + a^s \in C$. Аналогично $a^r + (1 + a^s) \in C$.

II. Рассмотрим суммы вида $(1 + a^r) + a^s$ и $1 + (a^r + a^s)$. Пусть $r = hi_1 + mj_1$ и $s = hi_2 + mj_2$ имеют разложения (7).

1. Если $1 + a^r \in C$ или $a^s \in C$ или $a^r + a^s \in C$, то по лемме 10 имеем $(1 + a^r) + a^s \in C$ или $1 + (a^r + a^s) \in C$.

Также, если $k \leqslant mj_2 \leqslant n$, то по лемме 11 выполняется $(1 + a^r) + a^s = 1 + (a^r + a^s) = a^{mj_2} \in C$.

2. Пусть $1 + a^r \notin C$, $a^s \notin C$, $a^r + a^s \notin C$, $1 \leqslant mj_2 < k$. Тогда $1 + a^r = a^{mj_1}$ и имеет место система

$$\begin{cases} 1 \leqslant r = hi_1 + mj_1 < k, \\ 1 \leqslant s = hi_2 + mj_2 < k, \\ 1 \leqslant mj_1 < k, \\ mj_1 - hi_1 \geqslant k. \end{cases}$$

Заметим, что

$$-k+1<1-mj_2\leqslant hi_2<k-mj_2\leqslant k-1,$$
$$-k+1<mj_2-mj_1<k-1.$$

Пусть $1+(a^r+a^s)\notin C$. Тогда возможны два случая: (a) $r<s$ и (b) $r>s$.

В случае (a) имеем $1+(a^r+a^s)=1+a^{hi_1+mj_1}(1+a^{(hi_2-hi_1)+(mj_2-mj_1)})$.

Если $mj_2-mj_1=0$, то по следствию 1 сумма $1+a^{(hi_2-hi_1)+(mj_2-mj_1)}$ лежит в цикле C и $1+(a^r+a^s)\in C$, противоречие.

Если $0<mj_2-mj_1<k-1$, то

$$1+a^{(hi_2-hi_1)+(mj_2-mj_1)}=a^{mj_2-mj_1}$$

(поскольку в другом случае $1+(a^r+a^s)\in C$), откуда по правилу сложения (a) из теоремы 2 верно

$$(mj_2-mj_1)-(hi_2-hi_1)\geqslant k.$$

С другой стороны, учитывая, что $hi_1\leqslant mj_1-k$ и $hi_2+k>0$, имеем:

$$(mj_2-mj_1)-(hi_2-hi_1)\leqslant(mj_2-mj_1)-hi_2+mj_1-k=mj_2-(hi_2+k)<k,$$

противоречие.

Если $-k+1<mj_2-mj_1<0$, то

$$1+a^{(hi_2-hi_1)+(mj_2-mj_1)}=a^{mj_2-mj_1+n},$$
$$1+(a^{hi_1+mj_1}+a^{hi_2+mj_2})=1+a^{hi_1+mj_2+n},$$

откуда по правилу сложения (a) из теоремы 2 выполняется

$$mj_2-(hi_1+n)\geqslant k.$$

С другой стороны, учитывая, что $hi_1+n>0$ и $mj_2<k$ имеем

$$mj_2-(hi_1+n)<k,$$

противоречие.

Случай (b) также приводит к противоречию.

Таким образом, $1+(a^r+a^s)\in C$.

Аналогично, выполняется $(a^r+a^s)+1\in C$ или $a^r+(a^s+1)\in C$. $\square$

Теорема 4. *В циклическом полукольце $S=(a)$ типа (k,n), где $k\leqslant n$, с неидемпотентным некоммутативным сложением сумма любых трех элементов лежит в цикле C.*

Доказательство. По лемме 12 и в силу ассоциативности сложения в полукольце S для любых $r, s \in \mathbb{N}_0$ выполняется

$$(1 + a^r) + a^s = 1 + (a^r + a^s) \in C,$$
$$a^r + (a^s + 1) = (a^r + a^s) + 1 \in C,$$
$$(a^r + 1) + a^s = a^r + (1 + a^s) \in C. \square$$

Теорема 5. *Пусть $S = (a)$ — циклическая полугруппа типа (k, n), где $k \leqslant n$, со сложением, последовательно заданным правилами* (а) *и* (б) *из теоремы* 2 *и правилом* (5). *Тогда для того, чтобы S было полукольцом, необходимо и достаточно выполнение следующих условий (для любых $r, s \in \mathbb{N}_0$):*

(а) $(a^r + 1 \in C, \quad 1 + a^s \notin C) \Rightarrow a^r + (1 + a^s) \in C,$
(б) $(a^r + 1 \notin C, \quad 1 + a^s \in C) \Rightarrow (a^r + 1) + a^s \in C,$
(в) $1 + a^r \in C \Rightarrow 1 + (a^r + a^s) \in C,$
(г) $1 + a^r \notin C \Rightarrow (1 + a^r) + a^s \in C,$
(д) $a^s + 1 \in C \Rightarrow (a^r + a^s) + 1 \in C,$
(е) $a^s + 1 \notin C \Rightarrow a^r + (a^s + 1) \in C.$

Доказательство. Доказательство следует из лемм 10, 11, 12 и теоремы 4. $\square$

Для полного описания полуколец с неидемпотентным некоммутативным сложением осталось только изучить такие полукольца с поглощающим элементом.

Автор выражает благодарность своему научному руководителю профессору Е.М. Вечтомову за постановку задачи и постоянное внимание к работе.

Литература

1. **Вечтомов Е. М.** Введение в полукольца. Киров: Изд-во ВятГГУ, 2000. 44 с.

2. **Вечтомов Е. М., Лубягина И. В.** Циклические полукольца с идемпотентным некоммутативным сложением // *Фундаментальная и прикладная математика. 2011/2012. Т. 17. Вып. 1. С. 33–52.*

3. **Бестужев А. С.** О строении конечных циклических полуколец // *Вестник ВятГГУ. Информатика. Математика. Язык. 2010. Вып. 6. С. 143–148.*

Summary

Orlova (Lubyagina) I. V. About finite cyclic semirings with non-idempotent non-commutative addition

In this paper finite cyclic semirings with non-idempotent non-commutative addition are reduced to such semirings with absorbing element and finite cyclic semifields (theorem 1). Finite cyclic semirings with non-idempotent non-commutative addition and short tail are studied. Theorems 2 and 4 give necessary conditions on the addition of the studied semirings, theorem 3 gives the sufficient condition on the addition of the cyclic multiplicative semigroup, turning it in the cyclic semiring with non-idempotent non-commutative addition. Theorem 5 is the criterion for recognizing of the fact whether the finite multiplicative cyclic semigroup with short tail and with defined on it addition semiring.

Keywords: semiring, semifield, cyclic semiring, nonidempotent addition, noncommutative addition.

Вятский государственный
гуманитарный университет

Поступила 25.09.2012