Циклические полукольца с неидемпотентным некоммутативным сложением*

Е. М. ВЕЧТОМОВ
Вятский государственный университет
e-mail: vecht@mail.ru

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

УДК 512.55

Ключевые слова: циклическое полукольцо, некоммутативное сложение, идемпотентное полукольцо, неидемпотентное полукольцо, конечное полуполе, идеал, конгруэнция.

Аннотация

В статье рассматривается строение циклических полуколец с неидемпотентным некоммутативным сложением. Также приведены некоторые общие результаты о циклических полукольцах с некоммутативным сложением.

Abstract

E. M. Vechtomov, I. V. Orlova, Cyclic semirings with nonidempotent noncommutative addition, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 6, pp. 17—41.

The article discusses the structure of cyclic semirings with nonidempotent noncommutative addition. Also here are some general results about cyclic semirings with noncommutative addition.

Введение

Данная работа является продолжением статьи [3] о циклических полукольцах с некоммутативным сложением. Напомним, что строение бесконечных циклических полуколец с коммутативным сложением известно [2]. Конечные циклические полукольца с коммутативным сложением изучал А. С. Бестужев [1]. В [3] дано описание циклических полуколец с идемпотентным некоммутативным сложением. В бесконечном случае сложение идемпотентно и является либо левым, либо правым. 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, являющемся циклическим полуполем.

*Работа выполнена в рамках проектной части госзадания Минобрнауки РФ № 1.1375.2014/К.

В разделе 1 приводятся основные понятия, связанные с циклическими полукольцами. В разделе 2 приводятся общие результаты о циклических полукольцах с некоммутативным сложением. В разделе 3 описываются некоторые свойства идемпотентных циклических полуколец, не вошедшие в [3]. В разделе 4 изучаются неидемпотентные циклические полукольца с некоммутативным сложением. В разделе 5 дано полное описание идеалов и конгруэнций циклических полуколец с некоммутативным сложением, а также приведены некоторые результаты по циклическим подполукольцам изучаемых полуколец.

1. Основные понятия

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*.

Полукольцо с тождеством $x + x = x$ называется *идемпотентным*, в противном случае *неидемпотентным*. В случае полукольца с единицей идемпотентность эквивалентна равенству $1 + 1 = 1$.

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 $S = (a)$.

Определение 4. Циклическую полугруппу

$$\{1, a, a^2, \ldots, a^k, \ldots, a^{k+n-1}\},$$

в которой $a^{k+n} = a^k$, где $k \in \mathbb{N}_0$, $n \in \mathbb{N}$ ($|S| = k + n \geqslant 2$), назовём *полугруппой типа* (k, n).

Определение 5. Полукольцо с мультипликативной циклической полугруппой типа (k, n) будем называть *полукольцом типа* (k, n).

Определение 6. Неидемпотентное полукольцо типа (k, n) с условием $1 + 1 = a^r$ для некоторого $r \in \mathbb{N}$ будем называть *полукольцом типа* (r, k, n).

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

Элемент x полукольца S с единицей 1 назовём *коммутирующим с единицей*, если $1 + x = x + 1$, и *не коммутирующим с единицей* в противном случае.

По предложениям 1 и 2 из [3] будем рассматривать только циклические полукольца без нуля.

2. Общие результаты о циклических полукольцах

При изучении циклических полуколец необходимо выяснить, как складываются элементы мультипликативно циклической полугруппы данного полукольца. Важно найти элементы циклического полукольца, коммутирующие с единицей, и элементы, не коммутирующие с единицей. Рассмотрим сначала циклические полутела.

Лемма 1. *Все элементы конечного полутела, кроме* 1*, являются не коммутирующими* с 1.

Доказательство. Пусть C — конечное полутело. По [3, теорема A] любое конечное полутело C изоморфно $(C+1)\times(1+C) = C'$. Пусть (x, y), где $x \in C+1$, $y \in 1+C$ — коммутирующий с 1 элемент полутела C'. По [3, лемма 6] сложение в $C+1$ левое, а в $1+C$ — правое. Тогда $(x, y)+(1, 1) = (1, 1)+(x, y)$, $x+1 = 1+x$, $y + 1 = 1 + y$, откуда следует, что $x = 1$ и $y = 1$. □

Следствие 1. *Конечное полутело с коммутативным сложением тривиально.*

Из леммы 1 вытекает следующее утверждение.

Предложение 1. *Все элементы конечного циклического полуполя, кроме* 1*, являются не коммутирующими* с 1.

Приведём правило сложения в конечном циклическом полуполе в более общем виде, чем в [3].

Предложение 2. *В конечном циклическом полуполе* $C = (c)$ *для любых* $r, s \in \mathbb{N}_0$

$$c^r + c^s = c^t, \quad \text{где} \quad t \equiv hi_1 + mj_2 \pmod{n}, \quad r = hi_1 + mj_1, \quad s = hi_2 + mj_2,$$
$$m = |C + 1|, \quad h = |1 + C|, \quad (1)$$

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

Доказательство. Достаточно заметить, что $c^r = c^{r+ni}$ и $c^s = c^{s+nj}$ для любых $r, s, i, j \in \mathbb{N}_0$, и воспользоваться [3, предложение 3]. □

Перейдём к рассмотрению циклических полуколец.

Лемма 2. *Сложение в конечном циклическом полукольце* $S = (a)$ *типа* (k, n)*, где* $n \geqslant 2$*, некоммутативно.*

Доказательство. Утверждение следует из [3, теорема 2] и следствия 1. □

Правило сложение в циклическом полукольце выводится из правила сложения в его цикле, являющемся по [3, теорема 2] циклическим полутелом.

Лемма 3. *В конечном циклическом полукольце $S = (a)$ типа (k, n) с циклом C, $n \geqslant 2$, для любых $r, s \in \mathbb{N}_0$*

$$a^r + a^s = a^t, \quad \text{где} \quad t \equiv hi_1 + mj_2 \pmod{n}, \quad r = hi_1 + mj_1, \quad s = hi_2 + mj_2,$$
$$m = |C + e|, \quad h = |e + C|, \quad e\,\text{— единица цикла } C, \tag{2}$$

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

Доказательство. По [3, теорема 2] цикл C полукольца S является циклическим полуполем с образующим a^{nl+1} и единицей $e = a^{nl}$ для некоторого $l \in \mathbb{N}_0$, такого что $nl \geqslant k > n(l-1)$. По предложению 2

$$a^{nl}(a^{hi_1+mj_1} + a^{hi_2+mj_2}) = a^{(nl+1)(hi_1+mj_1)} + a^{(nl+1)(hi_2+mj_2)} = a^{(nl+1)t'},$$

где $t' \equiv hi_1 + mj_2 \pmod{n}$, откуда получаем утверждение леммы. □

Замечание 1. Элемент c^t циклического полуполя в условиях предложения 2 определён однозначно, а элемент a^t циклического полукольца в условиях леммы 3 может принимать разные значения.

Предложение 3. *Пусть в циклическом полукольце $S = (a)$ типа (k, n), $n \geqslant 2$, сложение не левое и не правое. Тогда все коммутирующие с 1 элементы полукольца S имеют вид a^s, где $s \equiv 0 \pmod{n}$.*

Доказательство. Пусть a^s, где $s = hi + mj$ — коммутирующий с 1 элемент полукольца S. Тогда по лемме 3

$$1 + a^s = a^t, \quad \text{где} \quad t \equiv mj \pmod{n},$$
$$a^s + 1 = a^q, \quad \text{где} \quad q \equiv hi \pmod{n},$$

откуда следует, что $a^t = 1 + a^s = a^s + 1 = a^q$, $mj \equiv hi \pmod{n}$. Тогда $mj \equiv 0 \pmod{h}$ и $hi \equiv 0 \pmod{m}$. Учитывая, что $(m, h) = 1$, имеем $j \equiv 0 \pmod{h}$, $mj \equiv 0 \pmod{n}$, $i \equiv 0 \pmod{m}$, $hi \equiv 0 \pmod{n}$. Таким образом, $s = hi + mj \equiv 0 \pmod{n}$. □

Дополним лемму 7 из [3] эквивалентным условием.

Лемма 4. *В конечном циклическом полукольце $S = (a) \neq C$ типа (k, n) с некоммутативным сложением 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*;
5) *сложение в S левое (правое).*

Доказательство. Докажем импликацию 1) $\Longrightarrow$ 2). По [3, лемма 2] из того, что $1+a^s=1$ для некоторого $s\in\mathbb{N}$, вытекает, что $1+a^{si}=1$ для любого $i\in\mathbb{N}$, в частности, для $i=nl$ имеем $1+a^{s(nl)}=1+a^{nl}=1$.

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

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

Используя соотношения (2) из [3], для любого $j\in\mathbb{N}$ получаем, что

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

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 $t\leqslant nl$ следует, что $a^t(1+a^{nl-t})=1$, следовательно, $a^q=1$ для некоторого $q\geqslant t>0$, откуда выводим, что S — полутело. Из $t\geqslant nl$ также вытекает, что S — полутело.)

Учитывая [3, 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 $i,j\in\mathbb{N}$

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

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) $\Longrightarrow$ 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 вытекает, что $1+a=1$. По [3, лемма 2] имеем, что $1+a^i=1$ для любого $i\in\mathbb{N}$.

Докажем импликацию 4) $\Longrightarrow$ 5). Пусть $1+1=a^r$, где $r>0$. Тогда $a^r+1=1+a^r=1$ и по доказанному выше для любого $i\in\mathbb{N}$ выполняется $a^i+1=1=1+a^i$; сложение в S коммутативно; противоречие. Таким образом, $1+1=1$.

Пусть $a+1=a^q$, $q\geqslant 0$. Если $q=0$, т. е. $a+1=1$, то по доказанному выше имеем, что $a^i+1=1$ 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 $q\geqslant 1$. 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 $r\leqslant s$, то $a^r+a^s=a^r(1+a^{s-r})=a^r$. Если $r\geqslant s$, то $a^r+a^s=a^s(a^{r-s}+1)=a^s\cdot a^{r-s}=a^r$. Значит, сложение в S левое.

Импликация 5) $\Longrightarrow$ 1) очевидна.

Аналогично получается эквивалентность утверждений в скобках. □

Лемма 5. *В конечном циклическом полукольце $S=(a)\neq C$ типа (k,n) с некоммутативным сложением (не левым и не правым) для любых $s,t\in\mathbb{N}_0$ выполняется*

$$a^s+a^t=a^q,\quad \text{где}\quad q\geqslant\max\{s,t\}. \tag{3}$$

Доказательство. В случае $s=t=0$ утверждение леммы верно.

Рассмотрим случай $s=0$ и $0\neq t<k$. Домножая равенство $1+a^t=a^q$ на a^{k-t}, получаем, что $a^{k-t}+a^k=a^{k+q-t}$. По [3, предложение 4, леммы 4, 9] имеем, что $a^{k-t}+a^k\in C$, откуда следует, что $q\geqslant t$. Таким образом, $q\geqslant\max\{s,t\}$.

Аналогично проверяется, что утверждение верно для $s\neq 0$ и $t=0$.

Пусть $0\neq s<k$ и $0\neq t<k$. Тогда, учитывая вышеприведённые доказательства, получаем, что в случае $s\leqslant t$ верно $a^s+a^t=a^s(1+a^{t-s})=a^q$, где $q\geqslant\max\{s,t\}$; в случае $s>t$ выполняется $a^s+a^t=a^t(a^{s-t}+1)=a^q$, где $q\geqslant\max\{s,t\}$.

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

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

На конечном циклическом полукольце $S\neq C$ с некоммутативным сложением зададим бинарное отношение $\sim$ формулой

$$x\sim y\iff x,y\in C\quad\text{или}\quad x=y. \tag{4}$$

Лемма 6. *Отношение $\sim$ является конгруэнцией.*

Доказательство. По [3, предложение 4] в полукольце S возможны три случая. По лемме 4 в первом случае имеем левое сложение в S, во втором — правое сложение в S. Утверждение леммы в этих случаях очевидно.

В третьем случае достаточно воспользоваться леммой 9 из [3]. □

Отношение $\sim$ «склеивает» элементы цикла C в один класс, а каждый из оставшихся элементов полукольца S образует одноэлементный класс. Фактор-полукольцо $S/{\sim}$ также является конечным циклическим полукольцом, но с поглощающим элементом $[a^k]_\sim$.

3. Идемпотентные циклические полукольца

В [3] выяснялось строение идемпотентных циклических полуколец с некоммутативным сложением. По [3, теорема 1] в бесконечном случае сложение всегда идемпотентно и является либо левым, либо правым. Поэтому верно утверждение: все элементы бесконечного циклического полукольца с некоммутативным сложением, кроме 1, являются не коммутирующими с 1.

По [3, теорема 3] всякое конечное идемпотентное циклическое полукольцо с некоммутативным сложением и поглощающим элементом имеет либо левое сложение, либо правое сложение. Отсюда следует, что все элементы конечного идемпотентного циклического полукольца с некоммутативным сложением и поглощающим элементом, кроме 1, являются не коммутирующими с 1.

По [3, теоремы 4, 5] в конечном аддитивно идемпотентном циклическом полукольце с циклом сложение сводится к сложению в циклическом подполукольце с коммутативным сложением и поглощающим элементом по умножению и сложению в цикле, являющемся циклическим полуполем.

Лемма 7. *Пусть в конечном идемпотентном циклическом полукольце $S = (a)$ типа (k, n), $n \geqslant 2$, сложение не левое и не правое. Тогда элементы полукольца S вида a^s, где $s \equiv 0 \pmod{n}$, и только они являются коммутирующими с 1.*

Доказательство. По предложению 3 все коммутирующие с 1 элементы имеют вид a^s, где $s \equiv 0 \pmod{n}$.

По [3, теорема 4] множество $T = \{1, a^n, a^{2n}, \ldots, a^{nl}\}$ для такого натурального l, что $n(l-1) < k \leqslant nl$, является циклическим подполукольцом в полукольце S, имеющим коммутативное сложение. Поэтому любой элемент вида a^s, где $s \equiv 0 \pmod{n}$, является коммутирующим с 1. □

Рассмотрим отношение ρ, заданное на идемпотентной аддитивной полугруппе $\langle S, +\rangle$ идемпотентного циклического полукольца $S = (a)$ с некоммутативным сложением следующим образом:

$$x \,\rho\, y \iff (x + y + x = x \quad \text{и} \quad y + x + y = y).$$

Отношение ρ является конгруэнцией [4].

Предложение 4. *Конгруэнция ρ, заданная на конечном идемпотентном циклическом полукольце S с некоммутативным сложением, в случае левого (правого) сложения в S «склеивает» все элементы полукольца S в один класс, в остальных случаях сложения «склеивает» элементы цикла C в один класс, а каждый из остальных элементов полукольца S образует одноэлементный класс.*

Доказательство. Пусть $S = (a)$ — идемпотентное циклическое полукольцо типа (k, n) с некоммутативным сложением и циклом C.

Если сложение в S левое (правое), то для любых элементов $x, y \in S$ выполняется $x + y + x = x$ и $y + x + y = y$, поэтому $x \,\rho\, y$.

Пусть сложение в S не левое и не правое. По [3, теорема 2, лемма 5] для любых элементов $x, y \in C$ верно $x \ \rho \ y$. Следовательно, конгруэнция ρ «склеивает» элементы цикла C в один класс.

Пусть для некоторых $x = a^r$ и $y = a^s$ выполняется $x \ \rho \ y$ и $x \notin C$. Тогда $r < k$ и $a^r + a^s + a^r = a^r$. Для определённости положим, что $r < s$. Обозначим $a^r + a^s = a^t$. Тогда $a^r(1 + a^{s-r}) = a^t$. Если $t = r$, то $1 + a^{s-r} = 1$, и по лемме 4 сложение в S левое; противоречие. В случае $t > r$ имеем, что $a^t + a^r = a^r(a^{t-r} + 1) = a^r$, откуда следует, что $a^{t-r} + 1 = 1$, и по лемме 4 сложение в S правое; противоречие. В случае $t < r$ получаем, что S — полуполе.

Случай $r > s$ также приводит к противоречиям.

Следовательно, $r = s$ и каждый из элементов хвоста полукольца S образует одноэлементный класс. □

4. Неидемпотентные циклические полукольца

Лемма 8. *В неидемпотентном циклическом полукольце $S = (a)$ типа (k, n) с некоммутативным сложением выполняется $1 + 1 = a^{ni}$ для некоторого натурального числа i, такого что $ni \geqslant 2$. В частности, если $k \leqslant n$ (короткий хвост), то $1 + 1 = a^n \in C$.*

Доказательство. По [3, теорема 2, лемма 4] $a^{nl} + a^{nl} = a^{nl}$, где $nl \geqslant k > n(l-1)$. Тогда $a^{nl}(1+1) = a^{nl}$, откуда следует, что $1+1 = a^{ni}$ для некоторого натурального i.

Пусть $ni = 1$, т. е. $1+1 = a$. Тогда для любого натурального j $a^j = (1+1)^j = \underbrace{1 + \ldots + 1}_{2^j}$, поэтому $1 + a^j = \underbrace{1 + \ldots + 1}_{2^j+1} = a^j + 1$, т. е. сложение в S коммутативно; противоречие. Следовательно, $ni \geqslant 2$. □

Лемма 9. *В неидемпотентном циклическом полукольце $S = (a)$ типа (k, n) с некоммутативным сложением выполняется $1 + a^{nl} = a^{nl} + 1 = a^{nl}$, где $nl \geqslant k > n(l-1)$.*

Доказательство. По [3, предложение 4] возможны три случая. В первом случае ($1 + a^{nl} = 1$) по лемме 4 имеем левое сложение в S, что невозможно из-за неидемпотентности сложения в S. Во втором случае ($a^{nl} + 1 = 1$) имеем правое сложение, что также невозможно. Следовательно, $1 + a^{nl} = a^{nl} + 1 = a^{nl}$. □

Лемма 10. *В неидемпотентном циклическом полукольце $S = (a)$ типа (k, n) с некоммутативным сложением*

$$\text{для любых } x, y \in S \text{ если } x \in C \text{ или } y \in C, \text{ то } x + y,\ y + x \in C.$$

Доказательство. Утверждение вытекает из леммы 9 и [3, лемма 9]. □

Лемма 11. *В неидемпотентном циклическом полукольце $S = (a) \neq C$ типа (k, n) с некоммутативным сложением для любых $r, s \in \mathbb{N}_0$*

$$a^r + a^s = a^t, \quad \text{где} \quad t > \max\{r, s\}. \tag{5}$$

Доказательство. Учитывая лемму 5, достаточно доказать, что равенство $t = \max\{r, s\}$ не выполняется ни для каких $r, s \in \mathbb{N}_0$.

При $r = 0$ и $s = 0$ по лемме 8 имеем $t \geqslant 2$. Таким образом, $t \neq \max\{r, s\}$.

Рассмотрим случай, когда $r = 0$ и $0 \neq s < k$. Пусть s — наименьшее натуральное число, такое что $1 + a^s = a^s$. Добавляя слева к последнему равенству элемент 1 и используя лемму 8, получаем, что $a^{ni} + a^s = a^s$ для некоторого натурального i, такого что $ni \geqslant 2$. В случае $ni = s$ получаем противоречие с неидемпотентностью сложения. Если $ni < s$, то $a^{ni}(1 + a^{s-ni}) = a^s$, откуда следует, что $1 + a^{s-ni} = a^{s-ni}$, и получаем противоречие с тем, что s — наименьшее число с таким свойством. Если $ni > s$, то $a^s(a^{ni-s} + 1) = a^s$, откуда следует, что $a^{ni-s} + 1 = 1$, и по лемме 4 сложение в S правое; противоречие с неидемпотентностью сложения в S. Следовательно, $1 + a^s \neq a^s$ для любого $s < k$, т. е. $t \neq \max\{r, s\}$.

Таким образом, для $r = 0$ и $0 \neq s < k$ 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 вышеприведённые доказательства, в случае $r \leqslant s$ получаем, что $a^r + a^s = a^r(1 + a^{s-r}) = a^t$, 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 $t > \max\{r, s\}$.

Утверждение леммы верно и в случае, когда $r \geqslant k$ или $s \geqslant k$. Действительно, по лемме 10 $t \geqslant k$. 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 12. *В циклической полугруппе $S = (a)$ типа (k, n) со сложением, заданным правилами (2) и (5) и удовлетворяющим правилу (для любых r и s, $0 \leqslant r \leqslant k + n - 1$, $0 \leqslant s \leqslant k + n - 1$)*

$$a^r + a^s = \begin{cases} a^r(1 + a^{s-r}) & \text{при } r \leqslant s, \\ a^s(a^{r-s} + 1) & \text{иначе,} \end{cases} \tag{6}$$

умножение дистрибутивно относительно сложения.

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

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

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 (2) $p \equiv q \pmod{n}$. Пусть $s \leqslant t$.

Если $r + t \leqslant k + n - 1$, то $r + s \leqslant r + t \leqslant k + n - 1$. Тогда равенство $a^r(a^s + a^t) = a^{r+s}(1 + a^{t-s}) = a^{r+s} + a^{r+t}$ вытекает из правила сложения (6).

В случае $r + t > k + n - 1$ по правилу (5) верно $p > r + t > k + n - 1$, и $a^p \in C$. Элемент a^q принадлежит C также по правилу (5). Таким образом, $a^p = a^q$.

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

Лемма 13. *В циклической полугруппе $S = (a)$ типа (k, n) со сложением, заданным правилами* (2) *и* (5)

$$\text{если } r \geqslant k, \text{ или } s \geqslant k, \text{ или } t \geqslant k, \text{ то } (a^r + a^s) + a^t = a^r + (a^s + a^t).$$

Рассмотрим введённое формулой (4) бинарное отношение $\sim$, которое по лемме 6 является конгруэнцией.

Фактор-полукольцо $S/\sim$ является неидемпотентным циклическим полукольцом с некоммутативным сложением и поглощающим элементом $[a^k]_\sim$.

Выясним условия, при которых из неидемпотентного циклического полукольца $S' = (a)$ с некоммутативным сложением и поглощающим элементом a^k и циклического полуполя C' порядка n можно построить неидемпотентное циклическое полукольцо S типа (k, n) с 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 неидемпотентное циклическое полукольцо $S' = \{1, a, a^2, \ldots, a^k\}$ с некоммутативным сложением и поглощающим элементом a^k, некоторое циклическое полуполе $C' = \{e = c^n, c, c^2, \ldots, c^{n-1}\}$ порядка n, где $|C' + e| = m$, $|e + C'| = h$. Циклическое полукольцо $S = (a)$ типа (k, n), фактор-полукольцо которого по конгруэнции $\sim$ совпадает с полукольцом S', т. е. $S/\sim = S'$, а цикл C полукольца S изоморфен полуполю C', т. е. $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$, существует тогда и только тогда, когда в S' для любых $r, s \in \mathbb{N}_0$ выполняется условие*

$$\begin{aligned} a^r + a^s = a^t, \quad \text{где} \quad & t \equiv hi_1 + mj_2 \pmod{n}, \\ & t > \max\{r, s\}, \quad r = hi_1 + mj_1, \quad s = hi_2 + mj_2. \end{aligned} \tag{7}$$

Доказательство. Пусть $S = (a)$ — неидемпотентное циклическое полукольцо типа (k, n) с некоммутативным сложением, в котором $S/\sim = S'$ и $\langle C, +, \cdot\rangle \cong \langle C', +, \cdot\rangle$. По леммам 3 и 11 сложение в S удовлетворяет условию (7). Из $S/\sim = S'$ следует, что условие (7) выполняется и в S'.

Проведём доказательство в обратную сторону. Пусть в S' выполняется условие (7). Построим неидемпотентное циклическое полукольцо типа (k, n) с 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 ($z = hi + mj$)

$$\begin{aligned} 1 + a^z = a^p, &\quad \text{где } p \equiv mj \pmod{n}, \ p > z, \\ a^z + 1 = a^q, &\quad \text{где } q \equiv hi \pmod{n}, \ q > z. \end{aligned}$$

Суммы остальных элементов полугруппы S зададим по правилу (6). С учётом введённого на S сложения условие (7) в S выполняется.

По лемме 12 умножение дистрибутивно относительно сложения.

Докажем ассоциативность сложения в S, т. е. что 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 (7) имеем $p \equiv q \pmod{n}$.

Если $r \geqslant k$, или $s \geqslant k$, или $t \geqslant k$, то по лемме 13 имеем $a^p = a^q$.

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

Если $(a^r + a^s) + a^t \in C$ в S, то $(a^r + a^s) + a^t = a^k$ в S'. По ассоциативности сложения в S' выполняется $a^r + (a^s + a^t) = (a^r + a^s) + a^t = a^k$, следовательно, $a^r + (a^s + a^t) \in C$ в S и верно, что $(a^r + a^s) + a^t = a^r + (a^s + a^t)$ в S.

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

Установим изоморфизм мультипликативных полугрупп:

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

Учитывая правило сложения (1) в полуполе C' и условие (7) 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 2. Из лемм 3 и 11 следует, что полукольцо S из теоремы 1 единственно (если оно существует).

Предложение 5. *Хвост T полукольца S из теоремы 1 совпадает с $S' \setminus \{a^k\}$, т. е. $\langle T, +, \cdot\rangle = \langle S' \setminus \{a^k\}, +, \cdot\rangle$, 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 $|C'| \neq 1$. По идемпотентности сложения в цикле C полукольца S имеем, что $a^k + a^k = a^k$, откуда, учитывая неидемпотентность сложения в S, получаем, что $a^{k-1} + a^{k-1} = a^{k+n-1}$. Отсюда, принимая во внимание, что $a^k \neq a^{k+n-1}$, выводим, что $\langle T, +\rangle \neq \langle S' \setminus \{a^k\}, +\rangle$. Таким образом, $\langle T, +, \cdot\rangle \neq \langle S' \setminus \{a^k\}, +, \cdot\rangle$. □

Лемма 14. *Если u и v — коммутирующие с 1 элементы полукольца S, то $u + v$, $u + v + uv = u + uv + v = uv + u + v$ также являются коммутирующими с 1 элементами полукольца.*

Доказательство. Имеем

$$1 + (u + v) = u + 1 + v = (u + v) + 1,$$
$$(1 + u)(1 + v) = 1 + (u + v + uv),$$

$$(u+1)(v+1) = uv + u + v + 1 = u(v+1) + v + 1 = u(1+v) + v + 1 = \\ = u + (u+1)v + 1 = u + (1+u)v + 1 = (u+v+uv) + 1,$$

откуда следует, что

$$1 + (u+v+uv) = (1+u)(1+v) = (u+1)(v+1) = (u+v+uv) + 1,$$

и элемент $u+v+uv$ является коммутирующим с 1. Также верно, что

$$u + v + uv = u + (1+u)v = u + (u+1)v = u + uv + v = u(1+v) + v = \\ = u(v+1) + v = uv + u + v. \quad \square$$

Лемма 15. *Если a^s — коммутирующий с 1 элемент неидемпотентного циклического полукольца $S = (a)$ типа (r, k, n), то a^t, где $t \equiv s \,(\mathrm{mod}\, r)$, $t > s$, также является коммутирующим с 1 элементом.*

Доказательство. Достаточно воспользоваться тем, что $t = s + ir$ для некоторого $i \in \mathbb{N}$,

$$a^{ir} = (1+1)^i = \underbrace{1 + 1 + \ldots + 1}_{2^i}, \quad a^{s+ir} = \underbrace{a^s + a^s + \ldots + a^s}_{2^i},$$

и леммой 14. $\square$

Лемма 16. *Элемент a^r неидемпотентного циклического полукольца $S = (a)$ типа (r, k, n) является коммутирующими с 1.*

Доказательство. Действительно, $1 + a^r = 1 + 1 + 1 = a^r + 1$. $\square$

Лемма 17. *В неидемпотентном циклическом полукольце $S = (a)$ типа (r, k, n) с некоммутативным сложением существует не коммутирующий с 1 элемент a^s, такой что $s < r$.*

Доказательство. Элемент a^r является коммутирующим с 1 по лемме 16. Пусть все элементы вида a^s, где $s < r$, также являются коммутирующими с 1. Тогда любой элемент a^t, где $t > r$, является коммутирующим с 1. Действительно, всегда существует $s \leqslant r$ и $s \equiv t \,(\mathrm{mod}\, r)$, такой что a^s — коммутирующий с 1 элемент полукольца S. Тогда по лемме 15 элемент a^t также является коммутирующим с 1. Получаем, что все элементы полукольца S являются коммутирующими с 1 и сложение в S коммутативно. Противоречие. $\square$

Далее рассмотрим неидемпотентные циклические полукольца с коротким хвостом.

Задача заключается в нахождении правила сложения в неидемпотентных циклических полукольцах S типа (k, n) с некоммутативным сложением и коротким хвостом. По лемме 8 такие полукольца являются полукольцами типа (n, k, n).

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

$$z = hi_1 + mj_1, \quad \text{где } 1 \leqslant mj_1 \leqslant n, \tag{8}$$

$$z = hi_2 + mj_2, \quad \text{где } 1 \leqslant hi_2 \leqslant n, \tag{9}$$

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 неидемпотентное циклическое 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 следующие равенства:*

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

где z удовлетворяет (8);

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

где z удовлетворяет (9).

Доказательство. Пусть $z = hi_1 + mj_1 \in \mathbb{N}_0$ удовлетворяет (8). Отметим, что $1 + a^z \neq 1$ ни для какого z по лемме 11. Тогда по лемме 3 верно, что $1 + a^z = a^{mj_1}$ или $1 + a^z = a^{mj_1+n}$. Если $k \leqslant mj_1 \leqslant n$, то $1 + a^z = a^{mj_1} = a^{mj_1+n}$.

Возможны следующие случаи.

1. Если $z = 0$, то $mj_1 \equiv 0 \pmod h$, откуда следует, что $j_1 \equiv 0 \pmod h$, $mj_1 \equiv 0 \pmod n$, $mj_1 = n \geqslant k$. Этот случай рассмотрен выше.

2. Пусть $z \geqslant k$. Тогда, учитывая лемму 10, получаем, что $1 + a^z = a^{mj_1+n}$.

Так как $z = hi_1 + mj_1 \geqslant k$, в случае $mj_1 - hi_1 \geqslant k$ верно, что $mj_1 \geqslant k$ 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 3 и 10

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

откуда, учитывая, что $a^{k-hi_1-mj_1} + a^k \in C$ (по лемме 10), получаем, что

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

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 3 и 11 $a^{-hi_1} + 1 = a^{-hi_1+n} \in C$, по лемме 10 $(a^{-hi_1} + 1) + a^{hi_1+mj_1} \in C$. Тогда

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

противоречие.

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

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

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

Следствие 3. *Если в условиях теоремы 2 $m = 1$ или $h = 1$, то сложение в полукольце S сводится к сложению в цикле C следующим образом*:

$$a^r + a^s = a^{r_1} + a^{s_1}, \tag{10}$$

где $r_1 \geqslant k$, $s_1 \geqslant k$, $r_1 \equiv r \pmod{n}$, $s_1 \equiv s \pmod{n}$.

Сложение в циклическом полукольце $S = (a)$ типа (k, n), определяемое равенством (10), назовём *сложением «намотка»*.

Предложение 6. *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 неидемпотентных полукольца $S = (a)$ типа (k, n) с некоммутативным сложением. По следствию 3 это сложение является «намоткой».*

Замечание 3. Для нахождения неидемпотентных циклических полуколец с 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 следующей таблице приведено количество полуколец $S = (a)$ с некоммутативным сложением для $n \leqslant 12$.

(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

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 два. Остальные четыре полукольца типа $(4, 6)$ имеют сложение «намотка».

Теорема 2 даёт необходимые условия существования неидемпотентных циклических полуколец с 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.

Пример 1. Возьмём полугруппу $S = (a)$ типа $(70, 88)$ и числа $m = 8$, $h = 11$. Зададим на S сложение по правилу а) (I) из теоремы 2 так, что

$$1 + a^4 = 1 + a^{11\cdot(-4)+8\cdot 6} = a^{48}, \quad 1 + a^{53} = 1 + a^{11\cdot(-1)+8\cdot 8} = a^{64}.$$

Это сложение не ассоциативно, так как, например, $(1 + a^5) + a^9 \neq 1 + (a^5 + a^9)$. Действительно,

$$\begin{aligned}(1 + a^5) + a^9 &= \bigl(1 + a^{11\cdot(-1)+8\cdot 2}\bigr) + a^{11\cdot(-5)+8\cdot 8} = \\ &= a^{8\cdot 2+8\cdot 11} + a^{11\cdot(-5)+8\cdot 8} = a^{8\cdot 8+8\cdot 11} = a^{152} \in C, \\ 1 + (a^5 + a^9) &= 1 + \bigl(a^{11\cdot(-1)+8\cdot 2} + a^{11\cdot(-5)+8\cdot 8}\bigr) = \\ &= 1 + a^{11\cdot(-1)+8\cdot 2}\bigl(1 + a^{11\cdot(-4)+8\cdot 6}\bigr) = \\ &= 1 + a^{11\cdot(-1)+8\cdot 2}\cdot a^{8\cdot 6} = 1 + a^{11\cdot(-1)+8\cdot 8} = a^{64} \notin C.\end{aligned}$$

Достаточные условия для сложения в неидемпотентных циклических полукольцах с 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*

$$\begin{aligned}&\text{а)}\quad 1 + a^z = a^{mj_1+nl}, \quad \text{где } z \text{ удовлетворяет (8)},\\ &\text{б)}\quad a^z + 1 = a^{hi_2+nl}, \quad \text{где } z \text{ удовлетворяет (9)},\end{aligned}$$

превращающее S в циклическое полукольцо.

Доказательство. Зададим операцию сложения $+$ на цикле

$$C = \{a^k, \ldots, a^{k+n-1}\}$$

по формуле

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

для любых $i_1, i_2, j_1, j_2 \in \mathbb{N}$.

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 (8), 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 (9), имеем $a^z + 1 = a^{hi_2+nl}$. □

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

Замечание 4. Если в условиях теоремы 3 полугруппа $S = (a)$ 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 5. 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 (8), 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 (6).

Лемма 18. *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* (6), *для любых $r,s \in \mathbb{N}_0$*

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

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

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

Докажем первое равенство. Пусть $z = hi + mj \in \mathbb{N}_0$ удовлетворяет (8) 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 $p = mj < k$, $mj - hi \geqslant k$, поэтому $hi < 0$, следовательно, $hi + mj < mj$, т. е. $p > z$.

Второе равенство доказывается аналогично. □

Лемма 19. *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* (6), *для любых $r,s \in \mathbb{N}_0$*

$$a^r + a^s = a^t, \quad \text{где} \quad t \equiv hi_1 + mj_2 \pmod n, \quad r = hi_1 + mj_1, \quad s = hi_2 + mj_2.$$

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

$$1 + a^z = a^p, \quad \text{где } p \equiv mj \pmod n,$$
$$a^z + 1 = a^q, \quad \text{где } q \equiv hi \pmod n,$$

откуда, используя дистрибутивность умножения (6), выводим утверждение леммы. □

Лемма 20. *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* (6), *выполняются следующие соотношения*:

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

Доказательство. I. Рассмотрим суммы $(a^r + 1) + a^s$ и $a^r + (1 + a^s)$, где r и s имеют разложения (9) и (8) соответственно.

Если $a^r + 1 \in C$ или $1 + a^s \in C$, то по лемме 18 $(a^r + 1) + a^s \in C$ или $a^r + (1 + a^s) \in C$.

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 18, получаем систему

$$\begin{cases} 1\leqslant hi_1+mj_1<k,\\ 1\leqslant hi_2+mj_2<k,\\ 1\leqslant hi_1<k,\\ 1\leqslant mj_2<k,\\ hi_1-mj_1\geqslant k,\\ mj_2-hi_2\geqslant k. \end{cases} \tag{11}$$

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

а) Если $hi_1=hi_2+mj_2$, то $mj_2\equiv 0\,(\mathrm{mod}\,h)$. Учитывая четвёртое неравенство системы (11), приходим к выводу, что таких mj_2 не существует.

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

$$a^{hi_1}+a^{hi_2+mj_2}=\begin{cases} a^{hi_1+mj_2+n}, & \text{если } \ mj_2+hi_1-hi_2<k,\\ a^{hi_1+mj_2} \ \text{ или } \ a^{hi_1+mj_2+n} & \text{в иных случаях.} \end{cases} \tag{12}$$

в) Если $hi_1>hi_2+mj_2$, то

$$hi_1-hi_2>mj_2\geqslant 1. \tag{13}$$

Учитывая второе, третье и четвёртое неравенства системы (11), получаем, что

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

откуда, принимая во внимание неравенство (13), выводим, что

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

В случае $1<hi_1-hi_2\leqslant n$ также получаем систему (12).

Пусть теперь $n<hi_1-hi_2<k+n-1$. Тогда $0<hi_1-hi_2-n<k-1$. Учитывая четвёртое неравенство системы 11 ($mj_2<k\leqslant n$), получаем, что $(hi_1-hi_2-n)-(-mj_2+n)<k$. Тогда по правилу сложения б) из теоремы 2

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

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

Обобщая случаи б) и в), имеем

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

Пусть $(a^r+1)+a^s=a^{hi_1}+a^{hi_2+mj_2}\notin C$. Обозначим $f=hi_1$, $b=mj_1$, $c=hi_2$, $d=mj_2$. Тогда числа f, b, c, d удовлетворяют системе

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

следовательно,

$$\begin{cases} 1 \leqslant f < k, \\ 1 \leqslant d < k, \\ 1 \leqslant f + b < k, \\ 1 \leqslant c + d < k, \\ f - b \geqslant k, \\ d - c \geqslant k, \\ f - c + d \geqslant k, \\ f + d < k. \end{cases}$$

Из третьего и пятого уравнений системы следует, что $1 - f \leqslant f - k$, $f \geqslant (k+1)/2$, из четвёртого и шестого — что $1-d \leqslant d-k$, значит, $d \geqslant (k+1)/2$. Тогда из последнего неравенства системы вытекает, что $(k+1)/2 + (k+1)/2 \leqslant$ $\leqslant f + d < k$, откуда следует, что $k + 1 < k$. Противоречие.

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

II. Рассмотрим суммы вида $(1 + a^r) + a^s$ и $1 + (a^r + a^s)$. Пусть r и s имеют разложения (8).

Если $1 + a^r \in C$, или $a^s \in C$, или $a^r + a^s \in C$, то по лемме 18 имеем, что $(1 + a^r) + a^s \in C$ или $1 + (a^r + a^s) \in C$.

Если $k \leqslant mj_2 \leqslant n$, то по лемме 19 $(1 + a^r) + a^s = 1 + (a^r + a^s) = a^{mj_2} \in C$.

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

$$\begin{cases} 1 \leqslant hi_1 + mj_1 < k, \\ 1 \leqslant hi_2 + mj_2 < k, \\ 1 \leqslant mj_1 < k, \\ 1 \leqslant mj_2 < k, \\ mj_1 - hi_1 \geqslant k. \end{cases} \tag{14}$$

Из второго, третьего и четвёртого неравенств системы (14) получаем, что

$$-k+1 < 1 - mj_2 \leqslant hi_2 < k - mj_2 \leqslant k - 1, \quad -k+1 < mj_2 - mj_1 < k - 1. \tag{15}$$

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

В случае а) имеем

$$1 + (a^r + a^s) = 1 + a^{hi_1+mj_1}\bigl(1 + a^{(hi_2-hi_1)+(mj_2-mj_1)}\bigr).$$

Если $mj_2 - mj_1 = 0$, то по следствию 2 сумма $1 + a^{(hi_2-hi_1)+(mj_2-mj_1)}$ лежит в цикле C и $1 + (a^r + a^s) \in C$ по лемме 18, 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 $1 + (a^r + a^s) \in C$), тогда по правилу сложения а) из теоремы 2

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

С другой стороны, из пятого неравенства системы (14) получаем, что $hi_1 \leqslant \leqslant mj_1 - k$, и, учитывая неравенство (15), имеем, что $hi_2 + k > 0$. Тогда

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

противоречие.

Если $-k + 1 < mj_2 - mj_1 < 0$, то

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

(в противном случае $1 + (a^r + a^s) \in C$), тогда по правилу сложения а) из теоремы 2 выполняется

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

С другой стороны, учитывая неравенство (15) и четвёртое неравенство системы (14), получаем, что $hi_1 + n > 0$ и $mj_2 < k$, значит,

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

противоречие.

Случай б) также приводит к противоречию.

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

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

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

Доказательство. По лемме 20 и в силу ассоциативности сложения в полукольце S для любых $r, s \in \mathbb{N}_0$

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

откуда, используя дистрибутивность умножения относительно сложения, получаем утверждение теоремы. $\square$

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* (6). *Тогда для того чтобы* S *было полукольцом, необходимо и достаточно, чтобы выполнялись следующие условия* (*для любых* $r, s \in \mathbb{N}_0$):

а) *из того что* $a^r + 1 \in C$, $1 + a^s \notin C$, *следует, что* $a^r + (1 + a^s) \in C$;
б) *из того что* $a^r + 1 \notin C$, $1 + a^s \in C$, *следует, что* $(a^r + 1) + a^s \in C$;
в) $1 + a^r \in C$ *влечёт* $1 + (a^r + a^s) \in C$;
г) $1 + a^r \notin C$ *влечёт* $(1 + a^r) + a^s \in C$;
д) $a^s + 1 \in C$ *влечёт* $(a^r + a^s) + 1 \in C$;
е) $a^s + 1 \notin C$ *влечёт* $a^r + (a^s + 1) \in C$.

Доказательство. Доказательство следует из лемм 18—20 и теоремы 4. □

5. Идеалы, конгруэнции, циклические подполукольца

Определение 7 [2]. Непустое подмножество I полукольца S называется *идеалом* в S, если для любых $a, b \in I$ и $s \in S$ элементы $a + b$, sa, as принадлежат I.

Теорема 6. *Множества вида* $A_s = \{a^s, \ldots, a^k, \ldots, a^{k+n-1}\}$, *где* $s \leqslant k$, *циклического полукольца* $S = (a)$ *типа* (k, n) *и только они являются идеалами в* S. *В частности, при* $s = k$ $A_s = A_k = C$ *и это множество является наименьшим идеалом в* S.

Доказательство. Пусть $A_s = \{a^s, \ldots, a^k, \ldots, a^{k+n-1}\}$ для некоторого $s \leqslant k$. Очевидно, что множество A_s выдерживает умножение на элементы полукольца S. В случае $S = C$ имеем $A_s = A_k = C = S$, и очевидно, что A_s замкнуто относительно сложения. Пусть теперь $S \neq C$, a^r и a^t — произвольные элементы множества A_s и $a^r + a^t = a^q$. Если сложение в S левое (правое), то $a^q = a^r$ ($a^q = a^t$). Если сложение в S не левое и не правое, то по лемме 5 $q \geqslant \max\{r, t\}$. Значит, A_s замкнуто относительно сложения. Таким образом, множество A_s — идеал в S.

Пусть I — идеал в S и s — наименьшее число (можно считать, что $s \leqslant k + n - 1$), такое что $a^s \in I$. Тогда $a^t = a^{t-s} \cdot a^s \in I$ для любого $t > s$. Также имеем, что $a^k = a^{k+n-s} \cdot a^s \in I$. Учитывая, что s наименьшее, получаем, что $s \leqslant k$. При $s < k$ $I = \{a^s, \ldots, a^k, \ldots, a^{k+n-1}\}$, а при $s = k$ $I = \{a^k, \ldots, a^{k+n-1}\} = A_s = C$ и I является наименьшим идеалом в S. Таким образом, идеал I имеет вид множества A_s. □

Из теоремы 6 выводятся следствия.

Следствие 4. *Множества* $S = A_0 \supset A_1 \supset \ldots \supset A_{k-1} \supset A_k = C$ — *цепь идеалов циклического полукольца* $S = (a) \neq C$ *типа* (k, n).

Следствие 5. *Конечное циклическое полуполе не имеет собственных идеалов.*

Заметим, что любая подгруппа (c^d) циклической группы $C = (c)$ порядка n образует класс некоторой конгруэнции ρ:

$$c^r \; \rho \; c^{r_1} \iff r - r_1 \equiv 0 \pmod d, \tag{16}$$

где d — делитель n.

Обозначим конгруэнцию на конечной циклической группе, задаваемую формулой (16), через ρ_d.

Лемма 21. *Конгруэнция, заданная на мультипликативной группе конечного циклического полуполя, является полукольцевой конгруэнцией.*

Доказательство. Обозначим через ρ_d конгруэнцию на мультипликативной группе конечного циклического полуполя $C = (c)$ порядка n. Покажем, что ρ_d сохраняет сложение.

Пусть $c^r \; \rho_d \; c^{r_1}$ и $c^s \; \rho_d \; c^{s_1}$, где $r, r_1, s, s_1 \in \mathbb{N}_0$. Из формулы (16) выводим, что $r_1 = r + q_1 d$, $s_1 = s + q_2 d$ для некоторых $q_1, q_2 \in \mathbb{N}_0$. Пусть $m = |C + 1|$, $h = |1 + C|$, $1 = hi + mj$ для некоторых чисел $i, j \in \mathbb{Z}$. Тогда по предложению 2

$$\begin{aligned} c^r + c^s &= c^{hri+msj+un}, && \text{где } u \in \mathbb{Z}, \\ c^{r_1} + c^{s_1} &= c^{h(r+q_1d)i+m(s+q_2d)j+vn}, && \text{где } v \in \mathbb{Z}. \end{aligned}$$

Имеем

$$(h(r+q_1d)i + m(s+q_2d)j + vn) - (hri + msj + un) = (hq_1i + mq_2j)d + wn,$$

где $w = v - u \in \mathbb{Z}$. Как отмечено выше, n делится на d. Тогда из формулы (16) следует, что $(c^r + c^s) \; \rho_d \; (c^{r_1} + c^{s_1})$. □

Рассмотрим произвольные числа t и d, такие что $0 \leqslant t \leqslant k$, d — делитель числа n. Обозначим через $\rho(t, d)$ отношение эквивалентности, заданное на конечном циклическом полукольце $S = (a)$ типа (k, n) и удовлетворяющее следующим условиям:

1) $a^r \; \rho(t,d) \; a^s$ тогда и только тогда, когда $r < t$, $s < t$ или $r \geqslant t$, $s \geqslant t$;
2) если $r < t$ и $s < t$, то $a^r \; \rho(t,d) \; a^s$ тогда и только тогда, когда $r = s$;
3) если $r \geqslant t$ и $s \geqslant t$, то $a^r \; \rho(t,d) \; a^s$ тогда и только тогда, когда $r - s \equiv 0 \pmod d$.

Таким образом, «до» элемента a^t отношение $\rho(t,d)$ является отношением равенства, а «начиная» с элемента a^t отношение $\rho(t,d)$ удовлетворяет формуле (16).

Заметим, что при $d = n$ и любом t все классы отношения $\rho(t,d)$ одноэлементные.

Замечание 6. Отношение $\sim$, заданное на конечном циклическом полукольце $S \neq C$ с некоммутативным сложением формулой (4), является отношением вида $\rho(k, 1)$.

Теорема 7. *На любом конечном циклическом полукольце с некоммутативным сложением отношения вида $\rho(t,d)$ и только они являются конгруэнциями.*

Доказательство. Пусть $S=(a)$ — конечное циклическое полукольцо типа (k,n) с циклом C порядка n, $|C+e|=m$, $|e+C|=h$, $1=hi+mj$ для некоторых $i,j\in\mathbb{Z}$.

Пусть ρ — конгруэнция на конечном циклическом полукольце $S=(a)$ типа (k,n). По [3, теорема 2] цикл C полукольца S является конечным циклическим полуполем. Тогда конгруэнция ρ на мультипликативной группе цикла C полукольца S имеет вид ρ_d, где d — некоторый делитель порядка n цикла C.

Если $d=n$, то все классы конгруэнции ρ одноэлементны и $\rho=\rho(t,n)$, где $0\leqslant t\leqslant k$.

Если $d\neq n$, то существуют неодноэлементные классы конгруэнции ρ. Пусть r — наименьшее число, такое что $r\leqslant k$ и $a^r\ \rho\ a^{r_1}$ $(r\neq r_1)$. Тогда, учитывая, что $a^{k-r}\ \rho\ a^{k-r}$, получаем, что $a^k\ \rho\ a^{k+(r_1-r)}$, откуда следует, что $r_1-r\equiv 0 \pmod d$. Принимая $t=r$, получаем, что «до» a^t классы конгруэнции ρ одноэлементные, а «начиная» с a^t $\rho=\rho_d$. Таким образом, $\rho=\rho(t,d)$.

Пусть $\rho(t,d)$ — отношение эквивалентности, заданное на конечном циклическом полукольце $S=(a)$ типа (k,n). Покажем, что оно является конгруэнцией. Пусть $a^r\ \rho(t,d)\ a^{r_1}$ и $a^s\ \rho(t,d)\ a^{s_1}$.

Если $r=r_1$ и $s=s_1$, то $r+s=r_1+s_1$, откуда следует, что $a^{r+s}=a^{r_1+s_1}$ и $a^r+a^s=a^{r_1}+a^{s_1}$. Тогда $(a^ra^s)\ \rho(t,d)\ (a^{r_1}a^{s_1})$ и $(a^r+a^s)\ \rho(t,d)\ (a^{r_1}+a^{s_1})$.

Пусть хотя бы одно из равенств $r=r_1$ и $s=s_1$ не выполняется. Не теряя общности, будем считать, что $r\neq r_1$. Тогда $r\geqslant t$, $r_1\geqslant t$, $r_1-r\equiv 0 \pmod d$. Отметим, что $s_1-s\equiv 0 \pmod d$. По лемме 3 $a^r+a^s=a^{hri+msj+un}$, где $u\in\mathbb{Z}$. Также $a^{r_1}+a^{s_1}=a^{hr_1i+ms_1j+vn}$, где $v\in\mathbb{Z}$. Если сложение в S левое или правое, то очевидно, что $(a^r+a^s)\ \rho(t,d)\ (a^{r_1}+a^{s_1})$. Если $S=C$, то $t=0$, и $hri+msj+un\geqslant t$ и $hr_1i+ms_1j+vn\geqslant t$. Если $S\neq C$ и сложение в S не левое и не правое, то упомянутые неравенства следуют из леммы 5. Составим разность показателей степеней $hi(r_1-r)+mj(s_1-s)+n(v-u)$. Все слагаемые разности делятся на d, следовательно, $(a^r+a^s)\ \rho(t,d)\ (a^{r_1}+a^{s_1})$. Также имеем $r+s\geqslant t$, $r_1+s_1\geqslant t$, $(r_1-r)+(s_1-s)\equiv 0 \pmod d$, отсюда следует, что $a^{r+s}\ \rho(t,d)\ a^{r_1+s_1}$.

Таким образом, $\rho(t,d)$ является конгруэнцией на S. □

Замечание 7. Лемма 6 вытекает из теоремы 7.

Следствие 6. *Количество конгруэнций на конечном циклическом полукольце типа (k,n) равно $(k+1)\sigma_0(n)$, где $\sigma_0(n)$ — число делителей n.*

Рассмотрим циклические подполукольца конечных циклических полуколец с некоммутативным сложением.

Теорема 8. *Пусть (c) — циклическое полуполе. Множество (c^r) для любого $r\in\mathbb{N}$ является циклическим подполуполем в C.*

Доказательство. Замкнутость множества (c^r), где $r \in \mathbb{N}$, относительно умножения очевидна. Проверим замкнутость относительно сложения. Достаточно проверить, что для всех $q \in \mathbb{N}$ выполняется $1 + c^{rq} = c^{rq_1}$ и $c^{rq} + 1 = c^{rq_2}$ для некоторых $q_1, q_2 \in \mathbb{N}$.

Пусть $|(c)| = n$, $n = m \cdot h$, $(m, h) = 1$, $1 = hi + mj$. По предложению 2

$$1 + c^{rq} = c^{rqmj+nv}$$

для некоторого $v \in \mathbb{Z}$. Имеем, что

$$c^{rqmj+nv} = c^{rqmj+nv+n(rx-v)} = c^{r(mjq+nx)} = c^{rq_1},$$

где $rx > v$, $x \in \mathbb{Z}$. Таким образом, $1 + c^{rq} = c^{rq_1}$ для некоторого $q_1 \in \mathbb{N}$.

Аналогично $c^{rq} + 1 = c^{rq_2}$ для некоторого $q_2 \in \mathbb{N}$.

Имеем, что (c^r) замкнуто относительно сложения и умножения, следовательно, является циклическим подполуполем. □

Рассмотрим теперь циклические подполукольца циклического полукольца $S = (a)$ типа (k, n).

Предложение 7. *Пусть $S = (a)$ — циклическое полукольцо типа (k, n), $n \geqslant 2$, с некоммутативным сложением. Множество (a^d), где d — делитель числа n, является циклическим подполукольцом в S.*

Доказательство. Множество (a^d) замкнуто относительно умножения для всех $d \in \mathbb{N}$.

Докажем замкнутость относительно сложения. Достаточно доказать, что для всех $q \in \mathbb{N}$ выполняется $1 + a^{dq} = a^{dq_1}$ и $a^{dq} + 1 = a^{dq_2}$ для некоторых $q_1, q_2 \in \mathbb{N}$.

Пусть C — цикл полукольца S, $|C| = n$, $n = m \cdot h$, $(m, h) = 1$, $1 = hi + mj$. По предложению 3

$$1 + a^{dq} = a^{dqmj+nv} = a^{d(qmj+\frac{n}{d}v)} = a^{dq_1}$$

для некоторых $v \in \mathbb{Z}$ и $q_1 \in \mathbb{N}$.

Аналогично $a^{dq} + 1 = a^{dq_2}$ для некоторого $q_2 \in \mathbb{N}$. Следовательно, множество (a^d) замкнуто относительно сложения. □

Следствие 7. *Пусть $S = (a)$ — циклическое полукольцо типа (k, n), $n \geqslant 2$, с некоммутативным сложением.*

1. *Если $h \,\vdots\, q$, то (a^{mq}) — циклическое подполукольцо в S.*
2. *Если $m \,\vdots\, q$, то (a^{hq}) — циклическое подполукольцо в S.*
3. *Множества (a^m), (a^h), (a^n) — циклические подполукольца в S.*

Предложение 8. *Пусть $S = (a)$ — циклическое полукольцо типа (k, n), $n \geqslant 2$, с некоммутативным сложением. Если все суммы элементов S лежат в цикле полукольца, то для каждого $r \in \mathbb{N}$ множество (a^r) — циклическое подполукольцо в S.*

Доказательство аналогично доказательству предложения 7. □

Литература

[1] Бестужев А. С. О строении конечных мультипликативно-циклических полуколец // Ярослав. пед. вестн. — 2013. — Т. 3, № 2. — С. 14—18.

[2] Вечтомов Е. М. Введение в полукольца. — Киров: Вят. гос. пед. ун-т, 2000.

[3] Вечтомов Е. М., Лубягина И. В. Циклические полукольца с идемпотентным некоммутативным сложением // Фундамент. и прикл. матем. — 2011/2012. — Т. 17, вып. 1. — С. 33—52.

[4] Brown T., Lazerson E. On finitely generated idempotent semigroups // Semigroup Forum. — 2009. — Vol. 78, no. 1. — P. 183—186.