УДК 512.55

А. С. Бестужев

О строении конечных мультипликативно-циклических полуколец

В данной статье продолжается изучение неидемпотентных мультипликативно-циклических полуколец. Вначале излагаются факты, доказанные автором ранее и опубликованные в предыдущих работах. Далее рассматриваются новые свойства с их доказательством, на основе которых строится алгоритм нахождения всевозможных циклических полуколец для частного случая.

Ключевые слова: полукольцо, конечное полукольцо, мультипликативно-циклическое полукольцо, поглощающий элемент.

A. S. Bestuzhev

On the Structure of the Multiplicative Cyclic Semirings

In this article, we continue to study idempotent multiplicative-cyclic semirings. Initially, we have given the facts that the author proved and published in previous works. Then we explained new properties and their proofs. We constructed an algorithm for finding all the cyclic semirings for the particular case.

Keywords: a semiring, a final semiring, idempotent multiplicative-cyclic semirings, an absorbing element.

Полукольцом называется алгебраическая структура $\langle S, +, \cdot, 0, 1\rangle$, в которой $\langle S, +, 0\rangle$ – коммутативный моноид, $\langle S, \cdot, 1\rangle$ – полугруппа, выполняются законы дистрибутивности умножения $\cdot$ относительно сложения $+$ и тождество $0\cdot s=s\cdot 0=0$.

Мультипликативно-циклическим полукольцом называется полукольцо, все элементы которого, кроме нуля и единицы, являются натуральными степенями некоторого элемента a ($a\neq 0$ и $a\neq 1$), нуль же может являться, а может и не являться степенью элемента a; считаем, что $a^0=1$. В дальнейшем такие полукольца будем называть просто циклическими.

Строение бесконечных циклических полуколец известно и определяется законами сложения: $a^m+a^n=a^{min\{m,n\}}$ или $a^m+a^n=a^{max\{m,n\}}$ [4, с. 28]. Ниже рассматриваются только конечные циклические полукольца.

Возможны два случая:

- одна из степеней элемента a равна нулю;
- среди степеней элемента a нет нуля.

Если нулевой элемент является степенью элемента a, то $a^m+a^n=a^{min\{m,n\}}$[2, с. 144].

Во втором случае полукольцо представляет собой либо конечное поле, либо оно устроено следующим образом: элементы $1, a, \ldots, a^k$ – различные, $a^k=a^{k+1}$ [2, с. 145].

Далее будем рассматривать только такие полукольца с поглощающим элементом a^k.

Сумма $1+a^k$ может принимать одно из двух значений: 1 или a^k [2, с. 145].

$1+a^k=1$. $S\backslash\{0\}$ – циклическое полукольцо с нулевым элементом a^k. Строение таких полуколец нам известно. Само полукольцо S получается присоединением нуля к полукольцу $S\backslash\{0\}$ [2, с. 145].

Второй случай: $1+a^k=a^k$. Умножим обе части равенства на a^n. Получаем: $a^n+a^k=a^k$. Это значит, что поглощающий по умножению элемент будет еще и поглощающим по сложению.

Среди таких полуколец существуют *идемпотентные,* в которых $1+1=1$, и *неидемпотентные,* в которых $1+1=a^m$, где $m>0$.

Аддитивная полугруппа циклических идемпотентных полуколец является верхней полурешеткой [1, с. 71–78].

В дальнейшем будут рассматриваться только неидемпотентные циклические полукольца $S=\{1, a, \ldots, a^k, 0\}$, где $a^k=a^{k+1}$.

Чтобы задать полугруппу по сложению для такого полукольца, достаточно задать суммы единиц со всеми элементами, оставшиеся суммы находятся по свойству дистрибутивности.

Выражение $a^{3,4}$ означает, что на его месте может стоять как элемент a^3, так и элемент a^4; выражение $a^{3,\dots,7}$ означает, что на месте $a^{3,\dots,7}$ может находиться любой из элементов a^3, a^4, a^5, a^6 или a^7. Приведем пример. Равенство $1+a=a^{3,4}$ можно понимать двояко: сумма $1+a$ равна a^3 или a^4, или сумма $1+a$ может быть равна любому из значений a^3 или a^4.

У нас есть циклическое полукольцо S с поглощающим элементом a^k, где $k=m+n+p+1$. Числа m, n и p такие, что в полукольце S выполняются равенства:

$a^m+a^{m+n}=a^{m+n+p}$; $a^{0,\dots,k}+a^{m+n+1,\dots,k}=a^{m+1,\dots,k}+a^{m+n}=a^k$.

Иными словами, сумма $a^m+a^{m+n}=a^{m+n+p}$ является «первой сверху» суммой, не равной a^k. Доказано, что $p>m$ [2, с. 147].

Возможен один из следующих четырех случаев:

1) $n-1\le m$;

2) $n-1>m$, $p\ge n$;

3) $n>p$, $1+1=a^{n+1,\dots,k}$;

4) $n-1\ge p+m$, $1+1=a^n$.

Для первых трех вариантов получены формулы, описывающие строение всех таких полуколец [2, с. 145–149]. Изучение неидемпотентных циклических полуколец остановилось на случае: $n-1\ge p+m$, $1+1=a^n$. Для него найдены возможные значения сумм единицы со всеми элементами:

$1+a^k=\dots=1+a^{m+n+1}=a^k$

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

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

...

$1+a^{n+1}=a^{n+p+1,\dots,k}$

$1+a^n=a^{n+p}$

$1+a^{n-1}=a^{n+p,\dots,k}$

…

$1+a^{n-s}=a^{n+p+1-s,\dots,k}$ $(1\le s\le p-m)$

...

$1+a^{n-r}=a^{m+n+1,\dots,k}$ $(r=p-m)$

...

$1+a^{m+1}=a^{m+n+1,\dots,k}$

$1+a^m=a^{n+m,\dots,k}$

$1+a^{m-1}=a^{n+m-1,\dots,k}$

...

$1+1=a^n$ [2, с. 145–149]

Данную таблицу назовем таблицей возможных полуколец.

Во всех приведенных равенствах, кроме тех, где степень суммы однозначно определяется, вместо единицы можно подставить любой элемент $a1,\dots,k$ – они окажутся верными (в том смысле, что каждая сумма из левой части равенства может принимать лишь возможное значение из правой части равенства).

Теорема. *Пусть положительные числа s и r такие, что* $s+r\le m$. *Тогда:*

1) $1+a^s=a^{n+s}\Leftrightarrow 1+a^{n+s}=a^s+a^n=a^{n+s+p}$;

2) $1+a^s=a^{n+s+r}\Leftrightarrow 1+a^{n+s}=1+a^{n+s+r}=a^s+a^n=a^{s+r}+a^n=a^{n+s+r+p}$;

3) $1+a^s=a^{n+m+1,\dots,k}\Leftrightarrow 1+a^{n+s}=a^s+a^n=a^k$ [3, с. 55–57].

Следствие. *Положительные числа s и r такие, что* $s,r\le m$. *Тогда* $a^r+a^{n+s}=a^s+a^{n+r}$.

С помощью данной теоремы получаем усовершенствованный алгоритм, по которому можно находить полукольца:

Возьмем таблицу возможных полуколец. Перебираем варианты сумм единицы с элементами a, …, a^m среди возможных. Для каждого набора сначала находим значения сумм: $1+a^{n-m}$, …, $1+a^{n-1}$, $1+a^{n+1}$, …, $1+a^{n+m}$ (точные или оценку). Далее проверяем справедливость равенств: $1+(a^r+a^s)=(1+a^r)+a^s=a^r+(1+a^s)$ $(0<r<s\le m)$. Если все они окажутся верными, то вносим в таблицу изменения для найденных сумм, а также подошедший вариант для сумм $1+a$, …, $1+a^m$. Получившаяся структура является полукольцом. В противном случае структура не будет полукольцом.

Этот алгоритм позволяет находить всевозможные полукольца для четвертого случая. Однако вариантов для перебора слишком много. Сумма $1+a^m$ может принимать значение a^{n+m} или $a^{n+m+1,\ldots,k}$, сумма $1+a^{m-1} – a^{n+m-1}$, a^{n+m}, $a^{n+m+1,\ldots,k}$ и т. д. Получаем $(m+1)!$ вариантов. Этот поиск можно сократить, доказав различные утверждения.

Утверждение 1. *Если для какого-то элемента* a^s $(0<s<m)$ *выполняется равенство* $1+a^s=a^{n+s}$, *то для всех натуральных* l *таких, что* $ls\le m$, *верно:* $1+a^{ls}=a^{n+ls}$.

Доказательство. Докажем по индукции. Известно, что: $1+a^{n+s}=a^s+a^n=a^{n+s+p}$. Пусть $1+a^s=a^{n+s}$, …, $1+a^{(r-1)s}=a^{n+(r-1)s}$, $rs\le m$. Докажем, что $1+a^{rs}=a^{n+rs}$.

Рассмотрим равенство: $a^{rs}+(1+a^{(r-1)s})=(a^{rs}+1)+a^{(r-1)s}$. Левая часть этого равенства равна: $a^{rs}+(1+a^{(r-1)s})=a^{rs}+a^{n+(r-1)s}=a^{(r-1)s}(a^s+a^n)=a^{n+rs+p}$.

Если степень суммы $1+a^{rs}$ больше, чем $n+rs$, то выражение в правой части равенства имеет степень больше, чем $n+rs+p$. В то же время степень суммы $1+a^{rs}$ не меньше чем $n+rs$, получаем, что $1+a^{rs}=a^{n+rs}$.

Утверждение 2. *Если положительные числа* s *и* r *такие, что* $s+r\le m$, $1+a^s=a^{n+s+r}$, *то* $1+a^r=a^{n+r}$.

Доказательство. Из равенства $1+a^s=a^{n+s+r}$ по теореме следует: $1+a^{s+r}=a^{n+s+r}$. Далее, рассмотрим тождество: $a^s+(1+a^{s+r})=(1+a^s)+a^{s+r}$.

Левая часть равенства равна: $a^s+(1+a^{s+r})=a^s+a^{n+s+r}=a^s(1+a^{n+r})$.

Правая часть равенства равна: $(1+a^s)+a^{s+r}=a^{n+s+r}+a^{s+r}=a^{n+s+r+p}$.

Итак, $a^s(1+a^{n+r})=a^{n+s+r+p}$, $a^{n+s+r+p}\ne a^k$, откуда: $1+a^{n+r}=a^{n+r+p}$. По теореме (обратный случай), $1+a^r=a^{n+r}$.

Данное утверждение имеет следствие.

Следствие. *Не существует такого числа* s $(1<s\le m)$, *что* $1+a^{s-1}=a^{n+s}$.

Доказательство. Допустим, такое число существует и $1+a^{s-1}=a^{n+s}$. По утверждению 2 $1+a=a^{n+1}$, а по утверждению 1, $1+a^{s-1}=a^{n+s-1}$ – противоречие.

Докажем следующую лемму.

Лемма. *Если в полукольце не все суммы единицы с элементами* $a^{1,\ldots,m}$ *равны* $a^{n+m+1,\ldots,k}$, *то найдется такой элемент* a^l $(0<l\le m)$, *что* $1+a^l=a^{n+l}$.

Доказательство. По условию найдется такой элемент a^r, что $1+a^r=a^{n+r+s}$ $(0<r,\ 0\le s,\ r+s\le m)$. Если $s=0$, то лемма доказана, в противном случае по теореме, а также по утверждению 2 имеем: $1+a^{r+s}=a^{n+r+s}$, $1+a^r=a^{n+r}$. Итак, данными элементами являются элементы a^{r+s} и a^r. Лемма доказана.

Очевидно, что среди элементов, удовлетворяющих этому условию, найдется элемент с наименьшей степенью. Только его и будем в дальнейшем обозначать a^l, и больше ни для какого другого элемента обозначение a^l использовать не будем.

Утверждение 3. *Пусть* $0\le r<s\le m$, $t\le m$, $a^r+a^s=a^{n+t}$. *Тогда возможны два случая:*

1) $t=s$, $t\ge l+r$;

2) $t\ge s+l$.

Доказательство. Из равенства $a^r+a^s=a^{n+t}$ следует $1+a^{s-r}=a^{n+t-r}$ (выполняется и при $r=0$).

Если $t-r=s-r$, то $t-r\ge l$, иначе возникает противоречие с определением числа l. Итак, $t-r=s-r$, $t-r\ge l$, откуда $t=s$, $t\ge l+r$.

Если $t-r>s-r$, то по утверждению 2 $1+a^{t-s}=a^{n+t-s}$. Чтобы не возникло противоречия с определением числа l, должно выполняться: $t-s\ge l$, откуда: $t\ge s+l$.

Очевидны также следующие утверждения:

Если $s>m-l$ *и выполняются остальные условия утверждения, то* $a^r+a^s=a^{n+s}$ *(и* $s\ge l+r$*) или* $a^r+a^s=a^{n+m+1,\ldots,k}$.

Доказательство от противного вытекает из утверждения 3.

Сумма любых двух неодинаковых элементов в полукольце имеет степень не меньше чем $n+l$.

Данное утверждение имеет следующее следствие.

Следствие. *Пусть* $0\le r,s,t\le m$, $r<s$, $a^r+a^{n+s}=a^s+a^{n+r}=a^{n+t+p}$. *Тогда возможны два случая:*

1) $t=s$, $t\ge l+r$;

2) $t\ge s+l$.

Доказательство. Из данного в условии равенства $a^r+a^{n+s}=a^{n+t+p}$ следует равенство: $1+a^{n+s-r}=a^{n+t-r+p}$. По обратной теореме $1+a^{s-r}=a^{n+t-r}$, откуда: $a^r+a^s=a^{n+t}$. Осталось применить утверждение 3. Верно также следующее утверждение.

Если $s>m-l$ и выполняются остальные условия утверждения, то $a^s+a^{n+r}=a^r+a^{n+s}=a^{n+s+p}$ (и $s\geq l+r$) или $a^s+a^{n+r}=a^r+a^{n+s}=a^k$.

Утверждение 4. *Пусть* $1+a^{l+r}=a^{n+l+r}$, $0<r<l$, $l+r\leq m$. *Тогда* $1+a^r=a^{n+l+r}$.

Доказательство. Степень суммы $1+a^r$ не может быть равна $n+r$, так как $r<l$, тогда по утверждению 3 она не меньше чем $l+r$. Далее, рассмотрим равенство: $(1+a^r)+a^{l+r}=1+(a^r+a^{l+r})$.

Правая его часть равна: $1+a^r(1+a^l)=1+a^{n+l+r}=a^{n+l+r+p}$.

Отсюда следует, что степень суммы $1+a^r$ не больше $n+l+r$, иначе выражение в левой части рассматриваемого равенства будет иметь степень больше, чем $n+l+r+p$. Объединив результаты, получаем, что $1+a^r=a^{n+l+r}$.

Утверждение 5. *Пусть выполняются равенства:*

$1+a^{l+r}=a^{n+l+r}$ *и* $1+a^{l+s}=a^{n+l+s}$, *где* $0<r<s<l$, $l+s\leq m$. *Тогда:*

$1+a^{s-r}=a^{n+l+s}$.

Доказательство. Рассмотрим равенство: $(1+a^{s-r})+a^{l+s}=1+(a^{s-r}+a^{l+s})$.

Правая часть равенства равна: $1+a^{s-r}(1+a^{l+r})=1+a^{s-r}a^{l+r}=a^{n+l+s+p}$.

Отсюда можно сделать вывод, что степень суммы $1+a^{s-r}$ не больше чем $n+l+s$, иначе выражение в левой части рассматриваемого равенства будет иметь степень больше, чем $n+l+s+p$. Докажем, что она равна именно $n+l+s$.

Степень суммы $1+a^{s-r}$ не меньше чем $n+l+s-r$ (по утверждению 3).

Предположим, что $1+a^{s-r}=a^{n+l+t}$, где $s-r\leq t<s$. Как уже было доказано:

$(1+a^{s-r})+a^{l+s}=a^{n+l+s+p}$.

Далее,

$a^{n+l+t}+a^{l+s}=a^{n+l+s+p}$, $a^{l+t}(a^n+a^{s-t})=a^{n+l+s+p}$, $a^n+a^{s-t}=a^{n+s-t+p}$.

По обратной теореме, $1+a^{s-t}=a^{n+s-t}$, а $s-t<l$. Получили противоречие. Итак, $1+a^{s-r}=a^{n+l+s}$.

Утверждения 4 и 5 можно объединить, если допустить, что $r=0$.

В оставшейся части статьи будет рассказываться, как устроены полукольца для случая $m\leq 2l$ (можно сказать, что утверждения 4 и 5 относятся как раз к этому случаю). Во всей оставшейся части статьи считается, что $m\leq 2l$. Сейчас будет сформулирован алгоритм, по которому можно находить все полукольца, для данного случая.

По утверждению 3 сумма $1+a^{l+t}$ ($0<t\leq m-l$) может принимать значения, равные $1+a^{n+l+t}$ или $a^{n+m+1,\ldots,k}$. Рассматриваем всевозможные варианты для сумм вида $1+a^{l+1,\ldots,m}$. Среди этих сумм не равны $a^{n+m+1,\ldots,k}$ суммы единицы со следующими степенями элемента a: $l+r_1$, …, $l+r_s$, где $0<r_1<\ldots<r_s\leq m-l$ (степени этих сумм, соответственно, будут следующие: $n+l+r_1$, …, $n+l+r_s$). А для всех остальных t: $0<t\leq m-l$, $t\neq r_i$ ($1\leq i\leq s$), верно: $1+a^{l+t}=a^{n+m+1,\ldots,k}$. Используя доказанные утверждения, можно определить значения некоторых сумм вида $1+a^{1,\ldots,l-1}$, а именно суммы единицы со следующим степенями элемента a: r_i ($1\leq i\leq s$) – по утверждению 3, r_i-r_j, ($1\leq j<i\leq s$) – по утверждению 4.

Всем оставшимся суммам вида $1+a^{1,\ldots,l-1}$ придаем значение, равное $a^{n+m+1,\ldots,k}$. Если не возникнет противоречий, то есть если окажется, что всякая сумма вида $1+a^{1,\ldots,l-1}$, не равная $a^{n+m+1,\ldots,k}$, определяется однозначно, то существует полукольцо с получившимся набором сумм вида $1+a^{1,\ldots,m}$, иначе полукольца с выбранным набором сумм вида $1+a^{l+1,\ldots,m}$ не существует.

Если в каком-то определенном случае не возникло противоречий, то есть полукольцо с получившимся набором сумм вида $1+a^{1,\ldots,m}$.

Докажем, что не существует двух различных полуколец, имеющих одинаковые наборы сумм единицы с элементами, степень которых больше, чем l (и не больше чем m), но разные наборы сумм единицы с элементами, степень которых меньше, чем l, полукольца считаются разными, если они отличаются названными суммами, не равными $a^{n+m+1,\ldots,k}$ (напомним, что рассматриваются полукольца, в которых $m\leq 2l$).

Предположим обратное. Возьмем полукольцо, в котором суммы единицы с элементами $a^{1,\ldots,l-1}$ определяются по описанному выше алгоритму. Возьмем другое полукольцо. В первом полукольце суммы единицы с элементами, степени которых меньше, чем l, полностью определяются суммами единицы с элементами, степень которых больше, чем l, в обоих полукольцах суммы единицы с элементами $a^{l+1,\ldots,m}$ совпадают. Значит, если в первом полукольце есть сумма вида $1+a^r=a^{l+r+t}$ ($0<r<l$, $0\leq t$, $l+r+t\leq m$), она есть и во втором полукольце. Эти полукольца различаются набором сумм единицы с

элементами $a^{1,\dots,l-1}$. Значит, найдется такой элемент a^r, что в первом полукольце $1+a^r=a^{n+m+1,\dots,k}$, а во втором – $1+a^r=a^{l+r+t}$ ($0<r$, $0\le t$, $l+r+t\le m$). Тогда во втором полукольце выполняются равенства: $1+a^{l+r+t}=a^{n+l+r+t}$ и $1+a^{l+t}=a^{n+l+t}$. Но эти же самые равенства должны выполняться и в первом полукольце, так как наборы сумм единицы с элементами $a^{n+l+1,\dots,m}$ совпадают. Тогда в первом полукольце по свойству 5 $1+a^r=a^{l+r+t}$ – противоречие. Получили, что для полуколец, в которых $m\le 2l$, суммы единицы с элементами $a^{1,\dots,l-1}$ определяются суммами единиц с элементами $a^{l+1,\dots,m}$. Тем самым получен алгоритм, позволяющий находить все полукольца для случая $m\le 2l$: перебираем всевозможные варианты для сумм вида $1+a^{l+1,\dots,m}$ и для каждого случая определяем, существует ли полукольцо с данным набором сумм или нет.

Библиографический список

1. Бестужев, А. С. Конечные идемпотентные циклические полукольца [Текст] / А. С. Бестужев // Математический вестник педвузов и университетов Волго-Вятского региона : Периодический межвузовский сборник научно-методических работ. Выпуск 13. – Киров : Изд-во ВятГГУ, 2011. – 396 с.

2. Бестужев, А. С. О строении конечных циклических полуколец [Текст] / А. С. Бестужев // Информатика, математика, язык. – 2013. – № 6. – С. 210.

3. Бестужев, А. С. О строении конечных циклических полуколец [Текст] / А. С. Бестужев // Информатика, математика, язык. – 2013. – № 7. – С. 114.

4. Вечтомов, Е. М. Введение в полукольца [Текст] : пособие для студентов и аспирантов / Е. М. Вечтомов. – Киров : изд-во Вятского гос. пед. ун-та, 2000. – 44 с.

Bibliograficheskij spisok

1. Bestuzhev, A. S. Konechnyye idempotentnyye tsiklicheskiye polukol'tsa [Tekst] / A. S. Bestuzhev // Matematicheskiy vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona : Periodicheskiy mezhvuzovskiy sbornik nauchno-metodicheskikh rabot. Vypusk 13. – Kirov : Izd-vo VyatGGU, 2011. – 396 s.

2. Bestuzhev, A. S. O stroyenii konechnykh tsiklicheskikh polukolets [Tekst] / A. S. Bestuzhev // Informatika, matematika, yazyk. – 2013. – № 6. – S. 210.

3. Bestuzhev, A. S. O stroyenii konechnykh tsiklicheskikh polukolets [Tekst] / A. S. Bestuzhev // Informatika, matematika, yazyk. – 2013. – № 7. – S. 114.

4. Vechtomov, Ye. M. Vvedeniye v polukol'tsa [Tekst] : posobiye dlya studentov i aspirantov / Ye. M. Vechtomov. – Kirov : izd-vo Vyatskogo gos. ped. un-ta, 2000. – 44 s.