Альтернативное сложение и умножение

К. Кориков

Основные результаты.

Определение 1. ***Область целостности*** – ассоциативное коммутативное кольцо с единицей и без делителей нуля.

Определение 2. ***Характеристика области целостности*** $\mathbb{Z}(+,\times)$ ($char\ \mathbb{Z}(+,\times)$) **–** наименьшее натуральное число *k,* такое, что $\underbrace{1+...+1}_{k} = 0$. Если же такого числа не существует, то $char\ \mathbb{Z}(+,\times)$ полагается равной нулю.

Обозначение. Пусть $'+'$ и $'\times'$ – некоторые бинарные операции, определенные на множестве целых чисел,

Теорема. Число $k \neq 0$ может быть характеристикой области целостности $\mathbb{Z}('+',\times)$ тогда и только тогда, когда $k = 3$.
(в частности, существует $\mathbb{Z}('+',\times)$, изоморфная $\mathbb{Z}_3[x](+,\times)$)

Замечание 1. Пусть $char\ \mathbb{Z}('+',\times) = 0$ и группа $\mathbb{Z}('+')$ – циклическая. Тогда область целостности $\mathbb{Z}('+',\times)$ изоморфна $\mathbb{Z}(+,\times)$.

Гипотеза. Любая область целостности $\mathbb{Z}('+',\times)$ изоморфна либо $\mathbb{Z}('+',\times)$, либо $\mathbb{Z}_3[x](+,\times)$.

Замечание 2. Существует единственное $\mathbb{Z}(+,'\times')$, для которого выполнено $a\ '\times'\ b = -(a \times b)\ \ \forall a, b \in \mathbb{Z}$, где $\times$ – стандартное умножение.

Выражаю благодарность ***Волкову В.В.*** за нахождение $\mathbb{Z}('+',\times)$ с характеристикой 3 (что обеспечивает достаточность теоремы) и ***Скопенкову А.Б.*** за ценные консультации.

Доказательства.

Лемма. Пусть $\mathbb{Z}('+', \times)$ – область целостности. Тогда $0_1 = 0$ и $(-'a) = (-a)\ \ \forall a \in \mathbb{Z},$ где 0_1 – нейтральный элемент, а a' - обратный элемент по $'+'$.

Доказательство леммы:

$\mathbf{0_1 = 0.}$
$0_1 = 0'-'0 = 0'-'0\times(a'-'b) = 0'-'(0\times a'-'0\times b) = 0'-'0'+'0 = 0$

$\mathbf{(-'1) = -1}.$
Пусть $1\ '+'\ (-1) = t.$ Тогда
$t = 1\times(1\ '+'\ (-1)) = (-1)\times((-1)\ '+'\ 1) = -t.$ Отсюда $t = 0.$

$\boldsymbol{(-'a) = (-a)\ \ \forall a \in \mathbb{Z}}.$
$a\ '+'\ (-a) = a\times 1\ '+'\ a\times(-1) = a\times(1\ '+'\ (-1)) = 0.$ ***QED***.

Доказательство теоремы:

Докажем, что число $\mathbf{k \neq 0}$ *не может быть характеристикой области целостности* $\mathbb{Z}('+', \times)$ *при* $k \neq 3$.

Будем доказывать от противного: пусть $char\,\mathbb{Z}('+', \times) = k,$ причем $k \neq 0$ и $k \neq 3$. $\mathbb{Z} \neq \{0\},$ значит $k \neq 1$. По лемме $(-'1) = -1,$ значит $k \neq 2$. Получаем, что $k > 3$. Обозначим $\underbrace{(1\ '+'\ \dots\ '+'\ 1)}_{t} = s_t$. Возьмем $m \in \{1, \dots, k\}$ такое, что s_m принимает максимальное по модулю значение. Так как $k > 3,$ то $\exists t:\ s_t \notin \{-1, 0, 1\}$. Пусть $m\times m = r\times k + q,\ \ r, k \in \mathbb{Z}$. Тогда $|s_{m\times m}| = |s_{r\times k}\ '+'\ s_q| = |r\times s_k\ '+'\ s_q| = |s_q| < |s_m|$. Но $|s_{m\times m}| = |s_m \times s_m| > |s_m|$ (так как $|s_m| > 1$), противоречие. Значит, исходное предположение неверно. *QED*.

Докажем, что число $k = 3$ *может быть характеристикой области целостности* $\mathbb{Z}('+', \times)$. *В частности, покажем, что существует* $\mathbb{Z}('+', \times)$, *изоморфная* $\mathbb{Z}_3[x](+, \times)$.

Пусть $\mathbb{Z}_3[x](+,\times)$ – кольцо многочленов над полем $\mathbb{Z}/3\mathbb{Z}$. Обозначим за $P_3[x]$ множество всех неприводимых многочленов над $\mathbb{Z}_3[x]$. $P_3[x]$ счетно, значит существует биекция $\varphi: P \to P_3[x]$, где P – множество простых чисел в $\mathbb{Z}$. Так как множества обратимых элементов в $\mathbb{Z}$ и $\mathbb{Z}_3[x]$ совпадают ($\{1,-1\}$), то мы можем доопределить $\varphi: \mathbb{Z} \to \mathbb{Z}_3[x]$ так, чтобы выполнялось $\varphi(a\times b) = \varphi(a)\times\varphi(b)\ \ \forall a, b \in \mathbb{Z}$:
$\varphi(1) = 1, \varphi(-1) = -1, \varphi(0) = 0,\ \varphi(p_1\times\ldots\times p_n) = \varphi(p_1)\times\ldots\times\varphi(p_n)$, где $P_i \in P$. Тогда определив
$\boldsymbol{a\ {'+'}\ b = \varphi^{-1}(\varphi(a) + \varphi(b))}\ \ \forall a, b \in \mathbb{Z}$, получим, что
$\varphi: \mathbb{Z}('+',\times) \to \mathbb{Z}_3[x](+,\times)$ – изоморфизм колец. Таким образом, существует $\mathbb{Z}('+',\times)$ с характеристикой 3. *QED.* ***Теорема доказана.***

Доказательство замечания 1:

Пусть $\mathbb{Z}('+',\times)$ – область целостности, причем группа $\mathbb{Z}('+')$ – циклическая. Тогда верны следующие утверждения:

1 – порождает $\mathbb{Z}('+')$. Иначе $a \neq \pm 1, a \in \mathbb{Z}$ – порождающий элемент, значит $1 = \underbrace{a\ {'+'}\ \ldots\ {'+'}\ a}_{k} = a\times\underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{k}$,

противоречие. Значит $\forall a\in\mathbb{Z}\ \ \exists f(a)\in\mathbb{Z}:\ \underbrace{1\ {'+'}\ \ldots\ {'+'}\ 1}_{f(a)} = a$, f– биекция.

$\boldsymbol{p \in P \ \Rightarrow\ f(p) \in P}$. Иначе
$f(p) = r\times s,\ \ p = \underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{r}\times\underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{s} = f^{-1}(r)\times f^{-1}(s)$.
$r, s \notin \{-1, 0, 1\}\ \Rightarrow\ f^{-1}(r), f^{-1}(s) \notin \{-1, 0, 1\}$. Противоречие.

$\boldsymbol{p \in P \ \Rightarrow\ f^{-1}(p) \in P}$. Иначе
$f^{-1}(p) = r\times s = \underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{f(r)}\times\underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{f(s)} = \underbrace{(1\ {'+'}\ \ldots\ {'+'}\ 1)}_{f(r)\times f(s)}$,
$r, s \notin \{-1, 0, 1\}\ \Rightarrow\ f(r), f(s) \notin \{-1, 0, 1\}$. Противоречие.

$\boldsymbol{f(p_1\times\ldots\times p_2) = f(p_1)\times\ldots\times f(p_s)}$. Это следует из дистрибутивности:

$$\underbrace{(1\ '+'\dots'+'\ 1)}_{p_1}\times\dots\times\underbrace{(1\ '+'\dots'+'\ 1)}_{p_s}=\underbrace{(1\ '+'\ \dots\ '+'\ 1)}_{p_1\times\dots\times p_s}.$$

Объединяя эти утверждения, получаем:
$f(a\times b)=f(a)\times f(b)\ \ \forall a,b\in\mathbb{Z}$. Но
$f(a\ '+'\ b)=f(a)+f(b)\ \ \forall a,b\in\mathbb{Z}$ (из определения *f*). Тогда
$f\ :\ \mathbb{Z}(+,\times)\to\mathbb{Z}('+',\times)$ – изоморфизм, $\mathbb{Z}(+,\times)$ – область целостности, значит и $\mathbb{Z}('+',\times)$ – область целостности. ***QED.***

Доказательство замечания 2:

$\boldsymbol{a\ '\times'\ 0=0\ \ \forall a}$. Это общее свойство кольца.
$\boldsymbol{|e|=1}$. (***e*** – нейтральный элемент по $'\times'$).
Пусть $e>1$. Тогда $1=e\ '\times'\ 1=\underbrace{(1+\dots+1)}_{e}\ '\times'\ 1=$

$$=\underbrace{(1\ '\times'\ 1)+\dots+(1\ '\times'\ 1)}_{e}=(1\ '\times'\ 1)\times e,$$ что по модулю больше 1.

Противоречие. Аналогично для случая $e<-1$.
Пусть $e=-1$. Тогда $\boldsymbol{a\ '\times'\ b=-(a\times b)\ \ \forall a,b\in\mathbb{Z}}$.
$0=1\ '\times'\ (1+(-1))=(-1)'\times'1+1'\times'1=1+1'\times'1$. Значит
$1'\times'1=-1$

$$\boldsymbol{\forall a\in\mathbb{Z}\ \ 1'\times'a=}\ 1\ '\times'\ \underbrace{(1+\dots+1)}_{a}=$$

$$=(1'\times'1)+\dots+\underbrace{(1'\times'1)}_{a}=a\times(1'\times'1)\boldsymbol{=-a}.$$

$$\boldsymbol{\forall a,b\in\mathbb{Z}\ \ a\ '\times'\ b}=(1\times a)\ '\times'\ (1\times b)=$$
$$=(1\ '\times'\ 1)\times(a\times b)=\boldsymbol{-(a\times b)}.$$ ***QED.***

Литература.

1. Винберг Э. Б. *Курс алгебры.* – 2001.
2. Ван дер Варден Б.Л. *Алгебра.* – 1979.
3. Айерлэнд К., Роузен М. *Классическое введение в современную теорию чисел.* – 1987.