ЧЕБЫШЕВСКИЙ СБОРНИК

Том 18 Выпуск 2

УДК 512.536.2

DOI 10.22405/2226-8383-2017-18-2-6-17

О КОЛЬЦЕВЫХ СТРУКТУРАХ
НА МНОЖЕСТВЕ ЦЕЛЫХ ЧИСЕЛ

Д. Ю. Артемов (г. Москва)

Аннотация

Хорошо известно, что кольцо целых чисел $\mathbb{Z}$ является E -кольцом, следовательно, на аддитивной группе $\mathbb{Z}$ можно задать единственную (с точностью до изоморфизма) структуру кольца с единицей. Возникает естественный вопрос о единственности структуры кольца с единицей на мультипликативном моноиде $\mathbb{Z}$. В работе показано, что данный вопрос решается отрицательно. Более того, построен и описан метод, позволяющий получать различные кольцевые структуры на мультипликативном моноиде $\mathbb{Z}$ с помощью мультипликативных автоморфизмов. Для мультипликативного моноида $\mathbb{Z}$ введено понятие базиса и доказано, что с точностью до знака не существует базисов, отличных от базиса, состоящего из всех простых чисел, и базисов, получающихся из него путём перестановки элементов. В конце работы приводится пример задания нового кольца на множестве $\mathbb{Z}$ при фиксированном стандартном умножении. Новое сложение на мультипликативном моноиде $\mathbb{Z}$ получается с помощью перестановки простых чисел (в подробно разобранный примере — это перестановка $2 \mapsto 3 \mapsto 5 \mapsto 2$). Из полученных в статье результатов, в частности, следует, что кольцо $\mathbb{Z}$ не является кольцом с однозначным сложением (UA-кольцом).

Ключевые слова: кольцо целых чисел, E -кольцо, аддитивная группа, кольцо с однозначным сложением, мультипликативная полугруппа кольца, моноид.

Библиография: 15 названий.

ABOUT RING STRUCTURES
ON THE SET OF INTEGERS

D. Yu. Artemov (Moscow)

Abstract

It is well known that the ring of integers $\mathbb{Z}$ is an E -ring, therefore it is possible to define unique (up to isomorphism) structure of a ring with identity on the additive group $\mathbb{Z}$. A natural question arises about the uniqueness of the ring structure with identity constructed on a multiplicative monoid $\mathbb{Z}$. It is shown in this paper that this question is solved negatively. Moreover, a method of construction new various ring structures on the multiplicative monoid $\mathbb{Z}$ by dint of multiplicative automorphisms was developed and described. The concept of basis was introduced for the multiplicative monoid $\mathbb{Z}$, and it was shown that there are no bases (up to sign) that are differ to a basis consists of all prime numbers, and bases that are obtain of that basis by a permutations of its elements. The example of construction a new ring structure on the set $\mathbb{Z}$ for fixed standart multiplication is given in the end of this paper. The new addition on the multiplicative monoid $\mathbb{Z}$ is obtained by a permutation of prime numbers (it is $2 \mapsto 3 \mapsto 5 \mapsto 2$ permutation in the detailed example). From the results obtained in the paper it follows in particular, that the ring $\mathbb{Z}$ is not an unique addition ring (UA-ring).

Keywords: ring of integers, E -ring, additive group, unique addition ring, multiplicative semigroup of a ring, monoid.

Bibliography: 15 titles.

1. Введение

Цель данной работы заключается в построении различных кольцевых структур на множестве $\mathbb{Z}$. Все основные понятия и обозначения стандартны и соответствуют [1], [2] и [3]. Под *кольцом* здесь понимается абелева группа, на которой задана вторая бинарная операция, дистрибутивная слева и справа относительно первой.

Напомним, что ассоциативное кольцо R называется E -кольцом, если R коммутативно и $\text{End } R^+ \cong R$. E -кольца были определены Ф. Шульцем в 70-х годах XX века [4], [5], [6]. Этим кольцам посвящено большое количество работ. Во всех книгах по теории абелевых групп, вышедших после 1973 года, имеются разделы, посвященные E -кольцам (см., например [7, глава 4]). Эти кольца интересны нам тем, что на их аддитивных группах возможно задать единственное (с точностью до изоморфизма) ассоциативное кольцо с единицей. В примере 1 без использования теории E -колец показано, что на аддитивной группе кольца $\mathbb{Z}$ возможна единственная структура кольца с единицей.

Рассмотрим произвольную абелеву группу A , записанную аддитивно.

ОПРЕДЕЛЕНИЕ 1 ([2]). *Умножением на группе A мы назовём отображение $\mu: A \times A \rightarrow A$, удовлетворяющее условию: для всех элементов $a, b, c \in A$ выполняются равенства*

$$\begin{aligned}\mu(a, b + c) &= \mu(a, b) + \mu(a, c), \\ \mu(b + c, a) &= \mu(b, a) + \mu(c, a).\end{aligned}$$

ТЕОРЕМА 1 ([2]). *Имеет место изоморфизм:*

$$\text{Mult } A \cong \text{Hom}(A, \text{End } A).$$

ПРИМЕР 1. Выявим структуру группы $\text{Mult } \mathbb{Z}$. Так как $\text{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$, то

$$\text{End } \mathbb{Z} = \text{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$$

и, окончательно, $\text{Mult } \mathbb{Z} \cong \mathbb{Z}$.

Следовательно, $\text{Mult } \mathbb{Z}$ является бесконечной циклической группой. Конкретный изоморфизм $f: \mathbb{Z} \rightarrow \text{Mult } \mathbb{Z}$ можно задать следующим образом. Пусть $1 \xrightarrow{f} \mu$, где μ — обычное умножение целых чисел, тогда для всякого $m \in \mathbb{Z} \setminus \{1\}$ положим $m \xrightarrow{f} m\mu$. Таким образом, любое умножение $\mu \in \text{Mult } \mathbb{Z}$ действует по закону:

$$\forall a, b \in \mathbb{Z} \quad \mu(a, b) = nab$$

для некоторого $n \in \mathbb{Z}$.

Наряду с соответствующей главой в [2] об аддитивных группах колец можно прочитать в более специализированных монографиях Ш. Фейгельстока [8] и Д. Арнольда [9].

Рассмотрим теперь произвольную полугруппу A , записанную мультипликативно.

ОПРЕДЕЛЕНИЕ 2. *Сложением на полугруппе A мы назовём новую бинарную операцию $*$ на A , удовлетворяющую условиям:*

1. $\langle A, * \rangle$ — абелева группа;
2. Операция $\cdot$ дистрибутивна относительно $*$, то есть для любых элементов $a, b, c \in A$ выполняются равенства

$$\begin{aligned}a \cdot (b * c) &= (a \cdot b) * (a \cdot c), \\ (b * c) \cdot a &= (b \cdot a) * (c \cdot a).\end{aligned}$$

Будем говорить, что на мультипликативной полугруппе кольца $\langle R, +, \cdot \rangle$ можно задать новое сложение $*$, если относительно операций $*$ и $\cdot$ множество R образует кольцо, отличное от кольца $\langle R, +, \cdot \rangle$.

Для описания сложений на полугруппе можно использовать следующее

УТВЕРЖДЕНИЕ 1 ([10]). Пусть R и S — кольца. Если существует мультипликативный, но не аддитивный изоморфизм колец $\varphi: R \rightarrow S$, то новое сложение $*$ на мультипликативной полугруппе R можно задать следующим образом:

$$\forall a, b \in R \quad a * b = \varphi^{-1}(\varphi(a) + \varphi(b)).$$

ДОКАЗАТЕЛЬСТВО. Проверим, удовлетворяет ли такое сложение определению 2. Так как аддитивная группа кольца S является абелевой группой, из этого очевидно, что $*$ ассоциативно и коммутативно. Также несложно проверить, что нулём кольца $\langle R, *, \cdot \rangle$ является элемент $e = \varphi^{-1}(0)$.

Теперь выясним, для всякого ли $a \in R$ существует $a' \in R$ такой, что $a * a' = e$.

$$\begin{aligned} a * a' = \varphi^{-1}(\varphi(a) + \varphi(a')) \quad \& \quad a * a' = e \quad \& \quad e = \varphi^{-1}(0) \quad \implies \\ \implies \quad \varphi^{-1}(\varphi(a) + \varphi(a')) = \varphi^{-1}(0) \quad \implies \quad \varphi(a) + \varphi(a') = 0. \end{aligned}$$

Следовательно, $a' = \varphi^{-1}(-\varphi(a))$, где $-\varphi(a)$ — элемент, противоположный элементу $\varphi(a)$ в кольце S .

Проверим теперь дистрибутивность $\cdot$ относительно $*$. Пусть $a, b, c \in R$. Тогда

$$\begin{aligned} a \cdot (b * c) &= a \cdot \varphi^{-1}(\varphi(b) + \varphi(c)) = \varphi^{-1}(\varphi(a)) \cdot \varphi^{-1}(\varphi(b) + \varphi(c)) = \\ &= \varphi^{-1}(\varphi(a) \cdot (\varphi(b) + \varphi(c))) = \varphi^{-1}(\varphi(a) \cdot \varphi(b) + \varphi(a) \cdot \varphi(c)) = \\ &= \varphi^{-1}(\varphi(a \cdot b) + \varphi(a \cdot c)) = (a \cdot b) * (a \cdot c), \\ (b * c) \cdot a &= \varphi^{-1}(\varphi(b) + \varphi(c)) \cdot a = \varphi^{-1}(\varphi(b) + \varphi(c)) \cdot \varphi^{-1}(\varphi(a)) = \\ &= \varphi^{-1}((\varphi(b) + \varphi(c)) \cdot \varphi(a)) = \varphi^{-1}(\varphi(b) \cdot \varphi(a) + \varphi(c) \cdot \varphi(a)) = \\ &= \varphi^{-1}(\varphi(b \cdot a) + \varphi(c \cdot a)) = (b \cdot a) * (c \cdot a). \end{aligned}$$

□

СЛЕДСТВИЕ 1. На мультипликативной полугруппе кольца $\langle R, +, \cdot \rangle$ можно задать новое сложение $*$ тогда и только тогда, когда существует мультипликативный, но не аддитивный автоморфизм кольца R .

Кольцо R называется *кольцом с однозначным сложением* (УА-кольцом), если на его мультипликативной полугруппе $\langle R, \cdot \rangle$ можно задать единственную бинарную операцию $+$, превращающую её в кольцо $\langle R, +, \cdot \rangle$.

Из теоремы Стефенсона следует, что кольцо R является УА-кольцом тогда и только тогда, когда любой мультипликативный изоморфизм колец $\varphi: R \rightarrow S$ (то есть изоморфизм их мультипликативных полугрупп) является изоморфизмом колец.

УА-кольцам посвящено множество работ. Они были введены ещё в 1969 г. в [10]. Наиболее подробно УА-кольца разобраны в [12]. В настоящее время теория УА-колец активно используется в теории абелевых групп и модулей (см., например, [13], [14], [15] и др.).

Кольцо $\mathbb{Z}$ не является УА-кольцом. Это вытекает, например, из того, что у колец $\mathbb{Z}$ и $\mathbb{Z}[x]$ изоморфны их мультипликативные полугруппы.

2. Кольцевые структуры на мультипликативном моноиде $\mathbb{Z}$

Рассмотрим кольцо $\mathbb{Z}$. Пусть ξ — мультипликативный, но не аддитивный автоморфизм кольца $\mathbb{Z}$. Тогда новое сложение $*$ на мультипликативной полугруппе кольца $\mathbb{Z}$, согласно следствию 1, можно задать следующим образом:

$$\forall a, b \in \mathbb{Z} \quad a * b = \xi^{-1}(\xi(a) + \xi(b)).$$

Оно задано корректно, но неконструктивно, поскольку неясно, как устроены мультипликативные автоморфизмы кольца $\mathbb{Z}$. Для их описания докажем серию вспомогательных утверждений.

Обозначим через $\mathcal{N}$ прямую сумму моноидов

$$\bigoplus_{\aleph_0} \mathbb{N}_0,$$

где $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ — множество целых неотрицательных чисел. $\mathcal{N}$ есть коммутативная полугруппа с нулём $\theta_{\mathcal{N}} = (0, 0, \dots)$. Обозначим через $\mathcal{Z}'$ полугруппу $\mathbb{Z}_2 \oplus \mathcal{N}$. Дополним множество $\mathcal{Z}'$ до множества $\mathcal{Z} = \mathcal{Z}' \cup \{e\}$, где e — внешний аннулятор, то есть такой элемент, что выполняется условие:

$$\forall a \in \mathcal{Z} \quad a + e = e + a = e.$$

Ясно, что $\mathcal{Z}$ — коммутативная полугруппа с нулём $\theta_{\mathcal{Z}} = (\bar{0}, 0, 0, \dots)$ и что все элементы $\mathcal{Z}'$ содержат лишь конечное число ненулевых координат.

ЛЕММА 1. *Рассмотренный выше моноид $\mathcal{Z}$ и мультипликативный моноид $\mathbb{Z}$ изоморфны.*

ДОКАЗАТЕЛЬСТВО. Пусть $\lambda p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ — каноническое разложение некоторого числа $m \in \mathbb{Z}$, отличного от нуля, где $\lambda = \text{sign}(m)$ и $p_i < p_{i+1}$ ($i \in \{1, 2, \dots, s-1\}$). Поставим в соответствие числу m элемент $(\varepsilon, k_1, k_2, \dots, k_s, 0, \dots) \in \mathcal{Z}'$, причём $\varepsilon = \bar{0}$, если $\lambda = 1$, и $\varepsilon = \bar{1}$, если $\lambda = -1$. Числу 0 поставим в соответствие внешний аннулятор $e \in \mathcal{Z}$. Несложно проверить, что отображение $\varphi: \mathbb{Z} \rightarrow \mathcal{Z}$, заданное таким образом, — искомый изоморфизм. $\square$

В силу доказанного изоморфизма мы получили возможность описания мультипликативных автоморфизмов кольца $\mathbb{Z}$ с помощью моноида $\mathcal{Z}$. Будем в дальнейшем отождествлять элемент b прямого слагаемого $\mathbb{Z}_2$ с элементом моноида $\mathcal{Z}'$ вида $(b, 0, \dots)$, а элемент $c = (c_1, c_2, \dots, c_k, 0, \dots)$ прямого слагаемого $\mathcal{N}$ — с элементом моноида $\mathcal{Z}'$ вида

$$(\bar{0}, c_1, c_2, \dots, c_k, 0, \dots).$$

ЗАМЕЧАНИЕ 1. Рассмотрим произвольный автоморфизм η моноида $\mathcal{Z}$. Покажем, что $\eta(e) = e$. Действительно, предположив противное и зафиксировав произвольный ненулевой элемент $d \in \mathcal{Z}'$, получим:

$$\eta(e) = \eta(e + d) = \eta(e) + \eta(d) \implies \eta(d) = \theta_{\mathcal{Z}},$$

то есть автоморфизм η ненулевой элемент $d \in \mathcal{Z}'$ перевёл в нуль, чего быть не может.

Далее, так как структура $\mathcal{Z}'$ есть прямая сумма моноидов, то

$$\forall a \in \mathcal{Z}' \quad \exists! b \in \mathbb{Z}_2 \quad \exists! c \in \mathcal{N} \quad a = b + c.$$

Тогда

$$\eta(a) = \eta(b + c) = \eta(b) + \eta(c).$$

Так как единственным автоморфизмом прямого слагаемого $\mathbb{Z}_2$ является тождественное отображение $\text{id}_{\mathbb{Z}_2}$ и $\eta(\mathbb{Z}_2) \subseteq \mathbb{Z}_2$, то

$$\eta(a) = b + \eta(c),$$

и задача описания автоморфизмов моноида $\mathcal{Z}$ сводится к задаче описания автоморфизмов моноида $\mathcal{N}$.

ОПРЕДЕЛЕНИЕ 3. Будем говорить, что совокупность элементов $B = \{b_i\}_{i \in \mathbb{N}} \subseteq \mathcal{N}$ линейно независима, если для любых $b_{i_1}, \dots, b_{i_k} \in B$ из равенства

$$\lambda_1 b_{i_1} + \dots + \lambda_k b_{i_k} = \theta_{\mathcal{N}},$$

где $\lambda_j \in \mathbb{N}_0$, следует $\lambda_1 = \lambda_2 = \dots = \lambda_k = 0$.

ОПРЕДЕЛЕНИЕ 4. Будем называть совокупность элементов $B = \{b_i\}_{i \in \mathbb{N}} \subseteq \mathcal{N}$ базисом моноида $\mathcal{N}$, если она линейно независима и любой элемент $\mathcal{N}$ линейно выражается через элементы этой совокупности с коэффициентами из множества $\mathbb{N}_0$ с точностью до порядка следования и слагаемых с нулевыми коэффициентами.

ПРИМЕР 2. Совокупность элементов $E = \{e_i\}_{i \in \mathbb{N}}$, где

$$e_1 = (1, 0, 0, 0, \dots), \quad e_2 = (0, 1, 0, 0, \dots), \quad e_3 = (0, 0, 1, 0, \dots), \quad \dots,$$

является базисом моноида $\mathcal{N}$.

Совокупность $F = \{f_i\}_{i \in \mathbb{N}}$, где

$$f_1 = e_2, \quad f_2 = e_1, \quad f_j = e_j \quad (j = 3, 4, \dots),$$

также образует базис моноида $\mathcal{N}$.

УТВЕРЖДЕНИЕ 2. Отображение $\xi: F \rightarrow G$, где $F = \{f_i\}_{i \in \mathbb{N}}$ — базис моноида $\mathcal{N}$, а $G = \{g_i\}_{i \in \mathbb{N}}$ — произвольные элементы моноида $\mathcal{N}$, единственным образом продолжается до эндоморфизма моноида $\mathcal{N}$.

ДОКАЗАТЕЛЬСТВО. Зафиксируем произвольный элемент $c \in \mathcal{N}$, тогда

$$c = \sum_{i=1}^k \gamma_i f_i,$$

где $\gamma_i \in \mathbb{N}_0$. Положим по определению

$$\xi(c) = \sum_{i=1}^k \gamma_i \xi(f_i) = \sum_{i=1}^k \gamma_i g_i.$$

Проверим, что ξ — эндоморфизм. Корректность вытекает из того, что разложение элементов моноида $\mathcal{N}$ по базису F единственно, что следует из определения 4. Проверим сохранение операции, пусть

$$a = \sum_{i=1}^k \alpha_i f_i \in \mathcal{N}, \quad b = \sum_{i=1}^m \beta_i f_i \in \mathcal{N},$$

где $\alpha_i, \beta_i \in \mathbb{N}_0$. Без потери общности можно считать, что $k = m$. Тогда

$$\xi(a + b) = \xi\left(\sum_{i=1}^k \alpha_i f_i + \sum_{i=1}^k \beta_i f_i\right) = \sum_{i=1}^k (\alpha_i + \beta_i) g_i = \xi(a) + \xi(b).$$

Докажем теперь, что такой эндоморфизм единственен. Пусть η — эндоморфизм моноида $\mathcal{N}$ такой, что

$$\forall f_i \in F \quad \eta(f_i) = \xi(f_i).$$

Покажем, что $\eta = \xi$. Действительно, если

$$c = \sum_{i=1}^k \gamma_i f_i \in \mathcal{N},$$

где $\gamma_i \in \mathbb{N}_0$, то

$$\eta(c) = \eta\left(\sum_{i=1}^k \gamma_i f_i\right) = \sum_{i=1}^k \gamma_i \eta(f_i) = \sum_{i=1}^k \gamma_i \xi(f_i) = \sum_{i=1}^k \gamma_i g_i = \xi(c).$$

Получили, что η и ξ действуют одинаково. $\square$

СЛЕДСТВИЕ 2. Эндоморфизм ξ из утверждения 2 является автоморфизмом в том и только в том случае, когда совокупность элементов G является базисом.

ДОКАЗАТЕЛЬСТВО. В самом деле, если ξ — автоморфизм моноида $\mathcal{N}$, то существует автоморфизм ξ^{-1} моноида $\mathcal{N}$ такой, что

$$\xi^{-1} \circ \xi = \xi \circ \xi^{-1} = \text{id}_{\mathcal{N}}.$$

Несложно проверить, что совокупность элементов G линейно независима. Пусть $c \in \mathcal{N}$, для него существует элемент $\tilde{c} = \xi^{-1}(c)$ такой, что

$$\tilde{c} = \sum_{i=1}^k \gamma_i f_i \implies \xi(\tilde{c}) = \sum_{i=1}^k \gamma_i g_i,$$

где $\gamma_i \in \mathbb{N}_0$. Последнее равенство равносильно тому, что элемент $\xi(\tilde{c}) = c$ линейно выражается через элементы совокупности G с коэффициентами из $\mathbb{N}_0$.

Обратно, если совокупность элементов G образует базис, то по предыдущему утверждению существует отображение $\eta: G \rightarrow F$, которое единственным образом продолжается до эндоморфизма. Несложно видеть, что

$$\eta \circ \xi = \xi \circ \eta = \text{id}_{\mathcal{N}}.$$

Следовательно, ξ — автоморфизм моноида $\mathcal{N}$. $\square$

Тогда новое сложение $*$ на мультипликативном моноиде $\mathbb{Z}$, согласно следствию 1, утверждению 2 и лемме 1, можно задать следующим образом:

$$\forall a, b \in \mathbb{Z} \quad a * b = (\varphi^{-1} \circ \xi^{-1} \circ \varphi)((\varphi^{-1} \circ \xi \circ \varphi)(a) + (\varphi^{-1} \circ \xi \circ \varphi)(b)),$$

где φ — изоморфизм моноидов $\mathbb{Z}$ и $\mathcal{Z}$ из леммы 1, а ξ — автоморфизм моноида $\mathcal{N}$ из утверждения 2, который мы можем отождествлять с автоморфизмом моноида $\mathcal{Z}$ в силу замечания 1. Обозначив композицию $\varphi^{-1} \circ \xi \circ \varphi$ через ψ , получим:

$$a * b = \psi^{-1}(\psi(a) + \psi(b)).$$

УТВЕРЖДЕНИЕ 3. В $\mathcal{N}$ не существует базисов, отличных от базиса E , и базисов, получающихся из E путём перестановки элементов, где E — базис из примера 2.

ДОКАЗАТЕЛЬСТВО. Там, где это будет необходимо, под соответствующими координатами элементов $\mathcal{N}$ будут подписаны их порядковые номера.

Пусть $F = \{f_i\}_{i \in \mathbb{N}}$ — произвольный базис моноида $\mathcal{N}$ такой, что

$$f_i = (a_i^1, a_i^2, \dots).$$

Рассмотрим элемент $e_j = (0, 0, \dots, 0, 1, 0, \dots) \in E$. Для него

$$\exists \beta_1, \beta_2, \dots, \beta_n \in \mathbb{N}_0 \quad e_j = \beta_1 f_1 + \beta_2 f_2 + \dots + \beta_n f_n,$$

то есть

$$e_j = \beta_1 (a_1^1, a_1^2, \dots) + \beta_2 (a_2^1, a_2^2, \dots) + \dots + \beta_n (a_n^1, a_n^2, \dots).$$

Хотя бы один коэффициент β_i ($1 \leq i \leq n$) отличен от нуля, иначе $e_j = \theta_{\mathcal{N}}$, чего быть не может. Пусть $\beta_k \neq 0$ ($1 \leq k \leq n$).

Перейдём к системе уравнений, соответствующей данному разложению. В этой системе есть ровно одно уравнение вида

$$1 = \beta_1 a_1^j + \beta_2 a_2^j + \dots + \beta_n a_n^j, \quad (1)$$

где j фиксировано и является порядковым номером элемента e_j в базисе E , и бесконечно много уравнений вида

$$0 = \beta_1 a_1^i + \beta_2 a_2^i + \dots + \beta_n a_n^i, \quad (2)$$

где i пробегает всё множество $\mathbb{N} \setminus \{j\}$.

Известно, что все $f_i \in \mathcal{N}$, поэтому $a_i^j \in \mathbb{N}_0$. Далее, так как $\beta_i \in \mathbb{N}_0$ и множество $\mathbb{N}_0$ замкнуто относительно умножения, то $\beta_i a_i^j \in \mathbb{N}_0$.

Рассмотрим произвольное уравнение системы, имеющее вид (2). Имеется сумма целых неотрицательных чисел, равная нулю. Тогда

$$\beta_1 a_1^i = \beta_2 a_2^i = \dots = \beta_n a_n^i = 0.$$

Следовательно, так как $\beta_k a_k^i = 0$ и $\beta_k \neq 0$, то $a_k^i = 0$. Уравнение вида (2) выбиралось произвольное, поэтому при условии $\beta_k \neq 0$ получаем, что все a_k^i ($i \in \mathbb{N} \setminus \{j\}$) равны нулю и $f_k = (0, 0, \dots, 0, a_k^j, 0, \dots)$.

Рассмотрим теперь уравнение системы, имеющее вид (1). Это сумма целых неотрицательных чисел, равная единице. Тогда

$$\beta_k a_k^j = 1 - \left(\beta_1 a_1^j + \beta_2 a_2^j + \dots + \beta_{k-1} a_{k-1}^j + \beta_{k+1} a_{k+1}^j + \dots + \beta_n a_n^j \right).$$

Обозначим сумму, стоящую в скобках, через δ . В силу того, что множество $\mathbb{N}_0$ замкнуто относительно сложения, получаем, что δ неотрицательно. Так как $\beta_k a_k^j \in \mathbb{N}_0$, то $\beta_k a_k^j = 0$ или

$$\exists m \in \mathbb{N}_0 \quad \beta_k a_k^j = m + 1.$$

Если $\beta_k a_k^j = 0$, то, так как $\beta_k \neq 0$, получаем $a_k^j = 0$ и $f_k = \theta_{\mathcal{N}} \in F$, что противоречит линейной независимости системы F . Значит, имеет место второй случай, и существует $m \in \mathbb{N}_0$ такое, что

$$\beta_k a_k^j = m + 1 \iff 1 - \delta = m + 1 \iff \delta = -m.$$

Так как $m \in \mathbb{N}_0$, то $m \geq 0$, и $-m \leq 0$. Следовательно, δ неположительно, однако выше было установлено, что δ неотрицательно. Таким образом, $\delta = 0$.

Вернувшись к исходному уравнению, получим:

$$1 = \beta_k a_k^j + \delta \iff 1 = \beta_k a_k^j + 0 \iff 1 = \beta_k a_k^j.$$

Коэффициент β_k отличен от нуля, поэтому $a_k^j = \frac{1}{\beta_k}$, и так как $a_k^j \in \mathbb{N}_0$, то $\beta_k = a_k^j = 1$ и, таким образом, $f_k = (0, 0, \dots, \underset{j-1}{0}, \underset{j}{1}, \underset{j+1}{0}, \dots) = e_j$.

Элемент $e_j \in E$ выбирался произвольно, следовательно, доказано утверждение:

$$\forall e_i \in E \quad \exists f_j \in F \quad f_j = e_i,$$

из чего следует требуемое. $\square$

Заметим, что из утверждения 3 и следствия 2 немедленно следует факт, состоящий в том, что не существует автоморфизмов моноида $\mathcal{N}$, отличных от тождественного автоморфизма $\text{id}_{\mathcal{N}}$ и автоморфизмов, порождённых перестановкой элементов базиса E .

Таким образом, в силу изоморфизма $\mathcal{Z} \cong \mathbb{Z}$ можно строить новые сложения непосредственно на мультипликативном моноиде $\mathbb{Z}$, взяв в качестве базиса множество P всех простых чисел. Из замечания 1 следует, что любой автоморфизм мультипликативного моноида $\mathbb{Z}$ сохраняет знак числа и ноль переводит в ноль. Поэтому автоморфизмы мультипликативного моноида $\mathbb{Z}$ и, как следствие, новые сложения на нём можно строить путём перестановки элементов базиса P .

3. Описание автоморфизмов моноида $\mathcal{N}$ с помощью матриц

Пусть $F = \{f_i\}_{i \in \mathbb{N}}$ — базис моноида $\mathcal{N}$, а $G = \{g_i\}_{i \in \mathbb{N}}$ — произвольные элементы моноида $\mathcal{N}$. Выясним, как можно конструктивно описать автоморфизмы $\mathcal{N}$. Поставим в соответствие каждому эндоморфизму моноида $\mathcal{N}$ матрицу размера $\aleph_0 \times \aleph_0$ с элементами из множества $\mathbb{N}_0$. Пусть эндоморфизм ξ из утверждения 2 порождается отображением $\xi: F \rightarrow G$ и

$$g_i = \sum_{j=1}^{k_i} a_i^j f_j,$$

тогда матрица M_ξ , поставленная в соответствие данному эндоморфизму ξ , примет вид:

$$M_\xi = \begin{pmatrix} a_i^1 & a_i^2 & \dots & a_i^{k_i} & 0 & \dots \end{pmatrix},$$

где $i \in \mathbb{N}$, то есть в i -той строке матрицы записаны коэффициенты разложения элемента g_i по базису F . Такая матрица *конечнострочна*, то есть в каждой её строке содержится лишь конечное число ненулевых элементов.

Обозначим через $\mathcal{M}$ множество конечнострочных матриц размера $\aleph_0 \times \aleph_0$ над $\mathbb{N}_0$. Зададим на $\mathcal{M}$ сложение и умножение, аналогичное обычному сложению и умножению матриц. Произведение двух матриц $M, N \in \mathcal{M}$ определено корректно, так как M и N конечнострочны. Нетрудно также убедиться в том, что $\langle \mathcal{M}, + \rangle$ — коммутативная полугруппа с нулём (нулевой матрицей Θ), а $\langle \mathcal{M}, \cdot \rangle$ — полугруппа с единицей (единичной матрицей E). Умножение дистрибутивно слева и справа относительно сложения, и выполняется мультипликативное свойство нуля: для всякой матрицы $M \in \mathcal{M}$ верно $\Theta \cdot M = M \cdot \Theta = \Theta$.

Таким образом, построенное множество $\mathcal{M}$ относительно операций обычного сложения и обычного умножения матриц образует полукольцо.

Обозначим через $M(a)$ координатный столбец элемента $a \in \mathcal{N}$, а через $M(\xi(a))$ — координатный столбец элемента $\xi(a)$ в базисе E из примера 2. Тогда по построению ясно, что

$$M(\xi(a)) = M_\xi^T \cdot M(a).$$

УТВЕРЖДЕНИЕ 4. *Эндоморфизм ξ моноида $\mathcal{N}$ является автоморфизмом в том и только в том случае, когда матрица, соответствующая ему, обратима в $\mathcal{M}$.*

ДОКАЗАТЕЛЬСТВО. Пусть эндоморфизм ξ является автоморфизмом. Зафиксируем произвольный элемент $a \in \mathcal{N}$, тогда

$$M(\xi(a)) = M_\xi^T \cdot M(a).$$

Так как ξ — автоморфизм, то у отображения ξ есть обратное отображение ξ^{-1} , также являющееся автоморфизмом, и $(\xi^{-1} \circ \xi)(a) = a$. Поставим в соответствие автоморфизму ξ^{-1} некоторую матрицу B по тому же правилу. На матричном языке последнее соотношение означает следующее:

$$M(a) = B^T \cdot M(\xi(a)).$$

Тогда $M(a) = B^T \cdot M_\xi^T \cdot M(a)$, то есть

$$B^T \cdot M_\xi^T = E \iff (M_\xi \cdot B)^T = E \iff M_\xi \cdot B = E.$$

Получили, что B является правой обратной к M_ξ . Аналогично проверяется, что B является левой обратной к M_ξ . Таким образом, M_ξ обратима в $\mathcal{M}$.

Обратно, пусть матрица, соответствующая эндоморфизму ξ , обратима в $\mathcal{M}$. Тогда существует матрица $M_\xi^{-1} \in \mathcal{M}$ такая, что $M_\xi^{-1} \cdot M_\xi = M_\xi \cdot M_\xi^{-1} = E$. Зафиксируем произвольный элемент $a \in \mathcal{N}$, тогда

$$M(\xi(a)) = M_\xi^T \cdot M(a).$$

Домножим левую и правую части последнего равенства на $(M_\xi^{-1})^T$ слева, получим:

$$\begin{aligned} (M_\xi^{-1})^T \cdot M(\xi(a)) &= (M_\xi^{-1})^T \cdot M_\xi^T \cdot M(a) \iff \\ &\iff (M_\xi^{-1})^T \cdot M(\xi(a)) = (M_\xi \cdot M_\xi^{-1})^T \cdot M(a) \iff \\ &\iff (M_\xi^{-1})^T \cdot M(\xi(a)) = M(a), \end{aligned}$$

то есть мы выразили координатный столбец элемента a через координатный столбец его образа $\xi(a)$ и обратную матрицу M_ξ^{-1} . Это в точности означает, что для эндоморфизма ξ существует обратное отображение, из чего, в свою очередь, следует, что эндоморфизм биективен, а значит, является автоморфизмом. $\square$

ЗАМЕЧАНИЕ 2. В силу утверждения 3, матрица всякого автоморфизма моноида $\mathcal{N}$ есть бинарная матрица, в каждой строке и каждом столбце которой содержится ровно одна единица, из чего следует, что она ортогональна. Данный факт позволяет довольно легко вычислять обратные матрицы: для всякого автоморфизма ξ моноида $\mathcal{N}$ справедливо равенство

$$M_\xi^{-1} = M_\xi^T.$$

4. Пример нового сложения на мультипликативном моноиде $\mathbb{Z}$

ПРИМЕР 3. Пусть автоморфизм ξ моноида $\mathcal{N}$ порождается перестановкой элементов базиса E такой, что

$$e_1 \xrightarrow{\xi} e_2, \quad e_2 \xrightarrow{\xi} e_3, \quad e_3 \xrightarrow{\xi} e_1, \quad e_j \xrightarrow{\xi} e_j \quad (j = 4, 5, \dots),$$

и пусть $a = 18 \in \mathbb{Z}$, $b = -21 \in \mathbb{Z}$. Выясним, чему равно $a * b$. Как было сказано выше, в силу замечания 1 можно отождествлять автоморфизм моноида $\mathcal{N}$ с автоморфизмом моноида $\mathcal{Z}$. Имеем:

$$\begin{aligned} a &= 2^1 \cdot 3^2 \xrightarrow{\varphi} (\bar{0}, 1, 2, 0, \dots) \xrightarrow{\xi} (\bar{0}, 0, 1, 2, 0, \dots) \xrightarrow{\varphi^{-1}} 3^1 \cdot 5^2 = 75, \\ b &= -3^1 \cdot 7^1 \xrightarrow{\varphi} (\bar{1}, 0, 1, 0, 1, 0, \dots) \xrightarrow{\xi} (\bar{1}, 0, 0, 1, 1, 0, \dots) \xrightarrow{\varphi^{-1}} -5^1 \cdot 7^1 = -35, \\ \psi(a) + \psi(b) &= 75 + (-35) = 40, \\ 40 &= 2^3 \cdot 5^1 \xrightarrow{\varphi} (\bar{0}, 3, 0, 1, 0, \dots) \xrightarrow{\xi^{-1}} (\bar{0}, 0, 1, 3, 0, \dots) \xrightarrow{\varphi^{-1}} 3^1 \cdot 5^3 = 375, \end{aligned}$$

то есть при новом сложении сумма $18 * (-21)$ равна 375. На языке целых чисел работа нового сложения $*$ выглядит следующим образом:

$$\begin{aligned} a &= 2^1 \cdot 3^2 \xrightarrow{\psi} 3^1 \cdot 5^2 = 75, \\ b &= -3^1 \cdot 7^1 \xrightarrow{\psi} -5^1 \cdot 7^1 = -35, \\ \psi(a) + \psi(b) &= 75 + (-35) = 40, \\ 40 &= 2^3 \cdot 5^1 \xrightarrow{\psi^{-1}} 3^1 \cdot 5^3 = 375. \end{aligned}$$

Теперь воспользуемся разработанным матричным описанием автоморфизмов. Вычислим, к примеру, $M((\xi \circ \varphi)(a))$ через матрицу автоморфизма M_ξ , которая имеет вид

$$M_\xi = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Имеем:

$$M((\xi \circ \varphi)(a)) = M_\xi^T \cdot M(\varphi(a)) = \begin{pmatrix} 0 & 0 & 1 & 0 & \dots \\ 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \\ \vdots \end{pmatrix},$$

и, в самом деле,

$$(\xi \circ \varphi)(a) = 0 \cdot e_1 + 1 \cdot e_2 + 2 \cdot e_3 + 0 \cdot e_4 + \dots = (\bar{0}, 0, 1, 2, 0, \dots).$$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Fuchs L. Infinite Abelian Groups. Vol. 1. New York–London: Academic Press, 1970.
2. Fuchs L. Infinite Abelian Groups. Vol. 2. New York–London: Academic Press, 1973.
3. Курош А.Г. Общая алгебра. М.: Наука, 1974.
4. Schultz P. Periodic homomorphism sequences of abelian groups // Arch. Math. 1970. Vol. 21. P. 132-135.

5. Schultz P. The endomorphism ring of the additive group of a ring // J. Austral. Math. Soc. 1973. Vol. 15. P. 60-69.
6. Bowshell R. A., Schultz P. Unital rings whose additive endomorphisms commute // Math. Ann. 1977. Vol. 228, №3. P. 197-214.
7. Крылов П. А., Михалев А. В., Туганбаев А. А. Абелевы группы и их кольца эндоморфизмов. М.: Факториал Пресс, 2006.
8. Feigelstock S. Additive groups of rings. Pitman advanced publishing program, London, 1983.
9. Arnold D. M. Finite rank torsion free abelian groups and rings. Lecture Notes in Math. Vol. 931. Springer, New York, 1982.
10. Stephenson W. Unique addition rings // Canad. J. Math. 1969. Vol. 21, №6. P. 1455-1461.
11. Nelius Chr.-F. Ring emit eindentiger Addition. Padeborn, 1974.
12. Михалев А. В. Мультипликативная классификация ассоциативных колец // Мат. сб. 1988. Том 135(177), №2. С. 210–224.
13. van der Merwe B. Unique addition modules // Communications in algebra. 1999. Vol. 27(9). P. 4103–4115.
14. Чистяков Д. С., Любимцев О. В. Об абелевых группах без кручения с UA-кольцом эндоморфизмов // Вестн. Томск. гос. ун-та. Матем. и мех. 2011. № 2(14). P. 55–58.
15. Любимцев О. В., Чистяков Д. С. Абелевы группы как UA-модули над кольцом $\mathbb{Z}$ // Матем. заметки. 2010. Том 87, №3. С. 412–416.

REFERENCES

1. Fuchs, L. 1970, "Infinite Abelian Groups vol. 1, New York–London: Academic Press.
2. Fuchs, L. 1973, "Infinite Abelian Groups vol. 2, New York–London: Academic Press.
3. Kurosh, A. G. 1974, "General Algebra Moscow, Nauka (russian).
4. Schultz, P. 1970, "Periodic homomorphism sequences of abelian groups *Arch. Math.*, vol. 21, pp. 132-135.
5. Schultz, P. 1973, "The endomorphism ring of the additive group of a ring" *J. Austral. Math. Soc.*, vol. 15. pp. 60-69.
6. Bowshell, R. A. & Schultz, P. 1977, "Unital rings whose additive endomorphisms commute *Math. Ann.*, vol. 228, no. 3, pp. 197-214
7. Krylov, P. A., Mikhalev, A. V. & Tuganbaev, A. A. 2013, "Endomorphism rings of Abelian groups vol. 2, Springer Science & Business Media.
8. Feigelstock, S. 1983, "Additive groups of rings Pitman advanced publishing program, London.
9. Arnold, D. M. 1982, "Finite rank torsion free abelian groups and rings Lecture Notes in Math, vol. 931, Springer, New York.
10. Stephenson, W. 1969, "Unique addition rings *Canad. J. Math.*, vol. 21, no. 6, pp. 1455-1461.

11. Nelius, Chr.-F. 1974, "Ring emit eindentiger Addition Padeborn, 1974.
12. Mikhalev, A. V. 1989, "Multiplicative classification of associative rings *Mathematics of the USSR-Sbornik*, vol. 63, no. 1, pp. 205-218.
13. van der Merwe, B. 1999. "Unique addition modules *Communications in algebra*, vol. 27, no. 9, pp. 4103-4115.
14. Chistyakov D. S. & Lyubimtsev O. V. 2011, "On abelian torsion free with UA-endomorphism rings *Vestnik TGU*, no. 2(14), pp. 55-58.
15. Chistyakov D. S. & Lyubimtsev O. V. 2010, "Abelian groups as UA-modules over the ring $\mathbb{Z}$ *Mathematical Notes*, vol. 87, no. 3, pp. 380-383.

Получено 4.02.2017 г.

Принято в печать 14.06.2017 г.