ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.541, 512.552, 512.711

О ДВУХ ОПРЕДЕЛЕНИЯХ СТЕПЕНИ ФУНКЦИИ НАД АССОЦИАТИВНЫМ КОММУТАТИВНЫМ КОЛЬЦОМ[1]

М. И. Анохин

Институт проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова, г. Москва, Россия

Пусть R — ассоциативное коммутативное кольцо и $\varphi\colon R^m \to R$, где $m \geqslant 0$. Обозначим через $\deg_{\Pi}\varphi$ наименьшее число $n \geqslant -1$, такое, что φ представима многочленом степени n от m переменных над R. (Степенью нулевого многочлена считаем -1.) Пусть также $\deg_{\mathrm{RM}}\varphi$ обозначает наименьшее число $n \geqslant -1$, такое, что $\partial_{v_1}\dots\partial_{v_{n+1}}\varphi = 0$ для всех $v_1,\dots,v_{n+1} \in R^m$. Здесь $(\partial_v\psi)(x) = \psi(x+v) - \psi(x)$ для любых $v, x \in R^m$ и любой функции $\psi\colon R^m \to R$. Если такого числа n не существует, то полагаем соответственно $\deg_{\Pi}\varphi = \infty$ или $\deg_{\mathrm{RM}}\varphi = \infty$. В работе рассматривается проблема характеризации класса $\mathfrak{D}$ всех ассоциативных коммутативных колец R, таких, что эти степени совпадают для функций над R, т. е. $\deg_{\Pi}\varphi = \deg_{\mathrm{RM}}\varphi$ для всех $m \geqslant 0$ и всех функций $\varphi\colon R^m \to R$. Проблема решается в случае, когда аддитивная группа $\mathcal{R}$ кольца R принадлежит некоторым широким классам абелевых групп. Основные результаты: 1) если $\mathcal{R}$ периодична или конечно порождена, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}/d\mathbb{Z}$ для некоторого свободного от квадратов числа $d \geqslant 1$; 2) если $\mathcal{R}$ не редуцирована, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong (\mathbb{Z}/d\mathbb{Z}) \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \geqslant 1$; 3) если $\mathcal{R}$ является прямой суммой подгрупп ранга 1, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}/d\mathbb{Z}$ или $R \cong (\mathbb{Z}/d\mathbb{Z}) \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \geqslant 1$; 4) если $\mathcal{R}$ редуцирована и копериодична, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \prod\limits_{p\in P}(\mathbb{Z}/p\mathbb{Z})$ для некоторого множества P простых чисел. Доказательство этих результатов основано на том факте, что любое кольцо из $\mathfrak{D}$ является E-кольцом.

Ключевые слова: *ассоциативное кольцо, коммутативное кольцо, абелева группа, аддитивная группа кольца, многочлен, степень функции, E-кольцо, формула Ньютона.*

DOI 10.17223/20710410/37/1

[1]Работа поддержана грантом РФФИ № 16-01-00226.

ON THE TWO DEFINITIONS OF DEGREE OF A FUNCTION OVER AN ASSOCIATIVE, COMMUTATIVE RING

M. I. Anokhin

Information Security Institute of Lomonosov University, Moscow, Russia

E-mail: anokhin@mccme.ru

Let R be an associative, commutative ring and let $\varphi\colon R^m \to R$, where $m \geqslant 0$. Denote by $\deg_\Pi \varphi$ the smallest integer $n \geqslant -1$ such that φ can be represented by an m-variate polynomial of degree n over R. (By convention, the degree of the zero polynomial is -1.) Also, let $\deg_{\mathrm{RM}} \varphi$ denote the smallest integer $n \geqslant -1$ such that $\partial_{v_1} \dots \partial_{v_{n+1}} \varphi = 0$ for all $v_1, \dots, v_{n+1} \in R^m$. Here $(\partial_v \psi)(x) = \psi(x+v) - \psi(x)$ for any $v, x \in R^m$ and any function $\psi\colon R^m \to R$. If no such integer n exists, then we put $\deg_\Pi \varphi = \infty$ or $\deg_{\mathrm{RM}} \varphi = \infty$, respectively. In this paper, we study the problem of characterizing the class $\mathfrak{D}$ of all associative, commutative rings R such that these degrees coincide for functions over R, i.e., $\deg_\Pi \varphi = \deg_{\mathrm{RM}} \varphi$ for all $m \geqslant 0$ and all functions $\varphi\colon R^m \to R$. We solve this problem when the additive group $\mathcal{R}$ of the ring R belongs to some large classes of abelian groups. Namely, our main results are as follows: 1) if $\mathcal{R}$ is torsion or finitely generated, then $R \in \mathfrak{D}$ if and only if $R \cong \mathbb{Z}/d\mathbb{Z}$ for some square-free integer $d \geqslant 1$; 2) if $\mathcal{R}$ is not reduced, then $R \in \mathfrak{D}$ if and only if $R \cong (\mathbb{Z}/d\mathbb{Z}) \oplus \mathbb{Q}$ for some square-free integer $d \geqslant 1$; 3) if $\mathcal{R}$ is a direct sum of rank 1 subgroups, then $R \in \mathfrak{D}$ if and only if $R \cong \mathbb{Z}/d\mathbb{Z}$ or $R \cong (\mathbb{Z}/d\mathbb{Z}) \oplus \mathbb{Q}$ for some square-free integer $d \geqslant 1$; 4) if $\mathcal{R}$ is reduced and cotorsion, then $R \in \mathfrak{D}$ if and only if $R \cong \prod\limits_{p \in P} (\mathbb{Z}/p\mathbb{Z})$ for some set P of prime numbers. The proof of these results is based on the fact that any ring in $\mathfrak{D}$ is an E-ring.

Keywords: *associative ring, commutative ring, Abelian group, additive group of a ring, polynomial, degree of a function, E-ring, Newton's formula.*

Введение

В настоящей работе аддитивная группа произвольного кольца обозначается рукописным вариантом буквы, обозначающей это кольцо. Например, $\mathcal{Q}$, $\mathcal{Z}$ и $\mathcal{Z}_n$ (где n — целое положительное число) — это аддитивные группы поля $\mathbb{Q}$ рациональных чисел, кольца $\mathbb{Z}$ целых чисел и кольца $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ соответственно. Для произвольного $k \in \mathbb{Z}$ положим $\mathbb{N}_k = \{n \in \mathbb{Z} : n \geqslant k\}$. Пусть также $\mathbb{P}$ — множество всех простых чисел. Все абелевы группы записываются аддитивно. Будем придерживаться соглашения о том, что сумма пустого множества элементов абелевой группы (в частности, аддитивной группы кольца) равна 0. Аналогично, произведение пустого набора элементов ассоциативного кольца с единицей считается равным 1; в частности, $r^0 = 1$ для любого элемента r такого кольца.

Для $m \in \mathbb{N}_0$ через X^m обозначается прямое произведение m экземпляров множества, группы или кольца X. В частности, X^0 состоит из одного элемента. Пусть $(X_i : i \in I)$ — семейство колец или абелевых групп. Тогда через $\prod\limits_{i \in I} X_i$ и $\bigoplus\limits_{i \in I} X_i$ будем обозначать соответственно прямое произведение (называемое также полной прямой суммой) и внешнюю прямую сумму этого семейства. Разумеется, если I конечно, то $\prod\limits_{i \in I} X_i = \bigoplus\limits_{i \in I} X_i$. Символом $\oplus$ обозначается бинарная операция прямой суммы (как внешней, так и внутренней). Операция $\prod$ используется и для произвольных (не обязательно

абелевых) групп, записываемых мультипликативно; для них она называется операцией декартова произведения. Элементы $\prod\limits_{i\in I} X_i$ обозначаются $(x_i : i \in I)$, где $x_i \in X_i$ для всех $i \in I$.

Пусть $m \in \mathbb{N}_0$ и R — ассоциативное коммутативное кольцо (вообще говоря, без единицы). Для каждого $n \in \mathbb{N}_{-1}$ обозначим через $\Pi_n(R, m)$ множество всех функций из R^m в R, представимых многочленами степени не более n от m переменных над кольцом R. Нулевому многочлену приписываем степень -1. Другими словами, $\Pi_n(R, m)$ состоит из всевозможных сумм функций вида $(x_1, \ldots, x_m) \mapsto r x_{i_1} \ldots x_{i_s}$ $(x_1, \ldots, x_m \in R)$, где $r \in R$, $0 \leqslant s \leqslant n$ и $1 \leqslant i_1 \leqslant \ldots \leqslant i_s \leqslant m$. В частности, $\Pi_{-1}(R, m) = \{0\}$ (функция, тождественно равная 0, также обозначается через 0). Из определения следует, что $\Pi_n(R, m) \subseteq \Pi_{n+1}(R, m)$ для всех $n \in \mathbb{N}_{-1}$. Пусть также $\Pi(R, m) = \bigcup\limits_{n=-1}^{\infty} \Pi_n(R, m)$. Естественно определить степень произвольной функции $\varphi\colon R^m \to R$ как $\min\{n \in \mathbb{N}_{-1} : \varphi \in \Pi_n(R, m)\}$, если $\varphi \in \Pi(R, m)$, и ∞ в противном случае. Эту степень обозначим через $\deg_\Pi \varphi$.

С другой стороны, для каждого $n \in \mathbb{N}_{-1}$ можно определить множество $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$, следуя [1]. Подчеркнём, что в определении этого множества участвует не кольцо R, а лишь его аддитивная группа $\mathcal{R}$. Приведём определение множеств $\mathrm{RM}_n(G, A)$ для произвольной группы G и произвольной абелевой группы A (см. также [2]; там эти множества обозначаются через $\Phi_n(G, A)$). Напомним, что *производной* функции $\varphi\colon G \to A$ по направлению $g \in G$ называется функция $\partial_g\varphi\colon G \to A$, определённая равенством $(\partial_g\varphi)(x) = \varphi(xg) - \varphi(x)$ для каждого $x \in G$. Множества $\mathrm{RM}_n(G, A)$ определяются индукцией по n следующим образом:

$$\mathrm{RM}_{-1}(G, A) = \{0\},$$
$$\mathrm{RM}_n(G, A) = \{\varphi\colon G \to A : \forall\, g \in G\ \ (\partial_g\varphi \in \mathrm{RM}_{n-1}(G, A))\} \quad \text{при } n \in \mathbb{N}_0.$$

Отметим, что в работе [1] таким образом определены множества $\mathrm{RM}_n(G, A)$ $(n \in \mathbb{N}_{-1})$ в случае, когда G и A — конечные абелевы группы. Легко видеть, что

$$\mathrm{RM}_n(G, A) = \{\varphi\colon G \to A : \forall\, g_1, \ldots, g_{n+1} \in G\ (\partial_{g_1} \ldots \partial_{g_{n+1}}\varphi = 0)\},$$

поэтому $\mathrm{RM}_n(G, A) \subseteq \mathrm{RM}_{n+1}(G, A)$ для каждого $n \in \mathbb{N}_{-1}$. Положим также $\mathrm{RM}(G, A) = \bigcup\limits_{n=-1}^{\infty} \mathrm{RM}_n(G, A)$.

Обозначение $\mathrm{RM}_n(G, A)$ указывает на связь этого множества с кодом Рида — Маллера порядка n. Действительно, p-ичный код Рида — Маллера порядка n и длины p^m (где p — простое число) может быть определён как $\Pi_n(\mathbb{Z}_p, m)$. В то же время известно, что $\Pi_n(\mathbb{Z}_p, m) = \mathrm{RM}_n(\mathcal{Z}_p^m, \mathcal{Z}_p)$ для всех $p \in \mathbb{P}$, $m \in \mathbb{N}_0$ и $n \in \mathbb{N}_{-1}$ ([3, свойство B7], а также следствие 1 ниже). Можно также рассматривать $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ как множество функций степени не более n, альтернативное $\Pi_n(R, m)$. Соответствующую степень произвольной функции $\varphi\colon R^m \to R$ обозначим через $\deg_{\mathrm{RM}} \varphi$, а именно:

$$\deg_{\mathrm{RM}} \varphi = \begin{cases} \min\{n \in \mathbb{N}_{-1} : \varphi \in \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})\}, & \text{если } \varphi \in \mathrm{RM}(\mathcal{R}^m, \mathcal{R}), \\ \infty & \text{в противном случае.} \end{cases}$$

Замечание 1. Непосредственно проверяется, что если $\pi \in \Pi_n(R, m)$, где $n \in \mathbb{N}_0$, то $\partial_v\pi \in \Pi_{n-1}(R, m)$ при любом $v \in \mathcal{R}^m$. Поэтому индукция по n показывает, что $\Pi_n(R, m) \subseteq \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ для всех $n \in \mathbb{N}_{-1}$. Следовательно, $\deg_{\mathrm{RM}} \varphi \leqslant \deg_\Pi \varphi$ для любой функции $\varphi\colon R^m \to R$.

В настоящей работе изучается следующий вопрос: для каких ассоциативных коммутативных колец R равенство $\deg_\Pi \varphi = \deg_{\mathrm{RM}} \varphi$ верно для всех $m \in \mathbb{N}_0$ и всех функций $\varphi\colon R^m \to R$? Эквивалентным образом этот вопрос можно сформулировать так: для каких ассоциативных коммутативных колец R равенство $\Pi_n(R, m) = \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ справедливо при любых $m \in \mathbb{N}_0$ и $n \in \mathbb{N}_{-1}$? Класс всех таких колец обозначим через $\mathfrak{D}$. Ранее было известно, что $\mathbb{Z}_p \in \mathfrak{D}$ для всех простых чисел p ([3, свойство B7]; для $p = 2$ этот факт отмечается в разд. 2 работы [1]). Отметим также результат А. В. Черемушкина [4, теорема 6]: для любой функции $\pi \in \Pi(\mathbb{Z}_{p^k}, m)$, где $p \in \mathbb{P}$ и $k, m \in \mathbb{N}_1$, имеет место равенство $\deg_\Pi \pi = \deg_{\mathrm{RM}} \pi$. Это утверждение эквивалентно тому, что $\Pi_n(\mathbb{Z}_{p^k}, m) = \mathrm{RM}_n(\mathcal{Z}^m_{p^k}, \mathcal{Z}_{p^k}) \cap \Pi(\mathbb{Z}_{p^k}, m)$ для всех $n \in \mathbb{N}_{-1}$ и всех p, k и m указанного вида. Отметим, что из этого результата, следствия 1, замечания 5 и эквивалентности из доказательства леммы 3 вытекает, что данный результат верен для колец $\mathbb{Z}_d$ и $\mathbb{Z}_d \oplus \mathbb{Q}$ при всех $d \in \mathbb{N}_1$, а также для колец вида $\prod\limits_{p \in P} \mathbb{Z}_{p^{k_p}}$, где $P \subseteq \mathbb{P}$ и $k_p \in \mathbb{N}_1$ для всех $p \in P$.

Полное описание класса $\mathfrak{D}$ автору неизвестно. В настоящей работе даётся частичное описание этого класса при некоторых достаточно общих предположениях о группе $\mathcal{R}$. Чтобы сформулировать основные результаты, напомним некоторые определения из теории абелевых групп. Пусть A — абелева группа. Определение ранга группы A дано, например, в [5, т. 1, разд. 16; 6, гл. 3, разд. 4]. Для наших целей достаточно знать, что группа A имеет ранг 1, если и только если A является либо ненулевой циклической p-группой, либо квазициклической p-группой (где p — простое число), либо изоморфна некоторой ненулевой подгруппе $\mathcal{Q}$ [5, т. 1, разд. 16, упр. 6 (b); 6, гл. 3, разд. 4, упр. (2)]. Группа A называется *делимой*, если $kA = A$ для всех $k \in \mathbb{N}_1$, *p-делимой* для простого числа p, если $pA = A$, и *редуцированной*, если она не содержит ненулевых делимых подгрупп [5, т. 1, разд. 20, 21; 6, гл. 4, разд. 1]. Наконец, группа A называется *копериодической*, если A имеет прямое дополнение во всякой своей абелевой надгруппе B, такой, что B/A не имеет кручения [5, т. 1, разд. 54; гл. 9, разд. 6].

Напомним, что число $d \in \mathbb{N}_1$ называется *свободным от квадратов*, если $d = p_1 \dots p_l$, где $l \in \mathbb{N}_0$ и $p_1, \dots, p_l$ — различные простые числа; поле называется *простым*, если оно не содержит собственных подполей. Известно, что поле просто тогда и только тогда, когда оно изоморфно $\mathbb{Q}$ или $\mathbb{Z}_p$ для некоторого простого числа p. Приведём основные результаты настоящей работы (см. теорему 1):

1. Если группа $\mathcal{R}$ периодична или конечно порождена, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}_d$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$.
2. Если группа $\mathcal{R}$ не редуцирована, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$.
3. Если группа $\mathcal{R}$ является прямой суммой подгрупп ранга 1, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}_d$ или $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$ (другими словами, когда R изоморфно прямой сумме конечного числа простых полей различных характеристик).
4. Если группа $\mathcal{R}$ редуцирована и копериодична, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \prod\limits_{p \in P} \mathbb{Z}_p$ для некоторого множества P простых чисел.

Здесь и далее через $\cong$ обозначается отношение изоморфизма. Доказательство основных результатов работы основано на том, что все кольца из класса $\mathfrak{D}$ являются E-кольцами (утверждение 1; определение E-кольца приведено в п. 3), а именно используются результаты П. Шульца [7] и Р. Боушелла и Шульца [8], в которых описаны E-кольца,

аддитивные группы которых удовлетворяют условиям, указанным в основных результатах, за исключением условия конечной порождённости (см. лемму 5).

Результаты работы позволяют описать все алгебры над полями, принадлежащие $\mathfrak{D}$, а именно: если R — алгебра над каким-либо полем F, то $R \in \mathfrak{D}$ тогда и только тогда, когда либо $R \cong F$, причём F — простое поле, либо $R = \{0\}$. Этот факт легко вывести как из приведённых выше основных, так и из некоторых промежуточных результатов (утверждение 2). В частности, поле принадлежит классу $\mathfrak{D}$, если и только если оно является простым.

1. Случай, когда R является прямым произведением

Введём некоторые обозначения. Через $\mathrm{Fun}(X, Y)$ обозначим множество всех функций из X в Y. Если $\varphi \in \mathrm{Fun}(X, Y)$ и $\psi \in \mathrm{Fun}(Y, Z)$, то $\psi(\varphi) \in \mathrm{Fun}(X, Z)$ — композиция функций φ и ψ (в этом порядке). Пусть также $\mathrm{Hom}(G, H)$ — множество всех гомоморфизмов группы G в группу H. Если H — абелева группа, то $\mathrm{Hom}(G, H)$ является абелевой группой относительно поточечного сложения. Кроме того, через $\mathrm{End}\, A$ обозначается кольцо всех эндоморфизмов абелевой группы A, в котором сложение осуществляется поточечно, а умножением является композиция.

Пусть G — группа и A — абелева группа. Удобно рассматривать множество $\mathrm{Fun}(G, A)$ как левый модуль над групповым кольцом $\mathbb{Z}G$, в котором сложение осуществляется поточечно, а действие кольца $\mathbb{Z}G$ определяется формулой $\left(\left(\sum\limits_{i=1}^{s} k_i g_i\right)\varphi\right)(x) = \sum\limits_{i=1}^{s} k_i \varphi(x g_i)$, где $\varphi \in \mathrm{Fun}(G, A)$; $x \in G$; $s \in \mathbb{N}_0$; $k_i \in \mathbb{Z}$ и $g_i \in G$ для всех $i \in \{1, \ldots, s\}$. Такой подход используется в работе [2] (там рассматривается несколько другое действие, однако его отличие от действия настоящей работы не принципиально). Очевидно, что если $\varphi \in \mathrm{Fun}(G, A)$ и $g \in G$, то

$$\partial_g \varphi = (g - 1)\varphi. \tag{1}$$

Поэтому

$$\varphi \in \mathrm{RM}_n(G, A) \iff \forall\, g_1, \ldots, g_{n+1} \in G\ ((g_1 - 1)\ldots(g_{n+1} - 1)\varphi = 0) \tag{2}$$

для произвольных $\varphi \in \mathrm{Fun}(G, A)$ и $n \in \mathbb{N}_{-1}$.

Замечание 2. Легко видеть, что $\mathrm{RM}_0(G, A)$ есть множество всех функций-констант из G в A, а $\mathrm{RM}_1(G, A)$ — множество всех функций вида $x \mapsto \eta(x) + a$ $(x \in G)$, где $\eta \in \mathrm{Hom}(G, A)$ и $a \in A$ [1, разд. 2; 2, замечание 5]. Поэтому если $\mathrm{Hom}(G, A) = \{0\}$, то $\mathrm{RM}(G, A)$ состоит из всех функций-констант из G в A, т. е. совпадает с $\mathrm{RM}_0(G, A)$.

Очевидно, что $\Pi_{-1}(R, m) = \{0\} = \mathrm{RM}_{-1}(\mathcal{R}^m, \mathcal{R})$. Используя приведённое выше описание $\mathrm{RM}_0(G, A)$, получаем, что $\Pi_0(R, m) = \mathrm{RM}_0(\mathcal{R}^m, \mathcal{R})$. Кроме того, $\Pi_n(R, 0) = \Pi_0(R, 0) = \mathrm{RM}_0(\mathcal{R}^0, \mathcal{R}) = \mathrm{RM}_{n'}(\mathcal{R}^0, \mathcal{R})$ для всех $n, n' \in \mathbb{N}_0$, так как все функции из одноэлементного множества R^0 в R являются константами.

Замечание 3. Пусть $\xi \in \mathrm{Hom}(G, H)$ для некоторой группы H. Продолжение этого гомоморфизма до гомоморфизма кольца $\mathbb{Z}G$ в кольцо $\mathbb{Z}H$ по линейности также будем обозначать через ξ. Непосредственно проверяется, что $\alpha(\psi(\xi)) = (\xi(\alpha)\psi)(\xi)$ для любых $\psi \in \mathrm{Fun}(H, A)$ и $\alpha \in \mathbb{Z}G$. Кроме того, функция $\psi \mapsto \psi(\xi)$ $(\psi \in \mathrm{Fun}(H, A))$ является гомоморфизмом аддитивной группы $\mathrm{Fun}(H, A)$ в аддитивную группу $\mathrm{Fun}(G, A)$. Таким образом, эта функция обладает свойством, аналогичным полулинейности. Легко также видеть, что если $\eta \in \mathrm{Hom}(A, B)$, где B — абелева группа, то функция $\varphi \mapsto \eta(\varphi)$ $(\varphi \in \mathrm{Fun}(G, A))$ — гомоморфизм $\mathbb{Z}G$-модуля $\mathrm{Fun}(G, A)$ в $\mathbb{Z}G$-модуль $\mathrm{Fun}(G, B)$.

Соберём нужные свойства множеств $\mathrm{RM}_n(G, A)$.

Замечание 4. Пусть $n \in \mathbb{N}_{-1}$. Тогда:

1) $\mathrm{RM}_n(G, A)$ — подмодуль $\mathbb{Z}G$-модуля $\mathrm{Fun}(G, A)$;
2) если A — подгруппа некоторой абелевой группы B, то $\mathrm{RM}_n(G, A) = \mathrm{RM}_n(G, B) \cap$ $\cap\, \mathrm{Fun}(G, A)$;
3) если $\varphi \in \mathrm{RM}_n(G, A)$, то $\varphi|_H \in \mathrm{RM}_n(H, A)$ для любой подгруппы H группы G;
4) если $\psi \in \mathrm{RM}_n(H, A)$ и $\xi \in \mathrm{Hom}(G, H)$ для некоторой группы H, то $\psi(\xi) \in$ $\in \mathrm{RM}_n(G, A)$;
5) если $\varphi \in \mathrm{RM}_n(G, A)$ и $\eta \in \mathrm{Hom}(A, B)$ для некоторой абелевой группы B, то $\eta(\varphi) \in \mathrm{RM}_n(G, B)$.

Все эти свойства проверяются непосредственно с использованием эквивалентности (2) и замечания 3 (см. также [2, замечания 2–4]).

Пусть $G = \prod\limits_{i \in I} G_i$ и $A = \prod\limits_{i \in I} A_i$, где G_i — группа и A_i — абелева группа для каждого $i \in I$. Для произвольного $i \in I$ считаем G_i подгруппой группы G, отождествляя произвольный элемент $g_i \in G_i$ с $(g_j : j \in I) \in G$, где $g_j = 1$ при всех $j \in I \setminus \{i\}$. Обозначим через ξ_i проекцию G на G_i, а через η_i — проекцию A на A_i $(i \in I)$.

Лемма 1. Предположим, что $\mathrm{Hom}(\prod_{j \in I \setminus \{i\}} G_j, A_i) = \{0\}$ для всех $i \in I$. Пусть $\varphi \in \mathrm{Fun}(G, A)$ и $n \in \mathbb{N}_{-1}$. Тогда

$$\varphi \in \mathrm{RM}_n(G, A) \iff \forall\, i \in I\ (\eta_i(\varphi) = \eta_i(\varphi(\xi_i)) \,\&\, \eta_i(\varphi|_{G_i}) \in \mathrm{RM}_n(G_i, A_i)).$$

Доказательство. Докажем импликацию «$\Longrightarrow$». Пусть $\varphi \in \mathrm{RM}_n(G, A)$ и $i \in I$. Обозначим через H_i подгруппу G, состоящую из всех $(g_j : j \in I) \in G$, таких, что $g_i = 1$. Тогда $H_i \cong \prod\limits_{j \in I \setminus \{i\}} G_j$ и G является прямым произведением подгрупп H_i и G_i. Пусть также $g_i \in G_i$. Из свойств 1, 3 и 5 замечания 4 следует, что $\eta_i((g_i\varphi)|_{H_i}) \in$ $\in \mathrm{RM}_n(H_i, A_i) \subseteq \mathrm{RM}(H_i, A_i)$. Но ввиду замечания 2 $\mathrm{RM}(H_i, A_i)$ состоит из функций-констант из $\mathrm{Fun}(H_i, A_i)$, так как $\mathrm{Hom}(H_i, A_i) = \{0\}$ согласно предположению леммы. Поэтому $\eta_i(\varphi(h_i g_i)) = \eta_i(\varphi(g_i)) = \eta_i(\varphi(\xi_i(h_i g_i)))$ для любого $h_i \in H_i$. Таким образом, $\eta_i(\varphi) = \eta_i(\varphi(\xi_i))$. Кроме того, из свойств 3 и 5 замечания 4 вытекает, что $\eta_i(\varphi|_{G_i}) \in$ $\in \mathrm{RM}_n(G_i, A_i)$. Импликация «$\Longrightarrow$» доказана.

Докажем теперь импликацию «$\Longleftarrow$». Предположим, что $\eta_i(\varphi) = \eta_i(\varphi(\xi_i))$ и $\eta_i(\varphi|_{G_i}) \in \mathrm{RM}_n(G_i, A_i)$ для всех $i \in I$. Пусть $g_1, \ldots, g_{n+1} \in G$. Положим для краткости $\alpha = (g_1 - 1) \ldots (g_{n+1} - 1)$. Тогда для каждого $i \in I$

$$\eta_i(\alpha\varphi) = \alpha(\eta_i(\varphi)) = \alpha(\eta_i(\varphi(\xi_i))) = ((\xi_i(g_1) - 1) \ldots (\xi_i(g_{n+1}) - 1)(\eta_i(\varphi)))(\xi_i) = 0$$

ввиду замечания 3 и эквивалентности (2). Следовательно, $\alpha\varphi = 0$. Таким образом, $\varphi \in \mathrm{RM}_n(G, A)$ (см. эквивалентность (2)). Импликация «$\Longleftarrow$» доказана. ■

Лемма 1 может быть сформулирована следующим образом: если $\mathrm{Hom}\left(\prod\limits_{j \in I \setminus \{i\}} G_j, A_i\right) =$ $= \{0\}$ для всех $i \in I$, то $\mathrm{RM}_n(G, A)$ $(n \in \mathbb{N}_{-1})$ состоит из тех и только тех функций $\varphi \in \mathrm{Fun}(G, A)$, которые имеют вид

$$(x_i : i \in I) \mapsto (\varphi_i(x_i) : i \in I) \quad (x_i \in G_i),$$

где $\varphi_i \in \mathrm{RM}_n(G_i, A_i)$ при любом $i \in I$. Очевидно, что функции φ_i определяются такой функцией φ однозначно, а именно: $\varphi_i = \eta_i(\varphi|_{G_i})$ для всех $i \in I$.

Пусть теперь $R = \prod\limits_{i\in I} R_i$, где R_i — ассоциативное коммутативное кольцо для каждого $i \in I$. Тогда R^m естественно отождествляется с $\prod\limits_{i\in I} R_i^m$. Для произвольного $i \in I$ считаем R_i идеалом кольца R, отождествляя произвольный элемент $r_i \in R_i$ с $(r_j : j \in I) \in R$, где $r_j = 0$ при всех $j \in I \setminus \{i\}$. Обозначим через η_i проекцию R на R_i, а через ξ_i — проекцию R^m на R_i^m, определённую равенством $\xi_i(x_1, \ldots, x_m) = (\eta_i(x_1), \ldots, \eta_i(x_m))$ для всех $x_1, \ldots, x_m \in R$.

Замечание 5. Пусть $\varphi \in \mathrm{Fun}(R^m, R)$ и $n \in \mathbb{N}_{-1}$. Тогда непосредственно проверяется, что

$$\varphi \in \Pi_n(R, m) \iff \forall\, i \in I\ (\eta_i(\varphi) = \eta_i(\varphi(\xi_i)) \,\&\, \eta_i(\varphi|_{R_i^m}) \in \Pi_n(R_i, m)).$$

Лемма 2.

1. Пусть $n \in \mathbb{N}_{-1}$. Тогда если $\Pi_n(R, m) = \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$, то $\Pi_n(R_i, m) = \mathrm{RM}_n(\mathcal{R}_i^m, \mathcal{R}_i)$ для всех $i \in I$.
2. Если $\Pi(R, m) = \mathrm{RM}(\mathcal{R}^m, \mathcal{R})$, то $\Pi(R_i, m) = \mathrm{RM}(\mathcal{R}_i^m, \mathcal{R}_i)$ для всех $i \in I$.

Доказательство. Докажем утверждение 1. Предположим, что $\Pi_n(R, m) = \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$. Пусть $i \in I$ и $\varphi_i \in \mathrm{RM}_n(\mathcal{R}_i^m, \mathcal{R}_i)$. Положим $\varphi = \varphi_i(\xi_i)$. Тогда $\varphi \in \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ ввиду свойств 4 и 2 замечания 4. Следовательно, $\varphi \in \Pi_n(R, m)$. Из замечания 5 вытекает, что $\varphi_i = \eta_i(\varphi_i) = \eta_i(\varphi|_{R_i^m}) \in \Pi_n(R_i, m)$ (очевидно, что $\varphi_i = \varphi|_{R_i^m}$). Таким образом, $\mathrm{RM}_n(\mathcal{R}_i^m, \mathcal{R}_i) \subseteq \Pi_n(R_i, m)$, а обратное включение имеет место ввиду замечания 1. Утверждение 1 доказано.

Утверждение 2 доказывается так же, за исключением того, что $\varphi \in \Pi_{n'}(R, m)$ и $\varphi_i \in \Pi_{n'}(R_i, m)$ для некоторого $n' \in \mathbb{N}_{-1}$, вообще говоря, отличного от n. Поэтому если $\Pi(R, m) = \mathrm{RM}(\mathcal{R}^m, \mathcal{R})$, то $\mathrm{RM}(\mathcal{R}_i^m, \mathcal{R}_i) \subseteq \Pi(R_i, m)$ для любого $i \in I$, а обратное включение следует из замечания 1. ■

Лемма 3. Предположим, что $\mathrm{Hom}(\prod_{j\in I\setminus\{i\}} \mathcal{R}_j, \mathcal{R}_i) = \{0\}$ для всех $i \in I$. Пусть $n \in \mathbb{N}_{-1}$. Тогда

$$\Pi_n(R, m) = \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R}) \iff \forall\, i \in I\ (\Pi_n(R_i, m) = \mathrm{RM}_n(\mathcal{R}_i^m, \mathcal{R}_i)).$$

В частности, $R \in \mathfrak{D}$, если и только если $R_i \in \mathfrak{D}$ для каждого $i \in I$.

Доказательство. Ввиду утверждения 1 леммы 2 достаточно доказать лишь импликацию «$\Longleftarrow$». Пусть $\varphi \in \mathrm{Fun}(R^m, R)$. Из предположения леммы следует, что $\mathrm{Hom}\left(\prod\limits_{j\in I\setminus\{i\}} \mathcal{R}_j^m, \mathcal{R}_i^m\right) = \{0\}$ для всех $i \in I$. Поэтому

$$\varphi \in \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R}) \iff \forall\, i \in I\ (\eta_i(\varphi) = \eta_i(\varphi(\xi_i)) \,\&\, \eta_i(\varphi|_{R_i^m}) \in \mathrm{RM}_n(\mathcal{R}_i^m, \mathcal{R}_i))$$

согласно лемме 1. Требуемая импликация «$\Longleftarrow$» непосредственно вытекает из замечания 5 и этой эквивалентности. ■

Отметим, что если множество I конечно (в этом случае $R = \bigoplus\limits_{i\in I} R_i$), то предположение леммы 3 выполнено тогда и только тогда, когда $\mathrm{Hom}(\mathcal{R}_i, \mathcal{R}_j) = \{0\}$ для любых различных $i, j \in I$.

2. Случай, когда R — простое поле

Далее предполагаем, что кольцо R содержит единицу. Для произвольного $k \in \mathbb{Z}$ будем обозначать элемент $k1$ этого кольца через k, если это не вызывает недоразумений. Аналогично предыдущему, рассматриваем множество $\mathrm{Fun}(\mathcal{R}^m, R)$ как модуль над групповым кольцом $R\mathcal{R}^m$. Для удобства записи элементов этого группового кольца введём формальный символ $\mathbf{g}$ и вместо произвольного элемента $v \in \mathcal{R}^m$ будем писать $\mathbf{g}^v$. При этом, разумеется, $\mathbf{g}^{u+v} = \mathbf{g}^u\mathbf{g}^v$ для любых $u, v \in \mathcal{R}^m$; обозначим также $\mathbf{g}^0$ через 1. Таким образом, элементы группового кольца $R\mathcal{R}^m$ будут записываться в виде $\sum\limits_{i=1}^{s} r_i\mathbf{g}^{v_i}$, где $s \in \mathbb{N}_0$, $r_i \in R$ и $v_i \in \mathcal{R}^m$ для всех $i \in \{1, \ldots, s\}$; результатом действия этого элемента на произвольную функцию $\varphi \in \mathrm{Fun}(\mathcal{R}^m, R)$ является функция $x \mapsto \sum\limits_{i=1}^{s} r_i\varphi(x + v_i)$ $(x \in \mathcal{R}^m)$. Сложение в $\mathrm{Fun}(\mathcal{R}^m, R)$ осуществляется поточечно. Формула (1) для производной в данной ситуации приобретает вид

$$\partial_v\varphi = (\mathbf{g}^v - 1)\varphi, \tag{3}$$

где $\varphi \in \mathrm{Fun}(\mathcal{R}^m, R)$ и $v \in \mathcal{R}^m$. Отметим, что если R конечно, то $\mathrm{Fun}(\mathcal{R}^m, R)$ и $R\mathcal{R}^m$ изоморфны как $R\mathcal{R}^m$-модули; изоморфизмом первого из этих модулей на второй является функция $\varphi \mapsto \sum\limits_{x\in\mathcal{R}^m} \varphi(x)\mathbf{g}^{-x}$ $(\varphi \in \mathrm{Fun}(\mathcal{R}^m, R))$.

Очевидно, что для любого $n \in \mathbb{N}_{-1}$ множества $\Pi_n(R, m)$ и $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ являются подмодулями $R\mathcal{R}^m$-модуля $\mathrm{Fun}(\mathcal{R}^m, R)$. Легко также видеть, что для любого $v \in \mathcal{R}^m$ оператор взятия производной по направлению v (обозначаемый через ∂_v) является эндоморфизмом $R\mathcal{R}^m$-модуля $\mathrm{Fun}(\mathcal{R}^m, R)$, отображающим $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ в $\mathrm{RM}_{n-1}(\mathcal{R}^m, \mathcal{R})$ для каждого $n \in \mathbb{N}_0$.

Для каждого $i \in \{1, \ldots, m\}$ положим $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, где единица стоит на i-м месте. В зависимости от контекста e_i может быть элементом как $\mathcal{R}^m$, так и $\mathbb{N}_0^m$. Будем рассматривать $\mathbb{N}_0^m$ как прямое произведение m упорядоченных множеств $\mathbb{N}_0$ с обычным отношением порядка $\leqslant$. Другими словами, $k \leqslant l$ (или $l \geqslant k$), где $k = (k_1, \ldots, k_m)$ и $l = (l_1, \ldots, l_m)$ — произвольные наборы из $\mathbb{N}_0^m$, если и только если $k_i \leqslant l_i$ для всех $i \in \{1, \ldots, m\}$. Для произвольной функции $\varphi \in \mathrm{Fun}(\mathcal{R}^m, R)$ и произвольного $k = (k_1, \ldots, k_m) \in \mathbb{N}_0^m$ положим $\partial_e^k\varphi = \partial_{e_1}^{k_1} \ldots \partial_{e_m}^{k_m}\varphi$.

Пусть теперь R — поле, c — его характеристика. Положим $I_c = \mathbb{N}_0$, если $c = 0$, и $I_c = \{0, \ldots, c - 1\}$ в противном случае. Пусть также

$$I_c^m(n) = \{(k_1, \ldots, k_m) \in I_c^m : k_1 + \cdots + k_m \leqslant n\}$$

для произвольного $n \in \mathbb{N}_{-1}$. Как обычно, если $y \in R$ и $t \in I_c$, то

$$\binom{y}{t} = \frac{y(y-1)\ldots(y-t+1)}{t!}.$$

Кроме того, для произвольных $x = (x_1, \ldots, x_m) \in R^m$ и $k = (k_1, \ldots, k_m) \in I_c^m$ положим

$$\binom{x}{k} = \binom{x_1}{k_1} \ldots \binom{x_m}{k_m}.$$

Лемма 4. Предположим, что R — простое поле. Пусть $\varphi \in \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$, где $n \in \mathbb{N}_{-1}$. Тогда для любого $x \in R^m$ имеет место равенство

$$\varphi(x) = \sum_{k \in I_c^m(n)} \binom{x}{k} (\partial_e^k \varphi)(0), \tag{4}$$

где c — характеристика поля R.

Доказательство. Пусть $l = (l_1, \ldots, l_m) \in I_c^m$. Непосредственно проверяется, что

$$\begin{gathered}\mathbf{g}^l \varphi = \left(\prod_{i=1}^m (\mathbf{g}^{e_i})^{l_i} \right) \varphi = \left(\prod_{i=1}^m ((\mathbf{g}^{e_i} - 1) + 1)^{l_i} \right) \varphi = \left(\prod_{i=1}^m \left(\sum_{k_i=0}^{l_i} \binom{l_i}{k_i} (\mathbf{g}^{e_i} - 1)^{k_i} \right) \right) \varphi = \\ = \sum_{k \in I_c^m : k \leqslant l} \binom{l}{k} \partial_e^k \varphi = \sum_{k \in I_c^m(n) : k \leqslant l} \binom{l}{k} \partial_e^k \varphi = \sum_{k \in I_c^m(n)} \binom{l}{k} \partial_e^k \varphi.\end{gathered} \tag{5}$$

Здесь мы воспользовались формулой (3) и следующими фактами:

— если $k \in I_c^m \setminus I_c^m(n)$, то $\partial_e^k \varphi = 0$ (вытекает из того, что $\varphi \in \mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$);

— если $k \in I_c^m$ и $k \not\leqslant l$, то $\binom{l}{k} = 0$ (вытекает из того, что $\binom{y}{t} = 0$ при любых $t \in I_c$ и $y \in \{0, \ldots, t-1\}$).

Взяв значения функций из (5) в 0, получаем

$$\varphi(l) = \sum_{k \in I_c^m(n)} \binom{l}{k} (\partial_e^k \varphi)(0). \tag{6}$$

Из этой формулы непосредственно вытекает утверждение леммы в случае, когда $c \neq 0$.

С этого момента и до окончания доказательства леммы будем рассматривать случай, когда $c = 0$. Тогда можно считать, что $R = \mathbb{Q}$. Для доказательства леммы в этом случае воспользуемся индукцией по n. При $n = -1$ утверждение леммы верно, так как $\mathrm{RM}_{-1}(\mathcal{Q}^m, \mathcal{Q}) = \{0\}$ и $I_0^m(-1) = \varnothing$. Пусть теперь $n \in \mathbb{N}_0$ и формула (4) верна для всех функций из $\mathrm{RM}_{n-1}(\mathcal{Q}^m, \mathcal{Q})$ и всех $x \in \mathbb{Q}^m$. Определим функцию $\pi \colon \mathbb{Q}^m \to \mathbb{Q}$ равенством

$$\pi(x) = \sum_{l \in I_0^m(n)} \binom{x}{l} (\partial_e^l \varphi)(0)$$

для всех $x \in \mathbb{Q}^m$ и положим $\psi = \varphi - \pi$. Очевидно, что $\pi \in \Pi_n(\mathbb{Q}, m) \subseteq \mathrm{RM}_n(\mathcal{Q}^m, \mathcal{Q})$ (см. замечание 1) и, следовательно, $\psi \in \mathrm{RM}_n(\mathcal{Q}^m, \mathcal{Q})$. Для завершения доказательства требуется показать, что $\psi = 0$. Так как $\psi(x) = 0$ для всех $x \in I_0^m = \mathbb{N}_0^m$ (ввиду формулы (6)), для этого достаточно доказать, что ψ — константа. В свою очередь, последнее условие эквивалентно тому, что $\partial_v \psi = 0$ для всех $v \in \mathcal{Q}^m$ (см. замечание 2). Положим $L = \{v \in \mathcal{Q}^m : \partial_v \psi = 0\}$ и покажем, что $L = \mathcal{Q}^m$. Это вытекает из следующих утверждений:

1) $e_1, \ldots, e_m \in L$;
2) L — подгруппа $\mathcal{Q}^m$;
3) если $v \in L$ и $d \in \mathbb{N}_1$, то $v/d \in L$.

Докажем утверждение 1. Пусть $i \in \{1, \ldots, m\}$ и $x \in \mathbb{Q}^n$. Из известного и легко проверяемого равенства

$$\binom{y+1}{t} - \binom{y}{t} = \binom{y}{t-1},$$

справедливого для всех $y \in \mathbb{Q}$ и $t \in \mathbb{N}_1$, следует, что

$$(\partial_{e_i} \pi)(x) = \sum_{l \in I_0^m(n) : l \geqslant e_i} \binom{x}{l - e_i} (\partial_e^l \varphi)(0) = \sum_{k \in I_0^m(n-1)} \binom{x}{k} (\partial_e^{k+e_i} \varphi)(0).$$

Здесь мы воспользовались тем, что $l \mapsto l - e_i$ — биекция $\{l \in I_0^m(n) : l \geqslant e_i\}$ на $I_0^m(n-1)$. С другой стороны, предположение индукции, применённое к $\partial_{e_i}\varphi$, даёт равенство

$$(\partial_{e_i}\varphi)(x) = \sum_{k \in I_0^m(n-1)} \binom{x}{k} (\partial_e^{k+e_i}\varphi)(0)$$

(очевидно, что операторы взятия производных по разным направлениям коммутируют). Поэтому $\partial_{e_i}\psi = \partial_{e_i}\varphi - \partial_{e_i}\pi = 0$, т. е. $e_i \in L$. Утверждение 1 доказано.

Утверждение 2 непосредственно вытекает из равенств $\partial_0\psi = 0$, $\partial_{u+v}\psi = \mathbf{g}^u\partial_v\psi + \partial_u\psi$ и $\partial_{-v}\psi = -\mathbf{g}^{-v}\partial_v\psi$, имеющих место для любых $u, v \in \mathcal{Q}^m$. Эти равенства легко получить, используя формулу (3).

Докажем утверждение 3. Обозначим через Δ фундаментальный идеал групповой алгебры $\mathbb{Q}\mathcal{Q}^m$, т. е. ядро гомоморфизма $\mathbb{Q}$-алгебр $\tau\colon \mathbb{Q}\mathcal{Q}^m \to \mathbb{Q}$, такого, что $\tau\left(\sum_{i=1}^{s} r_i\mathbf{g}^{v_i}\right) = \sum_{i=1}^{s} r_i$ для всех $s \in \mathbb{N}_0$, $r_i \in \mathbb{Q}$ и $v_i \in \mathcal{Q}^m$ ($i \in \{1, \ldots, s\}$). Легко видеть, что Δ порождается как векторное пространство над $\mathbb{Q}$ и как $\mathbb{Q}\mathcal{Q}^m$-идеал множеством $\{\mathbf{g}^v - 1 : v \in \mathcal{Q}^m\}$.

Пусть $v \in L$ и $d \in \mathbb{N}_1$. Положим $u = v/d$. Обозначим через $\Delta^{(n)}$ n-ю степень идеала Δ; при $n = 0$ полагаем $\Delta^{(0)} = \mathbb{Q}\mathcal{Q}^m$. Так как $\partial_u\psi \in \mathrm{RM}_{n-1}(\mathcal{Q}^m, \mathcal{Q})$, из формулы (3) вытекает, что $\Delta^{(n)}\partial_u\psi = \{0\}$ (см. также лемму 2 из [2]). Непосредственно проверяется (с использованием формулы (3)), что $\partial_v\psi = \alpha\partial_u\psi$, где $\alpha = 1 + \mathbf{g}^u + \cdots + \mathbf{g}^{(d-1)u} \in \mathbb{Q}\mathcal{Q}^m$. Теперь воспользуемся тем, что по модулю $\Delta^{(n)}$ любой элемент $\mathbb{Q}\mathcal{Q}^m \setminus \Delta$ (в частности, α) обратим, а именно: пусть $\delta = 1 - \alpha/d$ и $\beta = (1 + \delta + \cdots + \delta^{n-1})/d$. Тогда легко видеть, что $\delta \in \Delta$ (так как $\tau(\alpha) = d$) и $\beta\alpha = 1 - \delta^n \equiv 1 \pmod{\Delta^{(n)}}$. Поэтому $\partial_u\psi = \beta\alpha\partial_u\psi = \beta\partial_v\psi = 0$, т. е. $u = v/d \in L$. Утверждение 3 доказано. ■

Формулу (4) можно рассматривать как вариант формулы Ньютона. Другие варианты формулы Ньютона см., например, в [4, разд. 4; 9, разд. 6.2]. Из доказательства леммы 4 (см. формулу (6)) вытекает, что формула (4) верна, если R — произвольное поле характеристики 0 и $\varphi \in \Pi_n(R, m)$. (Здесь используется также известное утверждение о том, что если R — поле, X — его бесконечное подмножество, а φ и π — функции из $\Pi(R, m)$ такие, что $\varphi|_{X^m} = \pi|_{X^m}$, то $\varphi = \pi$.) Вероятно, этот факт известен специалистам, так же как и формула (4) для функций из $\Pi_n(\mathbb{Z}_p, m)$, где p — простое число. Однако нашей задачей является доказательство формулы (4) для функций из $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R})$ (а не просто из $\Pi_n(R, m)$), если R — простое поле. Это позволяет показать, что $\mathrm{RM}_n(\mathcal{R}^m, \mathcal{R}) \subseteq \Pi_n(R, m)$ для всех $n \in \mathbb{N}_{-1}$, так как в правой части формулы (4) стоит $\pi(x)$ для некоторой функции $\pi \in \Pi_n(R, m)$. Обратное включение имеет место ввиду замечания 1. Таким образом, получаем

Следствие 1. Все простые поля принадлежат классу $\mathfrak{D}$.

Для конечных простых полей это утверждение известно (см. [3, свойство B7], где оно сформулировано на языке степеней). При $p = 2$ оно отмечается в [1, разд. 2].

3. Доказательство основных результатов

Ассоциативное кольцо S с единицей называется *E-кольцом*, если выполнено любое из следующих эквивалентных условий:

- всякий эндоморфизм группы $\mathcal{S}$ является эндоморфизмом S как правого S-модуля, т. е. имеет вид $x \mapsto sx$ ($x \in S$) при некотором $s \in S$;
- кольцо S коммутативно и $S \cong \mathrm{End}\,\mathcal{S}$;
- кольцо $\mathrm{End}\,\mathcal{S}$ коммутативно

(см. [6, гл. 18, разд. 6; 7, разд. 3; 8, разд. 1]). Понятие E-кольца понадобится потому, что всякое кольцо из класса $\mathfrak{D}$ является E-кольцом (см. утверждение 1 далее).

Пусть $P \subseteq \mathbb{P}$. Через $\mathbb{Z}[1/P]$ будем обозначать подкольцо $\mathbb{Q}$, порождённое множеством $\{1\} \cup \{1/p \,|\, p \in P\}$. Другими словами, $\mathbb{Z}[1/P]$ — это множество всех k/l, где $k \in \mathbb{Z}$, $l \in \mathbb{N}_1$, причём все простые делители l принадлежат P. В частности, $\mathbb{Z}[1/\varnothing] = \mathbb{Z}$ и $\mathbb{Z}[1/\mathbb{P}] = \mathbb{Q}$. Для произвольного простого числа p через $\mathbb{J}_p$ будем обозначать кольцо целых p-адических чисел.

Замечание 6. Пусть S — кольцо с единицей, аддитивная группа которого является группой ранга 1 без кручения. Тогда для любого $s \in S$ существуют $k_s \in \mathbb{Z}$ и $l_s \in \mathbb{N}_1$, удовлетворяющие равенству $l_s s = k_s 1$. Непосредственно проверяется, что $s \mapsto k_s/l_s$ $(s \in S)$ — корректно определённый инъективный гомоморфизм из кольца S в поле $\mathbb{Q}$. Образ S при этом гомоморфизме содержит $\mathbb{Z}$, поэтому этот образ есть $\mathbb{Z}[1/X]$, где $X = \{p \in \mathbb{P} : 1 \in pS\}$ (см. теорему 2.2 из работы [10] и её доказательство). Таким образом, $S \cong \mathbb{Z}[1/X]$.

Утверждение 1. Кольцо R является E-кольцом (в частности, имеет единицу) тогда и только тогда, когда $\Pi_1(R, 1) = \mathrm{RM}_1(\mathcal{R}, \mathcal{R})$. В частности, если $R \in \mathfrak{D}$, то R — E-кольцо.

Доказательство. Согласно замечанию 2, $\mathrm{RM}_1(\mathcal{R}, \mathcal{R})$ есть множество всех функций вида $x \mapsto \epsilon(x) + r$ $(x \in \mathcal{R})$, где $\epsilon \in \operatorname{End}\mathcal{R}$ и $r \in \mathcal{R}$. Поэтому если R — E-кольцо, то $\mathrm{RM}_1(\mathcal{R}, \mathcal{R}) \subseteq \Pi_1(R, 1)$ и, следовательно, $\Pi_1(R, 1) = \mathrm{RM}_1(\mathcal{R}, \mathcal{R})$ ввиду замечания 1. Обратно, пусть $\Pi_1(R, 1) = \mathrm{RM}_1(\mathcal{R}, \mathcal{R})$. Тогда из описания множества $\mathrm{RM}_1(\mathcal{R}, \mathcal{R})$ вытекает, что все эндоморфизмы группы $\mathcal{R}$ имеют вид $x \mapsto sx$ $(x \in \mathcal{R})$, где $s \in R$. В частности, кольцо R имеет единицу. Таким образом, R является E-кольцом. ■

Приведём нужные свойства E-колец.

Лемма 5. Предположим, что R является E-кольцом. Тогда:

1) если $\mathcal{R} = A \oplus B$ для некоторых подгрупп A и B группы $\mathcal{R}$, то $\operatorname{Hom}(A, B) = \{0\}$;
2) если S — ассоциативное кольцо с единицей, такое, что $\mathcal{S} \cong \mathcal{R}$, то $S \cong R$;
3) если группа $\mathcal{R}$ периодична, то $R \cong \mathbb{Z}_d$ для некоторого $d \in \mathbb{N}_1$;
4) если группа $\mathcal{R}$ не редуцирована, то $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого $d \in \mathbb{N}_1$;
5) если группа $\mathcal{R}$ является прямой суммой подгрупп ранга 1, то $R \cong \mathbb{Z}_d \oplus \oplus \bigoplus_{i=1}^{k} \mathbb{Z}[1/X_i]$, где $d \in \mathbb{N}_1$; $k \in \mathbb{N}_0$; $X_1, \ldots, X_k$ — множества простых чисел, содержащие все простые делители числа d, причём $X_i \not\subseteq X_j$ при $i \neq j$ $(i, j \in \in \{1, \ldots, k\})$;
6) если группа $\mathcal{R}$ редуцирована и копериодична, то $R \cong \prod_{p \in P} R_p$, где $P \subseteq \mathbb{P}$ и $R_p \in \{\mathbb{Z}_{p^k} : k \in \mathbb{N}_1\} \cup \{\mathbb{J}_p\}$ для каждого $p \in P$.

Доказательство. Утверждение 1 следует из свойства D E-колец [6, гл. 18, разд. 6]. Впрочем, это утверждение легко доказать непосредственно: если $\mathcal{R} = A \oplus B$, ξ — проекция $\mathcal{R}$ на A и η — ненулевой гомоморфизм из A в B, то эндоморфизмы ξ и $\eta(\xi)$ группы $\mathcal{R}$ не коммутируют. Утверждение 2 вытекает из следствия 4 в [7]. Оно тоже легко доказывается: если $\mathcal{S} \cong \mathcal{R}$, то S — E-кольцо (так как $\operatorname{End}\mathcal{S}$ изоморфно коммутативному кольцу $\operatorname{End}\mathcal{R}$) и $S \cong \operatorname{End}\mathcal{S} \cong \operatorname{End}\mathcal{R} \cong R$. Утверждение 3 следует из теоремы 1 в [7] (см. также [6, гл. 18, лемма 6.4, (i); 8, предложение 1.4, (ii)]). Утверждение 4 вытекает из теоремы 3 работы [7] (см. также [6, гл. 18, лемма 6.4, (ii); 8, предложение 1.4, (iii)]). Пусть теперь $\mathcal{R}$ является прямой суммой подгрупп ранга 1. Тогда

из теоремы 2 в [7] следует, что $R \cong \mathbb{Z}_d \oplus \bigoplus\limits_{i=1}^{k} R_i$, где $d \in \mathbb{N}_1$; $k \in \mathbb{N}_0$; $R_1, \ldots, R_k$ — ассоциативные коммутативные кольца с единицей, аддитивные группы которых не имеют кручения, имеют ранг 1, являются p-делимыми для любого простого делителя p числа d и имеют попарно несравнимые типы. О типах абелевых групп без кручения ранга 1 см. [5, т. 2, разд. 85; 6, гл. 12, разд. 1]. Замечание 6 показывает, что $R_i \cong \mathbb{Z}[1/X_i]$ для каждого $i \in \{1, \ldots, k\}$, где $X_i \subseteq \mathbb{P}$. При этом множество X_i для каждого $i \in \{1, \ldots, k\}$ содержит все простые делители числа d, так как группа $\mathcal{Z}[1/X]$ p-делима (где $p \in \mathbb{P}$ и $X \subseteq \mathbb{P}$) тогда и только тогда, когда $p \in X$. Кроме того, тип $\mathcal{Z}[1/X]$ не превосходит типа $\mathcal{Z}[1/Y]$, если и только если $X \subseteq Y$ ($X, Y \subseteq \mathbb{P}$). Это показывает, что $X_i \nsubseteq X_j$ при $i \neq j$ ($i, j \in \{1, \ldots, k\}$). Таким образом, утверждение 5 доказано. Наконец, утверждение 6 доказано в теореме 3.3 в [8] (см. также [6, гл. 18, теорема 6.6]). ■

Утверждение 2. Пусть R — алгебра над каким-либо полем F. Тогда следующие условия эквивалентны:

1) $R \in \mathfrak{D}$;
2) $\Pi_1(R, 1) = \mathrm{RM}_1(\mathcal{R}, \mathcal{R})$;
3) R — E-кольцо;
4) либо $R \cong F$, причём F — простое поле, либо $R = \{0\}$.

Доказательство. Импликация $1 \Longrightarrow 2$ тривиальна, импликация $2 \Longrightarrow 3$ доказана в утверждении 1, а импликация $4 \Longrightarrow 1$ вытекает из следствия 1. Осталось доказать импликацию $3 \Longrightarrow 4$. Достаточно рассмотреть случай, когда R — ненулевое E-кольцо. Тогда группа $\mathcal{R}$ изоморфна прямой сумме $\dim_F R$ экземпляров группы $\mathcal{F}$. Из утверждения 1 леммы 5 следует, что $\dim_F R = 1$. Поэтому $\mathcal{R} \cong \mathcal{F}$ и $R \cong F$ (см. утверждение 2 леммы 5). Пусть теперь K — простое подполе поля F. Рассуждая аналогично, получим, что $F = K$. Импликация $3 \Longrightarrow 4$ доказана. ■

Замечание 7. Пусть $\pi \in \Pi(R, m)$. Пусть также I — идеал кольца R и $x_1, y_1, \ldots, x_m, y_m \in R$. Тогда легко видеть, что

$$\forall\, i \in \{1, \ldots, m\}\ (x_i \equiv y_i \pmod{I}) \implies \pi(x_1, \ldots, x_m) \equiv \pi(y_1, \ldots, y_m) \pmod{I}.$$

Лемма 6. Пусть p — простое число и $k \in \mathbb{N}_2$. Тогда $\Pi(\mathbb{Z}_{p^k}, 1) \neq \mathrm{RM}(\mathcal{Z}_{p^k}, \mathcal{Z}_{p^k})$. В частности, $\mathbb{Z}_{p^k} \notin \mathfrak{D}$.

Доказательство. Согласно теореме 2 (или теореме 1) из [2], $\mathrm{RM}(\mathcal{Z}_{p^k}, \mathcal{Z}_{p^k})$ совпадает с множеством всех функций из $\mathbb{Z}_{p^k}$ в $\mathbb{Z}_{p^k}$. Известно, что не все такие функции принадлежат $\Pi(\mathbb{Z}_{p^k}, 1)$. Действительно, из замечания 7 следует, что если функция $\varphi\colon \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}$ удовлетворяет условиям $\varphi(0) = 0$ и $\varphi(p) = 1$, то $\varphi \notin \Pi(\mathbb{Z}_{p^k}, 1)$. ■

Лемма 7. Пусть X — собственное подмножество множества $\mathbb{P}$. Тогда $\mathrm{RM}_p(\mathcal{Z}[1/X], \mathcal{Z}[1/X]) \nsubseteq \Pi(\mathbb{Z}[1/X], 1)$ для любого $p \in \mathbb{P} \setminus X$. В частности, $\Pi(\mathbb{Z}[1/X], 1) \neq \mathrm{RM}(\mathcal{Z}[1/X], \mathcal{Z}[1/X])$ и $\mathbb{Z}[1/X] \notin \mathfrak{D}$.

Доказательство. Пусть $p \in \mathbb{P} \setminus X$. Определим функцию $\pi \in \Pi_p(\mathbb{Z}[1/X], 1)$ формулой $\pi(x) = x^p - x$ ($x \in \mathbb{Z}[1/X]$). Легко видеть, что $\mathbb{Z}[1/X]/p\mathbb{Z}[1/X] \cong \mathbb{Z}_p$ (так как каждый элемент $\mathbb{Z}[1/X]$ представим дробью, знаменатель которой обратим по модулю p). Поэтому $\pi(\mathbb{Z}[1/X]) \subseteq p\mathbb{Z}[1/X]$ и π/p отображает $\mathbb{Z}[1/X]$ в $\mathbb{Z}[1/X]$. Кроме того, $\partial_{v_1} \ldots \partial_{v_{p+1}}(\pi/p) = (\partial_{v_1} \ldots \partial_{v_{p+1}}\pi)/p = 0$ для любых $v_1, \ldots, v_{p+1} \in \mathcal{Z}[1/X]$, так как $\pi \in \mathrm{RM}_p(\mathcal{Z}[1/X], \mathcal{Z}[1/X])$ (ввиду замечания 1). Поэтому $\pi/p \in \mathrm{RM}_p(\mathcal{Z}[1/X], \mathcal{Z}[1/X])$. Но легко видеть, что $\pi/p \notin \Pi(\mathbb{Z}[1/X], 1)$. Действительно, в противном случае функ-

ция π на бесконечном подмножестве $\mathbb{Z}[1/X]$ поля $\mathbb{Q}$ была бы представима многочленом с коэффициентами из $p\mathbb{Z}[1/X]$, что невозможно. ■

Замечание 8. В работе [11] Р. Димитрич ввёл понятие коузкой абелевой группы, а именно: абелева группа A *коузка*, если и только если $\mathrm{Hom}(A, \mathcal{Z}) = \{0\}$ или, что эквивалентно, A не содержит бесконечной циклической подгруппы, имеющей в A прямое дополнение (см. теорему 3 указанной работы). Предположим, что R — E-кольцо и $\Pi(R, 1) = \mathrm{RM}(\mathcal{R}, \mathcal{R})$ (ввиду утверждения 1 это верно, если $R \in \mathfrak{D}$). Покажем, что тогда группа $\mathcal{R}$ коузка. Пусть это не так. Тогда $\mathcal{R} \cong \mathcal{Z} \oplus B$ для некоторой абелевой группы B. Утверждение 1 леммы 5 показывает, что $\mathrm{Hom}(\mathcal{Z}, B) = \{0\}$. Следовательно, $B = \{0\}$, так как для любого $b \in B$ существует гомоморфизм из $\mathcal{Z}$ в B, переводящий 1 в b. Таким образом, $\mathcal{R} \cong \mathcal{Z}$ и $R \cong \mathbb{Z}$ (см. утверждение 2 леммы 5). Но тогда $\mathrm{RM}_p(\mathcal{R}, \mathcal{R}) \nsubseteq \Pi(R, 1)$ для любого $p \in \mathbb{P}$ ввиду леммы 7 (так как $\mathbb{Z} = \mathbb{Z}[1/\varnothing]$), что противоречит сделанному выше предположению.

Лемма 8. Пусть p — простое число. Тогда $\mathrm{RM}_p(\mathcal{J}_p, \mathcal{J}_p) \nsubseteq \Pi(\mathbb{J}_p, 1)$. В частности, $\Pi(\mathbb{J}_p, 1) \neq \mathrm{RM}(\mathcal{J}_p, \mathcal{J}_p)$ и $\mathbb{J}_p \notin \mathfrak{D}$.

Доказательство. Известно, что $\mathbb{J}_p/p\mathbb{J}_p \cong \mathbb{Z}_p$. Кроме того, $\mathbb{J}_p$ является бесконечным подкольцом поля p-адических чисел. Поэтому, рассуждая так же, как в доказательстве леммы 7, легко показать, что функция $x \mapsto (x^p - x)/p$ $(x \in \mathbb{J}_p)$ принадлежит $\mathrm{RM}_p(\mathcal{J}_p, \mathcal{J}_p)$, но не $\Pi(\mathbb{J}_p, 1)$. ■

Теорема 1.

1. Если группа $\mathcal{R}$ периодична или конечно порождена, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}_d$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$.
2. Если группа $\mathcal{R}$ не редуцирована, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$.
3. Если группа $\mathcal{R}$ является прямой суммой подгрупп ранга 1, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \mathbb{Z}_d$ или $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого свободного от квадратов числа $d \in \mathbb{N}_1$ (другими словами, когда R изоморфно прямой сумме конечного числа простых полей различных характеристик).
4. Если группа $\mathcal{R}$ редуцирована и копериодична, то $R \in \mathfrak{D}$ тогда и только тогда, когда $R \cong \prod\limits_{p \in P} \mathbb{Z}_p$ для некоторого множества P простых чисел.

Доказательство. Докажем сначала импликации «только тогда». Предположим, что $R \in \mathfrak{D}$. Тогда, в частности, R — E-кольцо и $\Pi(R, 1) = \mathrm{RM}(\mathcal{R}, \mathcal{R})$ (см. утверждение 1). Если $\mathcal{R}$ периодична, то $R \cong \mathbb{Z}_d$ для некоторого $d \in \mathbb{N}_1$ согласно утверждению 3 леммы 5. Если $\mathcal{R}$ конечно порождена, то из замечания 8 следует, что $\mathcal{R}$ конечна, поэтому данный случай сводится к предыдущему. Если $\mathcal{R}$ не редуцирована, то $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ для некоторого $d \in \mathbb{N}_1$ ввиду утверждения 4 леммы 5. Пусть теперь $\mathcal{R}$ является прямой суммой подгрупп ранга 1. Тогда утверждение 5 леммы 5 показывает, что $R \cong \mathbb{Z}_d \oplus \bigoplus\limits_{i=1}^{k} \mathbb{Z}[1/X_i]$, где $d \in \mathbb{N}_1$, $k \in \mathbb{N}_0$, а $X_1, \ldots, X_k$ — множества простых чисел, содержащие все простые делители числа d, причём $X_i \nsubseteq X_j$ при $i \neq j$ $(i, j \in \{1, \ldots, k\})$. Из утверждения 2 леммы 2 вытекает, что $\Pi(\mathbb{Z}[1/X_i], 1) = \mathrm{RM}(\mathcal{Z}[1/X_i], \mathcal{Z}[1/X_i])$ для всех $i \in \{1, \ldots, k\}$. Лемма 7 показывает теперь, что $X_1 = \cdots = X_k = \mathbb{P}$. Следовательно, $k \leqslant 1$, так как $X_i \nsubseteq X_j$ при $i \neq j$. Таким образом, в рассматриваемом случае $R \cong \mathbb{Z}_d$ или $R \cong \mathbb{Z}_d \oplus \mathbb{Q}$ (напомним, что $\mathbb{Z}[1/\mathbb{P}] = \mathbb{Q}$).

Для завершения доказательства импликаций «только тогда» в утверждениях 1–3 настоящей теоремы осталось доказать, что во всех рассмотренных выше случаях чис-

ло d свободно от квадратов. Пусть $d = \prod\limits_{p\in D} p^{k_p}$, где D — конечное подмножество $\mathbb{P}$, а $k_p \in \mathbb{N}_1$ для всех $p \in D$. Тогда $\mathbb{Z}_d \cong \bigoplus\limits_{p\in D} \mathbb{Z}_{p^{k_p}}$. Пусть теперь $p \in D$. Снова применив утверждение 2 леммы 2, получаем, что $\Pi(\mathbb{Z}_{p^{k_p}}, 1) = \mathrm{RM}(\mathcal{Z}_{p^{k_p}}, \mathcal{Z}_{p^{k_p}})$. Из леммы 6 вытекает требуемое равенство $k_p = 1$.

Пусть теперь $\mathcal{R}$ редуцирована и копериодична. Тогда утверждение 6 леммы 5 показывает, что $R \cong \prod\limits_{p\in P} R_p$, где $P \subseteq \mathbb{P}$ и $R_p \in \{\mathbb{Z}_{p^k} : k \in \mathbb{N}_1\} \cup \{\mathbb{J}_p\}$ для каждого $p \in P$. Из утверждения 2 леммы 2 вытекает, что $\Pi(R_p, 1) = \mathrm{RM}(\mathcal{R}_p, \mathcal{R}_p)$ для всех $p \in P$. Следовательно, $R_p = \mathbb{Z}_p$ ввиду лемм 6 и 8. Таким образом, импликации «только тогда» доказаны.

Докажем теперь импликации «тогда». Очевидно, что $\mathrm{Hom}(\mathcal{Z}_p, \mathcal{Z}_q) = \{0\}$ для любых различных простых чисел p и q. Легко также видеть, что $\mathrm{Hom}(\mathcal{Q}, \mathcal{Z}_p) = \{0\}$ (так как группа $\mathcal{Q}$ делима) и $\mathrm{Hom}(\mathcal{Z}_p, \mathcal{Q}) = \{0\}$ (так как группа $\mathcal{Q}$ не имеет кручения) для каждого $p \in \mathbb{P}$. Поэтому из следствия 1 и леммы 3 вытекает, что $\bigoplus\limits_{p\in D} \mathbb{Z}_p \in \mathfrak{D}$ и $\left(\bigoplus\limits_{p\in D} \mathbb{Z}_p\right) \oplus \mathbb{Q} \in \mathfrak{D}$ для любого конечного множества D простых чисел. Отсюда следуют импликации «тогда» в утверждениях 1–3 теоремы.

Пусть теперь P — произвольное подмножество $\mathbb{P}$. Тогда для любого $p \in P$ группа $\prod\limits_{q\in P\setminus\{p\}} \mathcal{Z}_q$ p-делима и, следовательно, $\mathrm{Hom}\left(\prod_{q\in P\setminus\{p\}} \mathcal{Z}_q, \mathcal{Z}_p\right) = \{0\}$. Поэтому $\prod\limits_{p\in P} \mathbb{Z}_p \in \mathfrak{D}$ ввиду следствия 1 и леммы 3, что и требовалось. Импликации «тогда» доказаны. ■

Замечание 9. Доказательство теоремы 1 показывает, что указанные в её формулировке изоморфизмы имеют место, даже если R — E-кольцо и $\Pi(R, 1) = \mathrm{RM}(\mathcal{R}, \mathcal{R})$ (а не только если $R \in \mathfrak{D}$). Поэтому если группа $\mathcal{R}$ удовлетворяет хотя бы одному из условий, указанных в теореме 1, то $R \in \mathfrak{D}$ тогда и только тогда, когда R является E-кольцом и $\Pi(R, 1) = \mathrm{RM}(\mathcal{R}, \mathcal{R})$

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Ященко В. В.* Некоторые характеристики «нелинейности» групповых отображений // Дискретный анализ и исследование операций. Сер. 1. 2001. Т. 8. № 1. С. 40–54.
2. *Анохин М. И.* О некоторых множествах групповых функций // Матем. заметки. 2003. Т. 74. № 1. С. 3–11.
3. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
4. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикладная дискретная математика. 2013. № 2(20). С. 26–38.
5. *Fuchs L.* Infinite Abelian Groups. Academic Press, 1970 (v. I), 1973 (v. II). Русс. пер.: *Фукс Л.* Бесконечные абелевы группы. М.: Мир, 1974 (т. 1), 1977 (т. 2).
6. *Fuchs L.* Abelian Groups. Springer, 2015.
7. *Schultz P.* The endomorphism ring of the additive group of a ring // J. Austral. Math. Soc. 1973. V. 15. No. 1. P. 60–69.
8. *Bowshell R. A. and Schultz P.* Unital rings whose additive endomorphisms commute // Math. Ann. 1977. V. 228. No. 3. P. 197–214.

9. *Riordan J.* Combinatorial identities. John Wiley & Sons, 1968. Русс. пер.: *Риордан Дж.* Комбинаторные тождества. М.: Наука, 1982.
10. *Jaballah A.* Subrings of **Q** // J. Sci. Technol. 1997. V. 2. No. 2. P. 1–13.
11. *Dimitrić R.* On coslender groups // Glasnik Matem. 1986. V. 21(41). No. 2. P. 327–329.

REFERENCES

1. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Nekotorye kharakteristiki "nelineynosti" gruppovykh otobrazheniy [Some characteristics of "nonlinearity" of group mappings]. Diskretn. Anal. Issled. Oper., Ser. 1, 2001, vol. 8, no. 1, pp. 40–54. (in Russian)
2. *Anokhin M. I.* On some sets of group functions. Math. Notes, 2003, vol. 74, no. 1, pp. 3–11.
3. *Cheremushkin A. V.* Additivnyy podkhod k opredeleniyu stepeni nelineynosti diskretnoy funktsii [An additive approach to nonlinear degree of discrete function]. Prikladnaya Diskretnaya Matematika, 2010, no. 2(8), pp. 22–33. (in Russian)
4. *Cheremushkin A. V.* Additivnyy podkhod k opredeleniyu stepeni nelineynosti diskretnoy funktsii na tsiklicheskoy gruppe primarnogo poryadka [An additive approach to nonlinearity degree of discrete functions on a primary cyclic group]. Prikladnaya Diskretnaya Matematika, 2013, no. 2(20), pp. 26–38. (in Russian)
5. *Fuchs L.* Infinite Abelian Groups. Academic Press, 1970 (v. I), 1973 (v. II).
6. *Fuchs L.* Abelian Groups. Springer, 2015.
7. *Schultz P.* The endomorphism ring of the additive group of a ring. J. Austral. Math. Soc., 1973, vol. 15, no. 1, pp. 60–69.
8. *Bowshell R. A. and Schultz P.* Unital rings whose additive endomorphisms commute. Math. Ann., 1977, vol. 228, no. 3, pp. 197–214.
9. *Riordan J.* Combinatorial identities. John Wiley & Sons, 1968.
10. *Jaballah A.* Subrings of **Q**. J. Sci. Technol., 1997, vol. 2, no. 2, pp. 1–13.
11. *Dimitrić R.* On coslender groups. Glasnik Matem., 1986, vol. 21(41), no. 2, pp. 327–329.