УДК 512.552.13

С. С. Коробков

РЕШЕТОЧНЫЕ ИЗОМОРФИЗМЫ КОНЕЧНЫХ КОЛЕЦ БЕЗ НИЛЬПОТЕНТНЫХ ЭЛЕМЕНТОВ

Введение

В данной работе рассматриваются ассоциативные кольца. Хорошо известно, что конечные кольца без ненулевых нильпотентных элементов разложимы в конечные прямые суммы конечных полей. Являясь коммутативными, такие кольца составляют важный подкласс в классе всех полупростых колец. До настоящего времени решеточные изоморфизмы полупростых колец не рассматривались (в отличие от ассоциативных алгебр, где первые работы по решеточным изоморфизмам были посвящены простым и полупростым алгебрам). В работе [1] автором изучены все случаи, когда аддитивная группа кольца, решеточно изоморфного кольцу с примарной аддитивной группой, не является примарной. Результаты этой работы позволяют рассматривать только те кольца, которые разложимы в прямые суммы конечных полей одинаковой характеристики. Всюду ниже R и R^φ — кольца с изоморфными решетками подколец, а φ — решеточный изоморфизм (иными словами — проектирование) кольца R на кольцо R^φ. При этом кольцо R^φ будем называть *проективным образом* кольца R, а само R — *проективным прообразом* кольца R^φ.

Работа состоит из трех частей. В первой части найдены все кольца, решеточно изоморфные произвольному конечному полю $GF(p^n)$. Оказалось, что за небольшим исключением (когда n — степень простого числа или произведение двух простых чисел) кольцо $(GF(p^n))^\varphi$ само является конечным полем, однако изоморфизма между $GF(p^n)$ и $(GF(p^n))^\varphi$ может и не быть (теорема 2.1, предложение 2.1).

Во второй части работы изучаются решеточные изоморфизмы колец, разложимых в прямые суммы конечных полей одной и той же характеристики. Здесь исследованы все случаи (их число равно двум), когда кольцо, решеточно изоморфное прямой сумме конечных полей, само неразложимо в прямую сумму полей (теорема 3.1). Основным результатом этой части работы является теорема 3.2, в которой доказано, что кольцо, решеточно изоморфное прямой сумме n конечных полей характеристики p при $n \geqslant 3$, также является прямой суммой n конечных полей характеристики q.

Пусть $R = F_1 \dotplus \cdots \dotplus F_n$, где $F_i \cong GF(p^{n_i})$ $(i = \overline{1,n})$. Главным вопросом, решаемым в третьей части работы, является вопрос о выполнении равенства

$$R^\varphi = F_1^\varphi \dotplus \cdots \dotplus F_n^\varphi. \tag{1}$$

Получены необходимые и достаточные условия для того, чтобы равенство (1) выполнялось для каждого решеточного изоморфизма φ кольца R. Эти условия заключаются в том, что каждое поле F_i не должно быть простым (теорема 4.1).

Часть результатов данной работы была анонсирована автором в [2].

Список принятых обозначений

$A \oplus B$	—	прямая сумма абелевых групп A и B
$A \dotplus B$	—	прямая сумма колец A и B
$\langle a_1, a_2, \ldots, a_n \rangle$	—	кольцо, порожденное элементами $a_1, a_2, \ldots, a_n$
$\mathbf{0} = \{0\}$	—	нулевое подкольцо кольца R
$L(R)$	—	решетка подколец кольца R
$l(R)$	—	длина кольца R, т. е. длина решетки $L(R)$
$char\, R$	—	характеристика кольца R
$o(r)$	—	аддитивный порядок элемента r
$ind\, r$	—	индекс нильпотентности элемента r
k, l, m, n	—	натуральные числа
p, q, p_i, q_j $(i, j \in \mathbb{N})$	—	простые числа

Малые греческие буквы с индексами и без индексов, если не оговорено специально, обозначают целые числа.

1. Предварительные сведения

Доказательство основных утверждений данной работы существенно опирается на описание колец длины 2 или 3, содержащееся в статье [6]. Для удобства читателя приведем необходимые сведения из этой статьи.

Лемма 1.1. *Решетка $L(R)$ имеет диаграмму, представленную на рис. 1, тогда и только тогда, когда кольцо R изоморфно одному из следующих колец:*

$R_1 = \langle e_1 \rangle \dotplus \langle e_2 \rangle$, $o(e_i) = p$, $e_i^2 = e_i$ $(i = 1, 2)$;
$R_2 = \langle e \rangle \oplus \langle r \rangle$, $o(e) = o(r) = 2$, $e^2 = e$, $r^2 = 0$, $er = r$, $re = 0$;
$R_3 = \langle e \rangle \oplus \langle r \rangle$, $o(e) = o(r) = 2$, $e^2 = e$, $r^2 = 0$, $er = 0$, $re = r$;
$R_4 = \langle r_1 \rangle \dotplus \langle r_2 \rangle$, $o(r_i) = 2$, $r_i^2 = 0$ $(i = 1, 2)$.

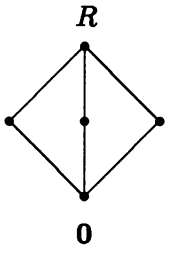


Рис. 1

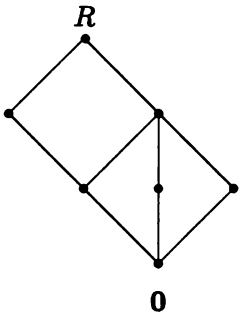


Рис. 2

Лемма 1.2. *Решетка $L(R)$ имеет диаграмму, представленную на рис. 2, тогда и только тогда, когда кольцо R изоморфно одному из следующих колец:*

$R_5 = GF(p^q) \dotplus GF(p)$;
$R_6 = \langle e \rangle \dotplus \langle r \rangle$, $o(e) = 2^2$, $o(r) = 2$, $e^2 = e$, $r^2 = 0$;
$R_7 = \langle e \rangle \oplus \langle r \rangle$, $o(e) = 2^2$, $o(r) = 2$, $e^2 = e$, $r^2 = 0$, $er = re = r$.

Лемма 1.3. *Пусть $R = \langle e_1 \rangle \dotplus \langle e_2 \rangle \dotplus \langle e_3 \rangle$, где $e_i^2 = e_i$, $o(e_i) = p$ $(i = 1, 2, 3)$. Тогда $R^\varphi = \langle e_1' \rangle \dotplus \langle e_2' \rangle \dotplus \langle e_3' \rangle$, где $e_i'^2 = e_i'$; $o(e_i') = q$ $(i = 1, 2, 3)$.*

Лемма 1.4. *Решетка подколец кольца $R = F_1 \dotplus F_2$, где $F_i = \langle f_i \rangle$ — поле с единицей e_i $(i = 1, 2)$, изоморфное $GF(p^q)$, имеет диаграмму, представленную на рис. 3.*

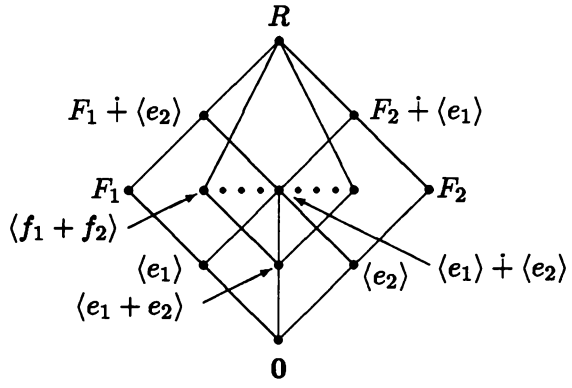


Рис. 3

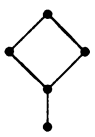
Это утверждение также доказано в [6]. Сделаем необходимое пояснение к рис. 3: многоточие означает, что кольцо R содержит q подколец, изоморфных полю $\langle f_1 + f_2 \rangle$. Все эти подкольца содержат подкольцо $\langle e_1 + e_2 \rangle$ и являются максимальными в R.

2. Кольца, решеточно изоморфные конечному полю

Предложение 2.1. *Кольца $GF(p^n)$ и $GF(q^m)$ решеточно изоморфны тогда и только тогда, когда либо $n = m = 1$, либо n и m имеют канонические разложения $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и $q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ соответственно.*

Доказательство. Любое ненулевое подкольцо конечного поля является подполем в нем и потому множество всех ненулевых подколец образует решетку, которая совпадает с решеткой подполей. Решетка подполей конечного поля $GF(p^n)$ изоморфна решетке натуральных делителей числа n (этот факт вытекает из критерия подполя конечного поля, см., например, [3, с. 68]). Решетки натуральных делителей чисел n и m изоморфны тогда и только тогда, когда либо $n = m = 1$, либо n и m имеют канонические разложения $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и $q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ соответственно.

Теорема 2.1. *Пусть $R \cong GF(p^n)$. Тогда либо $R^\varphi \cong GF(q^m)$, либо R^φ изоморфно одному из колец R_8–R_{11}, указанных в таблице.*

n	$L(R)$	R^φ
p_1^k, где $k \in \mathbb{N} \cup \{0\}$	Цепь длины $k+1$	$R_8 = \langle e \rangle$, $o(e) = q^{k+1}$, $e^2 = e$, $(k > 0)$ $R_9 = \langle r \rangle$, $o(r) = q^{k+1}$, $r^2 = q^s r$, $s = \overline{1, k+1}$ $R_{10} = \langle r \rangle$, $o(r) = q$, $r^2 \neq 0$, $r^3 = 0$, $(k = 1)$
$p_1 p_2$		$R_{11} = \langle e, r \rangle$, $o(e) = q^2$, $e^2 = e$, $o(r) = q$, $er = re = r$, $r^2 = \gamma q e$, причем либо $\gamma = 1$, либо $q \neq 2$ и γ — не квадрат в $GF(q)$

Доказательство. Так как конечное поле имеет дистрибутивную решетку подколец, то к кольцам R и R^φ можно применить описание колец с дистрибутивной решеткой подколец [5, теорема 11]. Согласно этому описанию и с учетом конечности решетки $L(R)$, заключаем, что либо $R^\varphi \cong GF(q^m)$, либо R^φ изоморфно одному из колец R_8–R_{11}, указанных в таблице. Если $R^\varphi \cong R_i$ $(i = 8, 9, 10)$, то $L(R)$ — цепь и потому $R \cong GF(p^{p_1^k})$; если $R^\varphi \cong R_{11}$, то $R \cong GF(p^{p_1 p_2})$.

Следствие 2.1. *Пусть $R \cong GF(p^n)$ и $n > 1$. Тогда, если n не является степенью простого числа и не является произведением двух простых чисел, $R^\varphi \cong GF(q^m)$.*

Следствие 2.2. *Пусть $R \cong GF(p^n)$ и $n > 1$. Тогда, если R^φ не содержит ненулевых нильпотентных элементов, $R^\varphi \cong GF(q^m)$.*

Следствие 2.3. *Пусть $R \cong GF(p^n)$. Тогда R^φ — коммутативное кольцо.*

3. Кольца, решеточно изоморфные прямым суммам конечных полей

Теорема 3.1. *Пусть $R = F_1 \dotplus F_2$, где $F_1 \cong GF(p^n)$, $F_2 \cong GF(p^m)$ и кольцо R^φ не разложимо в прямую сумму полей. Тогда R^φ изоморфно одному из колец R_2–R_4, R_6, R_7.*

Доказательство. Пусть e_i — единица поля F_i. Любое минимальное подкольцо кольца R содержится в подкольце $S = \langle e_1\rangle \dotplus \langle e_2\rangle$. Действительно, любое минимальное подкольцо в R порождено ненулевым идемпотентным элементом. Таких элементов в R всего три: e_1, e_2, e_1+e_2. Диаграмма решетки подколец кольца S представлена на рис. 4. Используя лемму 1.1, заключаем, что R^φ — q-кольцо. Предположим, что кольцо R^φ не разложимо в прямую сумму конечных полей. Тогда R^φ содержит ненулевой нильпотентный элемент. Согласно той же лемме 1.1 подкольцо S^φ изоморфно одному из колец R_2–R_4. Если $R = S$, то ясно, что $n = m = 1$.

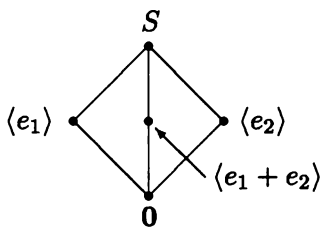


Рис. 4

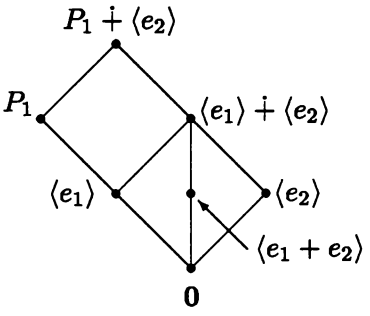


Рис. 5

Предположим далее, что $R \neq S$. Тогда хотя бы одно из полей F_1 или F_2 (пусть для определенности это будет поле F_1) содержит подполе P_1 длины 2. Согласно лемме 1.2 диаграмма решетки подколец подкольца $P_1 \dotplus \langle e_2\rangle$ представлена на рис. 5. При этом $P_1^\varphi = \langle e\rangle$, где $o(e) = 2^2$, $\langle e_1\rangle^\varphi = \langle 2e\rangle$. Если $R = P_1 \dotplus \langle e_2\rangle$, то, согласно той же лемме 1.2, $R^\varphi \cong R_i$, где $i = 6, 7$.

Допустим, что $F_2 \neq \langle e_2\rangle$. Тогда поле F_2 содержит подполе P_2 длины 2. Диаграмма решетки подколец подкольца $\langle e_1\rangle \dotplus P_2$ имеет такой же вид, как и диаграмма решетки подколец кольца $P_1 \dotplus \langle e_2\rangle$. Поэтому аналогично заключаем, что $P_2^\varphi \cong \langle u\rangle$, где u — идемпотентный элемент порядка 2^2, а $\langle e_2\rangle^\varphi = \langle 2u\rangle$.

Докажем, что элемент eu равен 0. Так как элементы $2e$ и $2u$ нильпотентны, то из описания колец R_6 и R_7 (а лишь им могут быть изоморфны подкольца $(P_1 \dotplus \langle e_2\rangle)^\varphi$ и $(\langle e_1\rangle \dotplus P_1)^\varphi$) следует, что $2(eu) = (2e)u \in \langle 2e\rangle$ и

$2(eu) = e(2u) \in \langle 2u\rangle$. Значит, $2(eu) \in \langle e\rangle \cap \langle u\rangle = \mathbf{0}$ и потому $2(eu) = 0$. Если $eu \neq 0$, рассмотрим в подкольце $\langle eu\rangle$ минимальное подкольцо $T = \langle t\rangle$. Пусть

$$t = \alpha_1(eu) + \alpha_2(eu)^2 + \cdots + \alpha_k(eu)^k. \tag{2}$$

Поскольку в кольце R все минимальные подкольца содержатся в подкольце S, то $T \subset \langle 2e\rangle \dotplus \langle 2u\rangle$. Это означает, что $t = \alpha(2e) + \beta(2u)$ для некоторых $\alpha, \beta \in \{0, 1\}$. С учетом равенства (2) имеем равенство

$$\alpha 2e + \beta 2u = \alpha_1(eu) + \alpha_2(eu)^2 + \cdots + \alpha_k(eu)^k. \tag{3}$$

Умножая обе части равенства (3) на e слева, а затем на u справа, получим

$$\alpha 2e + \beta 2u = \alpha 2e = \beta 2u,$$

откуда $\alpha = \beta = 0$ и потому $t = 0$. Это означает, что $eu = 0$. Аналогично доказывается, что $ue = 0$. Таким образом, кольцо $\langle e\rangle \dotplus \langle u\rangle$ состоит из 12 элементов. Нетрудно видеть, что это кольцо имеет диаграмму решетки подколец, представленную на рис. 6, *а*.

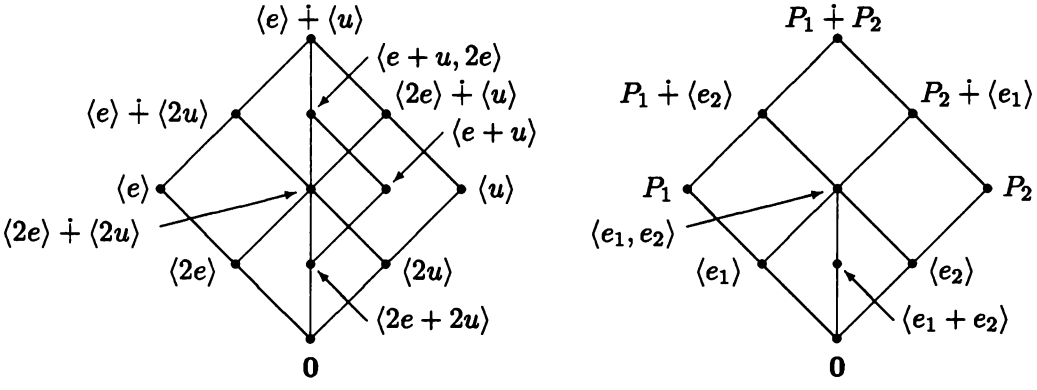


Рис. 6

Из леммы 1.4 следует, что $P_1 \not\cong P_2$. Покажем, что диаграмма решетки подколец кольца $P_1 \dotplus P_2$ имеет вид как на рис. 6, *б*. Диаграммы решеток подколец колец $P_1 \dotplus \langle e_2\rangle$ и $P_2 \dotplus \langle e_1\rangle$ представлены на рис. 6. Пусть $y \in P_1 \dotplus P_2$ и $y \notin P_1 \dotplus \langle e_2\rangle$, $y \notin P_2 \dotplus \langle e_1\rangle$. Тогда $y = y_1 + y_2$, где $y_i \in P_i \setminus \langle e_i\rangle$ $(i = 1, 2)$. Ясно, что $\langle y_i\rangle = P_i$. Пусть $f_1(x)$ — минимальный многочлен элемента y_1. Поскольку $P_1 \not\cong P_2$, то $f_1(y_2) \neq 0$, а значит, $f_1(y_1 + y_2) = f_1(y_2) \in \langle y_1 + y_2\rangle$.

Подкольцо $\langle f_1(y_2)\rangle$ является подполем в P_2 и потому содержит его единицу e_2. Отсюда следует, что $y_2 = (y_1 + y_2)e_2 \in \langle y_1 + y_2\rangle$ и, следовательно, $\langle y_1 + y_2\rangle = P_1 \dotplus P_2$. Это означает, что в $P_1 \dotplus P_2$ все собственные подкольца содержатся в подкольцах $P_1 \dotplus \langle e_2\rangle$ и $P_2 \dotplus \langle e_1\rangle$.

Сравнивая рис. 6,*а* и 6,*б*, убеждаемся в том, что решетки подколец колец $P_1 \dotplus P_2$ и $\langle e\rangle \dotplus \langle u\rangle$ не изоморфны. Следовательно, предположение о том, что $F_2 \neq \langle e_2\rangle$, неверно.

По предположению $P_1^\varphi = \langle e\rangle$ и $o(e) = 2^2$. Следовательно, кольцо F_1^φ не является полем и если $F_1 \neq P_1$, то по теореме 2.1 $F_1 = GF(p^{p_1p_2})$. Пусть для определенности $P_1 = GF(p^{p_1})$ и $P_3 = GF(p^{p_2})$. Тогда $P_3^\varphi = \langle r\rangle$, где r — нильпотентный элемент индекса 3 и $2r = 0$. Кольцо $P_3 \dotplus \langle e_2\rangle$ удовлетворяет условиям леммы 1.2, и потому диаграмма его решетки подколец имеет вид как на рис. 2. Из той же леммы следует, что кольца с такой решеткой подколец не содержат нильпотентных элементов индекса 3. Таким образом, предположение о том, что $F_1 \neq P_1$, неверно. Теорема доказана.

Следствие 3.1. *Пусть $R = F_1 \dotplus F_2$, где F_i — конечное поле характеристики p. Тогда если $l(F_1) + l(F_2) > 3$, то R^φ разложимо в прямую сумму конечных полей одной и той же характеристики.*

Лемма 3.1. *Пусть $R = \langle e_1\rangle \dotplus \cdots \dotplus \langle e_n\rangle$, где $n \geqslant 3$, $e_i^2 = e_i$, $o(e_i) = p$. Тогда $R^\varphi = \langle e_1'\rangle \dotplus \cdots \dotplus \langle e_n'\rangle$, где $e_i'^2 = e_i'$, $o(e_i') = q$.*

Доказательство. Покажем сначала, что в R^φ нет ненулевых нильпотентных элементов. Пусть $T' = \langle t'\rangle$ — минимальное подкольцо в R^φ, а $T = \langle e\rangle$ — его прообраз в кольце R. Ясно, что $e^2 = e \neq 0$. Пусть $e = \alpha_1e_1 + \cdots + \alpha_ne_n$. Очевидно, что все коэффициенты α_i принадлежат множеству $\{0, 1\}$. Кроме того, легко видеть, что найдутся три ортогональных идемпотента $u_1, u_2, u_3 \in R$, для которых $e \in U = \langle u_1\rangle \dotplus \langle u_2\rangle \dotplus \langle u_3\rangle$. Согласно лемме 1.3 U^φ — прямая сумма трех простых полей. Следовательно, элемент t не нильпотентен, а значит, R^φ не содержит ненулевых нильпотентных элементов. Поскольку кольцо R^φ конечно, то оно разложимо в прямую сумму полей. Так как для всякого элемента x из R выполнено равенство $x^p = x$, то R не содержит подполей длины 2. Это означает, что кольцо R^φ не содержит подполей длины $\geqslant 2$, а потому R^φ — прямая сумма простых полей одинаковой характеристики. Пусть $R^\varphi = \langle e_1'\rangle \dotplus \cdots \dotplus \langle e_m'\rangle$, где $e_i'^2 = e_i'$, $o(e_i') = q$. Кольца R и R^φ можно рассматривать как алгебры над полями $GF(p)$ и $GF(q)$ соответственно. Ясно, что $n = \dim R = l(R) = l(R^\varphi) = \dim R^\varphi = m$.

Следствие 3.2. *Пусть $R = F_1 \dotplus F_2$, где F_1, F_2 — конечные поля характеристики p, и пусть кольцо R^φ разложимо в прямую сумму полей. Тогда $R^\varphi = P_1 \dotplus P_2$, где P_1, P_2 — конечные поля характеристики q.*

Теорема 3.2. *Пусть кольцо R разложимо в прямую сумму n конечных полей характеристики p и $n \geqslant 3$. Тогда R^φ есть прямая сумма n конечных полей характеристики q.*

Доказательство. Пусть $R = F_1 \dot{+} \cdots \dot{+} F_n$ и e_i — единица поля F_i. Ясно, что все минимальные подкольца в R содержатся в подкольце $S = \langle e_1 \rangle \dot{+} \cdots \dot{+} \langle e_n \rangle$. По лемме 3.1 $S^\varphi = \langle e_1' \rangle \dot{+} \cdots \dot{+} \langle e_n' \rangle$, где $e_i'^2 = e_i' \neq 0$. Это означает, что R^φ не содержит ненулевых нильпотентных элементов и потому R^φ разложимо в прямую сумму конечных полей. Число слагаемых в этой сумме равно $l(S^\varphi)$, т. е. равно n.

Предложение 3.1. *Пусть R — конечное p-кольцо без ненулевых нильпотентных элементов. Тогда если кольцо R^φ не коммутативно, то $R \cong GF(p) \dot{+} GF(p)$, а $R^\varphi \cong R_5$.*

Доказательство. Если кольцо R^φ не коммутативно, то оно не равно нулю и не разложимо в прямую сумму полей. По следствию 2.3 R не является полем, а по теореме 3.2 R не разложимо в прямую сумму трех и более конечных полей. Следовательно, $R = F_1 \dot{+} F_2$, где $F_i \cong GF(p^{n_i})$ $(i = 1, 2)$. Поскольку R^φ не разложимо в прямую сумму полей, то по теореме 3.1 $R^\varphi \cong R_5$.

Поскольку для конечного ненулевого кольца условия не иметь ненулевых нильпотентных элементов и быть разложимым в прямую сумму конечных полей эквивалентны, то из теорем 2.1, 3.1 и 3.2 вытекает следующее

Предложение 3.2. *Пусть R — конечное p-кольцо без ненулевых нильпотентных элементов. Тогда если кольцо R^φ содержит ненулевые нильпотентные элементы, то $R^\varphi \cong R_i$, где $i = \overline{1,8}$.*

4. Инвариантность прямых сумм при проектированиях

Лемма 4.1. *Пусть $R = F_1 \dot{+} F_2$, где F_i — конечное поле характеристики p $(i = 1, 2)$. Пусть P — произвольное поле в R. Тогда справедливы следующие утверждения:*

1) $l(P) \leqslant \min\{l(F_1), l(F_2)\}$;

2) *если* $l(F_1) < l(P) \leqslant l(F_2)$, *то* $P \subseteq F_2$;

3) *если* $\langle U, V \rangle = U \dot{+} V$ *для некоторых подколец кольца R, то либо* $U \subseteq F_1$, $V \subseteq F_2$, *либо* $U \subseteq F_2$, $V \subseteq F_1$.

Доказательство. 1. Утверждение очевидно, если $P \subseteq F_1$ или $P \subseteq F_2$. Пусть $P \not\subseteq F_i$. Тогда $P = \langle f_1 + f_2 \rangle$, где $f_i \in F_i$. Ясно, что $f_i \neq 0$. Так как P — конечное поле, то для некоторого натурального числа k выполняется равенство

$(f_1+f_2)^k = f_1+f_2$, откуда следует, что $f_i^k = f_i$. Если k — наименьшее натуральное число с таким свойством для элемента f_1+f_2, то очевидно, что для любого натурального числа m, меньшего k, выполнено неравенство $f_i^m \neq f_i$. Следовательно, $\langle f_1+f_2\rangle \cong GF(k) \cong \langle f_i\rangle$ и потому $l(P) \leqslant \min\{l(F_1), l(F_2)\}$.

2. Пусть $l(F_1) < l(P) \leqslant l(F_2)$ и $P = \langle f_1+f_2\rangle$, где $f_i \in F_1$. Допустим, что $f_1 \neq 0$. Тогда $f_2 \neq 0$. Так же, как и выше, $\langle f_1+f_2\rangle \cong GF(k) \cong \langle f_1\rangle$ и потому $l(P) \leqslant l(\langle f_1\rangle) \leqslant l(F_1)$, что противоречит условию. Значит, $f_1 = 0$, а потому $P \subseteq F_2$.

3. Если a и b — делители нуля в R, то очевидно, что либо $a \in F_1$ и $b \in F_2$, либо $a \in F_2$ и $b \in F_1$

Лемма 4.2. *Пусть* $R = F_1 \dotplus F_2$, *где* $F_i \cong GF(p^q)$ $(i = 1,2)$. *Тогда* $R^\varphi = F_1^\varphi \dotplus F_2^\varphi$.

Доказательство. По следствиям 3.1 и 3.2 кольцо R^φ разложимо в прямую сумму двух конечных полей $P_1^\varphi \dotplus P_2^\varphi$ одинаковой характеристики. Предположим, что $F_1^\varphi \neq P_1^\varphi$ и $F_1^\varphi \neq P_2^\varphi$. Тогда F_1^φ — поле длины 2 в R^φ, содержащее единицу e' кольца R^φ. Согласно лемме 1.4 в R^φ найдется подполе T^φ, для которого $F_1^\varphi \cap T^\varphi = \langle e'\rangle$. Проективный прообраз T поля T^φ также является полем длины 2 в R. Поскольку $T \neq F_1$, то $T \cap F_1 = \mathbf{0}$. Получаем противоречие, из которого следует, что $F_1^\varphi = P_1^\varphi$ или $F_1^\varphi = P_2^\varphi$. В соответствии с этим имеем, что $F_2^\varphi = P_2^\varphi$ или $F_2^\varphi = P_1^\varphi$. Таким образом, $R^\varphi = F_1^\varphi \dotplus F_2^\varphi$.

Теорема 4.1. *Пусть* $R = F_1 \dotplus \cdots \dotplus F_n$, *где* $n > 1$, $F_i \cong GF(p^{k_i})$ $(i = \overline{1,n})$. *Тогда для того, чтобы для любого решеточного изоморфизма* φ *выполнялось равенство* (1), *необходимо и достаточно, чтобы* $l(F_i) > 1$ $(i = \overline{1,n})$.

Доказательство. Достаточность. Предположим сначала, что $n = 2$. По следствиям 3.1 и 3.2 кольцо R^φ разложимо в прямую сумму двух конечных полей $P_1^\varphi \dotplus P_2^\varphi$ одинаковой характеристики q. По следствию 2.2 проективный прообраз P_i поля P_i^φ является полем.

Рассмотрим случай, когда $\text{НОД}(n_1,n_2) < n_1 \leqslant n_2$. Пусть $P_1 = \langle f_1+f_2\rangle$, где $f_i \in F_1$ $(i = 1,2)$. Если $f_1 \neq 0$ и $f_2 \neq 0$, то ясно, что $\langle f_1\rangle \cong \langle f_2\rangle \cong GF(p^k)$, где $k \mid \text{НОД}(n_1,n_2)$. Поскольку $k \leqslant \text{НОД}(n_1,n_2) < n_1 \leqslant n_2$, то $l(P_1) < l(F_i)$ $(i = 1,2)$. По следствию 2.2 F_i^φ — поле $(i = 1,2)$ и так как $l(F_i^\varphi) = l(F_i) > l(P_1) = l(P_1^\varphi)$, то по лемме 4.1 $F_i^\varphi \subseteq P_2^\varphi$, что невозможно. Значит, либо $f_1 = 0$, либо $f_2 = 0$ и потому $P_1^\varphi = F_1^\varphi$ или $P_1^\varphi = F_2^\varphi$. Соответственно имеем $P_2^\varphi = F_2^\varphi$ или $P_2^\varphi = F_1^\varphi$, а значит, $R^\varphi = F_1^\varphi \dotplus F_2^\varphi$.

Пусть теперь $\text{НОД}(n_1,n_2) = n_1 \leqslant n_2$. Рассмотрим тогда в кольце R подкольцо $T = T_1 \dotplus T_2$, где $T_i \subseteq F_i$, $T_i \cong GF(p^q)$ и n делит $\text{НОД}(n_1,n_2)$. По лемме 4.2 $T^\varphi = T_1^\varphi \dotplus T_2^\varphi$, а по утверждению 3 леммы 4.1 либо $T_i^\varphi \subseteq P_i^\varphi$,

либо $T_1^\varphi \subseteq P_2^\varphi$ и $T_2^\varphi \subseteq P_1^\varphi$. В соответствии с этим имеем либо $F_i^\varphi \subseteq P_i^\varphi$, либо $F_1^\varphi \subseteq P_2^\varphi$ и $F_2^\varphi \subseteq P_1^\varphi$. Переходя к проективным прообразам колец F_i^φ и P_i^φ, получим $F_i \subseteq P_i$ и потому $F_i = P_i$ $(i = 1, 2)$ либо $F_1 \subseteq P_2$, $F_2 \subseteq P_1$ и потому $F_1 = P_2$, $F_2 = P_1$. В каждом из этих случаев выполнено равенство (1).

Пусть теперь $n > 2$. Тогда, согласно предыдущему, для любых $i, j = \overline{1,n}$ выполнено равенство $(F_i \dotplus F_j)^\varphi = F_i^\varphi \dotplus F_j^\varphi$. Следовательно, $R^\varphi = F_1^\varphi \dotplus \cdots \dotplus F_n^\varphi$.

Необходимость. Предположим, что $l(F_n) = 1$. Пусть e_i — единица поля F_i $(i = \overline{1,n})$. Обозначим подкольцо $F_1 \dotplus \cdots \dotplus F_{n-1}$ через F. Тогда ясно, что $R = F \dotplus \langle e_n \rangle$. Сделаем несколько очевидных замечаний об идемпотентах кольца R. Пусть E — множество всех его ненулевых идемпотентов. Тогда

1) $\forall u \in E \; \exists\, i_1, \ldots, i_k \in \{1, \ldots, n\}$ $(u = e_{i_1} + \cdots + e_{i_k})$;

2) элемент $e = e_1 + \cdots + e_n$ является единицей в кольце R;

3) $\forall u, v \in E \; \exists\, \overline{u} \in E \cup \{0\}$ $(uv = v \Longrightarrow u = v + \overline{u} \;\&\; u\overline{u} = 0)$.

Дальнейшее доказательство разобьем на несколько частей.

1. Пусть U — подкольцо в R, не содержащееся в F и не содержащее e_n. Тогда в U есть элемент $u = a + e_n$, где $a \in F \setminus \{0\}$. Зафиксируем такой многочлен $f(x) \in GF(p)[x]$, что $f(a) = b$ — единица подкольца $\langle a \rangle$. Пусть $f(e_n) = \alpha e_n$. Так как $f(u) = b + \alpha e_n$, то ясно, что $\alpha \not\equiv 0 \pmod p$. Если $\alpha \not\equiv 1 \pmod p$, то $\alpha^2 \not\equiv \alpha \pmod p$ и потому $(f(u))^2 - f(u) = (\alpha^2 - \alpha)e_n$. Тогда $e_n \in U$, что противоречит условию. Следовательно, $f(u) = b + e_n$, причем $b + e_n$ — единица в кольце $\langle u \rangle$. Рассмотрим множество

$$B = \{b \in F \mid b^2 = b \;\&\; b + e_n \in U\}.$$

Это множество конечно и не содержит нуля кольца R. Обозначим произведение всех элементов множества B через c. Тогда c — ненулевой идемпотент в кольце F и так как $c + e_n \in U$, то $c \in B$. Кроме того, по определению

$$\forall b \in B \; bc = c. \tag{4}$$

2. Рассмотрим идемпотент $c + e_n$. Предположим сначала, что $c + e_n$ — единица кольца U. Тогда для любого ненулевого идемпотента v из U $(c + e_n)v = v$ и потому из замечания 3 следует, что $c + e_n = v + d$ для некоторого идемпотента d из U, причем $vd = 0$. Предположим, что $d = d_1 + e_n$ для некоторого идемпотента d_1. Поскольку $d \in U$, то $d_1 \in B$, а значит, согласно (4), $d_1 c = c$. Имеем далее $d = d(c + e_n) = (d_1 + e_n)(c + e_n) = c + e_n$ и потому $v = 0$. Получаем противоречие, из которого следует, что $v = v_1 + e_n$ для некоторого идемпотента v_1 из F. Проводя аналогичные рассуждения, получим, что $d = 0$,

откуда $v = c + e_n$. Это означает, что U содержит единственный ненулевой идемпотент $c + e_n$ и потому U — поле с единицей $c + e_n$. Предположим, что это поле не является простым. Тогда в нем содержится элемент y, для которого $y^p \neq y$. Пусть $y = f + \alpha e_n$, где $f \in F$, $\alpha \in \mathbb{Z}$. Так как $y^p - y = f^p - f \neq 0$, то $\langle y \rangle \cap F \neq \mathbf{0}$. Но тогда в подкольце $\langle y \rangle$ найдется ненулевой идемпотент, отличный от $c + e_n$, что невозможно. Следовательно, U — простое поле, т. е. $U = \langle c + e_n \rangle$.

3. Допустим, что $c + e_n$ не является единицей кольца U. Рассмотрим тогда пирсовское разложение $U = (e - (c + e_n))U \dotplus (c + e_n)U$ кольца U по идемпотенту $c + e_n$. Поскольку $e - (c + e_n) \in F$ и F — идеал в R, то $(e - (c + e_n))U = T$ — подкольцо в F. Идемпотент $c + e_n$ является единицей в подкольце $(c + e_n)U$. Согласно предыдущему пункту доказательства $(c + e_n)U = \langle c + e_n \rangle$. Таким образом, $U = T \dotplus \langle c + e_n \rangle$.

4. Пусть U — произвольное подкольцо в R. Тогда из пп. 1–3 следует, что подкольцо U представимо, и притом единственным образом, в виде

$$U = \begin{cases} T; \\ T \dotplus \langle e_n \rangle; \\ T \dotplus \langle c + e_n \rangle, \end{cases}$$

где T — подкольцо в F, а c — ненулевой идемпотент из F, для которого $Tc = \mathbf{0}$.

5. Зададим отображение $\varphi : L(R) \to L(R)$ следующим образом:

$$U^\varphi = \begin{cases} U, \text{ если } U \subseteq F; \\ T \oplus \langle e \rangle, \text{ если } U = T \dotplus \langle e_n \rangle; \\ T \oplus \langle e - c \rangle, \text{ если } U = T \dotplus \langle c + e_n \rangle. \end{cases}$$

Покажем, что φ^2 — тождественное отображение $L(R)$ на себя. Действительно, пусть U — произвольное подкольцо из R. Тогда, если $U \subseteq F$, то $(U^\varphi)^\varphi = U^\varphi = U$.

Пусть $U = T \dotplus \langle e_n \rangle$. Тогда $U^\varphi = T \oplus \langle e \rangle$. Если $T = \mathbf{0}$, то

$$(U^\varphi)^\varphi = \langle e \rangle^\varphi = \langle e - (e_i + \cdots + e_{n-1}) \rangle = \langle e_n \rangle = U.$$

Если $T \neq \mathbf{0}$, то в подкольце T содержится единица t. Пусть $c = e - t - e_n$. Тогда $U^\varphi = T \dotplus \langle c + e_n \rangle$ и потому

$$(U^\varphi)^\varphi = T \oplus \langle e - c \rangle = T \oplus \langle t + e_n \rangle = T \dotplus \langle e_n \rangle = U.$$

Пусть $U = T \dotplus \langle c + e_n \rangle$. Согласно определению отображения φ имеем $U^\varphi = T \oplus \langle e - c \rangle$. В случае, когда $T = \mathbf{0}$, имеем

$$(U^\varphi)^\varphi = \langle e - c \rangle^\varphi = \langle e - (e - c - e_n) \rangle = \langle c + e_n \rangle = U.$$

Предположим, что $T \neq \mathbf{0}$. Тогда так же, как и выше, $T \oplus \langle e-c\rangle = T \dotplus \langle e-c-t\rangle$, где t — единица подкольца T. Следовательно,

$$(U^\varphi)^\varphi = T \oplus \langle e - (e - c - t - e_n)\rangle = T \oplus \langle c + t + e_n\rangle = T \dotplus \langle c + e_n\rangle = U.$$

Таким образом, φ — обратимое, а значит, и биективное отображение $L(R)$ на себя.

6. Пусть U, V — подкольца R и

$$U \subseteq V. \tag{5}$$

Докажем, что

$$U^\varphi \subseteq V^\varphi. \tag{6}$$

Включение (6) очевидно, если $U \subseteq F$ или $U = R$. Предположим, что $U = T_1 \dotplus \langle e_n\rangle$, где T_1 — подкольцо в F. Тогда подкольцо V содержит элемент e_n и потому $V = T_2 \dotplus \langle e_n\rangle$. Ясно, что $T_1 \subseteq T_2$, а значит,

$$U^\varphi = T_1 \oplus \langle e\rangle \subseteq T_2 \oplus \langle e\rangle = V^\varphi.$$

Пусть $U = T_1 \dotplus \langle c_1 + e_n\rangle$. Возможны два случая: либо $V = T_2 \dotplus \langle c_2 + e_n\rangle$, либо $V = T_2 \dotplus \langle e_n\rangle$. Предположим сначала, что $V = T_2 \dotplus \langle c_2 + e_n\rangle$. Так как $U \subseteq V$, то $T_1 = F \cap U \subseteq F \cap V = T_2$ и $c_1 c_2 = c_2$. Из последнего равенства следует, что $c_1 = c_2 + s$ для некоторого элемента s из T_2. Имеем

$$U^\varphi = T_1 \oplus \langle e - c_1\rangle = T_1 \oplus \langle e - c_2 - s\rangle \subseteq T_1 \vee \langle s\rangle \vee \langle e - c_2\rangle \subseteq T_2 \oplus \langle e - c_2\rangle = V^\varphi.$$

Пусть теперь $V = T_2 \dotplus \langle e_n\rangle$. Тогда $c_1 \in T_2$ и потому

$$U^\varphi = T_1 \oplus \langle e - c_1\rangle \subseteq T_2 \oplus \langle e\rangle = V^\varphi.$$

Из этих рассуждений следует, что φ — изотонное отображение.

Пусть теперь выполнено включение (6). Тогда $U = (U^\varphi)^\varphi \subseteq (V^\varphi)^\varphi = V$. Таким образом, $U \subseteq V \iff U^\varphi \subseteq V^\varphi$. Это с учетом биективности φ означает, что φ — автоморфизм решетки $L(R)$. При этом равенство (1) не выполняется, так как $F_n^\varphi = \langle e\rangle$. Теорема доказана.

Из теорем 2.1, 3.2, 4.1 и следствия 3.1 вытекает

Теорема 4.2. *Пусть* $R = F_1 \dotplus \cdots \dotplus F_n$, *где* $n > 1$, $F_i \cong GF(p^{l_i})$ $(i = \overline{1,n})$. *Пусть* $l_i > 1$ *и* $l_i = p_1^{\alpha_1} \cdots p_{k_i}^{\alpha_{k_i}}$ $(i = \overline{1,n})$. *Тогда* $R^\varphi = F_1^\varphi \dotplus \cdots \dotplus F_n^\varphi$, *где* $F_i^\varphi \cong GF(q^{m_i})$ *и* $m_i = q_1^{\alpha_1} \cdots q_{k_i}^{\alpha_{k_i}}$.

Литература

1. Коробков С. С. Решеточные изоморфизмы периодических ассоциативных колец. Свердловск, 1988. 18 с. Деп. в ВИНИТИ 01.03.88, №2132-88.

2. Коробков С. С. Решеточные изоморфизмы колец, разложимых в прямые суммы конечных полей // Kurosh Algebraic Conference'98. Abstracts of Talks. М.: Изд-во мех.-мат. фак-та МГУ, 1998. С.184.

3. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

4. Gilmer R. A note on rings with only finitely many subrings // Scripta Math. 1973. Vol. 29, №1–2. P. 37–38.

5. Фрейдман П. А. Кольца с дистрибутивной структурой подколец // Мат. сб. 1964. Т. 73(115). С. 513–534.

6. Коробков С. С., Свинина Е. М., Смирнов В. Д. Ассоциативные кольца малой длины. Свердловск, 1990. 40 с. Деп. в ВИНИТИ 15.03.90, №1441-90.

Статья поступила 21.03.2001 г.
Окончательный вариант 25.09.2001 г.