ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 25 № 4 2019

УДК 512.552

# ВОПРОСЫ СТРОЕНИЯ КОНЕЧНЫХ ПОЧТИ-ПОЛЕЙ

**О. В. Кравцова, В. М. Левчук**

Полуполем называют простое кольцо, в котором ненулевые элементы по умножению образуют лупу. К более общему понятию квазиполя (в случае ассоциативного кольца — почти-поля) приходим, ослабляя двустороннюю дистрибутивность до односторонней. Исследуемые вопросы строения конечных полуполей и квазиполей изучались в различных ситуациях уже давно. В последние годы они отмечались явно в ряде статей. Ранее эти вопросы были решены для полуполей Кнута — Ру́а и Хентзела — Ру́а — контрпримеры порядков 32 и 64 к известной гипотезе Венэ. Для описания некоторых квазиполей малых порядков использовались также методы компьютерной алгебры. Известно, что центр конечного полуполя всегда содержит простое подполе. Авторы показывают, что центр конечного почти-поля $Q$ содержит простое подполе $P$ кроме четырех почти-полей Цассенхауза порядков $5^2$, $7^2$, $11^2$, $29^2$. Ядро почти-поля $Q$ всегда содержит $P$. При достаточно общих условиях перечислены максимальные подполя конечного почти-поля. Группы автоморфизмов почти-поля $Q$ и его мультипликативной группы $Q^*$ были найдены ранее. Метацикличность группы $Q^*$ позволяет выписать явно спектр групповых порядков ее элементов.

Ключевые слова: квазиполе, полуполе, почти-поле, максимальное подполе, спектр.

**O. V. Kravtsova, V. M. Levchuk. Questions of the structure of finite near-fields.**

A semifield is a simple ring in which nonzero elements with respect to multiplication form a loop. Weakening distributivity from two-sided to one-sided yields the more general notion of quasifield (near-field under the condition of associativity). Problems of the structure of finite semifields and quasifields have been studied in various cases for a long time. In recent years, they have been mentioned in a number of papers. These problems were solved earlier for Knuth–Rúa and Hentzel–Rúa semifields, which are counterexamples of orders 32 and 64 to Wene's known hypothesis. The methods of computer algebra were used to describe some quasifields of small orders. It is known that the center of a finite semifield always contains the prime subfield. We show that the center of a finite near-field $Q$ contains the prime subfield $P$ except for Zassenhaus' four near-fields of orders $5^2$, $7^2$, $11^2$, and $29^2$. The kernel of a near-field $Q$ always contains $P$. The maximal subfields of a finite near-field are enumerated under sufficiently general conditions. The automorphism groups of a near-field $Q$ and of its multiplicative group $Q^*$ were found earlier. The group $Q^*$ is metacyclic, which makes it possible to explicitly find the spectrum of group orders of its elements.

Keywords: quasifield, semifield, near-field, maximal subfield, spectrum.

**MSC:** 12K05, 12K10, 17A35

**DOI**: 10.21538/0134-4889-2019-25-4-107-117

## Введение

*Полуполе* (квазитело в терминологии Куроша [1]) — это простое кольцо, в котором ненулевые элементы по умножению образуют лупу. К более общему понятию *квазиполя* приходим, ослабляя двустороннюю дистрибутивность до односторонней. Тесно связанные исследования проективных плоскостей трансляций и координатизирующих квазиполей проводятся уже более века (Диксон [2], Веблен и Маклаган Веддерберн [3]; см. также [4; 5]).

Следующие вопросы структурного строения конечных полуполей и квазиполей исследовались в различных ситуациях уже давно и записаны в [6].

**(A)** *Перечислить максимальные подполя, найти их число и возможные порядки.*

**(B)** *Выявить конечные квазиполя $Q$ с неоднопорожденной лупой $Q^*$.*

Г и п о т е з а: *лупа $Q^*$ всякого конечного полуполя $Q$ однопорождена.*

**(C)** *Выявить, какие возможны спектры лупы $Q^*$ конечного полуполя и квазиполя $Q$.*

**(D)** *Найти порядок группы автоморфизмов.*

Эти вопросы исследовались для полуполей порядка 16 — наименьший порядок собственных полуполей (т. е. не являющихся полем), полуполей Кнута — Ру́а и Хентзела — Ру́а — контрпримеры порядков 32 и 64 к гипотезе Венэ [7], для других квазиполей малых порядков (см. также [6]).

Целочисленные кратные единицы каждого конечного квазиполя естественно образуют его простое подполе (см. лемму 1 в разд. 1). Известно, что в случае полуполя простое подполе всегда лежит в центре. Оказывается, это не всегда верно даже в ассоциативном квазиполе (*почти-поле*). Все исключения перечисляет теорема 1. Она выявляет взаимосвязи центра, ядра и простого подполя для всех конечных почти-полей.

Вопросы (A)–(D) для конечных почти-полей удается в основном решить в разд. 2 и 3 (см. теоремы 2–4). Мы опираемся прежде всего на результаты Цассенхауза [8].

## 1. Почти-поля и 2-транзитивные группы

Отказ в определении поля от коммутативности приводит к понятию тела; отказываясь и от ассоциативности, приходят к понятию полуполя. К более общему понятию приводит ослабление двусторонней дистрибутивности до односторонней.

О п р е д е л е н и е. Множество $Q = (Q, +, \cdot)$ с бинарными операциями сложения $+$ и умножения $\cdot$ называют *правым квазиполем*, если выполняются следующие аксиомы:

1) $Q^+ = (Q, +)$ — абелева группа;

2) $Q^* = (Q\backslash\{0\}, \cdot)$ — лупа;

3) $x \cdot 0 = 0$ для любого $x \in Q$;

4) правый дистрибутивный закон $(x + y) \cdot z = x \cdot z + y \cdot z$ для любых $x, y, z \in Q$;

5) если $a, b, c \in Q$ и $a \neq b$, то уравнение $x \cdot a = x \cdot b + c$ однозначно разрешимо в $Q$.

*Левое квазиполе* определяют аналогично. Из аксиом 1 и 4 вытекает равенство $0 \cdot x = 0$. Для конечного правого квазиполя аксиома 5 следует из аксиом 1–4 (Хьюз и Пайпер [4, теорема 7.3]). Напомним, что множество $L$ с бинарной операцией $\cdot$ называется *лупой*, если в $L$ существует нейтральный элемент и уравнения $a \cdot x = b$ и $x \cdot a = b$ однозначно разрешимы при любых $a, b \in L$, [1; 9]. В частности, группа — это ассоциативная лупа.

В следующем известном утверждении [6, предложение 1] с доказательством в [10, лемма 2]) в любом квазиполе выделяется подкольцо, которое образуют целочисленные кратные единицы

$$ke := \underbrace{e + e + \ldots + e}_{k \text{ раз}} = ek, \quad (-k)e := -(ke) = e(-k) \quad (k > 0), \quad 0e = 0 = e0.$$

**Лемма 1.** *Пусть $Q$ — правое квазиполе с единицей $e$. Тогда*

(i) *отображение $\pi : k \to ke$ $(k \in \mathbb{Z})$ есть гомоморфизм кольца $\mathbb{Z}$ в $Q$;*

(ii) *$Q$ — левый $\pi(\mathbb{Z})$-модуль, и либо $\pi(\mathbb{Z}) \simeq \mathbb{Z}$, либо $\pi(\mathbb{Z}) \simeq \mathbb{Z}_p$ для некоторого простого числа $p$.*

В силу леммы 1 понятие характеристики поля переносится на квазиполя. Если характеристика $p = char\, Q$ квазиполя $Q$ положительна, то $\pi(\mathbb{Z})$ является единственным минимальным в $Q$ (и простым) подполем и $\pi(\mathbb{Z}) \cong \mathbb{Z}_p$. Любое полуполе есть кольцо и поэтому двусторонний $\pi(\mathbb{Z})$-модуль. Как следствие леммы 1 вытекает известное утверждение [5, замечание 5.56]: *в конечном полуполе простое подполе всегда лежит в центре.* Это не всегда так даже в ассоциативном (правом) квазиполе, называемом *почти-полем.*

*Центр $Z(Q)$ почти-поля $Q$* определяется равенством $Z(Q) = \{x \in Q \colon xy = yx \ \forall y \in Q\}$. Левый дистрибутивный закон в почти-поле не обязан выполняться. *Ядром почти-поля $Q$* называют множество $K(Q)$ элементов $x \in Q$, которые можно выносить за знак любой суммы

произведений, где $x$ участвует как общий левый множитель слагаемых:

$$K(Q) = \{x \in Q \colon x(y+z) = xy + xz \ \forall y, z \in Q\}.$$

Основной в этом разделе является теорема 1.

Далее для доказательства теоремы 1 и в следующих разделах нам потребуются некоторые известные понятия и результаты о конечных почти-полях.

Все конечные почти-поля описал в 1936 г. Цассенхауз [8], связывая с каждым из них определенную 2-транзитивную группу (см. также [9, гл. 20]). Группу $G$ подстановок множества $\Omega$ называют 2-*транзитивной*, если любая пара символов из $\Omega$ переводится подходящей подстановкой $T \in G$ в фиксированную (произвольно) пару символов из $\Omega$. Если каждая такая подстановка $T$ определена однозначно, группу $G$ называют *точно* 2-*транзитивной*. В этом случае группе $G$ в [8] сопоставлена алгебраическая система $K = (\Omega, +, \cdot)$ с нулем 0 и единицей 1:

$$a + 0 = a = 0 + a, \quad a0 = 0 = 0a, \quad a1 = a = 1a \quad (a \in \Omega).$$

Подстановки в $G$, переставляющие все символы, образуют вместе с единичной подстановкой нормальную абелеву подгруппу $A$, транзитивную на $\Omega$. Через $M$ обозначается стабилизатор символа 0. Сумма $y + b = z$ в $\Omega$ и произведение $xm = t$ ненулевых элементов в $\Omega$ корректно определяются выбором подстановок соответственно

$$\begin{pmatrix} 0 & \dots & y & \dots \\ b & \dots & z & \dots \end{pmatrix} \in A \ \text{ и } \ \begin{pmatrix} 0 & 1 & \dots & x & \dots \\ 0 & m & \dots & t & \dots \end{pmatrix} \in M.$$

Согласно [9, теорема 20.7.1] $K = (\Omega, +, \cdot)$ есть почти-поле, причем $K^* := (K \setminus \{0\}, \cdot) \simeq M$ и $(K, +) \simeq A$, а группа преобразований $y = xm + b$, $m \neq 0$, изоморфна $G$. Обратно, указанные преобразования любого конечного почти-поля $K$ образуют точно 2-транзитивную группу.

Известный способ построения конечного почти-поля как специального расширения его центра $GF(q)$ (поле Галуа порядка $q$) впервые начал применять еще Диксон. Это расширение, построенное на аддитивной группе $(GF(q^n), +)$, характеризуется порядком $q$ центра и степенью $n$ (*пара Диксона*), которые выбирают произвольно с условиями:

1) каждый простой делитель числа $n$ делит $q - 1$;

2) если $q \equiv 3 \pmod 4$, то $n \not\equiv 0 \pmod 4$.

Построенные конструкцией Диксона — Цассенхауза почти-поля порядка $q^n$ с центром $GF(q)$ называют *почти-полями Диксона*. По теореме Цассенхауза [8; 9, теорема 20.7.2] *все конечные почти-поля $Q$ исчерпываются почти-полями Диксона и, кроме того, семью исключительными почти-полями порядка $p^2$ для простых чисел $p = 5, 7, 11$ (два почти-поля), $23, 29, 59$.*

Известно и строение силовских подгрупп в $Q^*$ [9, лемма 20.7.K4]: *силовская $r$-подгруппа $S_r$ группы $Q^*$ является циклической или при $r = 2$ (обобщенной) кватернионной группой.*

**Теорема 1.** *В конечном почти-поле центр и ядро совпадают, являются подполями и содержат простое подполе. Исключения составляют точно четыре почти-поля $Q$, для которых порядки $|Q|$ равны $5^2$, $7^2$, $11^2$ и $29^2$, порядки центров $Z(Q^*)$ группы $Q^*$ равны $2, 2, 2$ и $14$ соответственно, а ядро $K(Q)$ есть простое подполе.*

Доказательство. Известно [4, теорема 7.2], что ядро любого квазиполя есть тело. Следовательно, в конечном почти-поле $Q$ ядро является подполем и содержит простое подполе. Непосредственно из определений ядра и центра получаем также включение $Z(Q) \subseteq K(Q)$.

Для почти-полей Диксона, по построению, центр является подполем и содержит простое подполе, а согласно [8; 11, § 2] ядро и центр совпадают.

Исключительным почти-полям $Q$ порядка $p^2$ (почти-поля Цассенхауза) присваиваем один из типов I–VII соответственно нумерации после теоремы 20.7.2 в [9]. В каждом из них ядро,

Т а б л и ц а 1

**Исключительные почти-поля $Q$**

| Тип $Q$ | $\|Q\|$ | $Q^*$ | $\|Z(Q^*)\|$ | $\|S_2\|$ |
|---|---|---|---|---|
| I | $5^2$ | $SL(2,3)$ | 2 | 8 |
| II | $11^2$ | $SL(2,3)\times\mathbb{Z}_5^+$ | 10 | 8 |
| III | $7^2$ | $2O$ | 2 | 16 |
| IV | $23^2$ | $2O\times\mathbb{Z}_{11}^+$ | 22 | 16 |
| V | $11^2$ | $SL(2,5)$ | 2 | 8 |
| VI | $29^2$ | $SL(2,5)\times\mathbb{Z}_7^+$ | 14 | 8 |
| VII | $59^2$ | $SL(2,5)\times\mathbb{Z}_{29}^+$ | 58 | 8 |

очевидно, совпадает с простым подполем $P=\pi(\mathbb{Z})\simeq\mathbb{Z}_p$. Силовская 2-подгруппа $S_2$ мультипликативной группы $Q^*$ является (обобщенной) кватернионной порядка 16 или 8, имеет единственную инволюцию и центр $Z(S_2)$ порядка 2. При $|Q|=7^2$ группа $Q^*$ порядка 48 представляется бинарной октаэдральной группой [12, § 6.5], обозначаемой через $2O$.

Отраженное в [9] строение группы $Q^*$ и ее центра резюмируется в табл. 1.

Для почти-полей $Q$ типа II, IV и VII порядок центра $Z(Q^*)$ мультипликативной группы $Q^*$ совпадает с $|P^*|=p-1$. Поэтому $P^*=Z(Q^*)$ и $P$ — центр $Z(Q)$ почти-поля $Q$. В остальных четырех случаях имеем $|Z(Q^*)|<p-1$, и поэтому центр $Z(Q)$ почти-поля $Q$ лежит в простом подполе $P$, но не совпадает с ним. В частности, вопрос о равенстве простого подполя и центра решается по-разному для двух почти-полей порядка $11^2$ — типа II и V.

Теорема доказана.

З а м е ч а н и е. Т. Н. Яковлева [10] редуцировала утверждение теоремы о связи простого подполя и центра к семи почти-полям Цассенхауза. Она же исследовала исключительное почти-поле порядка $5^2$ [10, пример 1], а одна из авторов статьи О. В. Кравцова — порядка $29^2$. Для остальных пяти почти-полей теорема доказана совместно тремя авторами.

## 2. Максимальные подполя конечного почти-поля

Исследуем вопрос **(A)** описания максимальных подполей для конечных почти-полей. Простое подполе является единственным максимальным подполем в почти-поле характеристики $p$ и порядка $p^r$ для любого простого числа $r$ в силу [10, теорема 3] (при $r=2$ — по теореме 1). Поэтому вопрос **(A)** редуцируется к почти-полям Диксона.

Класс всех почти-полей Диксона порядка $q^n$ с центром $GF(q)$, где $q=p^l$ для простого числа $p$ и $l>1$, обозначают через $DF(q,n)$. Отметим, что на под-почти-поля почти-поля $Q\in DF(q,n)$ переносится известное соответствие между подполями конечного поля и делителями степени его расширения над простым подполем. В силу основной теоремы Данкс в [13] и [14, лемма 1.2] это обобщенное соответствие можно представить следующей леммой.

**Лемма 2.** *Для любого под-почти-поля $H$ почти-поля $Q\in DF(p^l,n)$ существуют натуральные числа $h$ и $j$ такие, что $h\,|\,(ln)$, $0<j\leq n$, $|H|=p^h$, $H\in DF(p^z,h/z)$ для $z=\text{НОД}(jl,h)$, причем*

$$j\equiv\frac{p^{ln}-1}{p^h-1}\,(\bmod\, n). \tag{2.1}$$

*Обратно: если $h\,|\,(ln)$, то $Q\in DF(p^l,n)$ имеет единственное под-почти-поле $H$ порядка $p^h$.*

Выделим случай коммутативных под-почти-полей, или равносильно, подполей.

**Следствие.** *Под-почти-поле $H$ порядка $p^h$ почти-поля $Q\in DF(p^l,n)$ есть подполе тогда и только тогда, когда $h$ делит произведение $l\cdot\text{НОД}(j,n)$, где $j$ определено в* (2.1).

Известно (Фелгнер, [11, теорема 2.1]), что в почти-поле $Q$ максимальное подполе $M(Q)$, содержащее $Z(Q)$, единственно. В следующей теореме мы выявляем как меняются пары Диксона $(q,n)$ при переходе к максимальному под-почти-полю и вместе с тем находим явно порядок максимального подполя $M(Q)$. Запишем каноническое разложение числа $n$ и определим число $\lambda$

$$n = p_1^{n_1}p_2^{n_2}\dots p_r^{n_r}, \quad \lambda = p_1^{[n_1/2]}p_2^{[n_2/2]}\dots p_r^{[n_r/2]}. \tag{2.2}$$

**Теорема 2.** *Пусть $H$ — под-почти-поле порядка $p^h$ почти-поля $Q \in DF(q,n)$, $q = p^l$ и $h = ln/p_i$ для некоторого $p_i$ из (2.2). Тогда $H \in DF(q, n/p_i)$ при $n_i = 1$ и $H \in DF(q^{p_i}, n/p_i^2)$ при $n_i > 1$. Кроме того, под-почти-поле порядка $q^\lambda$ в $Q$ является единственным максимальным подполем в $Q$, содержащим $Z(Q)$.*

Д о к а з а т е л ь с т в о. В силу [15, лемма 2.3] для любой пары Диксона $(q,n)$ имеем

$$\frac{q^n-1}{q^m-1} \equiv \frac{n}{m} \pmod n \quad \forall m \mid n.$$

Если $n_i = 1$, то для числа $n' = n/p_i$ получаем равенства $h = ln'$ и $\text{НОД}(p_i, n') = 1$. Учитывая соответствие из леммы 2, имеем

$$\frac{p^{ln}-1}{p^{ln'}-1} \equiv \frac{n}{n'} \equiv p_i \pmod n,$$

$$z = \text{НОД}(lp_i, ln') = l \cdot \text{НОД}(p_i, n') = l, \quad \frac{h}{z} = n', \quad H \in DF(p^l, n/p_i).$$

Пусть $n_i > 1$. Положим $n' = n/p_i^2$. Тогда $h = lp_in'$ и с помощью леммы 2 получаем

$$\frac{p^{ln}-1}{p^{lp_in'}-1} \pmod n \equiv \frac{n}{p_in'} \equiv p_i \pmod n,$$

$$z = \text{НОД}(lp_i, lp_in') = lp_i, \quad \frac{h}{z} = n', \quad H \in DF\big(p^{lp_i}, n/p_i^2\big).$$

Построим теперь убывающую последовательность под-почти-полей

$$H_0 \supset H_1 \supset H_2 \supset \dots, \quad \text{где } |H_i| = p^{h_i}, \quad h_0 = ln \text{ и } h_{i+1}/h_i \text{ — простые числа}, \tag{2.3}$$

начинающуюся с $H_0 = Q$. Вначале выполним $k_1 = [(n_1+1)/2]$ шагов, переходя от $H_i$ к $H_{i+1}$ с простым числом $h_{i+1}/h_i = p_1$ из (2.2). Применяя доказанное первое утверждение теоремы, получаем под-почти-поле

$$H_{k_1} \in DF\big(q^{p_1^{[n_1/2]}}, n/(p_1^{n_1})\big).$$

Затем выполним $k_2 = [(n_2+1)/2]$ переходов от $H_i$ к $H_{i+1}$ с простым числом $h_{i+1}/h_i = p_2$. Аналогично получим

$$H_{k_1+k_2} \in DF\big(q^{p_1^{[n_1/2]}p_2^{[n_2/2]}}, n/(p_1^{n_1}p_2^{n_2})\big).$$

Итак, степень под-почти-поля $H_{k_1+k_2}$ над его центром получаем из степени $n$ в разложении (2.2), отбрасывая все простые сомножители $p_1$ и $p_2$. Ясно, что $Z(Q) \subseteq Z(H_{k_1}) \subseteq Z(H_{k_1+k_2})$.

Продолжая процесс, через $k = k_1 + k_2 + \dots + k_r$ шагов приходим к под-почти-полю $H_k$, соответствующему паре Диксона $(q^\lambda, 1)$. Поэтому $H_k$ совпадает со своим центром $Z(H_k)$ и, в частности, является подполем. Утверждение единственности в лемме 2 показывает, что подполе $H_k$ не зависит от последовательности переходов в нашем построении. С другой стороны, $Z(H_i) \neq H_i$ при $i < k$ для любой последовательности (2.3) от $H_0 = Q$ до $H_k$. Следовательно, $H_k$ — единственное максимальное подполе в $Q$, содержащее центр $Z(Q)$.

Теорема доказана.

Через $\pi(m)$ обозначим множество простых делителей числа $m$.

В связи с вопросом **(A)** нас интересует каждое под-почти-поле $H_i$ в (2.3), являющееся подполем, с наименьшим номером $i$ для данной последовательности. В силу теоремы 2 изучения требует случай, когда $h_i/h_{i+1} \notin \pi(n)$.

**Теорема 3.** *Пусть $H$ — под-почти-поле порядка $p^{l'n}$ почти-поля $Q \in DF(p^l, n)$. Тогда*
(i) *если* $\text{НОД}(l/l', n) = 1$ *и* $n|(p^{l'n} - 1)$, *то* $H \in DF(p^{l'}, n)$;
(ii) *если $n$ просто и не делит $p^{l'n} - 1$, то $H$ есть подполе.*
*Кроме того, если пересечение $\pi(n) \cap \pi(p-1)$ пусто, $l$ — простое число и $l$ не делит $n$, то $Q$ имеет точно два максимальных подполя — $M(Q)$ и подполе порядка $p^n$.*

Д о к а з а т е л ь с т в о. Полагая $k = l/l'$, имеем

$$\frac{p^{ln} - 1}{p^{l'n} - 1} = p^{l'n(k-1)} + p^{l'n(k-2)} + \cdots + 1.$$

Если $p^{l'n} \equiv 1(\bmod n)$, то сравнение (2.1) дает сравнение $j \equiv k(\bmod n)$, и в силу леммы 2

$$z = \text{НОД}(jl, l'n) = \text{НОД}(k^2 l', l'n) = l', \quad H \in DF(p^{l'}, n).$$

Таким образом, утверждение (i) доказано. Если $n$ не делит $p^{l'n} - 1$, то для простого $n$ получим $j = n$ и $z = l'n$. Отсюда $H \in DF(p^{l'n}, 1)$, т. е. $H$ — подполе, что доказывает (ii).

Докажем последнее утверждение теоремы. Пусть $l$ — простое число, не делящее $n$. Если под-почти-поле $H$ порядка $p^n$ не коммутативно, то $H \in DF(p^{n/k}, k)$ для некоторого делителя $k$ числа $n$. Тогда каждый простой делитель $p_i$ числа $k$ делит числа $p^{n/k} - 1$ и $p^l - 1$ в силу определения пары Диксона. Следовательно, $p_i$ делит и число $p^d - 1$, где $d = \text{НОД}(l, n/k) = 1$; что противоречит условию $p_i \notin \pi(p-1)$. Поэтому под-почти-поле $H$ коммутативно и является подполем. Его максимальность следует из простоты числа $l$.

Пусть теперь $P$ — любое другое максимальное подполе в $Q$. Его порядок равен $p^{lk}$ для некоторого делителя $k$ числа $n$. Тогда по следствию на с. 254 в [15] $P$ содержит центр почти-поля $Q$ и по теореме 2 совпадает с $M(Q)$.

Теорема доказана.

П р и м е р 1. Условие $\pi(n) \cap \pi(p-1) = \varnothing$ в теореме 3 существенно. Например, в почти-поле $Q \in DF(5^3, 2)$ центр $Z(Q)$ является единственным максимальным подполем. Действительно, $Q$ имеет под-почти-поле $H$ порядка $5^2$ по лемме 2. Однако $H$ не является подполем, поскольку

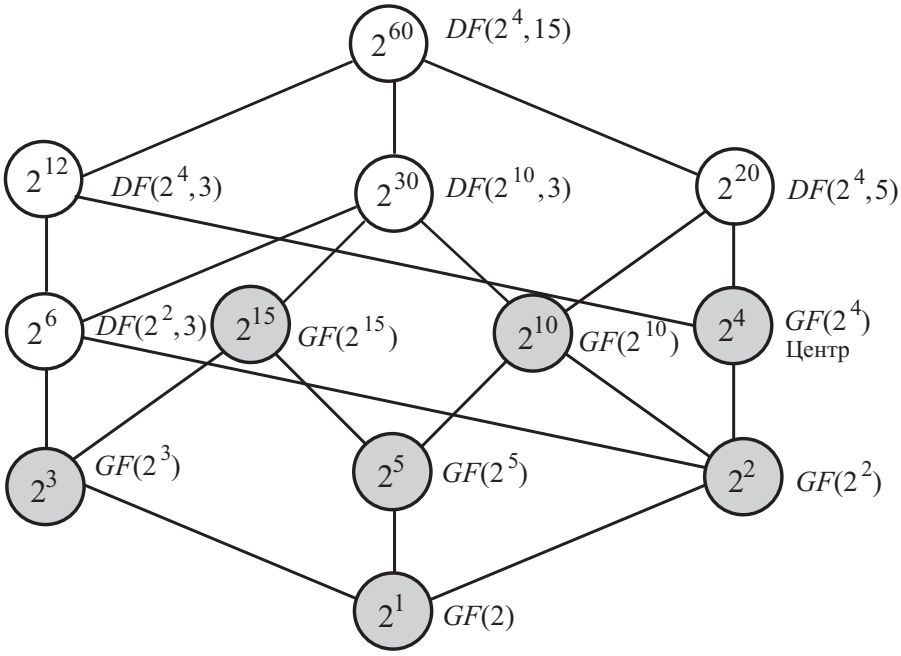
$$\frac{5^6 - 1}{5^2 - 1} = 5^4 + 5^2 + 1 \equiv 1(\bmod 2), \quad j = 1, \quad z = \text{НОД}(3, 2) = 1, \quad H \in DF(5^1, 2).$$

Отметим, что для другого почти-поля $P \in DF(5^2, 3)$ того же порядка $5^6$ условие теоремы 3 выполнено, и поэтому $P$ содержит точно два максимальных подполя, их порядки равны $5^3$ и $5^2$.

П р и м е р 2. Решетку под-почти-полей произвольного почти-поля порядка $2^{60}$ из класса $DF(2^4, 15)$ находим, используя теоремы 2 и 3 (см. рисунок ниже); это почти-поле имеет три максимальных подполя, их порядки равны $2^{15}$, $2^{10}$ и $2^4$. С другой стороны, почти-поле $Q \in DF(2^4, 45)$ порядка $2^{180}$ имеет три максимальные под-почти-поля

$$H \in DF(2^{10}, 9), \quad P \in DF(2^4, 9), \quad S \in DF(2^{12}, 5).$$

Их попарные пересечения дают три предмаксимальных (т. е. максимальных в максимальных) под-почти-поля, из которых два — $H \cap S = M(H)$ и $P \cap S = M(P) = M(S)$ — являются максимальными в $Q$ подполями порядков $2^{30}$ и $2^{12}$ соответственно. Из двух оставшихся предмаксимальных под-почти-полей одно (максимальное в $H$) порядка $2^{45}$ дает последнее максимальное в $Q$ подполе.




Решетка под-почти-полей в почти-поле Диксона порядка $2^{60}$

## 3. Мультипликативная группа и автоморфизмы конечного почти-поля

Исследуем вопросы **(B)**–**(D)** для конечных почти-полей.

Для решения вопроса **(B)** достаточно заметить, что если лупа $Q^*$ почти-поля $Q$ однопорождена, то она является циклической группой и поэтому почти-поле $Q$ коммутативно. Отсюда сразу вытекает

**Лемма 3.** *Почти-поле $Q$ является полем, если его лупа $(Q^*,\cdot)$ однопорождена.*

Для определения строения группы $Q^*$ конечного почти-поля $Q$ Цассенхауз [8] существенно использовал следующее свойство (см. также [9, лемма 20.7.K3]): *если числа $q$ и $s$ простые, то подгруппы порядков $q^2$ и $qs$ группы $Q^*$ циклические.*

Строение мультипликативных групп $Q^*$ семи исключительных почти-полей Цассенхауза отражено выше в табл. 1. Для почти-полей Диксона в [8] (см. также [16, предложения 1, 2; 17, теорема IV.1.5]) наряду с цикличностью центра $Z(Q^*)$ и фактор-группы $Q^*/Z(Q^*)$ (метациклличность группы $Q^*$) установлена

**Лемма 4.** *Мультипликативная группа $Q^*$ конечного почти-поля Диксона $Q\in DF(q,n)$ есть метациклическая двупорожденная группа:*

$$Q^*=\langle a,b\mid a^m=1,\ b^n=a^t,\ bab^{-1}=a^q\rangle,\quad \text{где}\ \ m=\frac{q^n-1}{n}\ \ \text{и}\ \ t=\frac{m}{q-1}. \tag{3.1}$$

*Кроме того, $Z(Q^*)=\langle a^t\rangle$ и* НОД$\,(n,t)=$ НОД$\,(q-1,t)\le 2$.

Как показано в [16, предложение 3], условие НОД$(q-1,t)=1$ равносильно цикличности силовской 2-подгруппы в $Q^*$.

П р и м е р 3. Если $Q\in DF(7,2)$, то силовская 2-подгруппа $Q^*$ есть обобщенная кватернионная группа порядка 16, а для $Q\in DF(5,2)$ — циклическая группа порядка 8.

Вопрос **(C)** о спектре порядков элементов группы $Q^*$ в обозначениях (3.1) решает следующая теорема.

**Теорема 4.** *Пусть $Q \in DF(q,n)$ — почти-поле Диксона, $Q^*$ — его мультипликативная группа. Тогда спектр группы $Q^*$ состоит из всех делителей числа $m = \dfrac{q^n-1}{n}$ и всех делителей $z$ числа $q^n-1$, минимальных с условием*

$$m \mid \Big(k\,\frac{q^{zs}-1}{q^s-1} + \frac{zst}{n}\Big), \quad k = 0,1,\dots,m-1, \quad s = 1,2,\dots,n-1. \tag{3.2}$$

Доказательство. Найдем порядки элементов в мультипликативной группе $Q^*$ почти-поля Диксона $Q \in DF(q,n)$. Используя ее определяющие соотношения (3.1) и факторизацию $Q^* = \langle a\rangle\langle b\rangle$, получаем

$$ba^kb^{-1} = a^{kq}, \quad b^2ab^{-2} = a^{q^2}, \dots, \quad b^sab^{-s} = a^{q^s}, \quad b^sa^kb^{-s} = a^{kq^s},$$

$$(a^kb^s)(a^kb^s) = a^k(b^sa^kb^{-s})b^{2s} = a^{k(1+q^s)}b^{2s}.$$

Поэтому для произвольных $k$ и $s$ из (3.2) имеем $(a^kb^s)^z = a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})}b^{zs}$.

Если $(a^kb^s)^z = 1$, то $a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})}b^{zs} = 1$. Деление $zs$ на $n$ с остатком дает $zs = nu + r$, $0 \le r < n$, так что

$$a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})}b^{nu+r} = 1,$$

и, следовательно, $a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})+tu} = b^{-r}$. Учитывая соотношения $b^n = a^t$ и $r < n$, получаем $r = 0$, и, следовательно,

$$u = \frac{zs}{n} \quad \text{и} \quad a^{k(1+q^s+q^{2s}+\cdots+q^{(z-1)s})+tu} = 1.$$

Таким образом, порядок элемента $a^kb^s \ne 1$ — это наименьшее натуральное число $z$, удовлетворяющее условию (3.2) и делящее $q^n-1$.

Теорема доказана.

Пример 4. Проиллюстрируем теорему на примере почти-поля $Q \in DF(5,2)$, где

$$Q^* = \{a^kb^s \mid k = 0,1,\dots,11,\ s = 0,1\}, \quad m = 12, \quad t = 3, \quad a^{12} = 1, \quad b^2 = a^3, \quad bab^{-1} = a^5.$$

Для произвольного элемента $a^kb \in \langle a\rangle b$ условие (3.2) принимает вид

$$12 \mid \Big(\frac{k(5^z-1)}{4} + \frac{3z}{2}\Big),$$

получаем $z = |a^kb| = 8$. Поэтому спектр группы $Q^*$ получается присоединением числа 8 к спектру циклической группы $\langle a\rangle$ порядка 12, т. е. равен $\{1,2,3,4,6,8,12\}$. Отметим для сравнения, что спектр мультипликативной группы почти-поля Цассенхауза $H$ порядка 25 совпадает со спектром группы $SL(2,3)$, то есть равен $\{1,2,3,4,6\}$. Подробнее см. табл. 2.

В связи с вопросом **(D)** отметим, что группу автоморфизмов конечного почти-поля $Q$ описал Цассенхауз. В случае $Q \in DF(3,2)$ имеем $\operatorname{Aut} Q \simeq S_3$; для других почти-полей Диксона $Q \in DF(p^l,n)$ группа $\operatorname{Aut} Q$ есть циклическая группа порядка $ln/g$, где $g$ — порядок $p$ по модулю $n$ [8, предложение 18]. Бойкетт и Хауэлл [18] описали группу $\operatorname{Aut} Q^*$. Группы автоморфизмов для семи исключительных почти-полей Цассенхауза (см. табл. 1) отражает табл. 3.

Таблица 2

**Число элементов порядка $z$ группы $K^*$ почти-полей $K$ порядка 25**

| Порядок $z$ элемента | **1** | **2** | **3** | **4** | **6** | **8** | **12** |
|---|---|---|---|---|---|---|---|
| Случай $K = Q$ | 1 | 1 | 2 | 2 | 2 | 12 | 4 |
| Случай $K = H$ | 1 | 1 | 8 | 6 | 8 | 0 | 0 |

Таблица 3

**Автоморфизмы исключительных почти-полей $Q$**

| Тип | $\lvert Q\rvert$ | $Q^*$ | $\mathrm{Aut}(Q^*)$ | $\lvert\mathrm{Aut}(Q)\rvert$ |
|---|---|---|---|---|
| I | $5^2$ | $SL(2,3)$ | $S_4$ | 4 |
| II | $11^2$ | $SL(2,3)\times\mathbb{Z}_5^+$ | $S_4\times\mathbb{Z}_4^+$ | 2 |
| III | $7^2$ | $2O$ | $S_4\times\mathbb{Z}_2^+$ | 3 |
| IV | $23^2$ | $2O\times\mathbb{Z}_{11}^+$ | $S_4\times\mathbb{Z}_2\times\mathbb{Z}_{10}^+$ | 1 |
| V | $11^2$ | $SL(2,5)$ | $S_5$ | 5 |
| VI | $29^2$ | $SL(2,5)\times\mathbb{Z}_7^+$ | $S_5\times\mathbb{Z}_6^+$ | 2 |
| VII | $59^2$ | $SL(2,5)\times\mathbb{Z}_{29}^+$ | $S_5\times\mathbb{Z}_{28}^+$ | 1 |

## СПИСОК ЛИТЕРАТУРЫ


1. **Курош А.Г.** Лекции по общей алгебре. Москва: Физматгиз, 1962. 396 с.
2. **Dickson L.E.** Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc. 1906. Vol. 7, no. 3. P. 370–390. doi: 10.2307/1986324 .
3. **Veblen O., Maclagan–Wedderburn J.H.** Non-desarguesian and non-Pascalian geometries // Trans. Amer. Math. Soc. 1907. Vol. 8, no. 3. P. 379–388. doi: 10.2307/1988781 .
4. **Hughes D.R., Piper F.C.** Projective planes. N Y Inc.: Springer-Verlag, 1973. 292 p. ISSN: 0-387-90044-6 .
5. **Johnson N.L., Jha V., Biliotti M.** Handbook of finite translation planes. London; N Y: Chapman Hall/CRC, 2007. 888 p. ISBN: 1420011146;.
6. **Levchuk V.M., Kravtsova O.V.** Problems on structure of finite quasifields and projective translation planes // Lobachevskii J. Math. 2017. Vol. 38, no. 4, P. 688–698. doi: 10.1134/S1995080217040138.
7. **Wene G.P.** On the multiplicative structure of finite division rings // Aeq. Math. 1991. Vol. 41. P. 222–233.
8. **Zassenhaus H.** Uber endliche Fastkörper // Abh. Math. Sem. Hamburg, 1936. Vol. 11, no. 1. P. 187–220. doi: 10.1007/BF02940723 .
9. **Холл М.** Теория групп. М.: Госиноиздат, 1962. 468 с.
10. **Яковлева Т.Н.** Вопросы строения квазиполей с ассоциативными степенями. Изв. Иркут. гос. ун-та. Сер. “Математика”. 2019. Т. 29. С. 107–119. doi: 10.26516/1997-7670.2019.29.107 .
11. **Felgner U.** Pseudo-finite near-fields // Near-rings and near-fields / ed. C. Betrh. N Y Inc.: Elsevier Science Publisher B. V. (North-Holland). 1987. P. 15–29. (Ser. North-Holland Mathematics Studies; vol. 137). doi: 10.1016/S0304-0208(08)72282-5 .
12. **Коксетер Г.С.М., Мозер У.О.Дж.** Порождающие элементы и определяющие соотношения дискретных групп. Москва: Наука, 1980. 240 с.
13. **Dancs S.** The sub-near-field structure of finite near-fields // Bull. Austral. Math. Soc. 1971. Vol. 5. P. 275–280. doi: 10.1017/S000497270004716X.
14. **Dancs Groves S.** Locally finite near-fields // Abh. Math. Sem. Univ. Hamburg. 1979. Vol. 48. P. 89–107. doi: 10.1017/S0004972700043914.
15. **Dancs S.** On finite Dickson near-fields // Abh. Math. Sem. Univ. Hamburg. 1972. Vol. 37. P. 254–257. doi: 10.1007/BF02999702 .
16. **Ellers E., Karzel H.** Endliche Inzidenzgruppen // Abh. Math. Sem. Hamburg. 1964. Vol. 27, no. 3-4. P. 250–264. doi: 10.1007/BF02993220 .
17. **Wähling H.** Theorie der Fastkörper. Vol. 1 of Thales Monographs. Essen: Thales-Verlag, 1987. 393 p.
18. **Boykett T., Howell K.-T.** The multiplicative automorphisms of a finite nearfield, with an application // Commun. Algebra. 2016. Vol. 44, iss. 6. P. 2336–2350. doi: 10.1080/00927872.2015.1044105 .


Поступила 3.09.2019
После доработки 28.10.2019
Принята к публикации 6.11.2019

Кравцова Ольга Вадимовна
канд. физ.-мат. наук, доцент
доцент кафедры высшей математики № 2,
Сибирский федеральный университет
г. Красноярск
e-mail: ol71@bk.ru

Левчук Владимир Михайлович
д-р физ.-мат. наук, профессор
зав. кафедрой алгебры и математической логики,
Сибирский федеральный университет
г. Красноярск
e-mail: vlevchuk@sfu-kras.ru

## REFERENCES

1. Kurosh A.G. *Lectures on general algebra*. International Ser. Monographs on Pure and Applied Math., vol. 70, N Y Inc.: Elsevier Ltd., 1965, 374 p. doi: 10.1016/C2013-0-01775-6 . Original Russian text published in Kurosh A.G. *Lektsii po obshchei algebre*. Moscow: Fizmatgiz Publ., 1962, 396 p.
2. Dickson L.E. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 1906, vol. 7, no. 3, pp. 370–390. doi: 10.2307/1986324 .
3. Veblen O., Maclagan-Wedderburn J.H. Non-desarguesian and Non-pascalian geometries. *Trans. Amer. Math. Soc.*, 1907, vol. 8, no. 3, pp. 379–388. doi: 10.2307/1988781 .
4. Hughes D.R., Piper F.C. *Projective planes*. N Y: Springer-Verlag, 1973, 292 p. ISBN: 0387900446 .
5. Johnson N.L., Jha V., Biliotti M. *Handbook of finite translation planes*. London; N Y: Chapman Hall/CRC, 2007, 888 p. ISBN: 1420011146 .
6. Levchuk V.M., Kravtsova O.V. Problems on structure of finite quasifields and projective translation planes. *Lobachevskii J. Math.*, 2017, vol. 38, no. 4, pp. 688–698. doi: 10.1134/S1995080217040138 .
7. Wene G.P. On the multiplicative structure of finite division rings. *Aeq. Math..*, vol. 41, no. 1, pp. 222–233. doi: 10.1007/BF02227457 .
8. Zassenhaus H. Über endliche Fastkörper. *Abh. Math. Semin. Univ. Hambg.*, vol. 11, no. 1, pp. 187–220. doi: 10.1007/BF02940723 .
9. Hall M. *The theory of groups*. N Y: Chelsea Pub. Co., 1976, 434 p. ISBN: 0828402884 . Translated to Russian under the title *Teoriya grupp*. Moscow: Izd. Inostr. Lit., 1962, 468 p.
10. Yakovleva T.N. Questions of construction of quasifields with associative powers. *Izv. Irkutsk. Gos. Univ., Ser. Mat.*, 2019, vol. 29, pp. 107–119 (in Russian). doi: 10.26516/1997-7670.2019.29.107 .
11. Felgner U. Pseudo-finite near-fields. In C. Betrh (ed.), *Near-rings and near-fields*, Ser. North-Holland Mathematics Studies, vol. 137, 1987, pp. 15–29. doi: 10.1016/S0304-0208(08)72282-5 .
12. Coxeter H.S.M., Moser W.O.J. *Generators and relations for discrete groups*. Berlin: Springer Verlag, 1972, 164 p. doi: 10.1007/978-3-662-21946-1 . Translated to Russian under the title *Porozhdayushchie elementy i opredelyayushchie sootnosheniya diskretnykh grupp*. Moscow: Nauka Publ., 1980, 240 p.
13. Dancs S. The sub-near-field structure of finite near-fields. *Bull. Austral. Math. Soc.*, 1971, vol. 5, pp. 275–280. doi: 10.1017/S000497270004716X .
14. Dancs Groves S. Locally finite near-fields. *Abh. Math. Sem. Univ. Hamburg*, 1979, vol. 48, pp. 89–107. doi: 10.1017/S0004972700043914 .
15. Dancs S. On finite Dickson near-fields. *Abh. Math. Sem. Univ. Hamburg*, 1972, vol. 37, no. 3-4, pp. 254–257. doi: 10.1007/BF02999702 .
16. Ellers E., Karzel H. Endliche Inzidenzgruppen. *Abh. Math. Semin. Univ. Hambg.*, vol. 27, no. 3-4, pp. 250–264. doi: 10.1007/BF02993220 .

17. Wähling H. *Theorie der Fastkörper*. Vol. 1 of Thales Monographs. Essen: Thales-Verlag, 1987. 393 p.
18. Boykett T., Howell K.T. The multiplicative automorphisms of a finite nearfield, with an application. *Commun. Algebra*, 2016, vol. 44, no. 6, pp. 2336–2350. doi: 10.1080/00927872.2015.1044105 .

Received September 3, 2019
Revised October 28, 2019
Accepted November 6, 2019

*Olga Vadimovna Kravtsova,* Cand. Sci. (Phys.-Math.), Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: ol71@bk.ru .

*Vladimir Mikhailovich Levchuk,* Dr. Phys.-Math. Sci., Prof., Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: vlevchuk@sfu-kras.ru .

Cite this article as: O. V. Kravtsova, V. M. Levchuk. Questions of the structure of finite near-fields, *Trudy Instituta Matematiki i Mekhaniki URO RAN*, 2019, vol. 25, no. 4, pp. 107–117 .