ВОПРОСЫ СТРОЕНИЯ КОНЕЧНЫХ ПОЧТИ-ПОЛЕЙ

О. В. Кравцова, В. М. Левчук (г. Красноярск)

Аннотация

Полуполем называют простое кольцо, в котором ненулевые элементы по умножению образуют лупу. К более общему понятию квазиполя (в ассоциативном случае — 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 вопросы 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, макисмальное подполе, спектр.

QUESTIONS OF THE STRUCTURE OF FINITE NEAR-FIELDS

O. V. Kravtsova, V. M. Levchuk (Krasnoyarsk)

Abstract

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.

1 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. [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.*

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*). Перечисляя исключения, теорема 1 выявляет взаимосвязи центра, ядра и простого подполя для всех конечных почти-полей.

Опираясь прежде всего на результаты Цассенхауза [8], в разд. 2 и 3 удается в основном решить вопросы **(A)**–**(D)** для конечных почти-полей (теоремы 2,3 и 4).

2 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) $Q^*=(Q\setminus\{0\},\cdot)$ — 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.

Следующее известное утверждение ([6, предложение 1], и с доказательством [10, лемма 2]) выделяет в любом квазиполе 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 почти-поля Q определяет равенство $Z(Q)=\{x\in Q\colon\ xy=yx\quad \forall y\in Q\}$. 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:

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

Основной в этом разделе является следующая теорема.

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 $Z(Q)\subseteq K(Q)$.

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 Ω называют 2-*транзитивной*, если любая пара символов из Ω переводится подходящей подстановкой $T\in G$ в фиксированную (произвольно) пару символов из Ω. 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 Ω. Через M обозначается стабилизатор символа 0. Сумма $y+b=z$ в Ω и произведение $xm=t$ ненулевых элементов в Ω корректно определяются выбором подстановок соответственно

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

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

Для почти-полей Диксона, по построению, центр является подполем и содержит простое подполе, а согласно [8] и [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, 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 резюмирует табл. 1.

Таблица 1

Исключительные почти-поля Q

Тип	$\lvert Q\rvert$	Q^*	$\lvert Z(Q^*)\rvert$	$\lvert S_2\rvert$
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

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.

Замечание 1. *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 порядка 29^2 — О. В. Кравцова. Для остальных пяти почти-полей теорема доказана совместно.*

3 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, тео-

рема 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 $GF(q)$, $q=p^l$, 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 леммы 1.2 в [14], обобщенное соответствие можно представить следующей леммой.

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

$$j\equiv\frac{p^{ln}-1}{p^h-1}\pmod n. \tag{1}$$

Обратно: если $h\mid(ln)$, то Q 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 $l\cdot$ НОД(j,n).*

Известно (Фелгнер, [11, теорема 2.1]), что в Q максимальное подполе $M(Q)\supseteq Z(Q)$ единственно. В следующей теореме мы выявляем изменения 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 выделим число λ:

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

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). 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^λ в Q является единственным максимальным подполем, содержащим центр $Z(Q)$.*

Доказательство. В силу [15, лемма 2.3], для любой пары Диксона (q,n) имеем

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

Когда $n_i=1$, для числа $n'=n/p_i$ получаем $h=ln'$ и НОД$(p_i,n')=1$. Учитывая соответствие из леммы 2, находим

$$\frac{p^{ln}-1}{p^{ln'}-1}\equiv\frac{n}{n'}(\bmod n)=p_i,$$

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

При $n_i>1$ полагаем $n'=n/p_i^2$. Тогда $h=lp_in'$ и с помощью леммы 2 находим

$$\frac{p^{ln}-1}{p^{lp_in'}-1}(\bmod n)=\frac{n}{p_in'}=p_i,$$

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

Построим сейчас убывающую последовательность под-почти-полей

$$H_0 \supset H_1 \supset H_2 \supset \dots, \qquad |H_i| = p^{h_i}, \quad h_0 = ln, \quad h_{i+1}/h_i \text{ — простые числа,} \tag{3}$$

начинающуюся с $H_0 = Q$. Вначале выполним $k_1 = [(n_1+1)/2]$ шагов ($[m]$ — целая часть числа m), переходя от H_i к H_{i+1} с простым числом $h_{i+1}/h_i = p_1$ из (2). Применяя альтернативу доказанного первого утверждения теоремы, получаем под-почти-поле

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

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

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

Итак, степень под-почти-поля $H_{k_1+k_2}$ над его центром получаем из степени n в разложении (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 (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 (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 НОД$(l/l', n) = 1$ *и* $n | (p^{l'n} - 1)$, *то* $H \in DF(p^{l'}, n)$;

(ii) если n простое 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 не делит n, то Q имеет точно два максимальных подполя — $M(Q)$ и подполе порядка p^n.

Доказательство. Полагая $k = l/l'$, находим

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

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

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

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 $l \not| n$ — простое число. 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 $d=\text{НОД}(l,n/k)=1$; это противоречит условию $p_i\notin\pi(p-1)$. Поэтому под-почти-поле H коммутативно и является подполем. Его максимальность следует из простоты 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.

Пример 1. Условие $\pi(n)\cap\pi(p-1)=\varnothing$ в теореме 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 — порядков 5^3 и 5^2.

Пример 2. Решетку под-почти-полей произвольного почти-поля порядка 2^{60} из класса $DF(2^4,15)$ находим, используя теоремы 2 и 3, см. рис. 1; это почти-поле имеет три максимальных подполя — порядков 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 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.

4 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 Цассенхауз [8] существенно использовал выявленное свойство (см. также [9, лемма 20.7.K3]): *Если числа q и s простые, то подгруппы порядков q^2 и qs группы Q^* циклические.*

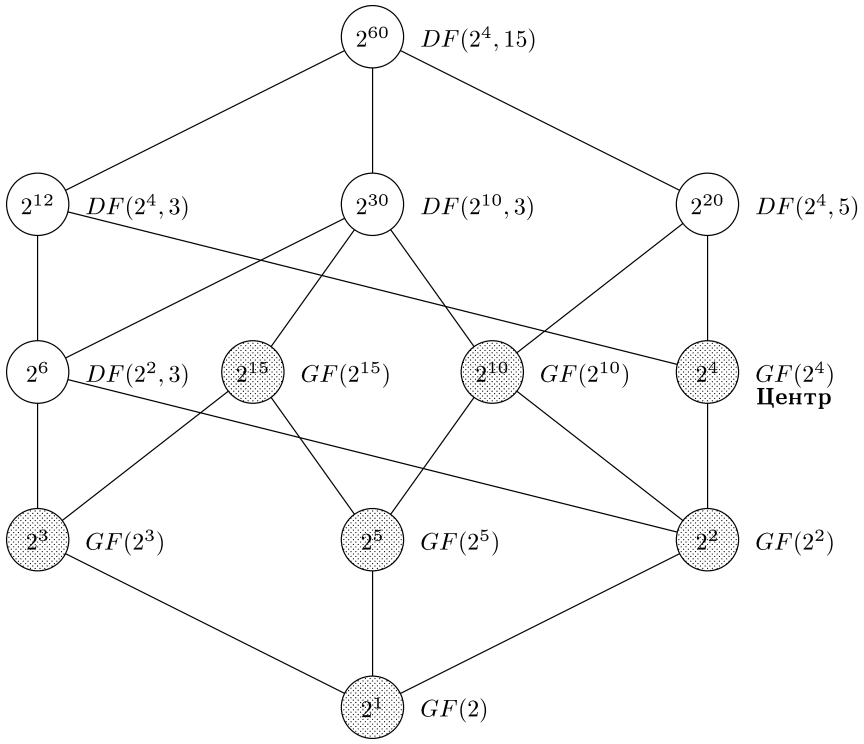

Рис. 1: Решетка под-почти-полей в почти-поле Диксона порядка 2^{60}

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] и [17, теорема IV.1.5]), наряду с цикличностью центра $Z(Q^*)$ и фактор-группы $Q^*/Z(Q^*)$ (метацикличность группы Q^*), установлена

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

$$Q^*=\langle a,b \mid a^m=1,\quad b^n=a^t,\quad bab^{-1}=a^q\rangle,\qquad m=\frac{q^n-1}{n},\quad t=\frac{m}{q-1}. \tag{4}$$

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 (4), решает

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

$$\left(k\,\frac{q^{zs}-1}{q^s-1}+\frac{zst}{n}\right)\ \vdots\ m,\qquad k=0,1,\ldots,m-1,\ s=1,2,\ldots,n-1. \tag{5}$$

Доказательство. Найдем порядки элементов в мультипликативной группе Q^* почти-поля Диксона $Q\in DF(q,n)$. Используя ее определяющие соотношения (4)

и факторизацию $Q^*=\langle a\rangle\langle b\rangle$, получаем

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

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

Поэтому для произвольных k и s из (5) 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

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

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 $a^kb^s\ne1$ – это наименьшее натуральное число z, удовлетворяющее условию (5) и делящее q^n-1.

Теорема доказана.

П р и м е р 4. Проиллюстрируем теорему на примере почти-поля $Q\in DF(5,2)$, где

$$Q^*=\{a^kb^s\mid k=0,1,\ldots,11,\ s=0,1\},$$

$$m=12,\quad t=3,\quad a^{12}=1,\quad b^2=a^3,\quad bab^{-1}=a^5.$$

Для произвольного элемента $a^kb\in\langle a\rangle b$ условие (5) принимает вид

$$\left(\frac{k(5^z-1)}{4}+\frac{3z}{2}\right)\ \vdots\ 12,$$

получаем $z=|a^kb|=8$. Поэтому спектр группы Q^* получается присоединением числа 8 к спектру циклической группы $\langle a\rangle$ порядка 12, то есть 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.

Т а б л и ц а 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

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

Таблица 3

Автоморфизмы исключительных почти-полей Q

Тип	$\lvert Q\rvert$	Q^*	$Aut(Q^*)$	$\lvert Aut(Q)\rvert$
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. М.: 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.

[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.

[4] **Hughes D.R., Piper F.C.** Projective planes. Springer–Verlag New–York Inc., 1973. 292 p.

[5] **Johnson N.L., Jha V., Biliotti M.** Handbook of finite translation planes. London New York, Chapman Hall/CRC. 2007. 888 p.

[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.

[7] **Wene G.P.** On the multiplicative structure of finite division rings. Aequationes Math. 1991. Vol. 41. P. 222–233.

[8] **Zassenhaus H.** Uber endliche Fastkörper // Abh. Math. Sem. Hamburg. 1936. Vol. 11. P. 187–220.

[9] **Холл М.** Теория групп. М.: Госиноиздат, 1962. 468 с.

[10] **Яковлева Т.Н.** Вопросы строения квазиполей с ассоциативными степенями. Известия Иркутского государственного университета. Серия «Математика». 2019. Т. 29, с. 107–119.

[11] **Felgner U.** Pseudo-finite near-fields // Near-rings and near-fields. Elsevier Science Publisher B. V. North-Holland. 1987. P. 15–29.

[12] **Коксетер Г.С.М., Мозер У.О.Дж.** Порождающие элементы и определяющие соотношения дискретных групп. М.: 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.

[14] **Dancs Groves S.** Locally finite near-fields // Abh. Math. Sem. Univ. Hamburg. 1979. Vol. 48. P. 89–107.

[15] **Dancs S.** On finite Dickson near-fields // Abh. Math. Sem. Univ. Hamburg. 1972. Vol. 37. P. 254–257.

[16] **Ellers E., Karzel H.** Endliche Inzidenzgruppen // Abh. Math. Sem. Hamburg. 1964. Vol. 27. P. 250–264.

[17] **Wähling H.** Theorie der Fastkörper. Volume 1 of Thales Monographs. Thales-Verlag, Essen, 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.