Серия «Математика»
2019. Т. 29. С. 107—119

Онлайн-доступ к журналу:
http://mathizv.isu.ru

И З В Е С Т И Я
Иркутского
государственного
университета

УДК 512.5
MSC 22E05
DOI https://doi.org/10.26516/1997-7670.2019.29.107

Вопросы строения квазиполей с ассоциативными степенями

Т. Н. Яковлева
Сибирский федеральный университет, Красноярск, Российская Федерация

Аннотация. Исследуется строение конечных квазиполей с ассоциативными степенями. Это прежде всего ассоциативные квазиполя, называемые почти-полями. К ним относят также квазиполя Муфанг, у которых лупы ненулевых элементов есть, по определению, лупы, введенные Рут Муфанг в 1935 г.

В работе приводятся основные определения, связанные с квазиполями. Показывается, что единица любого конечного (правого) квазиполя Q порождает простое подполе P, и Q всегда есть левый модуль над P, а двусторонний — не всегда. Как следствие, найдено новое доказательство известного утверждения: простое подполе конечного полуполя всегда лежит в центре. В то же время выявляются конечные почти-поля с простым подполем, не лежащим в центре. Известный вопрос о максимальных подполях конечных квазиполей полностью решен для класса конечных почти-полей порядка p^r с простыми числами p и r.

В решении вопросов о максимальных подполях и спектрах групповых порядков ненулевых элементов конечных квазиполей Муфанг предлагается использовать известные аналоги теоретико-групповых теорем Лагранжа и Силова. Перечислены все возможные двузначные порядки собственных квазиполей Муфанг.

Ключевые слова: конечные почти-поля Диксона, квазиполе, полуполе, лупа Муфанг, квазиполе Муфанг.

1. Введение

Исследования проективных плоскостей и координатизирующих квазиполей, проводимые уже более века, тесно связаны [13; 16; 20]. С середины прошлого века они используют компьютерные вычисления и отражались в 2007 г. в обширном обзоре [14].

В то же время строение даже известных собственных (или не являющихся полем) конечных квазиполей изучено мало. Более изучены конечные квазиполя с ассоциативными степенями. Вопросы о максимальных подполях и спектрах порядков ненулевых элементов конечных квазиполей в последние годы отмечались на конференциях [17], статьях [18] и [19] (вопросы **(A)** и **(C)**); там же отражаются их исследования для отдельных полуполей и квазиполей малых порядков.

В § 2 мы доказываем, что единица конечного (правого) квазиполя Q порождает простое подполе P, и Q всегда есть левый модуль над P (Лемма 2). Как следствие, найдено новое доказательство известного утверждения: простое подполе конечного полуполя всегда лежит в центре (Следствие 2). В то же время найдено конечное почти-поле с простым подполем, не лежащим в центре, и выявляется, что существует точно четыре конечных почти-поля с таким аномальным свойством (Пример 1 и Замечание 1).

Описание под-почти-полей конечного почти-поля Диксона ранее было установлено в работах [5; 6] и [9]. Опираясь на этот результат, мы полностью решаем отмеченный выше вопрос **(A)** для класса конечных почти-полей порядка p^r с простыми числами p и r (Теорема 3).

В решении вопросов **(A)** и **(C)** из [19] для конечных квазиполей Муфанг (у них, по определению, лупы ненулевых элементов — это лупы, введенные Рут Муфанг в 1935 г.) в § 4 предлагается использовать известные аналоги из [10; 11] и [12] теоретико-групповых теорем Лагранжа и Силова. Основная в этом параграфе теорема 6 перечисляет все возможные двузначные порядки собственных квазиполей Муфанг.

2. Простое подполе конечных квазиполей

Множество L с бинарной операцией $\cdot$ называется *лупой*, если в $(L, \cdot)$ существует нейтральный элемент и уравнения $a \cdot x = b$ и $x \cdot a = b$ однозначно разрешимы при любых $a, b \in L$, [2], [1]. В частности, группа — это ассоциативная лупа.

Отказываясь в определении поля от коммутативности, приходим к понятию тела. Отбрасывая также требования ассоциативности, приходим к понятию полуполя. К более общему понятию приводит ослабление дистрибутивности, см. [20], [13].

Определение 1. *Множество $Q = (Q, +, \cdot)$ с бинарными операциями сложения $+$ и умножения $\cdot$ называют правым квазиполем, если выполняются следующие условия:*

1) $(Q, +)$ — абелева группа;

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

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

4) *выполняется 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. Согласно теореме 7.3 Д. Хьюгеса и Ф. Пайпера [13], для конечного правого квазиполя аксиома 5 вытекает из аксиом 1–4, то есть является излишней. Далее, говорим «квазиполе» вместо «правое квазиполе».

Нам потребуются леммы о простом подполе.

Лемма 1. *Любая абелева аддитивная группа* $A = (A, +)$ *превращается в двусторонний* $\mathbb{Z}$*-модуль, если для элементов* $x \in A$ *и целых чисел* $k > 0$ *полагать* $0x := 0 = x0$ *и*

$$kx := \underbrace{x + x + \ldots\ + x}_{k\ \text{раз}} = xk, \quad (-k)x := -(kx) = x(-k).$$

Доказательство. Из ассоциативности сложения в группе A и соотношения $kx = xk$ для любых $x, y \in Q$ и $k, m \in \mathbb{Z}$ вытекают следующие равенства:

$$k(mx) = (km)x = x(km) = (xk)m, \quad (k+m)x = kx + mx = x(k+m).$$

Используя также коммутативность сложения для любых $x, y \in Q$ и $k, m \in \mathbb{Z}$, получаем

$$k(x+y) = kx + ky = (x+y)k.$$

Лемма доказана. □

Лемма 2. *Пусть* Q — *правое квазиполе с единицей* e. *Тогда:*

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

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

Доказательство. Очевидно, что для любых $k, m \in \mathbb{Z}$ имеем:

$$\pi(k+m) = (k+m)e = ke + me = \pi(k) + \pi(m).$$

Отображение π сохраняет также операцию умножения целых чисел – $\pi(km) = \pi(k)\pi(m)$, так как

$$ke \cdot me = k\big(e \cdot (me)\big) = \underbrace{e \cdot me + e \cdot me + \ldots\ + e \cdot me}_{k\ \text{раз}} =$$

$$= \underbrace{me + me + \ldots\ + me}_{k\ \text{раз}} = k(me) = (km)e \quad (k, m \in \mathbb{Z}).$$

Поэтому π является гомоморфизмом в Q кольца $\mathbb{Z}$ целых чисел, и утверждение а) леммы доказано.

Свойства коммутативности, ассоциативности и дистрибутивности кольца при гомоморфизмах сохраняются. Поэтому $\pi(\mathbb{Z}) = \{ke|k \in \mathbb{Z}\}$ — ассоциативное коммутативное подкольцо в Q, аддитивно порождаемое единицей, причем ненулевое, так как $e \neq 0$.

В силу известной теоремы о гомоморфизмах колец, кольцо $\pi(\mathbb{Z})$ изоморфно фактор-кольцу кольца $\mathbb{Z}$ по ядру $Ker(\pi)$ гомоморфизма π. Если ядро гомоморфизма π нулевое, то $\pi(\mathbb{Z}) \cong \mathbb{Z}$. Когда $Ker(\pi) \neq 0$, подкольцо $\pi(\mathbb{Z})$ изоморфно конечному кольцу вычетов кольца $\mathbb{Z}$ и не имеет делителей нуля, как подмножество в Q. Следовательно, $\pi(\mathbb{Z})$ изоморфно простому подполю $\mathbb{Z}_p$ для некоторого простого числа p. Существует $p > 0$ такое, что $pe = 0$, и p является минимальным. Тогда p — простое число и $p = km$. Получаем, что $\pi(\mathbb{Z}) \cong \mathbb{Z}_p$.

Наконец, следующие равенства показывают, что Q есть левый $\pi(\mathbb{Z})$-модуль и завершают доказательство:

$$me \cdot x = m(ex) = mx,$$

$$(ke) \cdot (me \cdot x) = k(e \cdot (me \cdot x)) = (km)x = (ke \cdot me) \cdot x,$$

$$me \cdot (x + y) = m(x + y) = mx + my = (me \cdot x) + (me \cdot y),$$

$$(ke + me)x = (ke)x + (me)x = k(ex) + m(ex) = ((k + m)e)x.$$

□

Из утверждения б) доказанной леммы сразу же вытекает

Следствие 1. *Порядок $|Q|$ всякого конечного квазиполя Q есть степень простого числа, равного порядку простого подполя $\pi(\mathbb{Z})$.*

По аналогии с леммой 2 показывается, что левое квазиполе является правым $\pi(\mathbb{Z})$-модулем. Произвольное полуполе является кольцом, а потому и двусторонним $\pi(\mathbb{Z})$-модулем. Как следствие, для конечных полуполей отсюда вытекает

Следствие 2. *В конечном полуполе S простое подполе всегда лежит в центре.*

Доказательство. Пусть P — простое подполе полуполя S, т. е.

$$P = \pi(\mathbb{Z}) = \{e, 2e, \ldots\ , (p - 1)e, pe = 0\}.$$

Докажем, что центр полуполя S содержит P. Требуемые равенства $(ke)x = x(ke)$ вытекают при любых $ke \in P^*$ и $x \in S$ из равенств:

$$(ke)x = \underbrace{(e + \ldots\ + e)}_{k\ \text{раз}}x = \underbrace{ex + \ldots\ + ex}_{k\ \text{раз}} = \underbrace{x + \ldots\ + x}_{k\ \text{раз}},$$

$$x(ke) = x\underbrace{(e + \ldots\ + e)}_{k\ \text{раз}} = \underbrace{xe + \ldots\ + xe}_{k\ \text{раз}} = \underbrace{x + \ldots\ + x}_{k\ \text{раз}}.$$

□

Полученное следствие дает новое доказательство известного утверждения; ранее (см., например, [14, Замечание 5.56]) утверждение следствия 2 устанавливалось с помощью понятий правого, левого и среднего ядер полуполя.

В следующем параграфе мы укажем примеры квазиполей (даже среди почти-полей), в которых простое подполе не лежит в центре.

3. Максимальные подполя конечных почти-полей

Всякое ассоциативное квазиполе называют *почти-полем* [2]. Ясно, что собственное конечное почти-поле, в отличие от полуполей, не обязано даже быть кольцом.

В этом параграфе, опираясь на классификацию Цассенхауза конечных почти-полей, мы исследуем для них вопрос **(A)** из [19] о максимальных подполях. Вместе с тем укажем примеры почти-полей, в которых простое подполе не лежит в центре.

В 1936 г. Цассенхауз [22] описал все конечные почти-поля, связывая с каждым из них определенную 2-транзетивную группу; см. также [2, Глава 20].

Рассмотрим кратко эту связь. 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. Когда каждая такая подстановка T определена однозначно (так что только единичная подстановка оставляет неподвижными 2 символа), группу G называют *точно 2-транзитивной*.

Пусть G — конечная точно 2-транзитивная группа подстановок множества Ω. Построим алгебраическую систему $K = (\Omega, +, \cdot)$ на множестве Ω. Один символ этой системы считаем нулем 0, а другой — единицей 1, так что при любом $a \in \Omega$ имеем

$$a + 0 = a = 0 + a, \qquad 0a = 0 = a0, \qquad a1 = a = 1a.$$

Подгруппу всех подстановок, оставляющих на месте символ 0, обозначим через M.

Известно [2, § 20.7], [22], что при $x, y \in \Omega$, в G существует не более одной подстановки, переводящей x в y и переставляющей все символы. Кроме того, подстановки в G, переставляющие все символы, образуют вместе с единичной подстановкой инвариантную абелеву подгруппу A, транзитивную на Ω. Если $b, x \in \Omega$, то в подгруппе A существует и единственна подстановка

$$A_b = \begin{pmatrix} 0 & \dots & x & \dots \\ b & \dots & y & \dots \end{pmatrix}.$$

Полагая $y = x + b$, получаем корректно определенное сложение на Ω. Для ненулевых элементов $m, x, y \in \Omega$ однозначно определены в G подстановка

$$M_m = \begin{pmatrix} 0 & 1 & \dots & x & \dots \\ 0 & m & \dots & y & \dots \end{pmatrix},$$

а поэтому и произведение $y = xm \ \ (x, m \in \Omega \setminus \{0\})$. Тем самым сложение и умножение определены на Ω корректно, причем

$$A_a A_b = A_{a+b}, \quad M_m M_t = M_{mt},$$

$$M_m^{-1} A_1 M_m = A_m, \quad M_t^{-1} A_m M_t = A_{mt} \quad (a, b, m, t \in \Omega, \ mt \neq 0).$$

Более того, согласно [2, Теорема 20.7.1], алгебраическая система $K = (\Omega, +, \cdot)$ есть почти-поле,

$$(K, +) \simeq A, \quad K^* := (K \setminus \{0\}, \cdot) \simeq M,$$

а группа его линейных преобразований $y = xm + b$, $m \neq 0$, изоморфна группе G. Обратно: группа указанных подстановок элементов любого конечного почти-поля K является точно 2-транзитивной.

В [2, Лемма 20.7.K4] доказана

Лемма 3. *Силовская r-подгруппа S_r группы M является циклической, или при $r = 2$ и подходящем $n \geq 3$ обобщенной кватернионной*

$$\langle a, b \mid a^{2^{n-1}} = 1, \ b^2 = a^{2^{n-2}}, \ ba = ab^{-1} \rangle.$$

Известный довольно общий 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 центра и степенью n, которые выбирают произвольно с условиями:

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

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

Почти-поля, построенные таким способом, Цассенхауз [22] называет *почти-полями Диксона.* Центр всякого почти-поля Диксона, по построению, является подполем и, очевидно, содержит простое подполе.

По теореме Цассенхауза [2, с. 420], все конечные почти-поля исчерпываются почти-полями Диксона и, кроме того, семью *исключительными почти-полями* порядка p^2; по одному почти-полю для каждого из простых чисел $p = 5, 7, 23, 29, 59$, а также два почти-поля при $p = 11$. Требуемый в конце предыдущего параграфа пример дает

Пример 1. Группа K^* исключительного почти-поля K порядка p^2 при $p = 5$ в [2] точно представлена группой $SL(2, 3)$ порядка 24. Ее порождают матрицы

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix} \tag{3.1}$$

над полем $GF(3)$. По лемме 3 силовская 2-подгруппа группы $SL(2, 3)$ является кватернионной порядка 8 с центром $\{E, -E\}$ порядка 2. Поэтому центр почти-поля K имеет порядок 3 и даже не является подполем, а поэтому не содержит простое подполе порядка 5.

Замечание 1. Все группы K^* исключительных почти-полей K представлены в [2, стр. 420–421] в списке $I - VII$. Используя указанное представление группы K^* и лемму 3, О. В. Кравцова, В. М. Левчук и автор недавно завершили перечисление исключительных почти-полей, в которых простое подполе не лежит в центре. Оказывается, простое подполе не совпадает с центром почти-поля точно в четырех из семи исключительных почти-полей. Таким образом, с учетом теоремы Цассенхауза, существует точно четыре конечных почти-поля, в которых простое подполе не лежит в центре.

В связи с вопросом **(A)** из [19], нам потребуется далее описание из С. Данкс [5], [6] и У. Филгнер [9] под-почти-полей Диксонова почти-поля. Зафиксируем конечное почти-поле Диксона K порядка q^n с центром $Z(K)$ порядка $q = p^l$ для некоторого простого числа p, $Z(K) \cong GF(q)$. Ядром почти-поля K называют совокупность

$$C(K) = \{x \in K \mid (y + z) \cdot x = y \cdot x + z \cdot x \quad \text{для всех} \quad y, z \in K\}.$$

Теорема 1. *Если H есть под-почти-поле в K, то $H = p^h$, $h \mid (l \cdot n)$. Обратно, если $h \mid (l \cdot n)$, то K имеет единственное под-почти-поле H порядка p^h, и H — почти-поле Диксона, причем*

$$Z(H) = C(H) \cong GF(p^z),$$

$$z = \text{НОД}(jl, \ h), \quad 0 < j \leq n, \quad j \equiv (q^n - 1)/(p^h - 1)(mod \ n).$$

С помощью этой теоремы в [9] выявляется единственность максимального подполя в почти-поле Диксона, содержащего центр. Более точно, в [9] доказана

Теорема 2. *Пусть почти-поле K выбрано, как в теореме 1, и λ — максимальное число такое, что $\lambda^2|n$. Тогда среди всех коммутативных подполей D в K с центром $Z(K) \subseteq D$ существует единственное максимальное подполе M порядка q^λ.*

Для одного класса конечных почти-полей мы можем описать максимальные подполя полностью (как требует вопрос **(A)** из [19]), в том числе, когда простое подполе не лежит в центре почти-поля.

Теорема 3. *Максимальное подполе конечного почти-поля порядка p^r с простыми числами p и r всегда совпадает с простым подполем.*

Доказательство. Согласно теореме 1 под-почти-поля конечного почти-поля Диксона K порядка q^n с центром $Z(K) \cong GF(q)$, $q = p^l$, взаимно-однозначно соответствуют делителям числа $l \cdot n$. Когда $|K| = p^r$, где r – простое число, это означает, что $l \cdot n = r$ и, следовательно, K имеет единственное под-почти-поле, отличное от K. Ясно, что оно совпадает с простым подполем и является единственным максимальным подполем. В каждом их семи исключительных почти-полей при $r = 2$ простое подполе, очевидно, также является единственным максимальным подполем. □

4. Квазиполя и лупы Муфанг

К квазиполям с ослабленной ассоциативностью приводят квазиполя Муфанг с лупой Муфанг ненулевых элементов, по определению. Согласно [3], *лупа Муфанг* — это лупа M, такая, что для всех $x, y, z \in M$ выполняется одно из (эквивалентных) тождеств:

$$(xy)(zx) = \big(x(yz)\big)x, \tag{4.1}$$

$$\big((xy)z\big)y = x\big(y(zy)\big), \tag{4.2}$$

$$x\big(y(xz)\big) = \big((xy)x\big)z. \tag{4.3}$$

Если квазиполе удовлетворяет тождеству Муфанг 4.1, то его называют *квазиполем Муфанг*, [15]. Из определений сразу же следует, что все почти-поля являются квазиполями Муфанг. Лупы Муфанг были введены Р. Муфанг [21] в 1930-х гг. См. также Р. Брук [3].

Тождества 4.1 – 4.3 называются *тождествами Муфанг.* Их эквивалентность устанавливает лемма 3.1 в [3]. В силу этой же леммы, лупа Муфанг M удовлетворяет также тождествам

$$(xx)y = x(xy), \quad (xy)x = x(yx), \quad (yx)x = y(xx).$$

Циклические лупы Муфанг — ассоциативны, и поэтому являются группами. В частности, циклические лупы Муфанг — это хорошо известные циклические группы.

Как доказано в [11], теоретико-групповая теорема Лагранжа переносится на конечные лупы Муфанг.

Теорема 4. *Порядок любой конечной лупы Муфанг M делится на порядок любой ее подлупы.*

Для доказательства этой теоремы Гришков и Заварницин использовали связь между лупами Муфанг и группами с тройственностью.

В [10; 12] на лупы Муфанг переносятся теоремы Силова.

Определение 2. *Подлупу P лупы Муфанг M называют p-подлупой, если порядок $|P|$ является p-примарным, и называют p-силовской, если порядок $|P|$ и индекс $|M : P|$ взаимно просты.*

Множество всех p-силовских подлуп в M обозначим как $Syl_p(M)$.

Теорема 5. *Если M — конечная лупа Муфанг и p — простой делитель порядка $|M|$, то $|Syl_p(M)| \equiv 1 \pmod p$.*

Сейчас несложно описать все возможные двузначные порядки собственных (не являющихся полем) квазиполей Муфанг.

Теорема 6. *Собственные квазиполя Муфанг порядка ≤ 100 могут существовать лишь для порядков 25, 49, 64 и 81.*

Доказательство. В статье Орина Чейна [4] перечислены все неассоциативные лупы Муфанг порядков ≤ 32. Более точно, существует 13 таких луп: по одной порядков 12, 20 и 28, пять - порядка 16, пять - порядка 24. Ясно, что лупа 3.1 порядка 24 приводит к собственному (исключительному) почти-полю K порядка 25; квазиполе порядка 21 не существует, в силу следствия 1. Очевидно, квазиполя порядков 13 и 29 являются полями, как и квазиполе любого простого порядка. Возможные порядки в интервале $32 < |M| \leq 100$ возможны только для порядков 49, 64 и 81, согласно построению всех почти-полей Диксона, которое приведено в параграфе 3. $\square$

Замечание 2. Теоремы 4 и 5 Гришкова, Заварницына и Гаголы, а также теорема 1 из § 3 позволяют решать вопрос **(C)** из [19] для почти-полей и квазиполей Муфанг.

5. Заключение

Получены следующие результаты.
1. Доказано, что единица конечного (правого) квазиполя Q порождает простое подполе P, и Q всегда есть левый модуль над P. Как следствие, найдено новое доказательство известного утверждения: простое подполе конечного полуполя всегда лежит в центре.
2. Выявляются конечные почти-поля с простым подполем, не лежащим в центре.
3. Известный вопрос о максимальных подполях конечных квазиполей полностью решен для класса конечных почти-полей порядка p^r с простыми числами p и r.
4. Перечислены все возможные двузначные порядки собственных квазиполей Муфанг.

Автор статьи выражает искреннюю благодарность профессору В. М. Левчуку за постановку задачи и внимание к данной работе.

Список литературы

1. Курош А. Г. Лекции по общей алгебре. СПб. : Лань, 2007. 560 с.
2. Холл М. Теория групп. М. : Издательство иностранной литературы, 1962. 460 с.
3. Bruck R. H. A survey of binary systems. Springer-Verlag, 1971. 188 p.
4. Chein O. Moufang loops of small order // Transactions of the American mathematical society. 1974. Vol.188, Iss. 2. P. 31–51. https://doi.org/10.1090/S0002-9947-1974-0330336-3
5. Dancs S. The sub-near-field structure of finite near-fields // Bull. Austral. Math. Soc. 1971. Vol.5. P. 275–280. https://doi.org/10.1017/S000497270004716X
6. Dancs S. On finite Dickson near-fields // Abh. Math. Sem. Univ. Hamburg. 1972. Vol. 37. P. 254–257. https://doi.org/10.1007/BF02999702
7. Dancs S. Groves Locally finite near-fields // Abhandl. Math. Seminar Hamburg. 1979. Vol. 48. P. 89-107. https://doi.org/10.1007/BF02941292
8. Dickson L. E. Linear algebras in which division is always uniquely possible // Trans. Amer. Math. Soc. 1906. Vol. 7. P. 370–390.
9. Felgner U. Pseudo-finite near-field // Proc. Conf. Tubingen, North-Holland, Amsterdam, 1987. P. 15–29. https://doi.org/10.1016/S0304-0208(08)72282-5
10. Gagola S. M. The conjugacy of triality subgroups of Sylow subloops of Moufang loops // Journal of Group Theory. 2010. Vol. 13, Iss. 6. P. 821–840. https://doi.org/10.1515/jgt.2010.026
11. Grishkov A. N., Zavarnitsine A. V. Lagrange's theorem for Moufang Loops // Math. Proc. Camb. Phil. Soc. 2005. N 1(139). P. 41–57. https://doi.org/10.1017/S0305004105008388
12. Grishkov A. N., Zavarnitsine A. V. Sylow's theorem for Moufang loops // Journal of Algebra. 2009. Vol. 321, Iss. 7. P. 1813–1825. https://doi.org/10.1016/j.jalgebra.2008.08.035
13. Hughes F. S., Piper F. C. Projective planes. New-York Inc., Springer–Verlag, 1973. 291 p.

14. Johnson N. L., Jha V., Biliotti M. Handbook of finite translation planes. London, New York, Chapman Hall/CRC, 2007. 861 p.
15. Kallaher M. J. Right Bol Quasi-Fields // Canadian journal of mathematics. 1969. Vol. 21. P. 1409–1420. https://doi.org/10.4153/CJM-1969-155-8
16. Knuth D. E. Finite semifields and projective planes // J. Algebra. 1965. Vol. 2. P. 182-217. https://doi.org/10.1016/0021-8693(65)90018-9
17. Levchuk V. M., Panov S. V., Shtukkert P. K. The structure of finite quasifields and their projective translation planes. // Proceed. XII Intern. Conf. on Algebra and Number Theory. Tula, 2014. P. 106–108.
18. Levchuk V. M., Shtukkert P. K. The structure of quasifields of small even orders // Proceed. Steklov Inst. Math. and Mechanics Ural Branch of RAS. Pleiades Publishing. 2015. Vol. 21, N 3. P. 197–212.
19. Levchuk V. M., Kravtsova O. V. Problems on structure of finite quasifields and projective translation planes // Lobachevskii Journal of Mathematics. 2017. Vol. 38, N 4. P. 688–698.
20. Luneburg H. Translation planes. Berlin–Heidelberg–New York, Springer–Verlag, 1980. 278 p. https://doi.org10.1007/978-3-642-67412-9
21. Moufang R. Zur Struktur von Alternativkorpern // Math. Ann. 1935. Vol. 110, N 1. P. 416–430. https://doi.org/10.1007/BF01448037
22. Zassenhaus H. Uber endliche Fastkorper // Abh. Math. Sem. Hamburg. 1935. Vol. 11, Iss. 1. P. 187–220. https://doi.org/10.1007/BF02940723

Татьяна Николаевна Яковлева, аспирант, Институт математики и фундаментальной информатики, Сибирский федеральный университет, Российская Федерация, 660041, г. Красноярск, пр. Свободный, 79, корп. 3, тел.: 89659139701 (e-mail: tnyakovleva@sfu-kras.ru)

Поступила в редакцию 08.05.19

Questions of Construction of Quasifields with Associative Powers

T. N. Yakovleva

Siberian Federal University, Krasnoyarsk, Russian Federation

Abstract. The structure of finite quasi-fields with associative degrees is investigated. These are, above all, associative quasifields, called near-fields. These also include the Moufang quasifields which have loops of nonzero elements are, by definition, loops introduced by Ruth Moufang in 1935.

The paper presents the main definitions associated with quasifields. It is shown that identity element of any finite (right) quasifield Q generates a simple subfield P, and Q is always a one-sided module over P , and a two-way — is not always. As a result, found new proof of a well-known statement: a simple subfield of a finite semifield always lies in the center. At the same time, the finite near-fields with a simple subfield that does not lie in the center. Famous the question of maximal subfields of finite quasifields is completely solved for a class of finite near-fields of order p^r with prime numbers p and r.

In solving the questions about maximal subfields and spectra of group orders of nonzero elements of finite Moufang quasifields, it is proposed to use the well-known analogues of the group-theoretic theorems of Lagrange and Sylow. All possible two-digit orders of the proper Moufang quasifields are listed.

Keywords: finite Dixon near-field, quasifield, semifield, Moufang loop, Moufang quasifield.

References

1. Kurosh A.G. *Lectures on general algebra* [Lekcii po obshhej algebre]. Saint-Petersburg, Lan Publ., 2007, 560 p.
2. Holl M. *Theory of group* [Teorija grupp]. Moscow, Foreign Literature Publishing House, 1962, 460 p.
3. Bruck R.H. *A survey of binary systems*. Springer-Verlag, 1971, 188 p.
4. Chein O. Moufang loops of small order. *Transactions of the American mathematical society*, 1974, vol.188, issue 2, pp. 31-51. https://doi.org/10.1090/S0002-9947-1974-0330336-3
5. Dancs S. The sub-near-field structure of finite near-fields. *Bull. Austral. Math. Soc.*, 1971, vol. 5, pp. 275–280. https://doi.org/10.1017/S000497270004716X
6. Dancs S. On finite Dickson near-fields. *Abh. Math. Sem. Univ. Hamburg*, 1972, vol. 37, pp. 254–257. https://doi.org/10.1007/BF02999702
7. Dancs S. Groves Locally finite near-fields. *Abhandl.Math.Seminar Hamburg*, 1979, vol. 48, pp. 89-107. https://doi.org/10.1007/BF02941292
8. Dickson L.E. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.* 1906, vol. 7, pp. 370-390.
9. Felgner U. Pseudo-finite near-field. textitProc. Conf. Tubingen, North-Holland, Amsterdam, 1987, pp. 15-29. https://doi.org/10.1016/S0304-0208(08)72282-5
10. Gagola S.M. The conjugacy of triality subgroups of Sylow subloops of Moufang loops. *Journal of Group Theory.*, 2010, vol. 13, issue 6, pp. 821-840. https://doi.org/10.1515/jgt.2010.026
11. Grishkov A.N., Zavarnitsine A.V. Lagrange's theorem for Moufang Loops. *Math. Proc. Camb. Phil. Soc.*, 2005, no. 1(139), pp. 41—57. https://doi.org/10.1017/S0305004105008388
12. Grishkov A.N., Zavarnitsine A.V. Sylow's theorem for Moufang loops. *Journal of Algebra*, 2009, vol. 321, issue 7, pp. 1813-1825. https://doi.org/10.1016/j.jalgebra.2008.08.035
13. Hughes F.S., Piper F.C. *Projective planes*. New-York Inc, Springer-Verlag, 1973, 291 p.
14. Johnson N.L., Jha V., Biliotti M. *Handbook of finite translation planes*. London New York, Chapman Hall/CRC, 2007, 861 p.
15. Kallaher M.J. Right Bol Quasi-Fields. *Canadian journal of mathematics*, 1969, vol. 21, pp. 1409-1420. https://doi.org/10.4153/CJM-1969-155-8
16. Knuth D.E. Finite semifields and projective planes. *J. Algebra*, 1965, vol. 2, pp. 182-217. https://doi.org/10.1016/0021-8693(65)90018-9
17. Levchuk V.M., Panov S.V., Shtukkert P.K. The structure of finite quasifields and their projective translation planes. *Proceed. XII Intern. Conf. on Algebra and Number Theory*. Tula, 2014, pp. 106-108.
18. Levchuk V.M., Shtukkert P.K. The structure of quasifields of small even orders. *Proceed. Steklov Inst. Math. and Mechanics Ural Branch of RAS*. Pleiades Publishing, 2015, vol. 21 (3), pp. 197-212.
19. Levchuk V.M., Kravtsova O.V. Problems on structure of finite quasifields and projective translation planes. *Lobachevskii Journal of Mathematics*, 2017, vol. 38, no. 4, pp. 688-698.

20. Luneburg H. *Translation planes*. Berlin, Heidelberg, New York, Springer-Verlag, 1980, 278 p. https://doi.org10.1007/978-3-642-67412-9
21. Moufang R. Zur Struktur von Alternativkorpern. *Math. Ann.*, 1935, vol. 110, no. 1, pp. 416-430. https://doi.org/10.1007/BF01448037
22. Zassenhaus H. Uber endliche Fastkorper. *Abh. Math. Sem. Hamburg*, 1935, vol. 11, issue 1, pp. 187-220. https://doi.org/10.1007/BF02940723

Tatiyana Yakovleva, Postgraduate, Siberian Federal University, 79, Svobodniy Avenue, Krasnoyarsk, 660041, Russian Federation,
tel.: 89659139701 (e-mail: tnyakovleva@sfu-kras.ru)

Received 08.05.19