Math-Net.Ru

Общероссийский математический портал

В. А. Тестов, Об аналоге основной теоремы арифметики в упорядоченных группоидах, *Матем. заметки*, 1997, том 62, выпуск 6, 910–915

DOI: <https://doi.org/10.4213/mzm1680>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.73.92

26 апреля 2023 г., 12:29:40

УДК 512.548.4

ОБ АНАЛОГЕ ОСНОВНОЙ ТЕОРЕМЫ АРИФМЕТИКИ В УПОРЯДОЧЕННЫХ ГРУППОИДАХ

В. А. Тестов

В заметке рассматриваются направленные группоиды с интерполяционным свойством Рисса: если $a_i \leq b_j$ ($i, j = 1, 2$), то найдется c такой, что $a_i \leq c \leq b_j$ ($i, j = 1, 2$). Для таких группоидов с условием минимальности для положительного конуса, в которых

$$\forall a, b \quad a \leq b \implies \exists u, v \quad au = va = b,$$

доказывается теорема, аналогичная основной теореме арифметики. Полученный результат является обобщением ранее известных результатов для решеточно упорядоченных моноидов, луп и квазигрупп.

Библиография: 7 названий.

Хорошо известно, что выполнение условия минимальности позволяет доказать для некоторых классов упорядоченных групп и моноидов теоремы, аналогичные основной теореме арифметики (см. [1, гл. 13, 19] и [2, гл. 5, 12]). Рядом авторов [3]–[5] аналогичные теоремы были доказаны для решеточно упорядоченных луп и квазигрупп. Для решеточно упорядоченных группоидов с некоторыми дополнительными условиями аналог основной теоремы арифметики был получен в работах [6], [7].

Вместе с тем, также хорошо известны примеры упорядоченных группоидов, в которых однозначность разложения на простые множители не выполняется.

ПРИМЕР 1. $G(+) = \{(m, n) \mid m, n \in \mathbb{Z}, m + n \in 2\mathbb{Z}\}$, где $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$ и $(a, b) \leq (c, d) \iff a \leq c \& b \leq d$.

ПРИМЕР 2. $K(\cdot) = \{x \in \mathbb{N} \mid x = 4n + 1, n = 0, 1, \dots\}$ с обычным умножением и с отношением делимости ' $\mid$ '.

В настоящей заметке устанавливается, что достаточным условием однозначности разложения на простые множители в упорядоченных группоидах является условие риссовости порядка. Это условие является и необходимым в коммутативных моноидах с сокращением.

Пусть $A(\cdot)$ – группоид (т.е. алгебра с одной бинарной операцией ' $\cdot$ ') с единицей e .

Группоид $A(\cdot)$ называется *естественно упорядоченным*, если на множестве его элементов A определено отношение порядка ' $\leq$ ' и выполняются следующие условия:

- 1) $\forall a, b, c \quad a \leq b \iff ac \leq bc \iff ca \leq cb$;
- 2) $\forall a, b \quad a \leq b \iff \exists u, v \quad au = va = b$.

Элементы u и v из условия 2) называются соответственно *правым* и *левым частными* и обозначаются $u = a \setminus b$, $v = b / a$.

Заметим, что в силу нашего определения частные для элементов b и a определены лишь в случае, когда $a \leq b$.

Нетрудно видеть, что в силу условия 1) естественно упорядоченный группоид является группоидом с сокращениями, поэтому левые и правые частные единственны.

Примерами естественно упорядоченных группоидов могут служить упорядоченные лупы и множество натуральных чисел $\mathbb{N}(\cdot)$ с отношением делимости $'|'$.

Отметим несколько простейших свойств правых частных (для левых аналогично).

1) Если $a \leq b$, то $e \leq a \setminus b$.

В самом деле, $a = ae \leq a(a \setminus b) \iff e \leq a \setminus b$.

2) Если $a \leq b_1 \leq b_2$, то $a \setminus b_1 \leq a \setminus b_2$.

В самом деле, пусть c_1 и c_2 таковы, что $ac_1 = b_1$, $ac_2 = b_2$, тогда $ac_1 \leq ac_2$ и $c_1 \leq c_2$, т.е. $a \setminus b_1 \leq a \setminus b_2$.

3) Если $a_1 \leq a_2 \leq b$, то $a_2 \setminus b \leq a_1 \setminus b$.

В самом деле, пусть $a_1c_1 = b$, $a_2c_2 = b$, тогда из $a_1 \leq a_2$ следует $a_1c_2 \leq a_2c_2 = b = a_1c_1$, или $c_2 \leq c_1$, т.е. $a_2 \setminus b \leq a_1 \setminus b$.

Множество $P = \{x \in A \mid e \leq x\}$ называется *положительным конусом* упорядоченного группоида A .

Естественно упорядоченный группоид назовем *риссовым естественно упорядоченным группоидом*, если порядок, заданный на множестве его элементов, является направленным (т.е. для любых $a, b \in A$ существуют c, d такие, что $c \leq a, b$ и $a, b \leq d$) и удовлетворяет интерполяционному свойству Рисса: если $a_i \leq b_j$ ($i, j = 1, 2$), то существует c такой, что $a_i \leq c \leq b_j$ ($i, j = 1, 2$).

Нетрудно видеть, что любой коммутативный моноид с сокращениями, в котором выполняется однозначность разложения на простые множители, является риссовым естественно упорядоченным группоидом (с отношением $'|'$).

Отметим следующие свойства группоидов с направленным порядком.

4) Если для $a, b \geq e$ существует $a \vee b$ (точная верхняя грань), то для любого c существуют $ca \vee cb$, $ac \vee bc$ и $ca \vee cb = c(a \vee b)$, $ac \vee bc = (a \vee b)c$.

Действительно, $a \leq a \vee b \iff ca \leq c(a \vee b)$ и $b \leq a \vee b \iff cb \leq c(a \vee b)$. Пусть $ca \leq d$, $cb \leq d$ для некоторого d , тогда, поскольку $c = ce \leq ca$, в силу свойства 2) $a \leq c \setminus d$, аналогично $b \leq c \setminus d$, поэтому $a \vee b \leq c \setminus d$, или $c(a \vee b) \leq d$.

5) Если для $a, b \geq e$ существует $a \wedge b$ (точная нижняя грань), то для любого c существуют $ca \wedge cb$, $ac \wedge dc$, и $c(a \wedge b) = ca \wedge cb$, $(a \wedge b)c = ac \wedge bc$.

Доказательство проводится двойственным образом.

6) Если $e \leq a \leq x$, $e \leq b \leq x$ и существует $a \wedge b$, то существует $(a \setminus x) \vee (b \setminus x)$ и $(a \wedge b) \setminus x = (a \setminus x) \vee (b \setminus x)$.

Действительно, так как $a \wedge b \leq a$, $a \wedge b \leq b$, то в силу свойства 3) $a \setminus x \leq (a \wedge b) \setminus x$ и $b \setminus x \leq (a \wedge b) \setminus x$. Пусть $a \setminus x \leq y$ и $b \setminus x \leq y$, тогда $x \leq ay$, $x \leq by$. Поскольку в силу свойства 5) $ay \wedge by$ существует, то $x \leq ay \wedge by$, откуда $x \leq (a \wedge b)y$, т.е. $(a \wedge b) \setminus x \leq y$.

7) Если $x \wedge y$ существует для $x, y \geq e$, то $x \vee y$ тоже существует, и $x \vee y = y((x \wedge y) \setminus x)$ и $x \vee y = x((x \wedge y) \setminus y)$.

В самом деле, так как $x \wedge y \leq x$, то частное $(x \wedge y) \setminus x$ существует. Далее, $y((x \wedge y) \setminus x) \geq (x \wedge y)((x \wedge y) \setminus x) = x$ и $y((x \wedge y) \setminus x) \geq y(x \setminus x) = ye = y$. Пусть $x \leq c$, $y \leq c$, т.е. $c = yb$, где $b \geq e$. Тогда $(x \wedge y)((x \wedge y) \setminus x) \wedge b = x \wedge ((x \wedge y)b) = x \wedge (xb) \wedge (yb) = x \wedge c = x$,

т.е. $(x \wedge y)((x \wedge y) \setminus x) \wedge b = (x \wedge y)((x \wedge y) \setminus x)$. Поэтому $((x \wedge y) \setminus x) \wedge b = (x \wedge y) \setminus x$, откуда $(x \wedge y) \setminus x \leq b$, а значит, $y((x \wedge y) \setminus x) \leq yb = c$. Второе равенство доказывается аналогично.

Элементы a и b риссова группоида называются *ортогональными* (запись: $a \perp b$), если $a \wedge b$ существует и $a \wedge b = e$.

Отметим несколько свойств ортогональных элементов.

8) Если $a \perp b$, то $a \vee b = ba = ab$.

Следует непосредственно из свойства 7).

9) Если $b \perp c$, то $a(bc) = (ab)c$.

Действительно, при наших предположениях $(ab) \wedge (ac) = a(b \wedge c) = ae = a$, поэтому, используя свойства 7) и 8), имеем

$$a(bc) = a(b \vee c) = (ab) \vee (ac) = (ab)((ab) \wedge (ac)) \setminus (ac) = (ab)(a \setminus (ac)) = (ab)c.$$

10) Если $a \perp b$ и $a \perp c$, то $a \perp (bc)$.

Действительно, $e = a \wedge c = a \wedge (a \wedge b)c = a \wedge (ac) \wedge (bc) = a \wedge (bc)$ (так как $a \leq ac$).

Из свойства 10) следует, что множество всех ортогональных к a элементов из A является подгруппоидом.

Элемент $p \in P$ называется *атомом*, если он покрывает единицу e , т.е. $e \leq x < p \iff x = e$. Иными словами, атомы – это минимальные элементы множества $P \setminus \{e\}$.

Элемент $p > e$ называется *простым*, если из $p \leq ab$ ($a, b \geq e$) следует $p \leq a$ или $p \leq b$.

Покажем сейчас, что эти два понятия для риссовых естественно упорядоченных групповидов совпадают.

ЛЕММА 1. Если p – атом, a – произвольный элемент из конуса P , то либо $p \perp a$, либо $p \leq a$.

ДОКАЗАТЕЛЬСТВО. В самом деле, $e \leq p, a$. Пусть $c \leq p, a$. Из условия Рисса следует существование d такого, что $e, c \leq d \leq p, a$. Так как $e \leq d \leq p$, то либо $d = e$ и тогда $c \leq e$ и $p \perp a$, либо $d = p$ и тогда $p \leq a$.

ПРЕДЛОЖЕНИЕ. Элемент $p \in P$ является атомом тогда и только тогда, когда p – простой.

ДОКАЗАТЕЛЬСТВО. В самом деле, пусть p – атом и $p \leq ab$. Если не выполняется ни $p \leq a$, ни $p \leq b$, то в силу леммы 1 $p \perp a$ и $p \perp b$, и по свойству 10) $p \perp (ab)$. Пришли к противоречию.

Обратно, пусть p простой и $e \leq a < p$, тогда существует b такой, что $ab = p$. Из простоты p вытекает либо $p \leq a$, либо $p \leq b$. Первое невозможно, поэтому из второго неравенства следует $ap \leq ab = p = ep \leq ap$, т.е. $a = e$, и p – атом.

Рассмотрим теперь группоид B , порожденный элементами $p_1, p_2, \dots$. Каждый элемент такого группоида B может быть представлен в виде конечного слова $w(p_1, p_2, \dots)$, составленного из символов $p_1, p_2, \dots$ и некоторой последовательности скобок. Количество вхождений символов $p_1, p_2, \dots$ в слово w назовем *длиной* слова w .

ЛЕММА 2. Если p – атом, то группоид B , порожденный элементом p , является полугруппой.

ДОКАЗАТЕЛЬСТВО. В силу свойства 10) если $x \in B$ и q – некоторый атом, отличный от p , то $x \perp q$. Пусть теперь x, y, z – произвольные элементы из B . Докажем, что $x(yz) = (xy)z$. Доказательство будем проводить индукцией по длине слова z .

Пусть длина слова равна 1, т.е. $z = p$. Надо доказать равенство $x(y p) = (x y)p$. В самом деле, $y p$ покрывает y , так как если $y p > u \geq y$, то $y \setminus (y p) > y \setminus u \geq y \setminus y$ или $p > y \setminus u \geq e$, откуда $y \setminus u = e$ и $u = y$. Далее, $x(y p)$ покрывает $x y$, так как если $x(y p) > u \geq x y$, то $x \setminus (x(y p)) > x \setminus u \geq x \setminus (x y)$ или $y p > x \setminus u \geq y$, откуда $u = x y$. Следовательно, $(x y) \setminus (x(y p))$ покрывает e и является некоторым атомом q , т.е. $q = (x y) \setminus (x(y p))$, откуда $x(y p) = (x y)q$. Если $q \neq p$, то, поскольку $x y > e$ и $(x y)q > q$, имеем $(x(y p)) \wedge q = ((x y)q) \wedge q$ или $e = q$ в силу свойства 10). Мы пришли к противоречию, следовательно, $q = p$. Таким образом, $x(y p) = (x y)p$.

Предположим теперь, что равенство $x(y z) = (x y)z$ справедливо для всех элементов $z \in B$, длина которых меньше n . Докажем, что тогда это равенство справедливо и для элемента z , длина которого равна n .

В самом деле, слово z может быть представлено в виде $z = z_1 z_2$, где z_1 и z_2 имеют длину меньшую, чем n . К этим словам мы можем применить наше индуктивное предположение:

$$x(y z) = x(y(z_1 z_2)) = x((y z_1) z_2) = (x(y z_1)) z_2 = ((x y) z_1) z_2 = (x y)(z_1 z_2) = (x y)z.$$

СЛЕДСТВИЕ 1. *Степени любого атома p определены однозначно.*

ЛЕММА 3. Пусть $w(p_1, p_2, \dots)$ – элемент в группоиде B , порожденном атомами $p_1, p_2, \dots$. Если w содержит m_i вхождений элемента p_i ($i = 1, 2, \dots$), то $w = \bigvee_i p_i^{m_i}$.

ДОКАЗАТЕЛЬСТВО будем проводить индукцией по длине слова w . Если длина слова w равна 1, утверждение справедливо.

Пусть утверждение справедливо для всех слов, длина которых меньше n . Докажем, что тогда утверждение справедливо и для слова w , длина которого равна n .

Пусть $w(p_1, p_2, \dots) = u(p_1, p_2, \dots)v(p_1, p_2, \dots)$. По индуктивному предположению

$$w = \bigvee_i p_i^{k_i} \cdot \bigvee_j p_j^{l_j},$$

где k_i и l_j – соответственно число вхождений атомов p_i и p_j в слова u и v . Будем предполагать, что в этом выражении для w каждое объединение $\bigvee_i p_i^{k_i}$, $\bigvee_j p_j^{l_j}$ содержит члены $p_s^{k_s}$, $p_s^{l_s}$ соответственно для каждого атома p_s , встречающегося в w (возможно, $p_s^0 = e$). В силу свойства 4) имеем

$$w = \bigvee_i p_i^{k_i} \cdot \bigvee_j p_j^{l_j} = \bigvee_i \bigvee_j (p_i^{k_i} \cdot p_j^{l_j}).$$

При этом если $i = j$, то $p_i^{k_i} \cdot p_i^{l_i} = p_i^{k_i + l_i}$ (в силу леммы 2). Если же $i \neq j$, то $p_i^{k_i} \cdot p_j^{l_j} = p_i^{k_i} \vee p_j^{l_j}$ (в силу свойства 8)).

Следовательно,

$$w = \left(\bigvee_i p_i^{k_i+l_i} \right) \vee x_1 \vee x_2 \vee \dots,$$

где каждый x_s равен либо $p_i^{k_i}$, либо $p_j^{k_j}$, поэтому $x_s \leq \bigvee_i p_i^{k_i+l_i}$. Таким образом, $w = \bigvee_i p_i^{m_i}$.

Из доказанной леммы и свойства 8) непосредственно вытекает

СЛЕДСТВИЕ 2. Слово $w(p_1, p_2, \dots)$ представимо в виде

$$w = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}.$$

СЛЕДСТВИЕ 3. Группоид B , порожденный атомами $p_1, p_2, \dots$, является коммутативной полугруппой.

ДОКАЗАТЕЛЬСТВО. В самом деле, пусть $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, $b = p_1^{l_1} p_2^{l_2} \dots p_n^{l_n}$, $c = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$. Тогда, воспользовавшись свойствами 4), 8), 9) и леммой 2, получим

$$\begin{aligned} ab &= \left(\bigvee_i p_i^{k_i} \right) \left(\bigvee_j p_j^{l_j} \right) = \bigvee_{i,j} p_i^{k_i} p_j^{l_j} = \bigvee_{j,i} p_j^{l_j} p_i^{k_i} = ba, \\ a(bc) &= \left(\bigvee_i p_i^{k_i} \right) \left(\left(\bigvee_j p_j^{l_j} \right) \left(\bigvee_r p_r^{m_r} \right) \right) = \bigvee_{i,j,r} p_i^{k_i} (p_j^{l_j} p_r^{m_r}) = \bigvee_{i,j,r} (p_i^{k_i} p_j^{l_j}) p_r^{m_r} = (ab)c. \end{aligned}$$

Будем считать, что для множества элементов положительного конуса P выполняется условие минимальности.

ТЕОРЕМА. Любой элемент a из положительного конуса P ($a \neq e$) риссова естественно упорядоченного группоида A , удовлетворяющего условию минимальности, представим в виде произведения атомов, притом однозначно (с точностью до порядка сомножителей).

ДОКАЗАТЕЛЬСТВО. В самом деле, пусть $a > e$ и a не является атомом. Рассмотрим подмножество $M_1 = \{x \in P \mid x \leq a\}$. В силу условия минимальности у множества $M_1 \setminus \{e\}$ найдется минимальный элемент – атом p_1 . Так как $a > p_1$ и группоид A естественно упорядочен, то найдется элемент $a_1 = p_1 \setminus a > p_1 \setminus p_1 = e$.

Рассмотрим подмножество $M_2 = \{x \in P \mid x \leq a_1\}$. У него найдется атом p_2 , следовательно, существует элемент $a_2 = p_2 \setminus a_1$. Продолжая процесс, получим цепочку элементов $a > a_1 > a_2 > \dots$, которая в силу условия минимальности оборвется на конечном шаге. Поэтому $a = p_1 p_2 \dots p_k$.

Докажем единственность такого представления.

Пусть $a = p_1 p_2 \dots p_k = q_1 q_2 \dots q_r$, тогда $p_1 \leq q_1 q_2 \dots q_r$. В силу предложения либо $p_1 \leq q_1$, либо $p_1 \leq q_2 \dots q_r$. Отсюда следует, что, проведя перенумерацию (если это необходимо), мы можем считать, что $p_1 \leq q_1$. Но из того, что q_1 – атом, следует $p_1 = q_1$. Поэтому $p_2 p_3 \dots p_k = q_2 q_3 \dots q_r$. Продолжая рассуждения, получим $p_2 = q_2, p_3 = q_3, \dots$, а также $k = r$.

СЛЕДСТВИЕ 4. Любой элемент $a \in P$ ($a > e$) однозначно представим в виде $a = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, где $p_1, p_2, \dots, p_n$ – различные атомы.

Утверждение непосредственно вытекает из доказанной теоремы и следствия 2.

Заметим, что отказ от риссовости порядка даже при сохранении условий направленности и естественной упорядоченности приводит к нарушению однозначности разложения на простые множители, о чем свидетельствуют примеры 1 и 2.

СЛЕДСТВИЕ 5. Положительный конус P риссова естественно упорядоченного группоида A является решеткой.

ДОКАЗАТЕЛЬСТВО. В самом деле, P является $\vee$ -полурешеткой в силу следствия 3 и леммы 3. Нетрудно видеть, что для любых $a, b \in P$ существует $a \wedge b$. В самом деле, пусть $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, $b = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$, тогда $a \wedge b = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, где $m_i = \min(k_i, l_i)$.

ЛЕММА 4. Любой элемент a из риссова естественно упорядоченного группоида A представим в виде левого (правого) частного $a = q \backslash b$ ($a = b / q$), где $q, b \in P$.

ДОКАЗАТЕЛЬСТВО. Действительно, если a – произвольный элемент из A , $b \geq e$, а и $b/a = q$, то $q = b/a \geq a/a = e$. Но $b = qa$ или $a = q \backslash b$.

СЛЕДСТВИЕ 6. Любой риссов естественно упорядоченный группоид с условием минимальности для положительного конуса P является решеточно упорядоченным.

ДОКАЗАТЕЛЬСТВО. Пусть a и b – произвольные элементы из A . В силу направленности порядка существует $c \leq a, b$, тогда $c \backslash a, c \backslash b \in P$, и в силу следствия 5 существует $d = (c \backslash a) \wedge (c \backslash b)$, откуда в силу свойства 5) $cd = a \wedge b$. Аналогично, существует $q = (c \backslash a) \vee (c \backslash b)$ и $cq = a \vee b$.

СЛЕДСТВИЕ 7. Всякая риссова естественно упорядоченная квазигруппа является решеточно упорядоченной и потому свободной абелевой группой.

Утверждение непосредственно вытекает из следствия 6 и основного результата статьи [6].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Биркгоф Г. Теория решеток. М.: Наука, 1984.
- [2] Фукс Л. Частично упорядоченные алгебраические системы. М.: Мир, 1965.
- [3] Evans T. Lattice-ordered loops and quasigroups // J. Algebra. 1970. V. 16. № 2. P. 218–226.
- [4] Склифос П. И. Об упорядоченных лупах // Алгебра и логика. 1970. Т. 9. № 6. С. 714–730.
- [5] Тестов В. А. К теории решеточно упорядоченных квазигрупп // Ткани и квазигруппы. Калинин, 1981. С. 153–157.
- [6] Bosbach B. Lattice ordered binary systems // Acta Sci. Math. 1988. V. 52. P. 257–289.
- [7] Тестов В. А. Решеточно упорядоченные группоиды // Деп. ВИНТИ. 1993. № 119-93.

Вологодский государственный педагогический университет

Поступило

10.04.95

Исправленный вариант

05.11.96