Imrich Abrhan

О простых идеалах в группоидах и в мультипликативных полугруппах классов вычетов (mod m)

Mathematica Slovaca, Vol. 34 (1984), No. 2, 121--133

Persistent URL: http://dml.cz/dmlcz/136354

Math. Slovaca 34, 1984, No. 2, 121—133

О ПРОСТЫХ ИДЕАЛАХ В ГРУППОИДАХ И В МУЛЬТИПЛИКАТИВНЫХ ПОЛУГРУППАХ КЛАССОВ ВЫЧЕТОВ (mod m)

ИМРИХ АБРГАН (IMRICH ABRHAN)

Dedicated to Academician Štefan Schwarz on the occasion of his 70th birthday

В работе вместо «$G = \langle G; \cdot \rangle$-группоид» мы будем писать «G-группоид».

Обозначим через $[x]$ идеал группоида G, порожденный элементом $x \in G$.

Пусть G-группоид. Будем говорить, что два элемента $x, y \in G$ находятся в отношении $\mathcal{J}$, если $[x]=[y]$. Очевидно, отношение $\mathcal{J}$ на G является отношением эквивалентности. Обозначим через $G/\mathcal{J}$ множество всех $\mathcal{J}$-классов, соответствующих отношению эквивалентности $\mathcal{J}$ на G, а символом $[x]\mathcal{J}$ обозначим $\mathcal{J}$-класс из $G/\mathcal{J}$, содержащий элемент $x \in G$. На множестве $G/\mathcal{J}$ определим отношение $\leqslant$ следующим образом: $[x]\mathcal{J} \leqslant [y]\mathcal{J}$ $(x, y \in G)$ тогда и только тогда, когда $[x] \subseteq [y]$. Очевидно, отношение на $G/\mathcal{J}$-частичная упорядоченность на множестве $G/\mathcal{J}$. Частично упорядоченное множество $G/\mathcal{J}$ относительно $\leqslant$ обозначим $(G/\mathcal{J}, \leqslant)$.

Будем говорить, что группоид G удовлетворяет условия (KR), если всякая убывающая цепь $\mathscr{C}$ в $(G/\mathcal{J}, \leqslant)$ имеет не более чем конечное число различных элементов.

Если A – непустое подмножество группоида G, то обозначим через $\mathcal{P}(A)$ множество всех таких идеалов N в G для которых имеет место $N \subseteq A$. Множество $\mathcal{P}(A)$ с отношением теоретико-множественного включения $\subseteq$ (в качестве отношения частичной упорядоченности) – обозначим через $(\mathcal{P}(A), \subseteq)$.

Будем говорить, что группоид удовлетворяет условию (kr), если всякая убывающая цепь $\mathscr{R}$ в $(\mathcal{P}(G), \subseteq)$ имеет не более чем конечное число различных элементов.

Пусть G-группоид и пусть $b \in G$. Символом $N(b)$ обозначим множество всех таких $x \in G$, что $[b]\mathcal{J} \nleqslant [x]\mathcal{J}$.

В работе [2] доказано следующее утверждение если G-друппоид, $b \in G$ и $N(b) \neq \emptyset$, то $N(b)$-идеал в G.

Идеал N группоида G назовем $\mathcal{J}$-идеалом в G, если существует такое $b \in G$, что $N = N(b)$; (см. [2]).

В первой части этой работы при помощи $\mathcal{J}$-идеалов в группоидах изучаются свойства простых и вполне изолированных идеалов в классе группоидов, удовлетворяющих условию (KR). Для группоида G, удовлетворяющего условия (KR), доказывается:

a) Необходимое и достаточное условие для того, чтобы непустое множество группоида G было простым или вполне изолированным идеалом в G.

b) Всякий полупростой идеал I в G и $I \neq G$ равняется пересечению всех минимальных простых идеалов $N(b)$ группоида G, содержащих I (см. [7], [10]).

c) Если пересечение I простых идеалов группоида G является непустым множеством и $I \neq G$, тогда I полупростой идеал в G (см. [7], [10]).

Во второй части этой работы при помощи $\mathcal{J}$-идеалов полугруппы S_m изучаются свойства вполне изолированных идеалов в S_m (S_m – мултипликативная полугруппа классов вычетов целых чисел по mod m и m любое натуральное число >1). Доказывается:

d) число вполне изолированных идеалов в S_m равняется числу 2^r, где r – число взаимно разных простых чисел в каноническом разложении натурального числа m на простые множители,

e) каждый вполне изолированный идеал в S_m имеет вид $N(\bar{e})$, где $\bar{e}$ – идемпотент в S_m и $\bar{e} \neq \bar{0}$ (символам и $\bar{a}$, $\bar{b}$, ..., $\bar{e}$, ... обозначим элементы в S_m, символом $\bar{0}$ обозначим нуль в S_m и через $\mathcal{J}_m$ обозначим отношение $\mathcal{J}$ в S_m),

f) если G – подгруппа полугруппы S_m, то существует такой положительный делитель d числа m, что $G = [\bar{d}]\mathcal{J}_m$ (подгруппы в S_m – точно 2^r см. [5]),

g) если $d \neq m$ – такой положительный делитель числа m, что $[\bar{d}]\mathcal{J}_m$-подгруппа в S_m, то $[\bar{d}]\mathcal{J}_m$ изоморфна с подгруппой $G_{m,d}$ полугруппы $S_{m,d}$ (символом $G_{m,d}$ обозначим подгруппу в $S_{m,d}$ всех таких элементов $\bar{a} \in S_{m,d}$, для которых a, m/d взаимно просты),

h) локальная теорема Эйлера (см. [8]).

Основным результатом второй части этой работы является утверждение g), т.е. теорема 2.8. При помощи утверждения g) можно к многим утверждениям относительно элементов G_m в S_m доказать в некотором смысле аналогичные утверждения о элементах каждой подгруппы полугруппы S_m см. напр. теорему 2.9.

Лемма 1.1. *Если группоид G удовлетворяет условию (kr), то G удовлетворяет условия (KR).*

Доказательство. Пусть группоид G удовлетворяет условию (kr). Предположим, что существует такая последовательность $\{a_n\}_{n=1}^{\infty}$, что $a_n \in G$ и $[a_n]\mathcal{J} > [a_{n+1}]\mathcal{J}$ для каждого натурального числа n. Из этого мы получаем, что существует такая последовательность $\{N(a_n)\}_{n=1}^{\infty}$, что $N(a_n) \in \mathcal{P}(G)$ и $N(a_n) \supsetneq N(a_{n+1})$ для каждого n. Это противоречит тому, что группоид G удовлетворяет условию (kr).

На примере мы покажем, что следующее утверждение не имеет места.

Если группоид G удовлетворяет условию (KR), то G удовлетворяет условию (kr).

Пример 1.1. Пусть $G_1 = \{a, e\} \cup N$, где N – множество всех натуральных чисел, $a \neq e$ и $\{a, e\} \cap N = \emptyset$. На множестве G_1 определим бинарную операцию следующим образом: $x \cdot x = x$, $x \cdot e = e \cdot x = e$ для всякого $x \in G_1$, $n \cdot a = a \cdot n = n$ для каждого $n \in N$, $m \cdot n = n \cdot m = e$ для каждых двух элементов m, $n \in N$ и $m \neq n$. Тогда G_1-группоид. Далее, для последовательности $\{A_n\}_{n=1}$, где

$$A_n = \bigcap_{k=1}^{n} N(k),$$

имеет место $A_n \in \mathcal{P}(G_1)$, $A_n \supsetneqq A_{n+1}$ для каждого $n \in N$, т.е. G не удовлетворяет условию (kr). Можно легко показать, что каждое непустое подмножество M множества $(G/J, \leqslant)$ имеет по крайней мере один минимальный элемент в M, т.е. группоид G_1 удовлетворяет условию (KR).

Лемма 1.2. *Пусть $N \in \mathcal{P}(G)$, $N \neq G$ и $b \in G \backslash N$. Тогда $N \subseteq N(b)$.*

Доказательство. Пусть x – произвольный элемент из N. Предположим, что $x \in N(b)$. Тогда $[b]\mathcal{J} \leqslant [x]\mathcal{J} \subseteq [x] \subseteq N$. Это противоречит тому, что $b \in G \backslash N$. Значит, $N \subseteq N(b)$.

Идеал Q группоида G назовем простым идеалом в G, если для каждых двух идеалов A, B в G из $AB \subseteq Q$ вытекает $A \subseteq Q$ или $B \subseteq Q$.

Лемма 1.3. *Пусть Q – простой идеал в группоиде G и $Q \neq G$. Пусть $M = \{[a]\mathcal{J} \mid a \in G \backslash Q\}$. Тогда: если $[c]\mathcal{J}$ – минимальный элемент в M, то $Q = N(c)$.*

Доказательство. Пусть $[c]\mathcal{J}$ – минимальный элемент в M. Тогда по лемме 1.2. $Q \subseteq N(c)$. Предположим, что $N(c) \nsubseteq Q$. Тогда существует такой элемент $b \in N(c)$, что $b \notin Q$. Так как согласно предположению Q – простой идеал в G, то $[c][b] \nsubseteq Q$. Пусть $d \in ([c][b] \cap (G \backslash Q))$. Тогда $d \in [c][b] \subseteq [c] \cap [b]$. Значит, $[d]\mathcal{J} \leqslant [c]\mathcal{J}$, $[d]\mathcal{J} \leqslant [b]\mathcal{J}$. Так как $[c]\mathcal{J}$ – минимальный элемент в M и $[d]\mathcal{J} \in M$, то $[d]\mathcal{J} = [c]\mathcal{J}$. Из предыдущих рассуждений вытекает $[c]\mathcal{J} \leqslant [b]\mathcal{J}$. Это значит, что $b \notin N(c)$. Это противоречит тому, что $b \in N(c)$. Значит, $Q = N(c)$.

Идеал P группоида G назовем полупростым идеалом в G, если для каждого идеала A в G из $A^2 \subseteq P$ вытекает $A \subseteq P$.

Лемма 1.4. *Пусть Q – полупростой идеал в G и пусть $Q \neq G$. Пусть $M = \{[a]\mathcal{J} \mid a \in G \backslash Q\}$. Тогда: если $[c]\mathcal{J}$ – минимальный элемент в M, тогда $N(c)$ – простой идеал в G.*

Доказательство. Пусть $[c]\mathcal{J}$ – минимальный элемент в M. Тогда по лемме 1.2. имеет место $Q \subseteq N(c)$. Предположим, что $N(c)$ не является про-

стым идеалом в G. Так как $[c]\mathcal{J}$ – минимальный элемент в M, то для каждого $x \in [c]$ и $x \notin [c]\mathcal{J}$, $x \in Q$. Отсюда следует что $A = Q \cup [c]\mathcal{J}$ – идеал в G. Так как согласно предположению $N(c)$ не является простым идеалом в G, то из предыдущего по теореме 2.5. из [2] мы получаем, что $A' \subseteq Q$. Это противоречит тому, что Q – полупростой идеал в G. Значит $N(c)$ – простой идеал в G.

Теорема 1.1. *Пусть группоид G удовлетворяет условию (KR). Тогда для каждого непустого подмножества Q в G и $Q \neq G$ имеет место: Q – простой идеал в G тогда и только тогда, когда существует такой элемент $c \in G \backslash Q$, что $Q = N(c)$ и $([c]\mathcal{J})^2 \cap [c]\mathcal{J} \neq \emptyset$.*

Доказательство. I. Пусть Q – непустое подмножество в G, $Q \neq G$ и пусть Q – простой идеал в G. Согласно предположению группоид G удовлетворяет условию (KR), тогда в множестве $M = \{[b]\mathcal{J} | b \in G \backslash Q\}$ существует минимальный элемент. Пусть $c \in G \backslash Q$ и $[c]\mathcal{J}$ – минимальный элемент в M. Тогда согласно лемме 1.3 $Q = N(c)$. Из этого по теореме 2.5 из [2] мы получаем, что $([c]\mathcal{J})^2 \cap [c]\mathcal{J} \neq \emptyset$.

II. Пусть $\emptyset \neq Q \subseteq G$, $Q \neq G$ и пусть существует такой элемент $c \in G \backslash Q$, что $Q = N(c)$ и $([c]\mathcal{J})^2 \cap [c]\mathcal{J} \neq \emptyset$. Согласно теореме 2.5 из [2] Q – простой идеал в G.

Будем говорить, что Q – минимальный простой идеал группоида G, содержащий идеал I в G, если не существует такой простой идеал Q' в G, что $I \subseteq Q' \subseteq Q$ $Q' \neq Q$.

Лемма 1.5. *Пусть группоид G удовлетворяет условно (KR). Пусть Q – полупростой идеал в G и пусть $Q \neq G$. Пусть $M = \{[c]\mathcal{J} | c \in G \backslash Q\}$. Тогда: N – минимальный простой идеал в G, содержащий Q, и $N \neq G$ тогда и только тогда, когда $N = N(b)$ и $[b]\mathcal{J}$ – минимальный элемент в M.*

Доказательство. Предположим что группоид G удовлетворяет условию (KR).

I. Пусть N – минимальный простой идеал в G, содержащий Q и $N \neq G$. Тогда по условию (KR) и по теореме 1.1 существует такой элемент b из $G \backslash N$, что $N = N(b)$. Предположим, что $[b]\mathcal{J}$ не является минимальным элементом в $M(G \backslash Q \subseteq G \backslash N)$. Тогда по условию (KR) существует такой минимальный элемент $[d]\mathcal{J}$ из M, что $[d]\mathcal{J} < [b]\mathcal{J}$. Из этого мы заключаем, что $Q \subseteq N(d) \subseteqq N(b)$. По условию (KR) и лемме 1.4 мы получаем, что $N(d)$ – простой идеал в G. Это противоречит тому, что N – минимальный простой идеал в G, содержащий Q.

II. Пусть $N = N(b)$ и $[b]\mathcal{J}$ – минимальный элемент в M. Согласно лемме 1.2, условию (KR) и теореме 1.4 имеет место: $Q \subseteq N(b)$ и $N(b)$ – простой идеал в G. Предположим, что существует такой идеал Q' в G, что $Q \subseteq Q' \subseteqq N(b)$. Из этого по условию (KR) и теореме 1.1 существует такой элемент c из G, что $Q' = N(c)$. Из предыдущего следует, что $Q \subseteq N(c) \subseteq$

$N(b)$. Тогда $[c]\mathcal{J} < [b]\mathcal{J}$. Это противоречит тому, что $[b]\mathcal{J}$ – минимальный элемент в M.

Теорема 1.2. *Пусть группоид G удовлетворяет условию (KR). Тогда:*

a) Всякий полупростой идеал I в G и $I \neq G$ равняется пересечению всех минимальных простых идеалов $N(b)$ группоида G, содержащих I.

b) Если пересечение I простых идеалов группоида G является не-пустым множеством и $I \neq G$, тогда I полупростой идеал в G.

Доказательство. a) Пусть I – полупростой идеал в G и $G \neq I$. Пусть $M = \{[a]\mathcal{J} | a \in G \backslash I\}$. Так как группоид G удовлетворяет условию (KR), то множество всех минимальных элементов в M является непустым. Пусть B – множество таких элементов из G, что $[b]\mathcal{J}$ – минимальный элемент в M для каждого $b \in B$ и для каждого минимального элемента $[c]\mathcal{J}$ из M существует такой один и только один элемент b из B, что $[b]\mathcal{J} = [c]\mathcal{J}$. Тогда по лемме 1.2 имеет место $I \subseteq \cap\{N(b) | b \in B\}$. Предположим, что существует такой элемент d из $\cap\{N(b) | b \in B\}$, что $d \notin I$. Тогда согласно условию (KR) существует такое b из B, что $[b_0]\mathcal{J} \leqslant [d]\mathcal{J}$. Значит, $\cap\{N(b) | b \in B\} \subseteq N(b_0) \subseteq N(d)$. Отсюда $d \notin \cap\{N(b) | b \in B\}$. Это противоречит тому, что $d \in \cap\{N(b) | b \in B\}$. Из передыдущих рассуждений вытекает $I = \cap\{N(b) | b \in B\}$. Из этого, по лемме 1.5. мы получаем утверждение a).

b) Очевидно имеет место утверждение: если I – пересечение простых идеалов в G и $I \neq G$, то I – полупростой идеал в G.

Пример 1.1. Пусть $G = \{x \in R | 0 \leqslant x \leqslant 1\}$, где R обозначает множество всех действительных чисел. На множестве G определим бинарную операцию следующим образом: для каждых двух x, $y \in G$ положим $x \cdot y = \min\{x, y\}$. Тогда $\boldsymbol{G} = \langle G, \cdot \rangle$ – коммутативная полугруппа. Пусть $A = \{x \in R | 0 \leqslant x \leqslant \frac{1}{3}\}$. Тогда:

a) A – простой идеал в G и $A \neq N(c)$ дла каждого $c \in G$,

b) $\{0\}$ – пересечение простых идеалов в G и $\{0\}$ не равняется пересечению минимальных простых идеалов $N(b)$ $(b \in G \backslash \{0\})$ в G, содержащих $\{0\}$,

c) A – полупростой идеал в G и не равняется пересечению минимальных простых идеалов $N(b)$ в G, содержащих A.

Ш. Шварц в работе [7] доказал (в общем случае см. [10]) следующее утверждение:

d) всякий изолированный идеал (идеал P полугруппы S называется изолированным, если для любого $a \in S$ из $a^2 \in P$ следует, что $a \in P$) коммутативной конечной полугруппы S является пересечением вполне изолированных идеалов в S (идеал полугруппы S называется вполне изолированным, если $S \backslash P$-полугруппы S).

Известно следующее утверждение:

Если G – коммутативная полугруппа, тогда для каждого идеала N в G имеет место:

i) N – *простой идеал в* G *тогда и только тогда, когда* N – *вполне изолированный идеал в* G,

ii) N – *полупростой идеал в* G *тогда и только тогда, когда* N – *изолированный идеал в* G.

Из предыдущего следует, что теорема 1.2 обобщает утверждение d) из [7].

Следствие 1.1. *Пусть* G – *коммутатывная полугруппа и удовлетворяет условию* (KR). *Тогда для каждого непустого подмножества* P *в* G *и* $P \neq G$ *имеет место:* P – *вполне изолированный идеал тогда и только тогда, когда существует такой элемент* $u \in G \backslash P$, *что* $P = N(u)$ *и* $([u]\mathcal{J})^2 \cap [u]\mathcal{J} \neq \emptyset$.

Доказательство: следствия 1.1 вытекает из утверждения i) и теоремы 1.1.

Следующие утверждения очевидны:

a) *Каждый вполне изолированный идеал группоида* G *является простым идеалом в* G.

b) *Каждый изолированный идеал группоида* G *является полупростым идеалом в* G.

На примере покажем, что следующие утверждения не имеют места:

a) Если G – коммутативный группоид и P – простой идеал в G, то P – вполне изолированный идеал в G.

b) Если G – коммутативный группоид и P – полупростой идеал в G, то P изолированный.

Пример 1.2. Пусть $G_2 = \{0, a, b, c\}$ и бинарная операция на G_2 определена таблицей:

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	0	b	c
b	0	b	a	0
c	0	c	0	c

Тогда G_2 – коммутативный группоид и имеют место следующие утверждения: a) $N(c)$ – простой идеал в G_2 и $N(c)$ не является вполне изолированым v G_2.

b) $N(c)$ – полупростой в G_2 и $N(c)$ не является изолированным в G_2.

Теорема 1.3. *Пусть группоид* G *удовлетворяет условию* (KR). *Тогда для каждого непустого подмножества* P *в* G *и* $P \neq G$ *имеет место:* P – *вполне изолированный идеал в* G *тогда и только тогда, когда существует такой элемент* $u \in G \backslash P$, *что* $P = N(u)$ *и* $G \backslash P$ – *подгруппоид в* G.

Доказательство: I. Пусть P – вполне изолированный идеал в G. Так как G удовлетворяет условию (KR), то по теореме 1.1 существует такой элемент $u \in G \backslash P$, что $P = N(u)$. Пусть a, b из $G \backslash P$. Предположим, что $ab \in P$. Так как

P – вполне изолированный идеал в G, то $a \in P$ или $b \in P$. Это противоречит тому, что $a, b \in G\backslash P$. Значит, $ab \in G\backslash P$.

II. Пусть P – непустое подмножество в G и $P \neq G$. Пусть существует такой элемент $u \in P\backslash G$, что $P = N(u)$ и пусть $G\backslash P$ – подгруппоид в G. Согласно предположению $P \neq \emptyset$ следовательно P – идеал в G. Пусть $a, b \in G$. Предположим, что $ab \in P$ и $a \notin P$, $b \notin P$. Так как $G\backslash P$ – подгруппоид в G, то $ab \in G\backslash P$. Это значит, что P вполне изолированный идеал в G.

Теорема 1.4. *Пусть группоид G удовлетворяет условию (KR). Пусть P – вполне изолированный идеал в G и $P \neq G$. Тогда:*

(a) *существует такой элемент $u \in G\backslash P$, что $P = N(u)$,*

(b) *$G\backslash P$ – подгруппоид в G,*

(c) *$[u]\mathcal{J}$ – минимальный идеал в $G\backslash P$.*

Доказательство. a) Утверждения (a), (b) вытекают из теоремы 1.3.

b) Пусть P – вполне изолированный идеал в G и $P \neq G$. Тогда согласно (a) существует такой элемент $u \in G\backslash P$, что $P = N(u)$ и согласно (b) $G\backslash P$ – модгруппоид в G. Пусть s – произвольный элемент из $G\backslash P$ и a – произвольный элемент из $[u]\mathcal{J}$. Тогда $[sa] \subseteq [a] = [u]$, т.е., $[su]\mathcal{J} \leqslant [u]\mathcal{J}$. Так как s, $a \in G\backslash P$, то $sa \in G\backslash P = G\backslash N(u)$. Из этого вытекает, что $[u]\mathcal{J} \leqslant [sa]\mathcal{J}$. Значит, $sa \in [u]\mathcal{J}$. Аналогично можно показать, что для каждого $s \in G\backslash P$ и каждого $a \in [u]\mathcal{J}$ имеет место $as \in [u]\mathcal{J}$. Это означает, что $[u]\mathcal{J}$ – идеал в $G\backslash P$. Предположим, что $[u]\mathcal{J}$ не является минимальным идеалом в $G\backslash P$. Отсюда следует, существует такой идеал L в $G\backslash P$, что $L \subsetneqq [u]\mathcal{J}$. Пусть s – произвольный элемент из G и пусть a – произвольный элемент из $N(u) \cup L$. Тогда $s \in N(u)$ или $s \in G\backslash N(u)$. Если $s \in N(u)$ то $sa \in N(u) \cup L (n(u) \in \mathcal{P}(G))$. Если $s \in G\backslash N(u) = G\backslash P$, то согласно предположению (L-идеал в $G\backslash P$) мы получаем, что $sa \in N(u) \cup L$. Аналогично можно показать, что для любого $a \in N(u) \cup L$ а для любого $s \in G$ имеет место $as \in N(u) \cup L$. Следовательно $N(u) \cup L$-идеал в G. Пусть x – любой элемент из L и y – любой элемент из $[u]\mathcal{J}\backslash L$. Тогда $[x] \subseteq N(u) \cup L$ и $y \notin N(u) \cup L$. Это означает, что $[x] \neq [y]$. Однако последнее противоречит тому, что $x, y \in [u]\mathcal{J}$. Из предыдущих рассуждений вытекает, что $[u]\mathcal{J}$ – минимальный идеал в $G\backslash P$.

2.

Под «числом» (поскольку не будет сказано по-другому) мы будем в дальнейшем понимать «целое число». Если число a делитель числа b, то мы будем записывать в виде $a|b$. Если же a не является делителем b, то мы будем писать $a \nmid b$. Наибольший общий делитель чисел a, b мы будем обозначать (a, b). Пусть в дальнейшем

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

– каноническое разложение натурального числа $m>1$ на простые множителя, где $p_1, p_2, \ldots, p_k$ – попарно различные простые числа $\alpha_1, \alpha_2, \ldots, \alpha_r$ – натуральные числа. Через S_m обозначим мультипликативную полугруппу классов вычетов целых чисел по модулю m и знаком $\bar{a}$ обозначим класс вычетов целых чисел по модулю m, который содержит число a. Через G_m обозначим множество всех таких классов $\bar{a} \in S_m$, что $(a, m)=1$. В теории чисел доказывается, что G_m является группой относительно мултипликативной операции в S_m и G_m имеет $\varphi(m)$ разных элементов, где φ — Эйлерова функция.

Знаком $[\bar{a}]$ обозначим идеал в S_m, порожденным элементом $\bar{a} \in S_m$.

Теорема 2.1. *$S_m \setminus G_m$ – максимальный идеал в S_m и для всякого идеала N в S_m и $N \neq S_m$ имеет место $N \subseteq S_m \setminus G_m$.*

Доказательство. а) Пусть $\bar{s} \in S_m$, $\bar{b} \in S_m \setminus G_m$. Тогда $(sb, m)=d>1$. Из этого вытекает, что для каждого $\bar{b} \in S_m \setminus G_m$ имеет место $\bar{s}\bar{b} \in S_m \setminus G_m$. Пусть $\bar{a}$ любой элемент из G_m. Тогда (см. напр. [3]) уравнение $\bar{a}\bar{x}=\bar{b}$ имеет одно и только одно решение для каждого $\bar{b} \in S_m$. Значит, для всякого $\bar{a} \in G_m$ имеет место $S_m\bar{a}=S_m$. Из передшествующих рассуждений вытекает, что $G_m=[\bar{1}]\mathcal{J}_m$ а $[\bar{1}]\mathcal{J}_m$ – наибольший элемент в $S_m/\mathcal{J}_m$. Из этого согласно теореме 2 и примечанию 4 из [1] мы получаем утверждение теоремы 2.1.

Лемма 2.1. *Для каждых двух элементов $\bar{a}, \bar{b} \in S_m$ имеет место: $[\bar{a}]\mathcal{J}_m \leqslant [\bar{b}]\mathcal{J}_m$ тогда и только тогда, когда $(b, m)|(a, m)$.*

Доказательство. Пусть $\bar{a}, \bar{b} \in S_m$.

I. Пусть $[\bar{a}]\mathcal{J}_m \leqslant [\bar{b}]\mathcal{J}_m$, т.е., $[\bar{a}] \subseteq [\bar{b}]$. Тогда существует такой элемент $\bar{v} \in S_m$, что $\bar{a}=\bar{b}\bar{v}$, т.е. $a \equiv bv \pmod m$. Отсюда $(a, m)=(bv, m)$. Значит, $(b, m)|(a, m)$.

II. Пусть $(b, m)|(a, m)$. Положим $d=(b, m)$. Тогда

$$\left(\frac{b}{d}, \frac{m}{d}\right)=1 \quad \text{и} \quad d|a.$$

Если $d=m$, то $[\bar{b}]\mathcal{J}_m=[\bar{a}]\mathcal{J}_m=[\bar{m}]\mathcal{J}_m$. Если $d<m$, о $G_{m,d}$ группа и

$$\left(\frac{\hat{b}}{d}\right) \in G_{m,d}$$

(через $\hat{a}$ обозначим класс вычетов по модулю m/d, содержащий число a). Это значит, что для $(\hat{b}/d)$ из $G_{m,d}$ существует обратный класс $(\hat{b}/d)^{-1}$. Тогда

$$\left(\frac{\hat{b}}{d}\right)\left(\left(\frac{\hat{b}}{d}\right)^{-1}\left(\frac{\hat{a}}{d}\right)\right)=\left(\frac{\hat{a}}{d}\right).$$

Положим

$$\hat{v}=\left(\frac{\hat{b}}{d}\right)^{-1}\left(\frac{\hat{a}}{d}\right).$$

Тогда

$$\left(\frac{\hat{b}}{d}\right)\hat{v}=\left(\frac{\hat{a}}{d}\right),\quad \text{т.е.}\quad \frac{b}{d}v\equiv\frac{a}{d}\left(\operatorname{mod}\frac{m}{d}\right),$$

отсюда $bv\equiv a \pmod m$, т.е. $\bar{b}\bar{v}=\bar{a}$. Значит, $[\bar{a}]\mathcal{J}_m\leqslant[\bar{b}]\mathcal{J}_m$.

Теорема 2.2. *Для каждых двух элементов $\bar{a}$, $\bar{b}\in S_m$ имеет место: $\bar{a}\mathcal{J}_m\bar{b}$ тогда и только тогда, когда $(a, m)=(b, m)$.*

Доказательство. Пусть $\bar{a}, \bar{b}\in S_m$. Тогда $\bar{a}\mathcal{J}_m\bar{b}$ тогда и только тогда, когда $[\bar{a}]\subseteq[\bar{b}]$ и $[\bar{b})\subseteq[\bar{a}]$, т.е. $[\bar{a}]\mathcal{J}_m\leqslant[\bar{b}]\mathcal{J}_m$ и $[\bar{b}]\mathcal{J}_m\leqslant[\bar{a}]\mathcal{J}_m$. Согласно лемме 2.1 $[\bar{a}]\mathcal{J}_m\leqslant[\bar{b}]\mathcal{J}_m$ и $[\bar{b}]\mathcal{J}_m\leqslant[\bar{a}]\mathcal{J}_m$ тогда и только тогда, когда $(b, m)|(a, m)$ и $(a, m)|(b, m)$, т.е. $(a, m)=(b, m)$.

Теорема 2.3. а) *Для каждого элемента $\bar{a}$ из S_m имеет место: $[\bar{a}]\mathcal{J}_m=[\bar{d}]\mathcal{J}_m=G_m\bar{d}$, где $d=(a, m)$.*

b) $|S_m/\mathcal{J}_m|=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$.

Через $|A|$ обозначим мощность множества A.

Доказательство. а) Пусть $[\bar{a}]\mathcal{J}_m$ любой элемент из $S_m/\mathcal{J}_m$. Если $\bar{a}\in G_m$, то очевидно, что $[\bar{a}]\mathcal{J}_m=[\bar{1}]\mathcal{J}_m=G_m\bar{1}$. Предположим, что $\bar{a}\notin G_m$. Тогда $[\bar{a}]\mathcal{J}_m\subseteq[\bar{a}]=[(S_m\setminus G_m)\cup G_m]\bar{a}=(S_m\setminus G_m)\bar{a}\cup G_m\bar{a}$. Так как для всякого $\bar{s}\in S_m\setminus G_m$ имеет место $\bar{s}\bar{a}\notin[\bar{a}]\mathcal{J}_m$, то $[\bar{a}]\mathcal{J}_m\subseteq G_m\bar{a}$. Очевидно, что $G_m\bar{a}\subseteq[\bar{a}]\mathcal{J}_m$. Из этого вытекает, что $G_m\bar{a}=[\bar{a}]\mathcal{J}_m$. Положим $d=(a, m)$. Тогда $[\bar{a}]\mathcal{J}_m=[\bar{d}]\mathcal{J}_m=G_m\bar{d}$.

b) Очевидно, что число всех взаимно различных положительных делителей числа $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ равняется числу $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$. Отсюда согласно теореме 2.2 и утверждению а) теоремы 2.3 мы получаем утверждение b) теоремы 2.3.

Обозначим знаком $D(m)$ множество всех взаимно различных положительных делителей числа m.

Теорема 2.4. *Если*

$$d\in D(m),\quad \text{то}\quad |[\bar{d}]\mathcal{J}_m|=\varphi\left(\frac{m}{d}\right).$$

Доказательство. Пусть φ – подмножество множества $[\hat{1}]\mathcal{J}_{m/d}\times S_m$ определено следующим образом: для каждого $(\hat{x}, \bar{y})\in[\hat{1}]\mathcal{J}_m\times S_m$ имеет место: $(\hat{x}, \bar{y})\in\psi$ тогда и только тогда, когда $\bar{y}=\bar{x}\bar{d}$. Пусть $\hat{x}$ – любой элемент из $[\hat{1}]\mathcal{J}_{m,d}$ и пусть x_1 – произвольное целое число из $\hat{x}$. Тогда $x_1\equiv x \pmod{(m/d)}$ и, следовательно, $x_1d\equiv xd \pmod m$, т.е. $\bar{x}_1\bar{d}=\bar{x}\bar{d}$. Это значит, что ψ – отображение множества $[\hat{1}]\mathcal{J}_{m/d}$ в S_m. Пусть $\hat{x}$ – любой элемент из $[\hat{1}]\mathcal{J}_{m/d}$, т.е. $(x, m/d)=1$. Тогда $(xd, m)=(d, m)=d$. По теореме 2.2 мы получаем, что $\bar{x}\bar{d}\in[\bar{x}\bar{d}]\mathcal{J}_m=[\bar{d}]\mathcal{J}_m$.

Пусть $\bar{u}$ – любой элемент из $[\bar{d}]\mathcal{J}_m$. Тогда

$$(u, m)=(d, m)=d,\quad \text{т.е.}\quad \left(\frac{u}{d};\ \frac{m}{d}\right)=1.$$

Отсюда вытекает

$$\psi\left(\frac{\hat{u}}{d}\right) = \overline{\frac{u}{d}\, d} = \bar{u}.$$

Из этого мы заключаем, что ψ – отображение множества $[\hat{1}]\mathcal{J}_{m,d}$ на $[\bar{d}]\mathcal{J}_m$.

Пусть $\hat{x}_1, \hat{x}_2 \in [\hat{1}]\mathcal{J}_{m,d}$. Предположим, что $\psi(\hat{x}_1) = \psi(\hat{x}_2)$, т.е. $\overline{x_1 d} = \overline{x_2 d}$ т.е. $x_1 d \equiv x_2 d \pmod{m}$. Тогда

$$x_1 = x_2 \left(\operatorname{mod} \frac{m}{d}\right), \quad \text{т.е.} \quad \hat{x}_1 = \hat{x}_2.$$

Из предыдущих рассуждений вытекает, что отображение ψ: $[\hat{1}]\mathcal{J}_{m,d} \to S_m$ взаимно однозначное отображение множества $[\hat{1}]\mathcal{J}_{m,d}$ на $[\bar{d}]\mathcal{J}_m$. Следовательно

$$|[\bar{d}]\mathcal{J}_m| = \varphi\left(\frac{m}{d}\right).$$

Следствие 2.1

$$\sum_{d \in D(m)} \varphi(d) = m.$$

Доказательство. Пусть $D(m) = \{d_0, d_1, \ldots, d_p\}$. Тогда

$$D(m) = \left\{\frac{m}{d_0}, \frac{m}{d_1}, \ldots, \frac{m}{d_p}\right\}.$$

Так как $S_m/\mathcal{J}_m$ – отношение эквивалентности на множестве S_m и $|S_m| = m$, силу теоремы 2.4 мы получаем, что

$$\sum_{d \in D(m)} \varphi(d) = \sum_{i=0}^{p} \varphi\left(\frac{m}{d_i}\right) = m.$$

Теорема 2.5. *Для всякого подмножества P в S_m, $P \neq \emptyset$ и $P \neq S_m$ имеет место: P – вполне изолированный идеал в S_m тогда и только тогда, когда существует такой элемент $d \in D(m)$, что $P = N(\bar{d})$, $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, где для всякого $i \in \{1, 2, \ldots, r\}$, $k_i = 0$ или $k_i = \alpha_i$ и по крайней мере для одного $i \in \{1, 2, \ldots, r\}$, $k_i = 0$.*

Доказательство. I. Пусть P – вполне изолированный идеал в S_m и $P \neq S_m$. Так как S_m – конечная коммутативная полугруппа, то S_m удовлетворяет условию (KR). Тогда согласно теореме 1.4. существует такой элемент $\bar{a} \in S_m$, что $P = N(\bar{a})$, $S_m \backslash P$ – подполугруппа в S_m и $[\bar{a}]\mathcal{J}_m$ – минимальный идеал v $S_m \backslash P$. Положим $d = (a, m)$. Тогда ввиду теоремы 2.3 $[\bar{a}]\mathcal{J}_m = [\bar{d}]\mathcal{J}_m$ и $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, где k_i – целое число и $0 \leqslant k_i \leqslant \alpha_i$ для всякого $i \in \{1, 2, \ldots, r\}$. Так как $[\bar{d}]\mathcal{J}_m$ – минимальный идеал в $S_m \backslash P$, то $\bar{d}^2 \in [\bar{d}]\mathcal{J}_m$. Предложим, что

существует по крайней мере одно такое $i \in \{1, 2, \ldots, r\}$, что $0 < k_i < \alpha_i$. Тогда $k_i + 1 \leqslant \alpha_i$ и $k_i + 1 \leqslant 2k_i$. Из этого для числа $p_i^{k_i+1}$ мы получаем, что $p_i^{k_i+1} | m$, $p_i^{k_i+1} | d^2$ и $p^{k_i+1} \nmid d$. Отсюда следует, что $(d^2, m) \neq (d, m)$, т.е. $[\bar{d}^2]\mathcal{J}_m \cap [\bar{d}]\mathcal{J}_m = \emptyset$. Это противоречит тому, что $\bar{d}^2 \in [\bar{d}]\mathcal{J}_m$. Тогда для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ или $k_i = \alpha_i$. Предположим, что для всякого $i \in \{1, 2, \ldots, r\}$ $k_i \neq 0$. Тогда $k_i = \alpha_i$ для каждого $i \in \{1, 2, \ldots, r\}$. Это значит, что $P = N(\bar{d}) = N(\bar{m}) = N(\bar{0}) = \emptyset$. Это противоречит тому, что $P \neq \emptyset$.

II. Пусть $d \in D(m)$, $P = N(\bar{d})$, $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, где для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = \alpha_i$ или $k_i = 0$ и по крайней мере для одного $i \in \{1, 2, \ldots, r\}$ $k_i = 0$. Тогда очевидно, что $(d^2, m) = (d, m)$ и $[\bar{d}]\mathcal{J}_m \neq [\bar{0}]\mathcal{J}_m$. Это означает, что $\bar{d}^2 \in [\bar{d}]\mathcal{J}_m$, т.е. $([\bar{d}]\mathcal{J}_m)^2 \cap [\bar{d}]\mathcal{J}_m \neq \emptyset$ и $S_m \neq N(\bar{d}) = \emptyset$, откуда согласно следствию 1.1 мы получаем, что $N(\bar{d})$ – вполне изолированный идеал в S_m.

Теорема 2.6. *Пусть $d \in D(m)$ и $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. Тогда:*

(a) *$[\bar{d}]\mathcal{J}_m$ – подгруппа полугруппы S_m тогда и только тогда, когда для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ или $k_i = \alpha_i$.*

(b) *$[\bar{d}]\mathcal{J}_m$ содержит идемпотент тогда и только тогда, когда для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ или $k_i = \alpha_i$.*

Доказательство. Пусть $d \in D(m)$ и $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$.

I. Пусть $[\bar{d}]\mathcal{J}_m$ – подгруппа полугруппы S_m. Если $d = m$, (т.е. $[\bar{d}]\mathcal{J}_m = \{\bar{0}\}$) то для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = \alpha_i$. Предположим, что $d \neq m$. Тогда $N(\bar{d}) \neq \emptyset$ $([\bar{d}]\mathcal{J}_m)^2 \cap [\bar{d}]\mathcal{J}_m \neq \emptyset$. Отсюда согласно следствию 1.1. мы получаем, что $N(\bar{d})$ – вполне изолированный идеал в S_m. Из этого согласно теореме 2.5 мы получаем, что $k_i = 0$ или $k_i = \alpha_i$.

II. Пусть для всякого $i \in \{1, 2, \ldots, r\}$ $k_i = \alpha_i$ или $k_i = 0$. Если для всякого $i \in \{1, 2, \ldots, r\}$ $k_i = \alpha_i$, то $\bar{d} = \bar{0}$, и следовательно, $[\bar{d}]\mathcal{J}_m$ – подгруппа в S_m. Если по крайней мере для одного $i \in \{1, 2, \ldots, r\}$ $k_i = 0$, то $\bar{d} \neq \bar{0}$. Тогда согласно теореме 2.5 $N(\bar{d})$ – вполне изолированный идеал в S_m. Из этого в силу теоремы 1.4. мы получаем, что $[\bar{d}]\mathcal{J}_m$ – минимальный идеал в $S_m \backslash N(\bar{d})$. Отсюда вытекает, что $[\bar{d}]\mathcal{J}_m$ – подгруппа в S_m.

b) Пусть $[\bar{d}]\mathcal{J}_m$ содержит идемпотент. Тогда $([d]\mathcal{J}_m)^2 \cap [\bar{d}]\mathcal{J}_m \neq \emptyset$. Из этого, согласно следствию 1.1 $N(d)$ – вполне изолированый идеал в S_m. Тогда по теореме 1.4 мы получаем, что $S \backslash N(\bar{d})$ – подполугруппа в S_m и $[\bar{d}]\mathcal{J}_m$ – минимальный идеал в $S \backslash N(\bar{d})$. Это значит, что $[\bar{d}]\mathcal{J}_m$ – подгруппа в S_m, откуда согласно утверждению а) мы заключаем, что для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ или $k_i = \alpha_i$.

Если для каждого $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ или $k_i = \alpha_i$, то согласно утверждению а) мы получаем, что $[\bar{d}]\mathcal{J}_m$ – подгруппа в S_m. Отсюда мы заключаем, что $[\bar{d}]\mathcal{J}_m$ содержит идемпотент.

Теорема 2.7. (a) *Полугруппа S_m содержит точно 2^r идемпотентов и каждый идемпотент можно писать в виде $\bar{e} = \bar{d}\bar{a}$, где $\bar{a}$ подходяще выбранный элемент*

из G_m *и* $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ *и где для каждого* $i \in \{1, 2, \ldots, r\}$ $k_i = 0$ *или* $k_i = \alpha_i$ *(см. [6]).*

(b) *Полугруппа* S_m *содержит точно* 2^r *вполне изолированных идеалов и каждый вполне изолированный идеал* P *в* S_m, $P \neq S_m$ *имеет вид* $N(\bar{e})$, *где* $\bar{e}$ *подходяще выбранный идемпотент из* S_m *и* $\bar{e} \neq \bar{0}$.

Доказательство теоремы 2.7. вытекает из теоремы 2.6 теоремы 2.3 и теоремы 2.5.

Теорема 2.8. *Пусть* $d \in D(m)$, $d \neq m$ *и* $[\bar{d}]\mathcal{J}_m$ *– подгруппа в* S_m. *Тогда* $[\bar{d}]\mathcal{J}_m$ *изоморфна с подгруппой* $G_{m/d}$ *полугруппы* $S_{m\,d}$.

Доказательство. Обозначим через $\bar{e}$ идемпотент подгруппы $[\bar{d}]\mathcal{J}_m$. Согласно теореме 2.7 существует такой элемент $\bar{a} \in G_m$, что $\bar{e} = \bar{d}\bar{a}$. Пусть ψ – подмножество множества $G_{m\,d} \times S_m$ определено следующим образом: Для каждого $(\hat{x}, \bar{y}) \in G_{m\,d} \times S_m$ имеет мето $(\hat{x}, \bar{y}) \in \psi$ тогда и только тогда, когда $\bar{y} = \overline{xda}$. Если $\hat{x}$ – любой элемент на $G_{m\,d}$ и x_1 – произвольное целое число из $\hat{x}$, то $x_1 \equiv x \pmod{m/d}$. Из этого $x_1 d \equiv xd \pmod{m}$. Тогда $x_1 da \equiv xda \pmod{m}$. Это означает, что ψ является отображением множества $G_{m\,d}$ в S_m.

Пусть $\hat{x}$ – любой элемент из $G_{m\,d} = [\hat{1}]\mathcal{J}_m$, т.е. $(x, m/d) = 1$; и так $(xd, m) = d$. Так как а из G_m, то $(a, m) = 1$. Из передыдущего мы получаем, что $(xda, m) = d$. Отсюда следует, что $\overline{xda} \in [\bar{d}]\mathcal{J}_m$. Значит, что $\psi(\hat{x}) = \overline{xda} \in [\bar{d}]\mathcal{J}_m$. Это значит, что ψ – отображение множества $G_{m/d}$ в $[\bar{d}]\mathcal{J}_m$.

Пусть $\hat{x}_1, \hat{x}_2 \in G_{m\,d}$. Предположим, что $\psi(\hat{x}_1) = \psi(\hat{x}_2)$, т.е. $\overline{x_1 da} = \overline{x_2 da}$. Так как $\bar{a} \in G_m$ и G_m – группа, то из передыдущего мы получаем, что $\overline{x_1 d} = \overline{x_2 d}$. Отсюда следует, что $x_1 \equiv x_2 \pmod{m/d}$, т.е. $\hat{x}_1 = \hat{x}_2$. Так как $G_{m\,d}$, $[\bar{d}]\mathcal{J}_m$ – конечные множества и согласно теореме 2.4 $|G_{m\,d}| = |[\bar{d}]\mathcal{J}_m|$, то ψ – взаимно однозначное отображение множества $G_{m/d}$ на $[\bar{d}]\mathcal{J}_m$. Покажем, что отображение ψ: $G_{m\,d} \to [\bar{d}]\mathcal{J}_m$ является гомоморфизмом $G_{m\,d}$ на $[\bar{d}]\mathcal{J}_m$. Пусть $\hat{x}$, $\hat{y}$ – произвольные элементы из $G_{m\,d}$. Тогда

$$\psi(\hat{x}\hat{y}) = \overline{xyda} = \overline{xye} = \overline{xyee} = \overline{xe} \cdot \overline{ye} = \overline{xda} \cdot \overline{yda} = \psi(\hat{x})\psi(\hat{y}).$$

Теорема 2.9. *Пусть* $d \in D(m)$, $d \neq m$. *Пусть* $[\bar{d}]\mathcal{J}_m$ *– подгруппа полугруппы* S_m *и пусть* $\bar{e}$ *– идемпотент группы* $[\bar{d}]\mathcal{J}_m$. *Тогда для каждого* $\bar{a} \in [\bar{d}]\mathcal{J}_m$ *имеет место:*

$$a^{\varphi(m\,d)} \equiv e \pmod{m} \quad \text{(см. [8])}$$

Доказательство. Согласно теореме 2.8. существует изоморфное отображение ψ группы $G_{m\,d}$ на группу $[\bar{d}]\mathcal{J}_m$. Пусть $\bar{a}$ – любой элемент из $[\bar{d}]\mathcal{J}_m$. Тогда существует такой элемент $\hat{b} \in G_{m/d}$, что $\bar{a} = \psi(\hat{b})$. Согласно теореме 5.1

фермата имеет место $b^{\varphi(m/d)} \equiv 1 \pmod{m/d}$, т.е. $\hat{b}^{\varphi(m/d)} = \hat{1}$. Тогда $\psi(\hat{b}^{\varphi(m/d)}) = \psi(\hat{1})$. Значит, $(\psi(\hat{b}))^{\varphi(m/d)} = \bar{e}$, т.е. $a^{\varphi(m/d)} \equiv e \pmod{m}$.

Теорема 2.10. *Пусть выполняются условия теоремы 2.9. Тогда для каждого элемента* $\bar{a} \in [\bar{d}]\mathcal{J}_m$ *имеет мето:* $a^{\lambda(m/d)} \equiv e \pmod{m}$, *где* λ – *обобщенная функция Эйлера.*

Доказательство теоремы 2.10. можно провести аналогичным образом как доказательство 2.9.

ЛИТЕРАТУРА

[1] АБРГАН, И.: О $\mathcal{J}$-подалгебрах в унарных алгебрах, о простых идеалах и $\mathcal{J}$-идеалах в группоидах и полугруппах.

[2] АБРГАН, И.: О $\mathcal{J}$-подалгебрах в унарных алгебрах, о простых полугруппах, Math. Slov. 28, 1978, 61–80.

[3] БУХШТАБ, А. А.: Теория чисел, Гос., ич. – пед. изд., Москва 1960.

[4] CLIFFORD, A. H.—PRESTON, G. B.: The algebraic theory of semigroups. Vol. I. Math. Surveys No. 7, Amer. Soc., Providence, R. I., 1961.

[5] PARIZEK, B.—SCHWARZ, Š.: O multiplikatívnej pologrupe zvyškových tried (mod m). Mat.-Fyz. Čas. 8, 1958, 136–150.

[6] PARIZEK, B.: O rozklade pologrupy zvyškov (mod m) na direktný súčin, Mat.-Fyz. Čas. 10, 1960, 18–20.

[7] ШВАРЦ, Ш.: О некоторой связи Галуа в теории характеров полугрупп, Czechoslovak Math. J., 1954, 296–313.

[8] SCHWARZ, Š.: The role of semigroups in the elementary theory of number, Math. Slov. 31, 1981, 369–395.

[9] KOLIBIAROVÁ, B.: O komutatívnych periodických pologrupách, Mat.-Fyz. Čas. 8, 1958, 127–133.

[10] PETRICH, M.: Introduction to semigroups. Charles E. Merrill Publishing Company, Ohio 1973.

Поступило 21. 11. 1980

Katedra matematiky a deskriptívnej geometrie
Strojníckej fakulty SVŠT
Gottwaldovo nám. 17
880 31 Bratislava