БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ ACADÉMIE BULGARE DES SCIENCES
ИЗВЕСТИЯ НА МАТЕМАТИЧЕСКИЯ ИНСТИТУТ
BULLETIN DE L'INSTITUT DE MATHÉMATIQUES
Том (Tome) IX

О НЕПРИВОДИМЫХ ПОРОЖДАЮЩИХ МНОЖЕСТВАХ КОНЕЧНОГО ПОРЯДКА В ПОЛУГРУППАХ

Станчо Димиев

Изучение неприводимых порождающих подмножеств полугруппы представляет самостоятельный интерес [1]. Всякая конечная полугруппа обладает неприводимыми порождающими подмножествами, однако в случае бесконечной полугруппы это не так.

В этой заметке вводится понятие неприводимого порождающего множества конечного порядка и доказывается, что если полугруппа содержит порождающее множество порядка k, то она обязательно будет содержать неприводимое порождающее множество такого же порядка k.

Порождающие множества конечного порядка встречаются в разных вопросах, например они имеют существенное значение в аддитивной теории чисел.

1. Пусть G полугруппа с единицей e. В дальнейшем будем рассматривать только подмножества X полугруппы G, содержащие единицу e.

Степень подмножества X определяется как обычно: если n натуральное число, X^n означает совокупность всевозможных произведений по n элементов из X. Ввиду $e \in X$, очевидно $X \subseteq X^n$.

Подмножество X полугруппы G называется порождающим множеством конечного порядка k, если $X^k = G$, однако для любого $n < k$ множество X^n является собственным подмножеством G.

Подмножество Y полугруппы G называется неприводимым порождающим множеством конечного порядка k, если оно является порождающим множеством порядка k для G и любое его собственное подмножество либо не является порождающим конечного порядка, либо имеет порядок не меньше чем $k+1$.

Конечно, если Y неприводимое порождающее подмножество конечного порядка k, то оно не обязано быть неприводимым порождающим множеством в обычном смысле.

2. В этом пункте устанавливается некоторое тождество теоретико-множественного характера, связывающего алгебраическую структуру полугруппы с операцией пересечения множеств. Сначала докажем, что имеет место следующая

Лемма. Для любого однозначного отображения $\varphi: S \to G$ множества S в множество G и для любой невозрастающей цепи подмножеств G

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_\iota \supseteq \cdots,\ \iota \in I,$$

с непустым пересечением имеет место равенство

(1) $$\left(\bigcap_{\iota \in I} X_\iota\right)\varphi = \bigcap_{\iota \in I} X_\iota \varphi,$$

где $X_\iota = A_\iota \varphi^{-1}$, $\iota \in I$, I — некоторое множество индексов.

Очевидно, включение $(\bigcap_{\iota \in I} X_\iota)\varphi \subseteq \bigcap_{\iota \in I} X_\iota \varphi$ имеет место. Обратное включение тоже нетрудно доказать. В самом деле, отображение φ индуцирует некоторое разбиение множества S. Если $a \in G$, множество прообразов $(a)\varphi^{-1}$ элемента a является классом указанного разбиения множества S. В таком случае для каждого $\iota \in I$ множество $X_\iota = A_\iota \varphi^{-1}$ будет являться объединением классов разбиения S.

Пусть $a \in \bigcap_{\iota \in I} X_\iota \varphi$; тогда для каждого $\iota \in I$ множество X_ι должно содержать хотя бы один прообраз элемента a. Но множество прообразов a является классом разбиения S и в таком случае, согласно отмеченному выше, оно должно содержаться в каждом X_ι и значит и в пересечении $\bigcap_\iota X_\iota$.

Заметим, что если $Y_0 \supseteq Y_1 \supseteq \cdots \supseteq Y_\iota \supseteq \cdots$, $\iota \in I$, любая цепь подмножеств множества S с непустым пересечением, то будет иметь место только включение $(\bigcap_\iota Y_\iota)\varphi \subseteq \bigcap_\iota Y_\iota \varphi$.

Т е о р е м а. Если $A_0 \supseteq A_1 \supseteq \cdots \supseteq A_\iota \supseteq \cdots$, $\iota \in I$, невозрастающая цепь подмножеств полугруппы G с непустым пересечением (I — некоторое множество индексов), то для любого натурального k

$$\left(\bigcap_{\iota \in I} A_\iota\right)^k = \bigcap_{\iota \in I} A_\iota^k.$$

Доказательство. Нетрудно убедиться в том, что включение

$$\left(\bigcap_\iota A_\iota\right)^k \subseteq \bigcap_\iota A_\iota^k$$

имеет место. Обратное включение докажем сначала для свободных полугрупп, а потом в общем случае.

Предположим, что S свободная полугруппа. Пусть $X_1 \supseteq X_2 \supseteq \cdots \supseteq X_\iota \supseteq \cdots$, $\iota \in I$, невозрастающая цепь подмножеств S с непустым пересечением.

Заметим, что в свободной полугруппе каждый элемент имеет лишь конечное число различных левых делителей.

Пусть $x \in \bigcap_\iota X_\iota^k$ где X_ι^k — k-тая степень множества X_ι. Тогда для каждого $\iota \in I$ имеем

$$x = x_\iota^{(1)} x_\iota^{(2)} \cdots x_\iota^{(k)}, \text{ где } x_\iota^{(i)} \in X_\iota \quad i = 1, 2, \ldots, k.$$

Согласно сделанному замечанию относительно левых делителей элементов S, будет существовать подцепь $\{x_{\iota'}^{(1)}\}$ цепи $\{x_\iota^{(1)}\}$ левых делителей x такой, что $x_{\iota'}^{(1)} = x_0^{(1)}$, $\iota' \in I' \subset I$. Ввиду того, что $\bigcap_{\iota' \in I'} X_{\iota'} = \bigcap_{\iota \in I} X_\iota$, можно утверждать, что $x_0^{(1)} \in \bigcap_{\iota \in I} X_\iota$. Дальше, рассмотрим цепь слов

$$x^{(2)}_{\iota'} x^{(3)}_{\iota'} \cdots x^{(k)}_{\iota'}, \quad \iota' \in I'.$$

Так как для каждого $\iota' \in I'$ слова $x_0^{(1)} x^{(2)}_{\iota'} x^{(3)}_{\iota'} \cdots x^{(k)}_{\iota'}$ совпадают между собой, то же самое можно утверждать о словах $x^{(2)}_{\iota'} x^{(3)}_{\iota'} \cdots x^{(k)}_{\iota'}$. Применяя к цепи $\{x^{(2)}_{\iota'}\}$, $\iota' \in I'$, буквально такие же рассуждения, какие уже применили к цепи $\{x^{(1)}_{\iota}\}$, выберем подцепь $\{x^{2}_{\iota'_{\iota''}}\}$, составленную из одинаковых слов $x^{(2)}_{\iota'_{\iota''}} = x_0^{(2)}$, $\iota'' \in I'' \subset I'$, где $x_0^{(2)} \in \bigcap X_\iota$. Таким образом $x = x_0^{(1)} x_0^{(2)} x^{(3)}_{\iota'_{\iota''}} \cdots x_{\iota'_{\iota''}}$, где $\iota'' \in I''$.

Повторяя эти рассуждения $k-2$ раз, соответственно к последующим членам произведения $x_0^{(1)} x_0^{(2)} x^{(3)}_{\iota'_{\iota''}} \ldots x^{(k)}_{\iota'_{\iota''}}$, в итоге получим

$$x = x_0^{(1)} x_0^{(2)} x_0^{(3)} \ldots x_0^{(k)}, \text{ где } x_0^{(i)} \in \bigcap_{\iota \in I} X_\iota, \quad i = 1, 2, \ldots, k.$$

Значит $x \in (\bigcap\limits_{\iota} X_\iota)^k$ и тем самым доказано, что имеет место обратное включение.

Рассмотрим сейчас общий случай любой полугруппы G. Пусть $\mathfrak{R}$ порождающее множество для G. Занумеруем элементы множества $\mathfrak{R}$, используя некоторое трансфинитное множество индексов A, т. е.

$$\mathfrak{R} = \{g_1, g_2, \ldots, g_a, \ldots\}, \; a \in A,$$

и каждому элементу $g_a \in \mathfrak{R}$ сопоставим символ свободной переменной x_a. Обозначим это отображение следующим образом

$$\varphi : x_a \to g_a \text{ или } (x_a)\varphi = g_a.$$

Если $S_{\mathfrak{R}}$ — свободная полугруппа всевозможных слов в алфавите свободных переменных $\{x_\iota\}$, то отображение φ можно продолжить до гомоморфизма $S_{\mathfrak{R}}$ на G. Так как продолжение φ является гомоморфизмом (его будем обозначать опять через φ), следует, что если $X_1, X_2, \ldots, X_m$ обозначают m подмножества полугруппы S, то будет иметь место

$$(X_1 X_2 \ldots X_m)\varphi = (X_1)\varphi (X_2)\varphi \ldots (X_m)\varphi. \tag{2}$$

Сейчас уже нетрудно доказать утверждение теоремы. Положим $(A_\iota)\varphi^{-1} = X_\iota$, т. е. $A_\iota = (X_\iota)\varphi$. Ввиду того, что φ гомоморфизм (2), будем иметь $A_\iota^k = (X_\iota^k)\varphi$, $\iota \in I$. Тогда согласно доказанной лемме (1)

$$\bigcap_\iota A_\iota^k = \bigcap_\iota (X_\iota^k)\varphi = (\bigcap_\iota X_\iota^k)\varphi.$$

Имея в виду уже доказанное в случае свободной полугруппы и применяя еще раз лемму, получим окончательно

$$\bigcap_\iota A_\iota^k = ((\bigcap_\iota X_\iota)^k)\varphi = (\bigcap_\iota X_\iota \varphi)^k = (\bigcap_\iota A_\iota)^k,$$

что и требовалось доказать.

3. Из доказанной в пункте 2 теоремы с помощью леммы Цорна, очевидно, сразу вытекает, что если в полугруппе G имеется порождающее подмножество конечного порядка k, то обязательно в G будет и непри-

водимое порождающее подмножество такого же порядка. Достаточно рассмотреть порождающие подмножества как частично упорядоченное множество относительно включения $X \subseteq Y$.

Оказывается, что в некоторых случаях можно дать полное описание порождающих подмножеств конечного порядка. Рассмотрим для примера полугруппу U, состоящую из всех натуральных чисел, операцией в которой является нахождение наибольшего общего делителя. Легко убедиться в том, что полугруппа U вовсе не обладает неприводимыми порождающими подмножествами в обычном смысле.

Пусть $\{n^1, n^2, \ldots, n^k\}$ набор, составленный из натуральных чисел, которые взаимно просты в совокупности $(n^1, n^2, \ldots, n^k) = 1$. Занумеруем множество всевозможных наборов взаимно простых в совокупности чисел:

$$\{n_1^1, n_1^2, \ldots, n_1^k\}, \ldots, \{n_\nu^1, n_\nu^2, \ldots, n_\nu^k\}, \ldots,$$

и рассмотрим бесконечную матрицу, элементами которой являются наборы $\{\mu n_\nu^1, \mu n_\nu^2, \ldots, \mu n_\nu^k\}$, т. е.

$$\begin{array}{llll}
\{n_1^1, n_1^2, \ldots, n_1^k\} & \{2n_1^1, 2n_1^2, \ldots, 2n_1^k\} \ldots & \{\mu n_1^1, \mu n_1^2, \ldots, \mu n_1^k\} \ldots \\
\{n_2^1, n_2^2, \ldots, n_2^k\} & \{2n_2^1, 2n_2^2, \ldots, 2n_2^k\} \ldots & \{\mu n_2^1, \mu n_2^2, \ldots, \mu n_2^k\} \ldots \\
\{n_\nu^1, n_\nu^2, \ldots, n_\nu^k\} & \{2n_\nu^1, 2n_\nu^2, \ldots, 2n_\nu^k\} \ldots & \{\mu n_\nu^1, \mu n_\nu^2, \ldots, \mu n_\nu^k\} \ldots
\end{array}$$

Имеет место следующее утверждение: для того, чтобы подмножество X полугруппы U являлось порождающим подмножеством порядка не больше чем k, необходимо и достаточно, чтобы оно совпадало с объединением некоторого множества элементов матрицы A, причем оно должно содержать хотя бы одного элемента из каждого столбца матрицы. Если оно будет содержать ровно по одному элементу из каждого столбца, обязательно оно будет неприводимым порядка k для U.

Докажем, что указанное утверждение является необходимым. Пусть X — порождающее множество порядка k для U и n натуральное число, такое, что $n = ((((n^1, n^2), n^3), \ldots), n^k)$, где $n^1, n^2, \ldots, n^k$ натуральные числа, принадлежащие порождающему множеству k-ого порядка X. Тогда найдутся натуральные числа $d_1, d_2, \ldots, d_i, n_1^k, n_1^{k-1}, \ldots, n_1^{k-i+1}$, такие, что

(3) $$(n_1^k, d_1) = 1, \ (n_1^{k-1}, d_2) = 1, \ldots, (n_1^{k-i+1}, d_i) = 1,$$

и

$$((((n^1, n^2), n^3), \ldots), n^{k-i}) = n \prod_{j=1}^{i} d_j, \quad n^{k-i+1} = n n_1^{k-i+1} \prod_{j=1}^{i-1} d_j,$$

где $i = 1, 2, \ldots, k$. Таким образом

$$n^1 = n d_1 d_2 \ldots d_{k-2} d_{k-1} n_1^1, \quad n_1^1 = 1,$$

$$n^2 = n d_1 d_2 \ldots d_{k-2} n_1^2,$$

$$n^{k-1} = nd_1 n_1^{k-1},$$
$$n^k = nn_1^k.$$

Очевидно $(n_1^1, n_1^2, \ldots, n_1^k) = 1$. Положим $\left(\frac{n^1}{n}, \frac{n^2}{n}, \ldots, \frac{n^k}{n}\right) = d$. Натуральное число d должно быть единицей, потому что в противном случае ввиду (3) окажется, что d будет делителем всех $n_1^1, n_1^2, \ldots, n_1^k$. Набор $\left(\frac{n^1}{n}, \frac{n^2}{n}, \ldots, \frac{n^k}{n}\right)$ имеет свое место в первом столбце матрицы A. Положим

$$d_1 d_2 \ldots d_{k-1} n_1^1 = n_\tau^1,$$
$$d_1 d_2 \ldots d_{k-2} n_1^2 = n_\tau^2,$$
$$d_1 n_1^{(k-1)} = n_\tau^{k-1},$$
$$n_1^k = n_\tau^k.$$

В таком случае $n = ((((nn_\tau^1, nn_\tau^2), nn_\tau^3), \ldots), nn_\tau^k)$.

Достаточность тоже нетрудно доказать.

Условие о неприводимости является очевидным.

ЛИТЕРАТУРА

1. Ляпин Е. С., Полугруппы, Москва, 1960.

Постъпила на 8. I. 1965 г.

ON THE MINIMAL GENERATING SETS OF A FINITE ORDER IN SEMI-GROUPS

Stancho Dimiev

(Summary)

Let G be a semi-group with unity e. We shall examine such subsets of G which contain the unity e. The power of a subset X is defined in the usual manner: X^n will mean the set of all possible products of n elements of X. Minimal generating subset of order k will be called every generating subset of order k, i. e. $X^k = G$, for which every proper subset is either not generating of a finite order, or if it is a generating one it is of an order not lower than $k+1$.

It is proved in the paper that if a semi-group has a generating subset of an order k, it will also have a minimal generating subset of the same order. An analogous assertion about the generating subsets in an ordinary sense is not valid since there exist semi-groups which have generating subsets without having minimal ones.