

**О ПОРОЖДАЮЩИХ МНОЖЕСТВАХ  $l$ -АРНОЙ ГРУППЫ  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . II****А.М. Гальмак***Белорусский государственный университет пищевых и химических технологий, Могилёв***ON SETS OF GENERATORS OF  $l$ -ARY GROUP  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . II****A.M. Gal'mak***Belarusian State University of Food and Chemical Technologies, Mogilev*

В статье продолжается изучение установленной ранее связи между порождающими множествами группы  $A$  и порождающими множествами полиадической группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  с  $l$ -арной операцией  $[ ]_{l, \sigma, k}$ , которая определяется на  $k$ -ой декартовой степени произвольной группы  $A$  для любого целого  $l \geq 2$  и любой подстановки  $\sigma$  из множества  $S_k$  всех подстановок множества  $\{1, 2, \dots, k\}$ .

**Ключевые слова:** группа,  $l$ -арная группа, порождающее множество.

The article goes on with the studies on the described earlier relationship between sets of generators in group  $A$  and sets of generators in polyadic group  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  with  $l$ -ary operation  $[ ]_{l, \sigma, k}$ , that is defined on Cartesian power  $A^k$  of group  $A$  for arbitrary integer  $l \geq 2$  and arbitrary substitution  $\sigma$  from the set  $S_k$  of all substitutions of the set  $\{1, 2, \dots, k\}$ .

**Keywords:** group,  $l$ -ary group, set of generators.

**Введение**

Данная статья, посвящённая изучению порождающих множеств  $l$ -арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , является продолжением статьи [1] и составляет с ней единое целое, что отражено в названиях обеих статей. В связи с этим нумерация разделов в настоящей статье продолжает нумерацию разделов в [1]. Сохраняется преемственность в отношении соглашений, определений и обозначений из [1], все они остаются в силе и в данной статье. В ней ссылки на результаты из работы [1] даются без указания на эту работу. Например, ссылка на теорему 4.1 означает, что имеется в виду теорема 4.1 из раздела 4 в [1].

Отметим, что ранее автором изучались порождающие множества  $l$ -арной полугруппы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . В частности, в [2, следствие 4.5] установлено, что если полугруппа  $A$  с единицей порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $k$  делит  $l-1$ , то для любого  $j \in \{1, 2, \dots, k\}$   $l$ -арная полугруппа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M) \cup \{\epsilon\}$ .

В [1] получен аналогичный результат (теорема 4.1) для  $l$ -арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ : Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $k$  делит  $l-1$ . Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M) \cup \{\epsilon\}$ .

Всю необходимую информацию из теории полиадических групп можно найти в [3], [4].

Основная цель данной статьи – нахождение условий, позволяющих заменить в указанных выше результатах порождающее множество  $U_j(M) \cup \{\epsilon\}$  порождающим множеством  $U_j(M)$ .

**6 Порождающее множество  $U_j(M)$** 

Покажем, что возможна ситуация, при которой элемент  $e$  может быть исключён из порождающих множеств как  $l$ -арной полугруппы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , так и  $l$ -арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ .

**Теорема 6.1.** Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ , существуют элементы

$$u_1, u_2, \dots, u_{r+1}, v_1, v_2, \dots, v_r \in M$$

такие, что

$$u_1 u_2 \dots u_{r+1} = v_1 v_2 \dots v_r = 1. \quad (6.1)$$

Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $U_j(M)$ .

**Доказательство.** По теореме 4.1 для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M) \cup \{\epsilon\}$ . Так как единица группы не принадлежит множеству  $M$ , то  $\epsilon \notin U_j(M)$ .

Зафиксируем  $j \in \{1, 2, \dots, k\}$ . По лемме 4.1, если

$$\mathbf{a}_i = (\underbrace{1, \dots, 1}_{j-1}, a_i, \underbrace{1, \dots, 1}_{k-j}) \in A^k, i = 1, 2, \dots, l,$$

$$[\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_l]_{l, \sigma, k} = (b_1, \dots, b_k),$$

то

$$b_j = a_j a_{k+1} a_{2k+1} \dots a_{rk+1}, \quad (6.2)$$

$$b_s = a_s a_{m_s+1} a_{k+m_s+1} a_{2k+m_s+1} \dots a_{(r-1)k+m_s+1}$$

для любого  $s \in \{1, \dots, j-1, j+1, \dots, k\}$ , где  $m_s$  однозначно определяется из условия  $\sigma^{m_s}(s) = j$ .

Так как для указанных  $s$  имеем  $a_s = 1$ , то

$$b_s = a_{m_s+1} a_{k+m_s+1} a_{2k+m_s+1} \dots a_{(r-1)k+m_s+1}. \quad (6.3)$$

Если положить

$$a_1 = u_1, a_{k+1} = u_2, a_{2k+1} = u_3, \dots, a_{rk+1} = u_{r+1},$$

$a_{m_s+1} = v_1, a_{k+m_s+1} = v_2, \dots, a_{(r-1)k+m_s+1} = v_r$   
для указанных выше  $s$ , то из (6.2) и (6.3) с учётом (6.1) следует

$$b_1 = \dots = b_k = 1,$$

то есть

$$[\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_l]_{l, \sigma, k} = \mathbf{e},$$

где  $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_l \in \mathbf{U}_j(M)$ . Следовательно, элемент  $\mathbf{e}$  может быть исключён из порождающего множества  $\mathbf{U}_j(M) \cup \{\mathbf{e}\}$   $l$ -арной группы  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ .  $\square$

**Замечание 6.1.** Выпишем в явном виде элементы  $b_1, \dots, b_k$ , определяемые равенствами (6.2) и (6.3) для  $j = 1$  в случае  $\sigma = (1, 2, \dots, k)$ . Так как в этом случае из условия  $\sigma^{m_s}(s) = 1$  следует

$$m_2 = k - 1, m_3 = k - 2, \dots, m_{k-1} = 2, m_k = 1,$$

то

$$\begin{aligned} b_1 &= a_1 a_{k+1} a_{2k+1} \dots a_{(r-1)k+1} a_{rk+1}, \\ b_2 &= a_k a_{2k} a_{3k} \dots a_{(r-1)k} a_{rk}, \\ b_3 &= a_{k-1} a_{2k-1} a_{3k-1} \dots a_{(r-1)k-1} a_{rk-1}, \\ &\dots \\ b_{k-1} &= a_3 a_{k+3} a_{2k+3} \dots a_{(r-2)k+3} a_{(r-1)k+3}, \\ b_k &= a_2 a_{k+2} a_{2k+2} \dots a_{(r-2)k+2} a_{(r-1)k+2}. \end{aligned}$$

Доказательство следующей теоремы почти дословно повторяет доказательство теоремы 6.1. Только вместо теоремы 4.1 используется предложение 4.1.

**Теорема 6.2.** Пусть полугруппа  $A$  порождается множеством  $M$ , не содержащим её единицу,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ , существуют элементы

$$u_1, u_2, \dots, u_{r+1}, v_1, v_2, \dots, v_r \in M$$

такие, что

$$u_1 u_2 \dots u_{r+1} = v_1 v_2 \dots v_r = 1.$$

Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная полугруппа  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $\mathbf{U}_j(M)$ .

Следующие две теоремы являются следствиями теорем 6.1 и 6.2, если в них положить

$$u_1 = u_2 = \dots = u_{r+1} = u, v_1 = v_2 = \dots = v_r = v.$$

**Теорема 6.3.** Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ , существуют элементы  $u, v \in M$  такие, что  $u^{r+1} = v^r = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $\mathbf{U}_j(M)$ .

**Теорема 6.4.** Пусть полугруппа  $A$  порождается множеством  $M$ , не содержащем её единицу,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ , существуют элементы  $u, v \in M$  такие, что  $u^{r+1} = v^r = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная полугруппа  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $\mathbf{U}_j(M)$ .

Следующие две теоремы являются формальными обобщениями теорем 6.3 и 6.4 соответственно, так как вытекают из них.

**Теорема 6.5.** Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ ,  $d$  делит  $r + 1$ ,  $c$  делит  $r$ , существуют элементы

$u, v \in M$  такие, что  $u^d = v^c = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $\mathbf{U}_j(M)$ .

**Теорема 6.6.** Пусть полугруппа  $A$  порождается множеством  $M$ , не содержащим её единицу,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $r \geq 2$ ,  $d$  делит  $r + 1$ ,  $c$  делит  $r$ , существуют элементы  $u, v \in M$  такие, что  $u^d = v^c = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $l$ -арная полугруппа  $\langle A^k, [\ ]_{l, \sigma, k} \rangle$ , где  $l = rk + 1$ , порождается множеством  $\mathbf{U}_j(M)$ .

## 7 Следствия и примеры

Полагая в теоремах 6.1 и 6.3  $r = 2$ , получим следующие два следствия.

**Следствие 7.1.** Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ , существуют элементы  $u_1, u_2, u_3, v_1, v_2 \in M$ , такие, что  $u_1 u_2 u_3 = v_1 v_2 = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $(2k + 1)$ -арная группа  $\langle A^k, [\ ]_{2k+1, \sigma, k} \rangle$  порождается множеством  $\mathbf{U}_j(M)$ .

**Следствие 7.2.** Пусть группа  $A$  порождается множеством  $M$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ , существуют элементы  $u, v \in M$ , такие, что  $u^3 = v^2 = 1$ . Тогда для любого  $j = 1, 2, \dots, k$   $(2k + 1)$ -арная группа  $\langle A^k, [\ ]_{2k+1, \sigma, k} \rangle$  порождается множеством  $\mathbf{U}_j(M)$ .

Для теорем 6.2 и 6.4 справедливы следствия, аналогичные следствиям 7.1 и 7.2.

Следующий пример показывает, что в формулировке теореме 4.1 нельзя обойтись без элемента  $\mathbf{e}$ .

**Пример 7.1.** Рассмотрим циклическую группу  $A = \{1, a\}$ , которая порождается множеством  $M = \{a\}$ . Тогда

$$A^2 = \{\mathbf{e} = (1, 1), \mathbf{u} = (1, a), \mathbf{v} = (a, 1), \mathbf{w} = (a, a)\},$$

$$\mathbf{U}_1(M) = \{\mathbf{v}\}, \mathbf{U}_2(M) = \{\mathbf{u}\}, \mathbf{U}(M) = \{\mathbf{u}, \mathbf{v}\}.$$

Согласно теореме 4.1, каждое из множеств

$$\mathbf{U}_1(M) \cup \{\mathbf{e}\} = \{\mathbf{e}, \mathbf{v}\}, \mathbf{U}_2(M) \cup \{\mathbf{e}\} = \{\mathbf{e}, \mathbf{u}\}$$

порождает тернарную группу  $\langle A^2, [\ ]_{3, (12), 2} \rangle$ .

Так как

$$[\mathbf{uuu}]_{3, (12), 2} = \mathbf{v}, [\mathbf{vvv}]_{3, (12), 2} = \mathbf{u},$$

$$[\mathbf{uuv}]_{3, (12), 2} = [\mathbf{vuu}]_{3, (12), 2} = \mathbf{u},$$

$$[\mathbf{vvu}]_{3, (12), 2} = [\mathbf{uvv}]_{3, (12), 2} = \mathbf{v},$$

$$[\mathbf{uvu}]_{3, (12), 2} = \mathbf{u}, [\mathbf{vuv}]_{3, (12), 2} = \mathbf{v},$$

то  $\langle \mathbf{U}(M) = \{\mathbf{u}, \mathbf{v}\}, [\ ]_{3, (12), 2} \rangle$  – тернарная подгруппа тернарной группы  $\langle A^2, [\ ]_{3, (12), 2} \rangle$ . Следовательно, каждое из множеств  $\mathbf{U}(M)$ ,  $\mathbf{U}_1(M)$  и  $\mathbf{U}_2(M)$  не порождает тернарную группу  $\langle A^2, [\ ]_{3, (12), 2} \rangle$ .

Равенства

$$[\mathbf{uuu}]_{3, (12), 2} = \mathbf{v}, [\mathbf{vvv}]_{3, (12), 2} = \mathbf{u}$$

показывают, что порождающее множество  $\{\mathbf{e}, \mathbf{u}, \mathbf{v}\}$  не является неприводимым, так как из него можно удалить либо элемент  $\mathbf{u}$ , либо элемент  $\mathbf{v}$ . Полученные порождающие множества  $\{\mathbf{e}, \mathbf{u}\}$  и  $\{\mathbf{e}, \mathbf{v}\}$  будут уже неприводимыми.

Так как

$$[\mathbf{uuw}]_{3, (12), 2} = \mathbf{e}, [\mathbf{uwe}]_{3, (12), 2} = \mathbf{v},$$

то  $\{\mathbf{u}, \mathbf{w}\}$  – еще одно порождающее множество, причем неприводимое. Неприводимым порождающим множеством является и множество  $\{\mathbf{v}, \mathbf{w}\}$ , так как

$$[\mathbf{vww}]_{3, (12), 2} = \mathbf{e}, [\mathbf{vwe}]_{3, (12), 2} = \mathbf{u}.$$

Таким образом, тернарную группу  $\langle A^2, [ ]_{3, (12), 2} \rangle$  порождает каждое из следующих четырех двухэлементных неприводимых множеств

$$\{\mathbf{e}, \mathbf{u}\}, \{\mathbf{e}, \mathbf{v}\}, \{\mathbf{u}, \mathbf{w}\}, \{\mathbf{v}, \mathbf{w}\}.$$

Отметим, что последние два множества не содержат  $\mathbf{e}$ .

Кроме множества  $\{\mathbf{e}, \mathbf{u}, \mathbf{v}\}$ , тернарную группу  $\langle A^2, [ ]_{3, (12), 2} \rangle$  порождает также каждое из следующих трехэлементных множеств

$$\{\mathbf{e}, \mathbf{u}, \mathbf{w}\}, \{\mathbf{e}, \mathbf{v}, \mathbf{w}\}, \{\mathbf{u}, \mathbf{v}, \mathbf{w}\}.$$

**Замечание 7.1.** Случай  $r=1$  исключён из теоремы 6.1, так как в этом случае множество  $\mathbf{U}_j(M)$  может быть как порождающим, так и не порождающим. В примере 7.1, соответствующем случаю  $r=1$ , множества  $\mathbf{U}_1(M)$  и  $\mathbf{U}_2(M)$  не являются порождающими для тернарной группы  $\langle A^2, [ ]_{3, (12), 2} \rangle$ . А в следующих примерах, для которых также  $r=1$ , множество  $\mathbf{U}_j(M)$  является порождающим для соответствующих тернарных групп.

**Пример 7.2.** Циклическая группа  $A$  порядка 3, порожденная элементом  $a$ , порождается также двухэлементным множеством  $M = \{a, a^2\}$ . Тогда по теореме 4.1 тернарная группа  $\langle A^2, [ ]_{3, (12), 2} \rangle$  порядка 9 порождается множеством  $\mathbf{U}_1(M) \cup \{\mathbf{e}\}$ , где

$$\mathbf{U}_1(M) = \{(a, 1), (a^2, 1)\}, \mathbf{e} = (1, 1).$$

Так как

$$[(a, 1)(a, 1)(a, 1)(a^2, 1)(a, 1)]_{3, (12), 2} = \\ = (a^3, a^3) = (1, 1) = \mathbf{e},$$

то элемент  $\mathbf{e}$  выражается с помощью тернарной операции  $[ ]_{3, (12), 2}$  через элементы множества  $\mathbf{U}_1(M)$ . Следовательно, тернарная группа  $\langle A^2, [ ]_{3, (12), 2} \rangle$  порождается двухэлементным множеством  $\mathbf{U}_1(M)$ . Двухэлементное множество  $\mathbf{U}_2(M)$  также является порождающим для  $\langle A^2, [ ]_{3, (12), 2} \rangle$ .

**Пример 7.3.** Циклическая группа  $A = \mathbf{Z}_6$  порядка 6, порожденная элементом  $a$ , порождается также двухэлементным множеством  $M = \{a^2, a^3\}$ . Тогда по теореме 4.1 тернарная группа  $\langle \mathbf{Z}_6^2, [ ]_{3, (12), 2} \rangle$  порядка 36 порождается множеством  $\mathbf{U}_1(M) \cup \{\mathbf{e}\}$ , где

$$\mathbf{U}_1(M) = \{(a^2, 1), (a^3, 1)\}, \mathbf{e} = (1, 1).$$

Положим

$$\begin{aligned} \mathbf{u} &= [(a^3, 1)(a^2, 1)(a^3, 1)]_{3, (12), 2}, \\ \mathbf{v} &= [(a^2, 1)(a^2, 1)(a^2, 1)]_{3, (12), 2}, \\ \mathbf{w} &= [(a^2, 1)\mathbf{uv}]_{3, (12), 2}. \end{aligned}$$

Так как

$$\mathbf{u} = (1, a^2), \mathbf{v} = (a^4, a^2),$$

то

$$\mathbf{w} = [(a^2, 1)(1, a^2)(a^4, a^2)]_{3, (12), 2} = (a^2, a^2),$$

откуда

$$\begin{aligned} [\mathbf{www}]_{3, (12), 2} &= [(a^2, a^2)(a^2, a^2)(a^2, a^2)]_{3, (12), 2} = \\ &= (1, 1) = \mathbf{e}, \end{aligned}$$

то есть  $[\mathbf{www}]_{3, (12), 2} = \mathbf{e}$ .

Таким образом, элемент  $\mathbf{e}$  выражается с помощью тернарной операции  $[ ]_{3, (12), 2}$  через элементы множества  $\mathbf{U}_1(M)$ :

$$\begin{aligned} \mathbf{e} &= [(a^2, 1)(a^3, 1)(a^2, 1)(a^3, 1)(a^2, 1)(a^2, 1)(a^2, 1) \\ &\quad (a^2, 1)(a^3, 1)(a^2, 1)(a^3, 1)(a^2, 1)(a^2, 1)(a^2, 1) \\ &\quad (a^2, 1)(a^3, 1)(a^2, 1)(a^3, 1)(a^2, 1)(a^2, 1)]_{3, (12), 2}. \end{aligned}$$

Следовательно, тернарная группа  $\langle \mathbf{Z}_6^2, [ ]_{3, (12), 2} \rangle$  порождается двухэлементным множеством  $\mathbf{U}_1(M)$ . Порождающим для этой тернарной группы является и двухэлементное множество  $\mathbf{U}_2(M)$ .

**Пример 7.4.** Пусть как и в примере 7.3  $A = \mathbf{Z}_6$  – циклическая группа порядка 6, порождаемая множеством  $M = \{a^2, a^3\}$ . Тогда по следствию 7.2 ( $u = a^2, v = a^3$ ) для любого цикла  $\sigma$  длины  $k$  из  $S_k$   $(2k+1)$ -арная группа  $\langle \mathbf{Z}_6^k, [ ]_{2k+1, \sigma, k} \rangle$  порождается двухэлементным множеством  $\mathbf{U}_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Пример 7.4 может быть извлечен и из следствия 7.2.

**Замечание 7.2.** В примере 7.4 значению  $k=2$  соответствует 5-арная группа. Поэтому пример 7.3, в котором фигурирует тернарная группа, не может быть получен из примера 7.4.

Так как симметрическая группа  $S_n$  порождается любым из следующих четырёх множеств [5]:

$$M_1 = \{\alpha_1 = (1 2), \alpha_2 = (1 2 \dots n)\};$$

$$M_2 = \{\alpha_1 = (1 2), \alpha_2 \alpha_1 = (2 3 \dots n)\};$$

$$M_3 = \{\beta_1 = (1 2), \beta_2 = (2 3), \dots, \beta_{n-1} = (n-1 \ n)\};$$

$$M_4 = \{\gamma_1 = (1 \ n), \gamma_2 = (2 \ n), \dots, \gamma_{n-1} = (n-1 \ n)\},$$

то теорема 4.1 позволяет сформулировать следствие, в котором  $\varepsilon$  – тождественная подстановка множества  $\{1, 2, \dots, n\}$ ,  $\mathbf{e} = (\underbrace{\varepsilon, \dots, \varepsilon}_k)$ .

**Следствие 7.3.** Для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle S_n^k, [ ]_{l, \sigma, k} \rangle$ , где  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $k$  делит  $l-1$ , порождается любым из следующих четырёх множеств:

$$\mathbf{U}_j(M_1) \cup \{\mathbf{e}\} = \{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}),$$

$$(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \alpha_2, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}, (\underbrace{\varepsilon, \dots, \varepsilon}_k));$$

$$\mathbf{U}_j(M_2) \cup \{\mathbf{e}\} = \{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}),$$

$$(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \alpha_2 \alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}, (\underbrace{\varepsilon, \dots, \varepsilon}_k));$$

$$\mathbf{U}_j(M_3) \cup \{\mathbf{e}\} = \{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \beta_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}), \dots,$$

$$\dots, (\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \beta_{n-1}, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}, (\underbrace{\varepsilon, \dots, \varepsilon}_k));$$

$$\mathbf{U}_j(M_4) \cup \{\mathbf{e}\} = \{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \gamma_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}), \dots,$$

$$\dots, (\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \gamma_{n-1}, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}, (\underbrace{\varepsilon, \dots, \varepsilon}_k)).$$

В частности, порождающими являются следующие множества:

$$\begin{aligned} \mathbf{U}_1(M_1) \cup \{\mathbf{e}\} &= \\ = \{(\alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\alpha_2, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\underbrace{\varepsilon, \dots, \varepsilon}_k)\}; \\ \mathbf{U}_1(M_2) \cup \{\mathbf{e}\} &= \\ = \{(\alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\alpha_2 \alpha_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\underbrace{\varepsilon, \dots, \varepsilon}_k)\}; \\ \mathbf{U}_1(M_3) \cup \{\mathbf{e}\} &= \\ = \{(\beta_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), \dots, (\beta_{n-1}, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\underbrace{\varepsilon, \dots, \varepsilon}_k)\}; \\ \mathbf{U}_1(M_4) \cup \{\mathbf{e}\} &= \\ = \{(\gamma_1, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), \dots, (\gamma_{n-1}, \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), (\underbrace{\varepsilon, \dots, \varepsilon}_k)\}. \end{aligned}$$

Для некоторых  $l$  в следствии 7.3 элемент  $\mathbf{e}$  может быть удалён из порождающего множества  $l$ -арной группы  $<\mathbf{S}_n^k, [\ ]_{l, \sigma, k}>$ .

Так как для чётного  $n$

$$(1 2)^n = (2 3 \dots n)^{n-1} = \varepsilon,$$

то, полагая в теореме 6.3  $r = n - 1$ ,  $u = (1 2)$ ,  $v = (2 3 \dots n)$ , получим

**Следствие 7.4.** Для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $<\mathbf{S}_n^k, [\ ]_{l, \sigma, k}>$ , где  $n \geq 4$  – чётное,  $l = (n-1)k + 1$ ,  $\sigma$  – цикл длины  $k$  из  $\mathbf{S}_k$ , порождается множеством

$$\begin{aligned} \mathbf{U}_j(M_2) = \{ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) , \\ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (2 3 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) \}. \end{aligned}$$

В частности, она порождается множеством

$$\mathbf{U}_1(M_2) = \{((1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), ((2 3 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1})\}.$$

Так как для нечётного  $n$

$$(1 2 \dots n)^n = (1 2)^{n-1} = \varepsilon,$$

то, полагая в теореме 6.3  $r = n - 1$ ,  $u = (1 2 \dots n)$ ,  $v = (12)$ , получим

**Следствие 7.5.** Для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $<\mathbf{S}_n^k, [\ ]_{l, \sigma, k}>$ , где  $n \geq 3$  – нечётное,  $l = (n-1)k + 1$ ,  $\sigma$  – цикл длины  $k$  из  $\mathbf{S}_k$ , порождается множеством

$$\begin{aligned} \mathbf{U}_j(M_1) = \{ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) , \\ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) \}. \end{aligned}$$

В частности, она порождается множеством

$$\mathbf{U}_1(M_1) = \{((1 2 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), ((1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1})\}.$$

**Пример 7.5.** Так как  $(1 2 3)^3 = (1 2)^2 = \varepsilon$ , то положив в следствии 7.5  $n = 3$ ,  $k = 2$ ,  $j = 1$ , получим 5-арную группу  $<\mathbf{S}_3^2, [\ ]_{5, (12), 2}>$ , которая согласно этому следствию порождается двухэлементным множеством  $\{((1 2 3), \varepsilon), ((1 2), \varepsilon)\}$ .

Равенство, позволяющее выразить элемент  $\mathbf{e}$  с помощью 5-арной операции  $[\ ]_{5, (12), 2}$  через элементы множества  $\mathbf{U}_1(M_1)$  имеет вид

$$\begin{aligned} &[((1 2 3), \varepsilon)((1 2), \varepsilon)((1 2 3), \varepsilon)((1 2), \varepsilon), \\ &((1 2 3), \varepsilon)]_{5, (12), 2} = ((1 2 3)^3, (1 2)^2) = (\varepsilon, \varepsilon) = \mathbf{e}. \end{aligned}$$

Это равенство получается из равенства, завершающего доказательство теоремы 6.1, из которой извлечена теорема 6.3.

Так как для нечётного  $n$

$$(1 2)^{n+1} = (1 2 \dots n)^n = \varepsilon,$$

то, полагая в теореме 6.3  $r = n$ ,  $u = (1 2)$ ,  $v = (1 2 \dots n)$ , получим

**Следствие 7.6.** Для любого  $j = 1, 2, \dots, k$   $(nk + 1)$ -арная группа  $<\mathbf{S}_n^k, [\ ]_{nk+1, \sigma, k}>$ , где  $n \geq 3$  – нечётное,  $\sigma$  – цикл длины  $k$  из  $\mathbf{S}_k$ , порождается множеством

$$\begin{aligned} \mathbf{U}_j(M_1) = \{ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) , \\ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) \}. \end{aligned}$$

В частности, она порождается множеством

$$\mathbf{U}_1(M_1) = \{((1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1}), ((1 2 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-1})\}.$$

**Пример 7.6.** Так как  $(1 2)^4 = (1 2 3)^3 = \varepsilon$ , то положив в следствии 7.6  $n = 3$ ,  $k = 2$ ,  $j = 1$ , получим 7-арную группу  $<\mathbf{S}_3^2, [\ ]_{7, (12), 2}>$ , которая согласно этому следствию порождается двухэлементным множеством

$$\{((1 2), \varepsilon), ((1 2 3), \varepsilon)\}.$$

Равенство, позволяющее выразить элемент  $\mathbf{e}$  с помощью 7-арной операции  $[\ ]_{7, (12), 2}$  через элементы множества  $\mathbf{U}_1(M_1)$  имеет вид

$$\begin{aligned} &[((1 2), \varepsilon)((1 2 3), \varepsilon)((1 2), \varepsilon)((1 2 3), \varepsilon), \\ &((1 2), \varepsilon)((1 2 3), \varepsilon)((1 2), \varepsilon)]_{7, (12), 2} = \\ &= ((1 2)^4, (1 2 3)^3) = (\varepsilon, \varepsilon) = \mathbf{e}. \end{aligned}$$

Это равенство получается из равенства, завершающего доказательство теоремы 6.1, из которой извлечена теорема 6.3.

Для нахождения полиадических групп вида  $<\mathcal{A}^k, [\ ]_{l, \sigma, k}>$ , порождаемых множеством  $\mathbf{U}_j(M)$ , можно воспользоваться непосредственно теоремой 6.1.

**Следствие 7.7.** Для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $<\mathbf{A}_n^k, [\ ]_{l, \sigma, k}>$ , где  $n \geq 4$  – нечётное,  $l = (2n-1)k + 1$ ,  $\sigma$  – цикл длины  $k$  из  $\mathbf{S}_k$ , порождается множеством

$$\begin{aligned} \{ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (3 4 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) , \\ &(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2 3), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}) \}. \end{aligned}$$

**Доказательство.** Известно, что для нечётного  $n \geq 4$  знакопеременная группа  $\mathbf{A}_n$  порождается [5] множеством

$$\{u = (3 4 \dots n), v = (1 2 3)\},$$

при этом

$$u^{n-2} = v^3 = (uv)^n = \varepsilon. \quad (7.1)$$

Положив в теореме 6.1  $r = 2n - 1$ ,

$$u_1 = u, u_2 = v, u_3 = u, u_4 = v, \dots, u_{2n-1} = u, u_{2n} = v,$$

$v_1 = v_2 = \dots = v_{2n-4} = u, v_{2n-3} = v_{2n-2} = v_{2n-1} = v$ , и, учитывая (7.1), получим

$$u_1 u_2 \dots u_{2n} = (uv)^n = \varepsilon, \\ v_1 v_2 \dots, v_{2n-1} = u^{2n-4} v^3 = (u^{n-2})^2 \varepsilon = \varepsilon.$$

По теореме 6.1 для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A_n^k, [ ],_{l, \sigma, k} \rangle$ , где  $l = (2n-1)k+1$ , порождается множеством, указанном в условии. Следствие доказано.

**Следствие 7.8.** Для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A_n^k, [ ],_{l, \sigma, k} \rangle$ , где  $n \geq 4$  – чётное,  $l = (2n-2)k+1$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ , порождается множеством

$$\{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1\ 2)(3\ 4 \dots n), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}), \\ (\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1\ 2\ 3), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j})\}.$$

*Доказательство.* Известно, что для чётного  $n \geq 4$  знакопеременная группа  $A_n$  порождается [5] множеством  $\{w = (1\ 2)(3\ 4 \dots n), v = (1\ 2\ 3)\}$ , при этом

$$w^{n-2} = v^3 = (wv)^{n-1} = \varepsilon. \quad (7.2)$$

Положив в теореме 6.1  $r = 2n-2$ ,

$$u_1 = u_2 = \dots = u_{2n-4} = w, u_{2n-3} = u_{2n-2} = u_{2n-1} = v, \\ v_1 = w, v_2 = v, v_3 = w, v_4 = v, \dots, = v_{2n-3} = w, \\ v_{2n-2} = v,$$

и, учитывая (7.2), получим

$$u_1 u_2 \dots u_{2n-1} = w^{2n-4} v^3 = (w^{n-2})^2 \varepsilon = \varepsilon, \\ v_1 v_2 \dots v_{2n-2} = (wv)^{n-1} = \varepsilon.$$

По теореме 6.1 для любого  $j = 1, 2, \dots, k$   $l$ -арная группа  $\langle A_n^k, [ ],_{l, \sigma, k} \rangle$ , где  $l = (2n-2)k+1$ , порождается множеством, указанном в условии.  $\square$

## 8 Обобщения теорем 6.3 и 6.4

Отметим, что теорему 6.3 можно сформулировать в более общем виде, показав, что в её условиях существует не одна, а бесконечно много полиадических групп  $\langle A^k, [ ],_{l, \sigma, k} \rangle$  различных арностей  $l$ , которые порождаются множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ . Указанная в формулировке теоремы 6.3  $(rk+1)$ -арная группа  $\langle A^k, [ ],_{rk+1, \sigma, k} \rangle$  – лишь одна из них.

**Теорема 8.1.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^{r+1} = b^r = 1$  для некоторого  $r \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} r((r+1)i+1)k+1, & \text{если } 1+ri > 0, \\ -(r+1)(1+ri)k+1, & \text{если } 1+ri < 0, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

При  $r \geq 2$  множество всех целых решений неравенства  $1+ri > 0$  имеет вид  $\{0, 1, 2, \dots\}$ , соответственно множество всех целых решений неравенства  $1+ri < 0$  имеет вид  $\{-1, -2, \dots\}$ . Поэтому теорему 8.1 можно переформулировать следующим образом.

**Теорема 8.2.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы

$a$  и  $b$  такие, что  $a^{r+1} = b^r = 1$  для некоторого  $r \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} r((r+1)i+1)k+1, & i = 0, 1, 2, \dots, \\ -(r+1)(1+ri)k+1, & i = -1, -2, \dots, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

**Замечание 8.1.** Теоремы 8.1 и 8.2 включает в себя теорему 6.3 при  $i = 0$ , то есть теоремы 8.1 и 8.2 можно рассматривать как обобщения теоремы 6.3.

Мы получим теоремы 8.1 и 8.2 как следствие более общего результата.

Из теории чисел известно [6], что для взаимно простых целых чисел  $m$  и  $n$  уравнение

$$mx + ny = 1 \quad (8.1)$$

имеет бесконечно много решений в целых числах. Если  $(x_0, y_0)$  – одно из таких решений, то множество всех решений диофантового уравнения (8.1) имеет вид

$$\{(x_0 - ni, y_0 + mi) \mid i \in \mathbb{Z}\}$$

или, что равносильно,

$$\{(x_0 + ni, y_0 - mi) \mid i \in \mathbb{Z}\}. \quad (8.2)$$

Ясно, что ненулевые компоненты любого решения  $(x_0, y_0)$  уравнения (8.1) имеют разные знаки:  $xy < 0$ .

**Теорема 8.3.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^m = b^n = 1$  для некоторых взаимно простых  $m \geq 2$  и  $n \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения (8.1). Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} n(mi - y_0)k + 1, & \text{если } x_0 + ni > 0, \\ -m(x_0 + ni)k + 1, & \text{если } x_0 + ni < 0, \end{cases} \quad (8.3)$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

*Доказательство.* Подставим любое решение из (8.2), которое имеет ненулевые компоненты, в (8.1):

$$m(x_0 + ni) + n(y_0 - mi) = 1. \quad (8.4)$$

Если  $x_0 + ni = 0$  или  $y_0 - mi = 0$ , то соответственно  $n = \pm 1$  или  $m = \pm 1$ , что противоречит неравенствам  $m \geq 2$  и  $n \geq 2$  из условия теоремы. Поэтому считаем

$$x_0 + ni \neq 0, y_0 - mi \neq 0. \quad (8.5)$$

Если  $x_0 + ni > 0$ , то из (8.4) и (8.5) следует

$$n(y_0 - mi) < 0,$$

откуда получаем  $y_0 - mi < 0$ . Так как в левой части этого неравенства стоит целое число, то на самом деле  $y_0 - mi \leq -1$  или, что равносильно,  $mi - y_0 \geq 1$ . Из последнего неравенства и неравенства  $n \geq 2$  следует  $n(mi - y_0) \geq 2$ . Положив

$$r = -n(y_0 - mi) = n(mi - y_0),$$

где  $r \geq 2$ , и, учитывая (8.4), получим

$$r + 1 = m(x_0 + ni).$$

Так как

$$a^{r+1} = a^{m(x_0+ni)} = (a^m)^{x_0+ni} = 1,$$

$$b^r = b^{n(mi-y_0)} = (b^n)^{mi-y_0} = 1,$$

то по теореме 6.3 ( $u = a$ ,  $v = b$ ),  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где  $l = n(mi - y_0)k + 1$ , порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Рассмотрим теперь неравенство  $x_0 + ni < 0$ , в левой части которого стоит целое число. Поэтому на самом деле  $x_0 + ni \leq -1$ , откуда ввиду  $m \geq 2$ , следует  $m(x_0 + ni) \leq -2$  или, что равносильно,  $-m(x_0 + ni) \geq 2$ . Положив

$$r = -m(x_0 + ni),$$

где  $r \geq 2$ , и, учитывая (8.4), получим

$$r + 1 = n(y_0 - mi).$$

Так как

$$b^{r+1} = b^{n(y_0-mi)} = (b^n)^{y_0-mi} = 1,$$

$$a^r = a^{-m(x_0+ni)} = (a^m)^{-(x_0+ni)} = 1,$$

то по теореме 6.3 ( $u = b$ ,  $v = a$ ),  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где

$$l = -m(x_0 + ni)k + 1,$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .  $\square$

**Замечание 8.2.** В теореме 8.3 формулу (8.3) можно заменить формулой

$$l = \begin{cases} n(mi - y_0)k + 1, & \text{если } y_0 - mi < 0, \\ -m(x_0 + ni)k + 1, & \text{если } y_0 - mi > 0. \end{cases}$$

Так как числа  $r$  и  $r + 1$  взаимно простые, то следующая теорема является следствием теоремы 8.3.

**Теорема 8.4.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^{r+1} = b^r = 1$  для некоторого  $r \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения

$$(r+1)x + ry = 1. \quad (8.6)$$

Тогда  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} r((r+1)i - y_0)k + 1, & \text{если } x_0 + ri > 0, \\ -(r+1)(x_0 + ri)k + 1, & \text{если } x_0 + ri < 0, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Так как пара  $(1, -1)$  является одним из решений диофантового уравнения (8.6), то теоремы 8.1 и 8.2 совпадают с теоремой 8.3 при  $x_0 = 1$ ,  $y_0 = -1$ .

**Замечание 8.3.** Теоремы 8.1–8.4, обобщающие теорему 6.3, является формальными её обобщениями, так как при доказательстве теоремы 8.3, а значит и вытекающих из неё теорем 8.1, 8.2 и 8.4, была использована теорема 6.3.

Результаты, аналогичные теоремам 8.1–8.4, справедливы и для  $l$ -арной полугруппы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ .

Доказательство следующего аналога теоремы 8.3 отличается от её доказательства только ссылкой на теорему 6.4 вместо ссылки на теорему 6.3.

**Теорема 8.5.** Пусть полугруппа  $A$  порождается множеством  $M$ , не содержащим её единицу, в котором имеются элементы  $a$  и  $b$  такие, что  $a^m = b^n = 1$  для некоторых взаимно простых  $m \geq 2$  и  $n \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения (8.1). Тогда  $l$ -арная полугруппа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} n(mi - y_0)k + 1, & \text{если } x_0 + ni > 0, \\ -m(x_0 + ni)k + 1, & \text{если } x_0 + ni < 0, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Из теоремы 8.5 вытекают результаты, аналогичные теоремам 8.1, 8.2 и 8.4. Ограничимся аналогом теоремы 8.2.

**Теорема 8.6.** Пусть полугруппа  $A$  порождается множеством  $M$ , не содержащим её единицу, в котором имеются элементы  $a$  и  $b$  такие, что  $a^{r+1} = b^r = 1$  для некоторого  $r \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Тогда  $l$ -арная полугруппа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} r((r+1)i + 1)k + 1, & i = 0, 1, 2, \dots, \\ -(r+1)(1 + ri)k + 1, & i = -1, -2, \dots, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

**Замечание 8.4.** Заменив в теоремах 8.1, 8.2, 8.4 и 8.6 равенства  $a^{r+1} = b^r = 1$  равенствами  $a^d = b^c = 1$ , где  $d$  делит  $r + 1$ ,  $c$  делит  $r$ , получим формальные обобщения этих теорем.

Приведём несколько следствий из теорем этого раздела.

Так как специальная линейная группа  $SL_2(\mathbf{Z})$  порождается [5] матрицами

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

при этом

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E,$$

то из теоремы 8.2 вытекает

**Следствие 8.1.** Для любого цикла  $\sigma$  длины  $k$  из  $S_k$   $l$ -арная группа  $\langle SL_2^k(\mathbf{Z}), [ ]_{l, \sigma, k} \rangle$ , где

$$l = \begin{cases} 3(4i+1)k + 1, & i = 0, 1, 2, \dots, \\ -4(3i+1)k + 1, & i = -1, -2, \dots, \end{cases}$$

порождается двухэлементным множеством

$$\left\{ \underbrace{(E, \dots, E)}_{j-1}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \underbrace{(E, \dots, E)}_{k-j}, \right. \\ \left. \underbrace{(E, \dots, E)}_{j-1}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \underbrace{(E, \dots, E)}_{k-j} \right\}$$

для любого  $j = 1, 2, \dots, k$ .

Известно, что простая группа Матье  $M_{11}$ , рассматриваемая как группа подстановок, порождается [7] двумя подстановками

$$(1 \ 2 \ \dots \ 11), (5 \ 6 \ 4 \ 10)(11 \ 8 \ 3 \ 7),$$

порядка 11 и 4 соответственно. Так как пара  $(3, -1)$  является одним из решений диофантового уравнения  $4x + 11y = 1$ , то из теоремы 8.3 вытекает

**Следствие 8.2.** Для любого цикла  $\sigma$  длины  $k$  из  $S_k$   $l$ -арная группа  $\langle M_{11}^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} 11(4i+1)k+1, & i = 0, 1, 2, \dots, \\ -4(11i+3)k+1, & i = -1, -2, \dots, \end{cases}$$

порождается двухэлементным множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2 \dots 11), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \right. \\ \left. \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (5 6 4 10)(11 8 3 7), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}$$

для любого  $j = 1, 2, \dots, k$ .

## 9 Случай инволюций

В ряде случаев порождающее множество группы содержит инволюции и элементы, нечётная степень которых совпадает с единицей группы. К таким группам применима теорема 8.3. при  $m = 2$  и  $n = 2t + 1$ , где  $t \geq 1$  или  $n = 2t - 1$ , где  $t \geq 2$ . Сформулируем соответствующий результат для случая  $m = 2$ ,  $n = 2t + 1$ , где  $t \geq 1$ .

**Теорема 9.1.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^2 = b^{2t+1} = 1$  для некоторого  $t \geq 1$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения

$$2x + (2t+1)y = 1. \quad (9.1)$$

Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2t+1)(2i-y_0)k+1, & \text{если } x_0 + (2t+1)i > 0, \\ -2(x_0 + (2t+1)i)k+1, & \text{если } x_0 + (2t+1)i < 0, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Так как пара  $(t+1, -1)$  является одним из решений диофантового уравнения (9.1), то неравенство  $x_0 + (2t+1)i > 0$  принимает вид

$$x_0 + (2t+1)i = t+1 + (2t+1)i > 0.$$

Из этого неравенства следует  $i > -\frac{t+1}{2t+1}$ , откуда

$i = 0, 1, 2, \dots$ . Соответственно из неравенства

$x_0 + (2t+1)i < 0$  следует  $i < -\frac{t+1}{2t+1}$ , откуда

$i = -1, -2, \dots$ . Поэтому из теоремы 9.1 вытекает

**Теорема 9.2.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^2 = b^{2t+1} = 1$  для некоторого  $t \geq 1$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2t+1)(2i+1)k+1, & i = 0, 1, 2, \dots, \\ -2(t+1+(2t+1)i)k+1, & i = -1, -2, \dots, \end{cases} \quad (9.2)$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Диэдральная группа  $D_{2n}$  порядка  $2n$ , то есть полная группа преобразований симметрии

правильного  $n$ -многоугольника порождается двухэлементным множеством  $M = \{a, b\}$ , где  $a$  – любое отражение,  $b$  – порождающий элемент циклической подгруппы  $Z_n$  поворотов. Так как  $a^2 = b^n = 1$ , то, положив в теореме 9.2  $A = D_{2(2t+1)}$ , где  $t \geq 1$ , получим

**Следствие 9.1.** Для любого цикла  $\sigma$  длины  $k$  из  $S_k$  и любого целого  $t \geq 1$   $l$ -арная группа  $\langle D_{2(2t+1)}^k, [ ],_{l,\sigma,k} \rangle$ , где арность  $l$  определяется равенством (9.2), порождается двухэлементным множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, a, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, b, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}.$$

для любого  $j = 1, 2, \dots, k$ .

Положив в теореме 9.2  $A = S_{2t+1}$ ,  $a = (12)$ ,  $b = (12 \dots 2t+1)$ , получим следующий результат, включающий в себя при  $i = -1$  следствие 7.5.

**Следствие 9.2.** Для любого цикла  $\sigma$  длины  $k$  из  $S_k$  и любого целого  $t \geq 1$   $l$ -арная группа  $\langle S_{2t+1}^k, [ ],_{l,\sigma,k} \rangle$ , где арность  $l$  определяется равенством (9.2), порождается двухэлементным множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \right. \\ \left. \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (1 2 \dots 2t+1), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}.$$

для любого  $j = 1, 2, \dots, k$ .

Следующий результат получается из теоремы 8.3 при  $m = 2$ ,  $n = 2s - 1$ , где  $s \geq 2$ .

**Теорема 9.3.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^2 = b^{2s-1} = 1$  для некоторого  $s \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения

$$2x + (2s-1)y = 1. \quad (9.3)$$

Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2s-1)(2i-y_0)k+1, & \text{если } x_0 + (2s-1)i > 0, \\ -2(x_0 + (2s-1)i)k+1, & \text{если } x_0 + (2s-1)i < 0, \end{cases}$$

порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Так как пара  $(s, -1)$  является одним из решений диофантового уравнения (9.3), то неравенство  $x_0 + (2s-1)i > 0$  принимает вид

$$x_0 + (2s-1)i = s + (2s-1)i > 0.$$

Из этого неравенства следует  $i > -\frac{s}{2s-1}$ , откуда

$i = 0, 1, 2, \dots$ . Соответственно из неравенства

$x_0 + (2s-1)i < 0$  следует  $i < -\frac{s}{2s-1}$ , откуда

$i = -1, -2, \dots$ . Поэтому из теоремы 9.3 вытекает

**Теорема 9.4.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $a$  и  $b$  такие, что  $a^2 = b^{2s-1} = 1$  для некоторого  $s \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Тогда  $l$ -арная группа  $\langle A^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2s-1)(2i+1)k+1, & i = 0, 1, 2, \dots, \\ -2(s+(2s-1)i)k+1, & i = -1, -2, \dots, \end{cases} \quad (9.4)$$

порождается множеством  $\mathbf{U}_j(M)$  для любого  $j = 1, 2, \dots, k$ .

Положив в теореме 9.4  $A = \mathbf{S}_{2s-1}$ ,  $a = (12)$ ,  $b = (12 \dots 2s-1)$ , получим следующий результат, включающий в себя при  $i = 0$  следствие 7.6.

**Следствие 9.3.** Для любого цикла  $\sigma$  длины  $k$  из  $\mathbf{S}_k$  и любого целого  $s \geq 2$   $l$ -арная группа  $\langle \mathbf{S}_{2s-1}^k, [ ],_{l,\sigma,k} \rangle$ , где арность  $l$  определяется равенством (9.4), порождается двухэлементным множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (12), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \right. \\ \left. \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (12 \dots 2s-1), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}$$

для любого  $j = 1, 2, \dots, k$ .

Положив в теореме 9.2  $A = \mathbf{S}_{2(t+1)}$ ,  $a = (12)$ ,  $b = (23 \dots 2(t+1))$ , получим следующий результат, включающий в себя при  $i = 0$  следствие 7.4.

**Следствие 9.4.** Для любого цикла  $\sigma$  длины  $k$  из  $\mathbf{S}_k$  и любого целого  $t \geq 1$   $l$ -арная группа  $\langle \mathbf{S}_{2(t+1)}^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2t+1)(2i+1)k+1, & i = 0, 1, 2, \dots, \\ -2(t+1+(2t+1)i)k+1, & i = -1, -2, \dots, \end{cases}$$

порождается множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (12), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \right. \\ \left. \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (23 \dots 2(t+1)), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}$$

для любого  $j = 1, 2, \dots, k$ .

Положив в теореме 9.4  $A = \mathbf{S}_{2s}$ ,  $a = (12)$ ,  $b = (23 \dots 2s)$ , получим следующий результат, включающий в себя при  $i = 0$  следствие 7.4.

**Следствие 9.5.** Для любого цикла  $\sigma$  длины  $k$  из  $\mathbf{S}_k$  и любого целого  $s \geq 2$   $l$ -арная группа  $\langle \mathbf{S}_{2s}^k, [ ],_{l,\sigma,k} \rangle$ , где

$$l = \begin{cases} (2s-1)(2i+1)k+1, & i = 0, 1, 2, \dots, \\ -2(s+(2s-1)i)k+1, & i = -1, -2, \dots, \end{cases}$$

порождается множеством

$$\left\{ \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (12), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right), \right. \\ \left. \left( \underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, (23 \dots 2s), \underbrace{\varepsilon, \dots, \varepsilon}_{k-j} \right) \right\}$$

для любого  $j = 1, 2, \dots, k$ .

**Замечание 9.1.** Теоремы 9.1 и 9.3 равносильны, так как вторая получается из первой заменой  $t = s-1$ , а первая из второй – заменой  $s = t+1$ . По этой же причине равносильны теоремы 9.2 и 9.4, следствия 9.2 и 9.3, а также следствия 9.4 и 9.5.

Каждый результат разделов 8 и 9 характеризуется тем, что фигурирующей в нём группе  $A$ , порождаемой множеством  $M$ , соответствует бесконечно много полиадических групп

$\langle A^k, [ ],_{l,\sigma,k} \rangle$  различных арностей  $l$ , порождаемых множеством  $\mathbf{U}_j(M)$  для любого  $j = 1, 2, \dots, k$ . При фиксированном  $k$  эти арности зависят только от  $m$  и  $n$ . Изменение  $m$  и  $n$  приводит к иной серии полиадических групп  $\langle A^k, [ ],_{l,\sigma,k} \rangle$  различных арностей  $l$ , порождаемых множеством  $\mathbf{U}_j(M)$  для любого  $j = 1, 2, \dots, k$ . Проиллюстрируем сказанное примером.

**Пример 9.1.** Так как симметрическая группа  $\mathbf{S}_5$  порождается [5] тремя подстановками,

$$(54321), (1234), (12)(345)$$

имеющими порядки 5, 4 и 6 соответственно, то согласно теореме 8.2 ( $r=4$ ),  $l$ -арная группа  $\langle \mathbf{S}_5^2, [ ],_{l,(12),2} \rangle$ , где

$$l = \begin{cases} 40i+9, & i = 0, 1, 2, \dots, \\ -40i-9, & i = -1, -2, \dots, \end{cases}$$

порождается любым из двух следующих трёхэлементных множеств

$$\{((54321), \varepsilon), ((1234), \varepsilon), ((12)(345), \varepsilon)\}, \\ \{(\varepsilon, (54321)), (\varepsilon, (1234)), (\varepsilon, (12)(345))\}. \quad (9.5)$$

Множество всех указанных выше арностей  $l$  имеет вид

$$\{9, 49, 89, 129, \dots\} \cup \{31, 71, 111, 151, \dots\}. \quad (9.6)$$

Так как  $((12)(345))^6 = (54321)^5 = \varepsilon$ , то согласно теореме 8.2 ( $r=5$ ),  $l$ -арная группа  $\langle \mathbf{S}_5^2, [ ],_{l,(12),2} \rangle$ , где

$$l = \begin{cases} 60s+11, & s = 0, 1, 2, \dots, \\ -60s-11, & s = -1, -2, \dots, \end{cases}$$

порождается любым из трёхэлементных множеств из (9.5). Множество всех указанных выше арностей  $l$  имеет вид

$$\{11, 71, 131, \dots\} \cup \{49, 109, 169, \dots\}. \quad (9.7)$$

и отличается от (9.6). При этом множества (9.6) и (9.7) имеют непустое пересечение.

Так как равносильные равенства

$$40i+9 = 60s+11, -40i-9 = -60s-11$$

при целых  $i$  и  $s$ , имеющих одинаковые знаки, невозможны, то для нахождения общих элементов множеств (9.6) и (9.7) достаточно найти  $i$  и  $s$ , удовлетворяющие равносильным равенствам

$$40i+9 = -60s-11, -40i-9 = 60s+11,$$

то есть решить диофантово уравнение

$$2i+3s=-1.$$

относительно  $i$  и  $s$ . Так как пара  $(1, -1)$  – частное решение этого уравнения, то

$$(i=3v+1, s=-2v-1)$$

– его общее решение. Таким образом, общие элементы множеств (9.6) и (9.7) находятся по формуле

$$l = \begin{cases} 120v+49, & v = 0, 1, 2, \dots, \\ -120v-49, & v = -1, -2, \dots, \end{cases}$$

Согласно следствию 9.2, при  $k=2$ ,  $t=2$ ,  $\sigma=(12)$   $l$ -арная группа  $\langle \mathbf{S}_5^2, [ ],_{l,(12),2} \rangle$ , где

$$l = \begin{cases} 20t+11, & t = 0, 1, 2, \dots, \\ -20t-11, & t = -1, -2, \dots, \end{cases}$$

порождается любым из двухэлементных множеств

$$\{((1\ 2), \varepsilon), ((1\ 2\ 3\ 4\ 5), \varepsilon)\}, \\ \{(\varepsilon, (1\ 2)), (\varepsilon, (1\ 2\ 3\ 4\ 5))\}.$$

Множество всех указанных выше арностей  $l$  имеет вид

$$\{11, 31, 51, 71, \dots\} \cup \{9, 29, 49, 69, \dots\}. \quad (9.8)$$

Можно заметить, что все арности из (9.6) и (9.7) содержатся в (9.8), но в (9.8) имеются арности, не входящие ни в (9.6), ни в (9.7). Это объясняется тем, что, с одной стороны,

$$20i + 11 = -40t - 9, \quad -20i - 11 = 40t + 9$$

при  $i = -2t - 1$ , а с другой стороны,

$$20i + 11 = 60s + 11, \quad -20i - 11 = -60s - 11$$

при  $i = 3s$ .

Подчеркнём, что полиадические группы  $\langle S_5^2, [ ]_{l, (12), 2} \rangle$  арностей (9.8) порождаются двухэлементными множествами, а полиадические группы  $\langle S_5^2, [ ]_{l, (12), 2} \rangle$  арностей (9.6) и (9.7) порождаются трёхэлементными множествами.

Теорема 8.3 применима в тех случаях, когда группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что  $u^m = v^n = 1$  для некоторых взаимно простых  $m \geq 2$  и  $n \geq 2$ . Если множество  $M$  содержит более двух элементов, то теорему 8.3 можно применять несколько раз, что увеличивает выбор арностей  $l$ , определяемых формулой (8.3). В этом смысле наибольший интерес представляют группы, у которых все элементы порождающего множества имеют разные порядки, любые два из которых являются взаимно простыми.

Так как простая группа Матье  $M_{24}$ , рассматриваемая как группа подстановок, порождается [7] тремя подстановками

$$\begin{aligned} \alpha &= (1\ 2\ 3, \dots\ 23), \\ \beta &= (3\ 17\ 10\ 7\ 9)(5\ 4\ 13\ 14\ 19) \times \\ &\quad \times (11\ 12\ 23\ 8\ 18)(21\ 16\ 15\ 20\ 22), \\ \gamma &= (1\ 24)(2\ 23)(3\ 12)(4\ 16)(5\ 18)(6\ 10) \times \\ &\quad \times (7\ 20)(8\ 14)(9\ 21)(11\ 17)(13\ 22)(19\ 15) \end{aligned}$$

порядков 23, 5 и 2 соответственно, то к ней теорема 8.3 может быть применима трижды.

**Следствие 9.6.** Для любого цикла  $\sigma$  длины  $k$  из  $S_k$   $l$ -арная группа  $\langle M_{24}^k, [ ]_{l, \sigma, k} \rangle$ , где  $l$  принимает любое из перечисленных ниже значений

$$l = \begin{cases} 23(2i+1)k+1, & i = 0, 1, 2, \dots, \\ -2(12+23i)k+1, & i = -1, -2, \dots, \end{cases} \quad (9.9)$$

$$l = \begin{cases} 5(2s+1)k+1, & s = 0, 1, 2, \dots, \\ -2(3+5s)k+1, & s = -1, -2, \dots, \end{cases} \quad (9.10)$$

$$l = \begin{cases} 23(5t-2)k+1, & t = 1, 2, \dots, \\ -5(23t-9)k+1, & t = 0, -1, -2, \dots, \end{cases} \quad (9.11)$$

порождается трёхэлементным множеством

$$\begin{aligned} &\{(\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \alpha, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}), (\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \beta, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j}), \\ &\quad (\underbrace{\varepsilon, \dots, \varepsilon}_{j-1}, \gamma, \underbrace{\varepsilon, \dots, \varepsilon}_{k-j})\gamma\}. \end{aligned}$$

для любого  $j = 1, 2, \dots, k$ .

**Доказательство.** Положив в теореме 9.2, являющейся следствием из теоремы 8.3,  $A = M_{24}$ ,  $a = \gamma$ ,  $b = \alpha$ , получим (9.9).

Положив в теореме 9.2  $A = M_{24}$ ,  $a = \gamma$ ,  $b = \beta$ , получим (9.10).

Положив в теореме 8.3  $A = M_{24}$ ,  $a = \beta$ ,  $b = \alpha$ ,  $m = 5$ ,  $n = 23$ , и, учитывая, что пара  $(-9, 2)$  является решением диофантового уравнения  $5x + 23y = 1$ , получим (9.11). Во всех трёх случаях  $l$ -арная группа  $\langle M_{24}^k, [ ]_{l, \sigma, k} \rangle$  порождается указанным в условии трёхэлементным множеством.  $\square$

**Замечание 9.2.** Значения  $t = 1, 2, \dots$  в (9.11) является следствием неравенства

$$x_0 + nt = -9 + 23t > 0$$

из теоремы 8.3, а значения  $t = 0, -1, -2, \dots$  – следствием неравенства

$$x_0 + nt = -9 + 23t < 0$$

из той же теоремы.

**Замечание 9.3.** При  $k = 2$  формулы (9.9) – (9.11) принимают вид

$$l = \begin{cases} 92i + 47, & i = 0, 1, 2, \dots, \\ -92i - 47, & i = -1, -2, \dots, \end{cases}$$

$$l = \begin{cases} 20s + 11, & s = 0, 1, 2, \dots, \\ -20s - 11, & s = -1, -2, \dots, \end{cases}$$

$$l = \begin{cases} 230t - 91, & t = 1, 2, \dots, \\ -230t + 91, & t = 0, -1, -2, \dots. \end{cases}$$

Для каждой из этих формул укажем некоторые значения  $l$ :

$$\{47, 139, 231, \dots\} \cup \{45, 137, 229, \dots\}, \quad (9.12)$$

$$\{11, 31, 51, 71, \dots\} \cup \{9, 29, 49, 69, \dots\}, \quad (9.13)$$

$$\{139, 369, 599, \dots\} \cup \{91, 321, 551, \dots\}. \quad (9.14)$$

Множества (9.12) и (9.13) имеют непустое пересечение, все элементы которого определяются формулой

$$l = \begin{cases} 460\eta - 231, & \eta = 1, 2, \dots, \\ -460\eta + 231, & \eta = 0, -1, -2, \dots. \end{cases}$$

Имеются общие элементы и у множеств (9.12) и (9.14), все они задаются формулой

$$l = \begin{cases} 460\mu - 139, & \mu = 1, 2, \dots, \\ -460\mu + 139, & \mu = 0, -1, -2, \dots. \end{cases}$$

Аналогично, все общие элементы множеств (9.13) и (9.14) задаются формулой

$$l = \begin{cases} 460v - 369, & v = 1, 2, \dots, \\ -460v + 369, & v = 0, -1, -2, \dots. \end{cases}$$

Общих арностей, принадлежащих множествам (9.12), (9.13) и (9.14), не существует, то есть пересечение трёх указанных множеств пусто.

Следующие две теоремы соответствуют теореме 9.1 для простого числа  $p = 2t + 1$  и теореме 9.2 для  $x_0 = \frac{p+1}{2}$ ,  $y_0 = -1$ .

**Теорема 9.5.** Пусть группа  $A$  порождается множеством  $M$ , в котором имеются элементы

*a и b такие, что  $a^2 = b^p = 1$  для некоторого нечётного простого p,  $\sigma$  – цикл длины k из  $S_k$ ,  $(x_0, y_0)$  – какое-либо решение диофантового уравнения*

$$2x + py = 1.$$

*Тогда l-арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где*

$$l = \begin{cases} p(2i - y_0)k + 1, & \text{если } x_0 + pi > 0, \\ -2(x_0 + pi)k + 1, & \text{если } x_0 + pi < 0, \end{cases}$$

*порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .*

**Теорема 9.6.** *Пусть группа A порождается множеством M, в котором имеются элементы a и b такие, что  $a^2 = b^p = 1$  для некоторого нечётного простого p,  $\sigma$  – цикл длины k из  $S_k$ . Тогда l-арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где*

$$l = \begin{cases} p(2i + 1)k + 1, & i = 0, 1, 2, \dots, \\ -(p + 1 + 2pi)k + 1, & i = -1, -2, \dots, \end{cases}$$

*порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .*

Сформулируем следствие из теоремы 9.6 для  $p = 3$ .

**Следствие 9.7.** *Пусть группа A порождается множеством M, в котором имеются элементы a и b такие, что  $a^2 = b^3 = 1$ ,  $\sigma$  – цикл длины k из  $S_k$ . Тогда l-арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где*

$$l = \begin{cases} 3(2i + 1)k + 1, & i = 0, 1, 2, \dots, \\ -(4 + 6i)k + 1, & i = -1, -2, \dots, \end{cases}$$

*порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .*

Полагая в следствии 9.7  $k = 2$ , получим

**Следствие 9.8.** *Пусть группа A порождается множеством M, в котором имеются*

*элементы a и b такие, что  $a^2 = b^3 = 1$ . Тогда l-арная группа  $\langle A^2, [ ]_{l, (12), 2} \rangle$ , где*

$$l = \begin{cases} 12i + 7, & i = 0, 1, 2, \dots, \\ -12i - 7, & i = -1, -2, \dots, \end{cases}$$

*порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .*

## ЛИТЕРАТУРА

1. Гальмак, А.М. О порождающих множествах l-арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . I / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 2 (47). – С. 69–76.

2. Гальмак, А.М. Порождающие множества l-арной полугруппы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  / А.М. Гальмак // Вестник МДУ им. А.А. Куляшовава. – 2021. – № 1 (57). – С. 35–52.

3. Post, E.L. Polyadic groups / E.L. Post // Trans. Amer. Math. Soc. – 1940. – Vol. 48, № 2. – P. 208–350.

4. Русаков, С.А. Алгебраические n-арные системы / С.А. Русаков. – Минск: Навука і тэхніка, 1992. – 245 с.

5. Коксетер, Г.С.М. Порождающие элементы и определяющие соотношения дискретных групп / Г.С.М. Коксетер, У.О.Дж. Мозер. – Москва: Наука, 1980. – 240 с.

6. Бухштаб, А.А. Теория чисел / А.А. Бухштаб. – Москва: Просвещение, 1966. – 384 с.

7. Горенстейн, Д. Конечные простые группы. Введение в их классификацию / Д. Горенстейн. – Москва: Мир, 1985. – 352 с.

Поступила в редакцию 24.06.2021.