УДК 512.548 DOI: https://doi.org/10.54341/20778708_2021_4_49_76

О ПОРОЖДАЮЩИХ МНОЖЕСТВАХ l-АРНОЙ ГРУППЫ $< A^k, [\ ]_{l,\sigma,k} >$. III

А.М. Гальмак

Белорусский государственный университет пищевых и химических технологий, *Могилёв*

ON SETS OF GENERATORS OF l-ARY GROUP $< A^k, [\ ]_{l,\sigma,k} >$. III

A.M. Gal'mak

Belarusian State University of Food and Chemical Technologies, *Mogilev*

Аннотация. В статье продолжается изучение связи между порождающими множествами группы A и порождающими множествами полиадической группы $< A^k, [\ ]_{l,\sigma,k} >$ 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 σ из множества $\mathbf{S}_k$ всех подстановок множества $\{1, 2, \ldots, k\}$.

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

Для цитирования: *Гальмак*, *А.М.* О порождающих множествах l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$. III / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 4 (49). – С. 76–80. – DOI: https://doi.org/10.54341/20778708_2021_4_49_76

Abstract. The article goes on with the studies on the earlier described relationship between sets of generators in group A and sets of generators in polyadic group $< A^k, [\ ]_{l,\sigma,k} >$ 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 σ from the set $\mathbf{S}_k$ of all substitutions of the set $\{1, 2, \ldots, k\}$.

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

For citation: *Gal'mak*, *A.M.* On sets of generators of l-ary group $< A^k, [\ ]_{l,\sigma,k} >$. III / A.M. Gal'mak // Problems of Physics, Mathematics and Technics. – 2021. – № 4 (49). – P. 76–80. – DOI: https://doi.org/10.54341/20778708_2021_4_49_76 (in Russian)

Введение

Данная статья, посвящённая изучению порождающих множеств l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$, является продолжением статей [1], [2] и составляет с ними единое целое. В связи с этим нумерация разделов в настоящей статье продолжает нумерацию разделов в [2]. Сохраняется преемственность в отношении соглашений, определений и обозначений из [1], [2], все они остаются в силе и в новой статье.

В [1] получен следующий результат (теорема 4.1) для l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$: *пусть группа A порождается множеством M, σ – цикл длины k из $\mathbf{S}_k$, k делит $l - 1$. Тогда для любого $j = 1, 2, \ldots, k$ l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$ порождается множеством $\mathbf{U}_j(M) \cup \{\mathbf{e}\}$, где* $\mathbf{e} = (\underbrace{1, \ldots, 1}_{k})$, *1 – единица группы A.* Аналогичный результат справедлив для l-арной полугруппы $< A^k, [\ ]_{l,\sigma,k} >$.

В [2] найдены условия, позволяющие заменить в указанных выше результатах порождающее множество $\mathbf{U}_j(M) \cup \{\mathbf{e}\}$ порождающим множеством $\mathbf{U}_j(M)$, то есть исключить элемент $\mathbf{e}$ из порождающих множеств как l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$, так и l-арной полугруппы $< A^k, [\ ]_{l,\sigma,k} >$ (теоремы 6.1 и 6.2): *пусть группа* (*полугруппа*) *A порождается множеством M, σ – цикл длины k из $\mathbf{S}_k$, $r \geq 2$, существуют элементы*

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

такие, что

$$u_1u_2 \ldots u_{r+1} = v_1v_2 \ldots, v_r = 1.$$

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

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

10 Обобщение теоремы 8.3

В [2, теорема 8.3] для нахождения полиадических групп вида $< A^k, [\ ]_{l,\sigma,k} >$, которые порождаются множеством $\mathbf{U}_j(M)$, не содержащим элемент $\mathbf{e}$, использовались решения линейного диофантового уравнения с двумя неизвестными. Покажем, что для этих же целей могут быть использованы решения линейного диофантового уравнения

$$n_1x_1 + n_2x_2 + \ldots + n_\nu x_\nu = 1 \qquad (10.1)$$

с числом неизвестных больше двух, которое, как известно (см., например, [5]), для взаимно простых целых коэффициентов $n_1, n_2, \ldots, n_\nu$ имеет бесконечно много решений.

Ясно, что если $(x_1, x_2, \ldots, x_\nu)$ – решение диофантового уравнения (10.1), то в его левой части имеются слагаемые разных знаков.

***Теорема* 10.1**. *Пусть $n_1, n_2, \ldots, n_\nu$ – взаимно простые целые числа, $(x_1, x_2, \ldots, x_\nu)$ – какое-либо* *решение диофантового уравнения* (10.1), $d_1, d_2, \ldots, d_\nu$ *– делители соответственно слагаемых* $n_1x_1, n_2x_2, \ldots, n_\nu x_\nu$, *причём*

$$|d_1| \geq 2,\ |d_2| \geq 2,\ \ldots,\ |d_\nu| \geq 2, \qquad (10.2)$$

σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* $u_1, u_2, \ldots, u_\nu$ *такие, что*

$$u_1^{|d_1|} = u_2^{|d_2|} = \ldots = u_\nu^{|d_\nu|} = 1, \qquad (10.3)$$

то найдётся такое l, *что* l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$ *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Доказательство. Пусть $n_{s_1}x_{s_1}, \ldots, n_{s_\mu}x_{s_\mu}$ – все положительные слагаемые в левой части равенства (10.1), $n_{t_1}x_{t_1}, \ldots, n_{t_\eta}x_{t_\eta}$ – все отрицательные слагаемые в левой части равенства (10.1), где $\mu + \eta = \nu$.

Так как

$$n_1x_1 + n_2x_2 + \ldots + n_\nu x_\nu =$$
$$= (n_{s_1}x_{s_1} + \ldots + n_{s_\mu}x_{s_\mu}) + (n_{t_1}x_{t_1} + \ldots + n_{t_\eta}x_{t_\eta}),$$

то из (10.1) следует

$$n_{s_1}x_{s_1} + \ldots + n_{s_\mu}x_{s_\mu} = -n_{t_1}x_{t_1} - \ldots - n_{t_\eta}x_{t_\eta} + 1 =$$
$$= \left|n_{t_1}x_{t_1}\right| + \ldots + \left|n_{t_\eta}x_{t_\eta}\right| + 1,$$

то есть

$$\left|n_{s_1}x_{s_1}\right| + \ldots + \left|n_{s_\mu}x_{s_\mu}\right| = \left|n_{t_1}x_{t_1}\right| + \ldots + \left|n_{t_\eta}x_{t_\eta}\right| + 1.$$

Из последнего равенства, введя обозначение

$$r = \left|n_{t_1}x_{t_1}\right| + \ldots + \left|n_{t_\eta}x_{t_\eta}\right|,$$

получим

$$r + 1 = \left|n_{s_1}x_{s_1}\right| + \ldots + \left|n_{s_\mu}x_{s_\mu}\right|.$$

Положим

$$u_{s_1 1} = \ldots = u_{s_1|n_{s_1}x_{s_1}|} = u_{s_1},$$
$$u_{s_2 1} = \ldots = u_{s_2|n_{s_2}x_{s_2}|} = u_{s_2},$$
$$\ldots,$$
$$u_{s_\mu 1} = \ldots = u_{s_\mu|n_{s_\mu}x_{s_\mu}|} = u_{s_\mu},$$
$$u_{t_1 1} = \ldots = u_{t_1|n_{t_1}x_{t_1}|} = u_{t_1},$$
$$u_{t_2 1} = \ldots = u_{t_2|n_{t_2}x_{t_2}|} = u_{t_2},$$
$$\ldots,$$
$$u_{t_\eta 1} = \ldots = u_{t_\eta|n_{t_\eta}x_{t_\eta}|} = u_{t_\eta}.$$

Тогда в силу (10.3) и равенств

$$n_{s_1}x_{s_1} = d_{s_1}c_{s_1},\ n_{s_2}x_{s_2} = d_{s_2}c_{s_2},\ \ldots,\ n_{s_\mu}x_{s_\mu} = d_{s_\mu}c_{s_\mu},$$

верных для некоторых целых $c_{s_1}, c_{s_2}, \ldots, c_{s_\mu}$, будем иметь

$$(u_{s_1 1} \ldots u_{s_1|n_{s_1}x_{s_1}|})(u_{s_2 1} \ldots u_{s_2|n_{s_2}x_{s_2}|})$$
$$\ldots$$
$$(u_{s_\mu 1} \ldots u_{s_\mu|n_{s_\mu}x_{s_\mu}|}) = u_{s_1}^{|n_{s_1}x_{s_1}|}u_{s_2}^{|n_{s_2}x_{s_2}|} \ldots u_{s_\mu}^{|n_{s_\mu}x_{s_\mu}|} =$$
$$= u_{s_1}^{|d_{s_1}c_{s_1}|}\, u_{s_2}^{|d_{s_2}c_{s_2}|} \ldots u_{s_\mu}^{|d_{s_\mu}c_{s_\mu}|} =$$
$$= (u_{s_1}^{|d_{s_1}|})^{|c_{s_1}|}\,(u_{s_2}^{|d_{s_2}|})^{|c_{s_2}|} \ldots (u_{s_\mu}^{|d_{s_\mu}|})^{|c_{s_\mu}|} = 1,$$

то есть в порождающем множестве M группы A имеется $r + 1$ элементов

$$u_{s_1 1}, \ldots, u_{s_1|n_{s_1}x_{s_1}|}, \ldots, u_{s_\mu 1}, \ldots, u_{s_\mu|n_{s_\mu}x_{s_\mu}|},$$

произведение которых равно её единице.

Аналогично, так как в ввиду (10.3) и равенств

$$n_{t_1}x_{t_1} = d_{t_1}e_{t_1},\ n_{t_2}x_{t_2} = d_{t_2}e_{t_2},\ \ldots,\ n_{t_\eta}x_{t_\eta} = d_{t_\eta}e_{t_\eta},$$

верных для некоторых целых $e_{s_1}, e_{s_2}, \ldots, e_{s_\eta}$, будем иметь

$$(u_{t_1 1} \ldots u_{t_1|n_{t_1}x_{t_1}|})(u_{t_2 1} \ldots u_{t_2|n_{t_2}x_{t_2}|})$$
$$\ldots$$
$$(u_{t_\eta 1} \ldots u_{t_\eta|n_{t_\eta}x_{t_\eta}|}) = u_{t_1}^{|n_{t_1}x_{t_1}|}\, u_{t_2}^{|n_{t_2}x_{t_2}|} \ldots u_{t_\eta}^{|n_{t_\eta}x_{t_\eta}|} =$$
$$= u_{t_1}^{|d_{t_1}e_{t_1}|}\, u_{t_2}^{|d_{t_2}e_{t_2}|} \ldots u_{t_\eta}^{|d_{t_\eta}e_{t_\eta}|} =$$
$$= (u_{t_1}^{|d_{t_1}|})^{|e_{t_1}|}\,(u_{t_2}^{|d_{t_2}|})^{|e_{t_2}|} \ldots (u_{t_\eta}^{|d_{t_\eta}|})^{|e_{t_\eta}|} = 1,$$

то в порождающем множестве M группы A имеется r элементов

$$u_{t_1 1}, \ldots, u_{t_1|n_{t_1}x_{t_1}|}, \ldots, u_{t_\eta 1}, \ldots, u_{t_\eta|n_{t_\eta}x_{t_\eta}|},$$

произведение которых равно её единице. По теореме 6.1 l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где $l = rk + 1$, порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$. □

Следующий результат получается из теоремы 10.1, если в ней положить

$$d_1 = n_1x_1,\ d_2 = n_2x_2,\ \ldots,\ d_\nu = n_\nu x_\nu.$$

***Теорема* 10.2**. *Пусть* $n_1, n_2, \ldots, n_\nu$ *– взаимно простые целые числа,* $(x_1, x_2, \ldots, x_\nu)$ *– какое-либо решение диофантового уравнения* (10.1), *причём*

$$|n_1x_1| \geq 2,\ |n_2x_2| \geq 2,\ \ldots,\ |n_\nu x_\nu| \geq 2,$$

σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* $u_1, u_2, \ldots, u_\nu$ *такие, что*

$$u_1^{|n_1x_1|} = u_2^{|n_2x_2|} = \ldots = u_\nu^{|n_\nu x_\nu|} = 1,$$

то найдётся такое l, *что* l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$ *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Следующий результат получается из теоремы 10.1, если в ней положить

$$d_1 = n_1,\ d_2 = n_2,\ \ldots,\ d_\nu = n_\nu.$$

***Теорема* 10.3**. *Пусть* $n_1, n_2, \ldots, n_\nu$ *– взаимно простые целые коэффициенты диофантового уравнения* (10.1), *причём*

$$|n_1| \geq 2,\ |n_2| \geq 2,\ \ldots,\ |n_\nu| \geq 2,$$

σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* $u_1, u_2, \ldots, u_\nu$ *такие, что*

$$u_1^{|n_1|} = u_2^{|n_2|} = \ldots = u_\nu^{|n_\nu|} = 1,$$

то найдётся такое l, *что* l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$ *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Для положительных $n_1, n_2, \ldots, n_\nu$ теорема 10.3 принимает следующий вид.

***Теорема* 10.4**. *Пусть* $n_1 \ge 2, n_2 \ge 2, \ldots, n_\nu \ge 2$ – *взаимно простые коэффициенты диофантового уравнения* (10.1), σ – *цикл длины* k *из* $\mathbf{S}_k$. *Если группа A порождается множеством M, в котором имеются элементы* $u_1, u_2, \ldots, u_\nu$ *такие, что*

$$u_1^{n_1} = u_2^{n_2} = \ldots = u_\nu^{n_\nu} = 1,$$

то найдётся такое l, что l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$ *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

***Замечание* 10.1**. В теоремах 10.2–10.4 арность l такая же, как и в теореме 10.1, то есть $l = rk + 1$, где число r определяется тем же равенством, что и в доказательстве теоремы 10.1.

***Замечание* 10.2**. Согласно теоремам 10.1–10.4 каждому решению диофантового уравнения (10.1) ставится в соответствие своя арность. Перебрав все решения уравнения (10.1), мы получим все возможные арности l, соответствующие данному уравнению, для которых l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$ порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

Доказательство следующей теоремы почти дословно повторяет доказательство теоремы 10.1. Только вместо теоремы 6.1 из [2] используется теорема 6.2 из [2].

***Теорема* 10.5**. *Пусть* $n_1, n_2, \ldots, n_\nu$ – *взаимно простые целые числа*, $(x_1, x_2, \ldots, x_\nu)$ – *какое-либо решение диофантового уравнения* (10.1), $d_1, d_2, \ldots, d_\nu$ – *делители соответственно слагаемых* $n_1x_1, n_2x_2, \ldots, n_\nu x_\nu$, *причём*

$$|d_1| \ge 2, |d_2| \ge 2, \ldots, |d_\nu| \ge 2,$$

σ – *цикл длины* k *из* $\mathbf{S}_k$. *Если полугруппа A порождается множеством M, не содержащим её единицу, в котором имеются элементы* $u_1, u_2, \ldots, u_\nu$ *такие, что*

$$u_1^{|d_1|} = u_2^{|d_2|} = \ldots = u_\nu^{|d_\nu|} = 1,$$

то найдётся такое l, что l-арная полугруппа $< A^k, [\ ]_{l,\sigma,k} >$ *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

11 Следствия и примеры

Проиллюстрируем теоремы из раздела 10 примерами.

***Пример* 11.1**. Рассмотрим симметрическую группу $\mathbf{S}_5$ из примера 9.1 из [2], которая порождается [6] тремя подстановками,

(1 2 3 4), (5 4 3 2 1), (1 2)(3 4 5),

имеющими порядки 4, 5 и 6 соответственно.

Так как одним из решений диофантового уравнения

$$4x_1 + 5x_2 + 6x_3 = 1$$

является тройка (– 2, 3, – 1), то по теореме 10.1 имеем

$$r = |n_1x_1| + |n_3x_3| = |4(-2)| + |6(-1)| = 14,$$

соответственно $l = rk + 1 = 14k + 1$. Таким образом, считая в теореме 10.3 или теореме 10.4 $n_1 = 4, n_2 = 5, n_3 = 6$, видим, что $(14k + 1)$-арная группа $< \mathbf{S}_5^k, [\ ]_{14k+1,\sigma,k} >$ порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$, где

M = {(1 2 3 4), (5 4 3 2 1), (1 2)(3 4 5)}.

В частности $(k = 2)$, 29-арная группа $< \mathbf{S}_5^2, [\ ]_{29,(12),2} >$ порождается любым из двух следующих трёхэлементных множеств:

M_1 = {((1 2 3 4),ε), ((5 4 3 2 1), ε), ((1 2)(3 4 5), ε)},
M_2 = {(ε,(1 2 3 4)), (ε, (5 4 3 2 1)), (ε, (1 2)(3 4 5))},
где ε – тождественная подстановка.

***Замечание* 11.1**. В примере 9.1 из [2] указаны арности (9.6) и (9.7) полиадических групп $< \mathbf{S}_5^2, [\ ]_{l,(12),2} >$, которые порождаются этими же трёхэлементными множествами. Заметим, что арности 29 среди этих арностей нет. Это означает, что теоремы 10.3 и 10.4 позволяют находить новые арности, отличные от арностей, существование которые гарантирует теорема 8.2 даже в случае, когда фигурирующие в этих теоремах полиадические группы порождаются одним и тем же множеством.

Можно заметить, что арность 29 содержится среди арностей (9.8) полиадических групп $< \mathbf{S}_5^2, [\ ]_{l,(12),2} >$ из того же примера 9.1, которые порождаются двухэлементными множествами.

***Пример* 11.2**. В следствии 9.6 из [2] для группы Матье $\mathbf{M}_{24}$, порождаемой трёхэлементным множеством M, состоящим из подстановок γ, β и α порядков 2, 5 и 23 соответственно [7], указаны арности (9.9) – (9.11) полиадических групп $< \mathbf{M}_{24}^k, [\ ]_{l,\sigma,k} >$, которые порождаются трёхэлементным множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

При $k = 2$ формулы (9.9)–(9.11) принимают вид (9.12)–(9.14).

Так как одним из решений диофантового уравнения

$$2x_1 + 5x_2 + 23x_3 = 1$$

является тройка (– 6, – 2, 1), то по теореме 10.3 или по теореме 10.4 имеем

$$r = |n_1x_1| + |n_2x_2| = |2(-6)| + |5(-2)| = 22,$$

соответственно $l = rk + 1 = 22k + 1$. Таким образом, согласно теореме 10.3 или теореме 10.4, $(22k + 1)$-арная группа $< \mathbf{M}_{24}^k, [\ ]_{22k+1,\sigma,k} >$ порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

В частности $(k = 2)$, 45-арная группа $< \mathbf{M}_{24}^2, [\ ]_{45,(12),2} >$ порождается любым из двух следующих трёхэлементных множеств $\mathbf{U}_1(M)$ и $\mathbf{U}_2(M)$: {(α, ε), (β, ε), (γ, ε)}, {(ε, α), (ε, β), (ε, γ)}.

Заметим, что арность 45 содержится среди арностей (9.12).

Так как (9, – 8, 1) – ещё одно решение диофантового уравнения

$$2x_1 + 5x_2 + 23x_3 = 1,$$

то согласно теореме 10.3 или теореме 10.4, имеем

$$r = |n_2x_2| = |5(-8)| = 40,$$

соответственно $l = rk + 1 = 40k + 1$. Таким образом, согласно теореме 10.3 или теореме 10.4, $(40k + 1)$-арная группа $< \mathbf{M}^k_{24}, [\ ]_{40k+1,\sigma,k} >$ порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

В частности ($k = 2$), 81-арная группа $< \mathbf{M}^2_{24}, [\ ]_{81,(12),2} >$ порождается любым из двух указанных выше трёхэлементных множеств $\mathbf{U}_1(M)$ и $\mathbf{U}_2(M)$.

Заметим, что арности 81 среди арностей (9.12)–(9.14) нет.

При $\nu = 2$ уравнения (10.1) принимает вид

$$mx + ny = 1, \qquad (11.1)$$

где m и n взаимно простые целые числа. Если (x_0, y_0) – одно из решений этого уравнения, то множество всех его решений имеет вид

$$\{(x_0 + ni, y_0 - mi) \mid i \in \mathbf{Z}\}. \qquad (11.2)$$

Ясно, что в левой части (11.1) одно из слагаемых является положительным, а другое – отрицательным.

При $\nu = 2$ теоремы 10.1–10.4 могут быть сформулированы в виде следующих следствий.

***Следствие* 11.1**. *Пусть m и n – взаимно простые целые числа, (x, y) – какое-либо решение диофантового уравнения* (11.1), *d и c – делители соответственно слагаемых mx и ny, причём, $|d| \geq 2$, $|c| \geq 2$, σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^{|d|} = v^{|c|} = 1,$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где

$$l = \begin{cases} -nyk + 1, \text{ если } mx > 0, \\ -mxk + 1, \text{ если } mx < 0, \end{cases} \qquad (11.3)$$

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

***Следствие* 11.2**. *Пусть m и n – взаимно простые целые числа, (x, y) – какое-либо решение диофантового уравнения* (11.1), *причём $|mx| \geq 2$, $|ny| \geq 2$, σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^{|mx|} = v^{|ny|} = 1,$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где арность l определяется формулой (11.3), *порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.*

***Следствие* 11.3**. *Пусть m и n – взаимно простые целые числа, (x, y) – какое-либо решение диофантового уравнения* (11.1), *причём $|m| \geq 2$, $|n| \geq 2$, σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^{|m|} = v^{|n|} = 1,$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где арность l определяется формулой (11.3), *порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.*

***Следствие* 11.4**. *Пусть $m \geq 2$ и $n \geq 2$ – взаимно простые, (x, y) – какое-либо решение диофантового уравнения* (11.1), *σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^m = v^n = 1,$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где

$$l = \begin{cases} -nyk + 1, \text{ если } x > 0, \\ -mxk + 1, \text{ если } x < 0, \end{cases} \qquad (11.4)$$

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

Подставив в (11.4) решение (11.2), получим теорему 8.3 из [2].

Для l-арной полугруппы $< A^k, [\ ]_{l,\sigma,k} >$ можно сформулировать результаты, аналогичные следствиям 11.1–11.4. Для этого достаточно в указанных следствиях группу заменить полугруппой, а l-арную группу – l-арной полугруппой.

12 Применение теорем 6.3 и 6.5

Применим теоремы 6.3 и 6.5 из [2] для получения новых результатов о полиадических группах вида $< A^k, [\ ]_{l,\sigma,k} >$, которые порождаются множеством $\mathbf{U}_j(M)$, не содержащим элемент $\mathbf{e}$.

***Теорема* 12.1**. *Пусть $a \geq 2$ и $n \geq 2$ – натуральные числа, d – делитель числа a^n, m – делитель числа $a^n - 1$, σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^d = v^m = 1, \qquad (12.1)$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где $l = (a^n - 1)k + 1$, порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

Доказательство. Положим $r = a^n - 1$, тогда $r + 1 = a^n$. Так как m делит $a^n - 1$, то $a^n - 1 = mc$ для некоторого натурального c. Кроме того, по условию $a^n = de$ для некоторого натурального e.

Так как ввиду (12.1),

$$u^{r+1} = u^{a^n} = u^{de} = (u^d)^e = 1,$$

$$v^r = v^{a^n - 1} = v^{mc} = (v^m)^c = 1,$$

то по теореме 6.3 из [2] l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где $l = (a^n - 1)k + 1$, порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$. □

Так как

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + a + 1),$$

то в качестве делителя m числа $a^n - 1$ в теореме 12.1 можно взять произведение $m = m_1 m_2$, где m_1 и m_2 – делители чисел $a - 1$ и

$$a^{n-1} + a^{n-2} + \ldots + a + 1$$

соответственно.

Полагая в теореме 12.1 $m = a - 1$, получим

***Следствие* 12.1**. *Пусть $a \geq 2$ и $n \geq 2$ – натуральные числа, d – делитель числа a^n, σ – цикл длины k из $\mathbf{S}_k$. Если группа A порождается множеством M, в котором имеются элементы u и v такие, что*

$$u^d = v^{a-1} = 1,$$

то l-арная группа $< A^k, [\ ]_{l,\sigma,k} >$, где $l = (a^n - 1)k + 1$, порождается множеством $\mathbf{U}_j(M)$ для любого $j = 1, 2, \ldots, k$.

Так как при чётном $n = 2t$ верно разложение

$$a^{2t} - 1 = (a + 1)(a^{2t-1} - a^{2t-2} + \ldots + a - 1),$$

то в качестве делителя m числа $a^n - 1$, в теореме 12.1 ($n = 2t$) можно взять произведение $m = m_1m_2$, где m_1 и m_2 – делители чисел $a + 1$ и

$$a^{2t-1} - a^{2t-2} + \ldots + a - 1$$

соответственно. В частности, для $m_1 = a + 1$, $m_2 = a - 1$ имеем $m = a^2 - 1$.

В следующем следствии из теоремы 12.1 $n = 2t$, $m_2 = 1$, $m = m_1 = a + 1$.

***Следствие* 12.2**. *Пусть* $a \geq 2$ *и* t *– натуральные числа*, d *– делитель числа* a^{2t}, σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^d = v^{a+1} = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где* $l = (a^{2t} - 1)k + 1$, *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Так как для нечётного натурального $b \geq 3$ число $b + 2$ делит $(b + 1)^{b-1} - 1$, то, полагая в теореме 12.1 $a = d = b + 1$, $m = b + 2$, $n = b - 1$, получим

***Следствие* 12.3**. *Пусть* b *– нечётное*, σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^{b+1} = v^{b+2} = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где*

$$l = ((b + 1)^{b-1} - 1)k + 1,$$

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

Следующая теорема может быть получена из теоремы 6.5 из [2], если в ней положить $r = a^{2t+1}$.

***Теорема* 12.2**. *Пусть* $a \geq 2$ *и* t *– натуральные числа*, d *– делитель числа* $a^{2t+1} + 1$, m *– делитель числа* a^{2t+1}, σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^d = v^m = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где* $l = a^{2t+1}k + 1$, *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Так как

$$a^{2t+1} + 1 = (a + 1)(a^{2t} - a^{2t-1} + \ldots + a^2 - a + 1),$$

то в качестве делителя d числа $a^{2t+1} + 1$ в теореме 12.2 можно взять произведение $d = d_1d_2$, где d_1 и d_2 – делители чисел $a + 1$ и

$$a^{2t} - a^{2t-1} + \ldots + a^2 - a + 1$$

соответственно.

Полагая в теореме 12.2 $d = a + 1$, получим

***Следствие* 12.4**. *Пусть* $a \geq 2$ *и* t *– натуральные числа*, m *– делитель числа* a^{2t+1}, σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^{a+1} = v^m = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где* $l = a^{2t+1}k + 1$, *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

Полагая в следствии 12.4 $a = m = b - 1$, $2t + 1 = b \geq 3$, получим

***Следствие* 12.5**. *Пусть* $b \geq 3$ *– нечётное число*, σ *– цикл длины* k *из* $\mathbf{S}_k$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^b = v^{b-1} = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где* $l = (b - 1)^b k + 1$, *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$.

В следствии 12.5 арность l может делиться на b. Для этого достаточно в этом следствии положить $k = (b - 1)^{2s}$, где $s \geq 1$. В этом случае $l = (b - 1)^{b+2s} + 1$, при этом нечётное b делит l. В частности, если $s = 1$, то $k = (b - 1)^2$, $l = (b - 1)^{b+2} + 1$. Таким образом, из следствия 12.5 вытекает

***Следствие* 12.6**. *Пусть* $b \geq 3$ *– нечётное число*, σ *– цикл длины* k *из* $\mathbf{S}_k$, *где* $k = (b - 1)^{2s}$, $s \geq 1$. *Если группа* A *порождается множеством* M, *в котором имеются элементы* u *и* v *такие*, *что*

$$u^b = v^{b-1} = 1,$$

то l*-арная группа* $< A^k, [\ ]_{l,\sigma,k} >$, *где* $l = (b - 1)^{b+2s} + 1$, *порождается множеством* $\mathbf{U}_j(M)$ *для любого* $j = 1, 2, \ldots, k$, *при этом* b *делит* l.

ЛИТЕРАТУРА

1. *Гальмак*, *А.М.* О порождающих множествах l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$. I / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 2 (47). – С. 69–78.
2. *Гальмак*, *А.М.* О порождающих множествах l-арной группы $< A^k, [\ ]_{l,\sigma,k} >$. II / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 3 (48). – С. 63–72.
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. *Бухштаб*, *А.А.* Теория чисел / А.А. Бухштаб. – Москва: Просвещение, 1966. – 384 с.
6. *Коксетер*, *Г.С.М.* Порождающие элементы и определяющие соотношения дискретных групп / Г.С.М. Коксетер, У.О.Дж. Мозер. – Москва: Наука, 1980. – 240 с.
7. *Горенстейн*, *Д.* Конечные простые группы. Введение в их классификацию / Д. Горенстейн. – Москва: Мир, 1985. – 352 с.

Поступила в редакцию 09.10.2021.

Информация об авторах

Гальмак Александр Михайлович – д.ф.-м.н., профессор