

УДК 512.548

DOI: [https://doi.org/10.54341/20778708\\_2022\\_1\\_50\\_55](https://doi.org/10.54341/20778708_2022_1_50_55)О ПОРОЖДАЮЩИХ МНОЖЕСТВАХ  $l$ -АРНОЙ ГРУППЫ  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . IV

А.М. Гальмак

*Белорусский государственный университет пищевых и химических технологий, Могилёв*ON SETS OF GENERATORS OF  $l$ -ARY GROUP  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . IV

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  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  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.

**Для цитирования:** Гальмак, А.М. О порождающих множествах  $l$ -арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . IV / А.М. Гальмак // Проблемы физики, математики и техники. – 2022. – № 1 (50). – С. 55–61. – DOI: [https://doi.org/10.54341/20778708\\_2022\\_1\\_50\\_55](https://doi.org/10.54341/20778708_2022_1_50_55)

**Abstract.** 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.

**For citation:** Gal'mak, A.M. On sets of generators of  $l$ -ary group  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . IV / Relativistic partial Green's functions of scattering states characterized by orbital quantum number  $l=1$  / А.М. Gal'mak // Problems of Physics, Mathematics and Technics. – 2022. – № 1 (50). – P. 55–61. – DOI: [https://doi.org/10.54341/20778708\\_2022\\_1\\_50\\_55](https://doi.org/10.54341/20778708_2022_1_50_55) (in Russian)

**Введение**

В данной статье продолжается изучение порождающих множеств  $l$ -арной группы  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , начатое в [1]–[3]. Поэтому в ней продолжена нумерация разделов, использовавшаяся в указанных статьях.

В [2], [3] для нахождения полиадических групп вида  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , которые порождаются множеством  $U_j(M)$ , не содержащим элемент  $e$ , были использованы линейные диофантовы уравнения со взаимно простыми коэффициентами. В данной статье показано, что для этих же целей могут быть использованы и некоторые другие результаты из теории чисел, в частности, теоремы Эйлера и Вильсона.

Как и прежде, всю необходимую информацию из теории полиадических групп можно найти в [4], [5].

**13 Порождающие и теорема Эйлера**

В этом разделе для нахождения полиадических групп вида  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , которые порождаются множеством  $U_j(M)$ , не содержащим элемент  $e$ , применяется теорема Эйлера, утверждающая, что для любых взаимно простых натуральных чисел  $a$  и  $m$  разность  $a^{\varphi(m)} - 1$ , где  $\varphi(m)$  – функция Эйлера, делится на  $m$ .

**Теорема 13.1.** Пусть  $a \geq 2$  и  $m \geq 2$  – взаимно простые натуральные числа,  $d$  – делитель числа  $a^{\varphi(m)}$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^d = v^m = 1, \quad (13.1)$$

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

**Доказательство.** Положим  $r = a^{\varphi(m)} - 1$ , тогда  $r + 1 = a^{\varphi(m)}$ . Так как по теореме Эйлера  $m$  делит  $a^{\varphi(m)} - 1$ , то  $a^{\varphi(m)} - 1 = mq$  для некоторого натурального  $q$ . Кроме того, по условию  $a^{\varphi(m)} = de$  для некоторого натурального  $e$ .

Так как ввиду (13.1),

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

$$v^r = v^{a^{\varphi(m)} - 1} = v^{mq} = (v^m)^q = 1,$$

то по теореме 6.3 из [2]  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где  $l = (a^{\varphi(m)} - 1)k + 1$ , порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .  $\square$

Заметим, что теорема 13.1 может быть получена как следствие теоремы 6.5 из [2] при  $c = m$  и теоремы Эйлера.

**Замечание 13.1.** В теореме 13.1 функцию Эйлера  $\varphi(m)$  можно заменить обобщённой функцией Эйлера  $L(m)$  или функцией Люка  $l(m)$ , для

каждой из которых справедлив аналог теоремы Эйлера [6].

Следующий результат получается из теоремы 13.1, если в ней положить  $d = a^{\varphi(m)}$ .

**Следствие 13.1.** Пусть  $a \geq 2$  и  $m \geq 2$  – взаимно простые натуральные числа,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^{a^{\varphi(m)}} = v^m = 1,$$

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

Следующий результат получается из теоремы 13.1, если в ней положить  $d = a$ .

**Следствие 13.2.** Пусть  $a \geq 2$  и  $m \geq 2$  – взаимно простые натуральные числа,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Полагая в теореме 13.1 и следствиях 13.1–13.2  $m = p$  – простое, получим следующие результаты. Эти же результаты можно получить, воспользовавшись малой теоремой Ферма.

**Теорема 13.2.** Пусть простое  $p$  не делит натуральное  $a \geq 2$ ,  $d$  – делитель числа  $a^{p-1}$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Заметим, что теорема 13.2 может быть получена как следствие теоремы 6.5 из [2] и малой теоремы Ферма.

Полагая в теореме 13.2  $d = a^{p-1}$ , получим

**Следствие 13.3.** Пусть простое  $p$  не делит натуральное  $a \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Полагая в теореме 13.2  $d = a$ , получим

**Следствие 13.4.** Пусть простое  $p$  не делит натуральное  $a \geq 2$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^a = v^p = 1,$$

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

**Пример 13.1.** Пусть как в примере 11.1 из [3],  $S_5$  – симметрическая группа, порождаемая тремя подстановками, имеющими порядки 4, 5 и 6 соответственно.

Полагая в следствии 13.4,  $A = S_5$ ,  $p = 5$ ,  $a = 4$ , получим

$$l = (4^4 - 1)k + 1 = 255k + 1,$$

при этом  $(255k + 1)$ -арная группа  $\langle S_5^k, [ ]_{255k+1, \sigma, k} \rangle$  порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ , где  $M$  такое же, как в примере 11.1 из [3].

В частности ( $k = 2$ ), 511-арная группа  $\langle S_5^2, [ ]_{511, (12), 2} \rangle$  порождается любым из двух множеств  $M_1, M_2$  из примера 11.1 из [3].

Если  $p$  оставить прежним, а вместо  $a = 4$  взять  $a = 6$ , то получим

$$l = (6^4 - 1)k + 1 = 1295k + 1,$$

при этом  $(1295k + 1)$ -арная группа  $\langle S_5^k, [ ]_{1295k+1, \sigma, k} \rangle$  порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ , где  $M$  такое же, как в примере 11.1 из [3].

В частности, 2591-арная группа  $\langle S_5^2, [ ]_{2591, (12), 2} \rangle$  порождается любым из двух множеств  $M_1, M_2$  из примера 11.1 из [3].

**Замечание 13.2.** Так как  $511 = -40 \cdot (-13) - 9$ , то арность 511, полученная в предыдущем примере для  $k = 2$  с помощью малой теоремы Ферма (следствие 13.4), содержится среди арностей (9.6) из примера 9.1 из [2], для получения которых для  $k = 2$  использовались решения линейного диофантового уравнения с двумя неизвестными (теорема 8.2 из [2]). Аналогично, так как  $2591 = -40 \cdot (-65) - 9$ , то арность 2591, из предыдущего примера также содержится среди арностей (9.6) из примера 9.1 из [2]. Так как все арности из (9.6) содержатся в (9.8), то арности 511 и 2591 содержатся и в (9.8).

Полагая в следствии 13.4  $a = p + 1$ , получим

**Следствие 13.5.** Пусть  $p$  – простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^{p+1} = v^p = 1,$$

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

$$l = ((p + 1)^{p-1} - 1)k + 1, \quad (13.2)$$

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

Следующий, похожий на следствие 13.5 результат, вытекает из теоремы 8.2 из [2] при  $a = u$ ,  $b = v$ ,  $r = p$ , где  $p \geq 2$  – простое.

**Следствие 13.6.** Пусть  $p$  – простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^{p+1} = v^p = 1,$$

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

$$l = \begin{cases} p((p+1)i+1)k+1, & i = 0, 1, 2, \dots, \\ -(p+1)(1+pi)k+1, & i = -1, -2, \dots, \end{cases} \quad (13.3)$$

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

Равенство (13.2) из следствия 13.5 для данных  $p$  и  $k$  определяет на декартовой степени  $A^k$  с помощью цикла  $\sigma$  единственную арность, а равенство (13.3) из следствия 13.6 для тех же  $p$  и  $k$  на декартовой степени  $A^k$  с помощью того же цикла  $\sigma$  определяет бесконечно много арностей. Так как элементы  $u$  и  $v$  в следствиях 13.5 и 13.6 удовлетворяют одним и тем же равенствам, то возникает естественный вопрос: не содержатся ли арности (13.2) в (13.3)?

Ответ на этот вопрос даёт следующее предложение.

**Предложение 13.1.** Множество всех  $l$ -арных групп, определяемых следствием 13.5, входит во множество всех  $l$ -арных групп, определяемых следствием 13.6.

*Доказательство.* Так как  $p$  делит  $(p+1)^{p-2} - 1$ , то

$$i = \frac{1}{p} ((p+1)^{p-2} - 1) \quad (13.4)$$

– целое число. Тогда

$$p((p+1)i+1) = p(p+1) \frac{1}{p} ((p+1)^{p-2} - 1) + 1 =$$

$$= p(p+1) \frac{1}{p} ((p+1)^{p-2} - 1) + p =$$

$$= (p+1)^{p-1} - p - 1 + p = (p+1)^{p-1} - 1,$$

то есть

$$(p+1)^{p-1} - 1 = p((p+1)i+1),$$

откуда следует

$$((p+1)^{p-1} - 1)k + 1 = p((p+1)i+1)k + 1,$$

где  $i$  определяется равенством (13.4). В полученном равенстве левая часть совпадает с правой частью равенства (13.2), а правая часть – с правой частью равенства (13.3) при  $i > 0$ , вычисляемом по формуле (13.4).  $\square$

**Замечание 13.3.** При доказательстве предложения 13.1 установлено, что арности  $l$ , определяемые равенствами (13.2) и (13.3) совпадают при  $i$ , вычисляемом по формуле (13.4). Например, для  $p = 2, 3, 5, 7$  соответственно имеем  $i = 0, 1, 43, 4681$ , а соответствующие арности имеют вид

$$2k + 1, 15k + 1, 1295k + 1, 262143k + 1,$$

которые при  $k = 2$  равны соответственно

$$5, 31, 2591, 524287.$$

Полагая в следствии 13.4  $a = p - 1$ , получим

**Следствие 13.7.** Пусть  $p$  – нечётное простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

$$l = ((p-1)^{p-1} - 1)k + 1, \quad (13.5)$$

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

Следующий, похожий на следствие 13.7 результат, вытекает из теоремы 8.2 из [2] при  $a = v$ ,  $b = u$ ,  $r = p - 1$ , где  $p \geq 3$  – простое.

**Следствие 13.8.** Пусть  $p$  – нечётное простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

$$l = \begin{cases} (p-1)(pi+1)k+1, & i = 0, 1, 2, \dots, \\ -p(1+(p-1)i)k+1, & i = -1, -2, \dots, \end{cases} \quad (13.6)$$

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

Так как элементы  $u$  и  $v$  в следствиях 13.7 и 13.8 удовлетворяют одним и тем же равенствам, то возникает естественный вопрос: не содержатся ли арности (13.5) в (13.6)?

Ответ на этот вопрос даёт следующее предложение.

**Предложение 13.2.** Множество всех  $l$ -арных групп, определяемых следствием 13.7, входит во множество всех  $l$ -арных групп, определяемых следствием 13.8.

*Доказательство.* Так как  $p - 2$  – нечётное, то  $p$  делит  $(p-1)^{p-2} + 1$ , то есть

$$i = -\frac{1}{p} ((p-1)^{p-2} + 1) \quad (13.7)$$

– целое число. Тогда

$$-p(1+(p-1)i) =$$

$$= -p(1 - \frac{1}{p} ((p-1)^{p-2} + 1)(p-1)) =$$

$$= -p + ((p-1)^{p-2} + 1)(p-1) =$$

$$= -p + (p-1)^{p-1} + p - 1 = (p-1)^{p-1} - 1,$$

то есть

$$(p-1)^{p-1} - 1 = -p(1+(p-1)i),$$

откуда следует

$$((p-1)^{p-1} - 1)k + 1 = -p(1+(p-1)i)k + 1,$$

где  $i$  определяется равенством (13.7). В полученном равенстве левая часть совпадает с правой частью равенства (13.5), а правая часть – с правой частью равенства (13.6) при  $i < 0$ , вычисляемом по формуле (13.7).  $\square$

**Замечание 13.4.** При доказательстве предложения 13.2 установлено, что арности  $l$ , определяемые равенствами (13.5) и (13.6) совпадают при  $i$ , вычисляемом по формуле (13.7). Например, для  $p = 3, 5, 7, 11$  соответственно имеем  $i = -1, -13, -1111, -90909091$ , а соответствующие арности имеют вид

$$3k + 1, 255k + 1, 46655k + 1, 9999999999k + 1,$$

которые при  $k = 2$  равны соответственно

$$7, 511, 93310, 19999999999.$$

Напомним, что натуральное число  $n$  называют псевдопростым по натуральному основанию  $a$ , если  $n$  делит  $a^{n-1} - 1$ .

Для псевдопростых чисел можно сформулировать аналог теоремы 13.2, доказательство

которого аналогично доказательству теоремы 13.1.

**Теорема 13.3.** Пусть  $n$  – псевдопростое число по основанию  $a$ ,  $d$  – делитель числа  $a^{n-1}$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Следующий результат получается из теоремы 13.3, если в ней положить  $d = a^{n-1}$ .

**Следствие 13.9.** Пусть  $n$  – псевдопростое число по основанию  $a$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Следующий результат получается из теоремы 13.3, если в ней положить  $d = a$ .

**Следствие 13.10.** Пусть  $n$  – псевдопростое число по основанию  $a$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Следствия 13.9 и 13.10 можно рассматривать как аналоги следствий 13.3 и 13.4.

Напомним, что число  $n$  называют числом Кармайкла, если оно псевдопростое по любому основанию  $a$ , взаимно простому с  $n$ , то есть, если  $n$  делит  $a^{n-1} - 1$  для любого  $a$  такого, что  $(n, a) = 1$ .

Следующая теорема может быть доказана аналогично предыдущей теореме, а может рассматриваться как её следствие.

**Теорема 13.4.** Пусть  $n$  – число Кармайкла,  $a$  – взаимно простое с ним число,  $d$  – делитель числа  $a^{n-1}$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Можно сформулировать следствия из теоремы 13.4, аналогичные следствиям 13.9 и 13.10.

#### 14 Порождающие и теорема Вильсона

В доказательстве следующей теоремы будет использована теорема Вильсона, утверждающая, что любое простое  $p$  делит  $(p-1)! + 1$ .

**Теорема 14.1.** Пусть  $p$  – нечётное простое,  $d \geq 2$  – делитель числа  $(p-1)!$ ,  $\sigma$  – цикл длины  $k$

из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^d = 1, \tag{14.1}$$

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

**Доказательство.** Положим  $r = (p-1)!$ , тогда  $r + 1 = (p-1)! + 1$ . Так как по теореме Вильсона  $p$  делит  $(p-1)! + 1$ , то  $(p-1)! + 1 = pq$  для некоторого натурального  $q$ . Кроме того, по условию  $(p-1)! = de$  для некоторого натурального  $e$ .

Ввиду (14.1),

$$u^{r+1} = u^{(p-1)!+1} = u^{pq} = (u^p)^q = 1, \\ v^r = v^{(p-1)!} = v^{de} = (v^d)^e = 1,$$

то есть верно равенство  $u^{r+1} = v^r = 1$  из теоремы 6.3 из [2], согласно которой  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , где  $l = (p-1)!k + 1$ , порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .  $\square$

Заметим, что теорема 14.1 может быть получена как следствие теоремы 6.5 из [2] и теоремы Вильсона.

Следующий результат получается из теоремы 14.1, если в ней положить  $d = (p-1)!$ .

**Следствие 14.1.** Пусть  $p$  – нечётное простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^{(p-1)!} = 1,$$

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

Если в теореме 14.1 положить  $d = 2$ , то получим

**Следствие 14.2.** Пусть  $p$  – нечётное простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^2 = 1,$$

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

Если в теореме 14.1 положить  $d = p-1$ , то получим

**Следствие 14.3.** Пусть  $p$  – нечётное простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Равенство (14.2) из следствия 14.3 для каждого  $k$  на декартовой степени  $A^k$  с помощью цикла  $\sigma$  определяет единственную арность, а равенство (13.6) из следствия 13.8 для каждого  $k$  на

той же декартовой степени  $A^k$  с помощью того же цикла  $\sigma$  определяет бесконечно много арностей. Возникает естественный вопрос: не содержатся ли арности (14.2) в (13.6)?

Положительный ответ на этот вопрос даёт следующее предложение.

**Предложение 14.1.** Множество всех  $l$ -арных групп, определяемых следствием 14.4, входит во множество всех  $l$ -арных групп, определяемых следствием 13.8.

*Доказательство.* По теореме Лейбница, являющейся следствием теоремы Вильсона, любое нечётное простое  $p$  делит  $(p-2)! - 1$ , то есть

$$i = \frac{1}{p}((p-2)! - 1). \quad (14.3)$$

– целое число. Тогда

$$pi + 1 = p \frac{1}{p}((p-2)! - 1) + 1 = (p-2)!,$$

то есть  $(p-2)! = pi + 1$ ,

откуда последовательно получаем

$$(p-2)!(p-1) = (p-1)(pi + 1),$$

$$(p-1)! = (p-1)(pi + 1),$$

$$(p-1)!k + 1 = (p-1)(pi + 1)k + 1,$$

где  $i$  определяется равенством (14.3). В полученном равенстве левая часть совпадает с правой частью равенства (14.2), а правая часть – с правой частью равенства (13.6) при  $i > 0$ , которое определяется равенством (14.3).  $\square$

**Замечание 14.1.** При доказательстве предложения 14.1 установлено, что арности  $l$ , определяемые равенствами (14.2) и (13.6) совпадают при  $i$ , вычисляемом по формуле (14.3). Например, для  $p = 3, 5, 7, 11$  соответственно имеем  $i = 0, 1, 17, 32989$ , а соответствующие арности имеют вид

$$2k + 1, 24k + 1, 720k + 1, 3628800k + 1,$$

которые при  $k = 2$  равны соответственно

$$5, 49, 1441, 7257601.$$

**Замечание 14.2.** В замечаниях 13.3 и 14.1 имеется общая арность  $2k + 1$ , которая определяется равенством (13.2) при  $p = 2$  и равенством (14.2) при  $p = 3$ . В связи с этим возникает естественный вопрос: имеются ли другие общие арности, определяемые равенствами (13.2) и (14.2), отличные от  $2k + 1$ .

Для ответа на этот вопрос сравним правую часть

$$((p+1)^{p-1} - 1)k + 1$$

равенства (13.2) и правую часть

$$(q-1)!k + 1$$

равенства (14.2), где  $p = q$  – простое.

Так как число  $(p+1)^{p-1} - 1$  – нечётное, а при  $q \geq 3$  число  $(q-1)!$  – чётное, то указанная выше арность  $2k + 1$  – единственная общая арность, определяемая равенствами (13.2) и (14.2). Другими словами,  $(2k+1)$ -арная группа  $\langle A^k, [ ]_{2k+1, \sigma, k} \rangle$  – единственная общая полиадическая группа, определяемая следствиями 13.5 и 14.3.

**Замечание 14.3.** Для ответа на вопрос:

имеются ли общие арности, определяемые равенствами (13.5) и (14.2), сравним правую часть

$$((p-1)^{p-1} - 1)k + 1$$

равенства (13.5) и правую часть

$$(q-1)!k + 1$$

равенства (14.2), где  $p = q$  – простое.

Так как для  $p \geq 3$  и  $q \geq 3$  число  $(p-1)^{p-1} - 1$  является нечётным, а число  $(q-1)!$  – чётным, то

$$((p-1)^{p-1} - 1)k + 1 \neq (q-1)!k + 1.$$

Следовательно, множество всех полиадических групп, определяемых следствием 13.7 и множество всех полиадических групп, определяемых следствием 14.3, не пересекаются.

Доказательство следующей теоремы аналогично доказательству теоремы 14.1, в котором теорема Вильсона заменяется теоремой Лейбница.

**Теорема 14.2.** Пусть  $p \geq 5$  – простое,  $d \geq 2$  – делитель числа  $(p-2)!$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

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

Заметим, что теорема 14.2 может быть получена как следствие теоремы 6.5 из [2] и теоремы Лейбница.

Для теоремы 14.2 можно сформулировать результаты, аналогичные следствиям 14.1–14.3. Ограничимся следствиями для  $d = p - 2$  и  $d = 2$ .

**Следствие 14.4.** Пусть  $p \geq 5$  – простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^{p-2} = v^p = 1,$$

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

**Следствие 14.5.** Пусть  $p \geq 5$  – простое,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^2 = v^p = 1,$$

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

**Замечание 14.4.** В следствии 14.4 возможен случай, когда  $p - 2$  и  $p$  – простые числа близнецы.

**Замечание 14.5.** Что можно сказать об арностях

$$(p-1)!k + 1, ((p-2)! - 1)k + 1$$

полиадических групп, фигурирующих в теоремах 14.1 и 14.2?

Если предположить наличие общей арности, то

$$(p-1)!k + 1 = ((q-2)! - 1)k + 1$$

для некоторых простых  $p \geq 3$  и  $q \geq 5, p \neq q$ , откуда

$$(p-1)! = (q-2)! - 1, \\ (q-2)! - (p-1)! = 1,$$

то есть  $m! - n! = 1$ , где

$$p-1 = n \geq 2, q-2 = m \geq 3.$$

При указанных  $m$  и  $n$  полученное равенство неверно, так как для них верно неравенство  $m! - n! > 2$ .

Следовательно, множество всех полиадических групп, определяемых теоремой 14.1 и множество всех полиадических групп, определяемых теоремой 14.2, не пересекаются.

### 15 Дальнейшие следствия

Перечень приведённых в предыдущих разделах примеров и следствий из полученных там результатов для полиадических групп вида  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , которые порождаются множеством  $U_j(M)$ , не содержащим элемент  $e$ , можно расширить.

Покажем, например, что арности указанных полиадических групп могут быть простыми числами Мерсенна.

**Пример 15.1.** Пусть  $p$  – нечётное простое, для которого  $2^p - 1$  – простое число, то есть  $2^p - 1$  – простое число Мерсенна. Пусть, кроме того, группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^2 = v^p = 1.$$

Тогда, полагая в следствии 13.4  $a = k = 2$ , получим

$$l = (2^{p-1} - 1)2 + 1 = 2^p - 1.$$

Следовательно,  $l$ -арная группа  $\langle A^2, [ ]_{l, (12), 2} \rangle$ , где  $l = 2^p - 1$  – простое число Мерсенна, порождается любым из множеств  $U_1(M), U_2(M)$ .

Следующая теорема получается из теоремы 6.5 из [2], если в ней положить  $r = k = F_m - 1$ , где  $F_m = 2^{2^m} + 1$  – число Ферма.

**Теорема 15.1.** Пусть  $d > 1$  – делитель числа Ферма  $F_m$ ,  $c > 1$  – делитель числа  $F_m - 1$ ,  $\sigma$  – цикл длины  $F_m - 1$  из  $S_{F_m - 1}$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

то  $F_{m+1}$ -арная группа  $\langle A^{F_m - 1}, [ ]_{F_{m+1}, \sigma, F_m - 1} \rangle$  порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, F_m - 1$ .

Таким образом, согласно теореме 15.1, любое число Ферма  $F_{m+1} \geq 5$ , в том числе и простое, может быть арностью полиадической группы вида  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , которая порождается множеством  $U_j(M)$ , не содержащим элемент  $e$ . В частности, для  $m = 0, 1, 2, 3$ , получаем следующие полиадические группы простой арности:

$$\langle A^2, [ ]_{5, (12), 2} \rangle, d = 3;$$

$$\langle A^4, [ ]_{17, \sigma, 4} \rangle, d = 5,$$

где  $\sigma$  – цикл длины 4 из  $S_4$ ;

$$\langle A^{16}, [ ]_{257, \sigma, 16} \rangle, d = 17,$$

где  $\sigma$  – цикл длины 16 из  $S_{16}$ ;

$$\langle A^{256}, [ ]_{65537, \sigma, 256} \rangle, d = 257,$$

где  $\sigma$  – цикл длины 256 из  $S_{256}$ .

Так как число Ферма  $F_5$  делится на 641, то арность полиадической группы

$$\langle A^{F_4 - 1}, [ ]_{F_5, \sigma, F_4 - 1} \rangle,$$

совпадающая с  $F_5$ , является составным числом. При этом можно считать  $d = 641$ ,  $c = 2$ , а  $\sigma$  – любой цикл длины  $F_4 - 1$  из  $S_{F_4 - 1}$ .

Полагая в теореме 15.1  $d = F_m$ ,  $c = 2$ , получим

**Следствие 15.1.** Пусть  $\sigma$  – цикл длины  $F_m - 1$  из  $S_{F_m - 1}$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$d^{F_m} = v^2 = 1,$$

то  $F_{m+1}$ -арная группа  $\langle A^{F_m - 1}, [ ]_{F_{m+1}, \sigma, F_m - 1} \rangle$  порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, F_m - 1$ .

Следующее предложение показывает, что в условиях теоремы 14.1 для любого простого  $q > p$  найдутся такие  $k$  и  $l$ , что  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  имеет арность  $l$ , делящуюся на  $q$ , и порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ . Для получения этого предложения достаточно в теореме 14.1 положить

$$k = p(p+1) \dots (q-1) \quad (15.1)$$

и заметить, что по теореме Вильсона  $q$  делит

$$l = (q-1)! + 1. \quad (15.2)$$

**Предложение 15.1.** Пусть  $p$  и  $q$  – простые,  $p$  – нечётное,  $q > p$ ,  $d \geq 2$  – делитель числа  $(p-1)!$ ,  $k$  и  $l$  определяются равенствами (15.1) и (15.2),  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

то  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M)$  для любого

$$j = 1, 2, \dots, p(p+1) \dots (q-1),$$

при этом  $q$  делит  $l$ .

Для предложения 15.1 можно сформулировать результаты, аналогичные следствиям 14.1 – 14.3. Ограничимся следствиями для  $d = p - 1$  и  $d = 2$ .

**Следствие 15.2.** Пусть  $p$  и  $q$  – простые,  $p$  – нечётное,  $q > p$ ,  $k$  и  $l$  определяются равенствами (15.1) и (15.2),  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

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

то  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M)$  для любого

$$j = 1, 2, \dots, p(p+1) \dots (q-1),$$

при этом  $q$  делит  $l$ .

**Следствие 15.3.** Пусть  $p$  и  $q$  – простые,  $p$  – нечётное,  $q > p$ ,  $k$  и  $l$  определяются равенствами

(15.1) и (15.2),  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^2 = 1,$$

то  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$  порождается множеством  $U_j(M)$  для любого

$$j = 1, 2, \dots, p(p+1) \dots + (q-1),$$

при этом  $q$  делит  $l$ .

**Теорема 15.2.** Пусть  $p = 4t + 1$  – простое,  $t \geq 1$ ,  $\sigma$  – цикл длины  $k$  из  $S_k$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^2 = 1,$$

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

$$l = (1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1})k + 1, \quad (15.3)$$

порождается множеством  $U_j(M)$  для любого

$$j = 1, 2, \dots, k.$$

*Доказательство.* Используя малую теорему Ферма, можно показать (см., например, [6]), что простое число  $p$  делит сумму

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} + 1.$$

В сумме

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \quad (15.4)$$

число чётных слагаемых совпадает с числом нечётных слагаемых и равно  $\frac{p-1}{2}$ . Поэтому, если

$p = 4t + 1$ , то число нечётных слагаемых в указанной сумме равно  $2t$ . Из чётности числа нечётных слагаемых следует чётность суммы (15.4).

Если теперь положить  $c = 2$ ,  $d = p = 4t + 1$  – простое, где  $t \geq 1$ ,

$$r = 1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1},$$

то  $c = 2$  делит  $r$ ,  $d = p$  делит  $r + 1$ . Поэтому по теореме 6.5 из [2]  $l$ -арная группа  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ , арность которой определяется равенством (15.3), порождается множеством  $U_j(M)$  для любого  $j = 1, 2, \dots, k$ .  $\square$

При  $k = 2$  из теоремы 15.2 вытекает

**Следствие 15.4.** Пусть  $p = 4t + 1$  – простое,  $t \geq 1$ . Если группа  $A$  порождается множеством  $M$ , в котором имеются элементы  $u$  и  $v$  такие, что

$$u^p = v^2 = 1,$$

то  $l$ -арная группа  $\langle A^2, [ ]_{l, (12), 2} \rangle$ , где

$$l = 2(1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1}) + 1,$$

порождается любым из множеств  $U_1(M)$ ,  $U_2(M)$ .

#### 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. 69–78.
2. Гальмак, А.М. О порождающих множествах  $l$ -арной группы.  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . II / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 3 (48). – С. 63–72.
3. Гальмак, А.М. О порождающих множествах  $l$ -арной группы.  $\langle A^k, [ ]_{l, \sigma, k} \rangle$ . III / А.М. Гальмак // Проблемы физики, математики и техники. – 2021. – № 4 (49). – С. 76–80.
4. Post, E.L. Polyadic groups / E.L. Post // Trans. Amer. Math. Soc. – 1940. – Vol. 48, № 2. – P. 208–350.
5. Русаков, С.А. Алгебраические  $n$ -арные системы / С.А. Русаков. – Минск: Навука і тэхніка, 1992. – 245 с.
6. Бухштаб, А.А. Теория чисел / А.А. Бухштаб. – Москва: Просвещение, 1966. – 384 с.

Поступила в редакцию 08.02.2022.

#### Информация об авторах

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