Записки научных
семинаров ПОМИ
Том 435, 2015 г.

М. Музычук, И. Пономаренко

О 2-ГРУППАХ ШУРА

§1. Введение

Следуя Р. Пёшелю [26], назовём конечную группу G *группой Шура*, если каждое S-кольцо над ней является *шуровым*, т.е. совпадает с модулем транзитивности стабилизатора точки в некоторой подгруппе группы $\mathrm{Sym}(G)$, содержащей все перестановки, индуцированные правыми умножениями в G (по поводу точных определений см. §2). Он доказал, что если число $p \geqslant 5$ является простым, то конечная p-группа является группой Шура тогда и только тогда, когда она циклическая. При $p = 2$ или 3, циклическая p-группа также является группой Шура, однако обратное утверждение уже неверно: простые вычисления показывают, что элементарная абелева группа порядка 4 или 9 является группой Шура. В этой статье мы интересуемся 2-группами Шура.

Недавно в статье [14] было доказано, что каждая конечная абелева группа Шура принадлежит одному из нескольких явно описанных семейств. В частности, из леммы 5.1 этой статьи следует, что известны все абелевы 2-группы Шура, за исключением группы $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ для $n \geqslant 5$. Мы докажем, что она также является группой Шура (теорема 10.1). Как следствие отсюда получается классификация всех абелевых 2-групп Шура.

Теорема 1.1. *Абелева 2-группа является группой Шура тогда и только тогда, когда она циклическая, элементарная абелева порядка, не большего чем* 32*, или изоморфна группе* $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ *при* $n \geqslant 1$.

Неабелевы группы Шура изучались в статье [25], где было доказано, что все они метабелевы. В частности, из теоремы 4.2 этой статьи следует, что известны все неабелевы 2-группы Шура, за исключением диэдральных и группы

$$M_{2^n} = \langle a, b : \ a^{2^{n-1}} = b^2 = 1, \ bab = a^{1+2^{n-2}} \rangle, \tag{1}$$

Ключевые слова: S-кольцо, группа Шура, разностное множество.
Работа второго автора поддержана грантом РФФИ 14-01-00156 А.

где $n \geqslant 4$. Здесь мы докажем, что последняя не является группой Шура (теорема 11.1). Как следствие отсюда получается следующее утверждение.

Теорема 1.2. *Неабелева* 2*-группа Шура порядка не меньшего, чем* 32*, является диэдральной.*

Мы не знаем, является ли группой Шура диэдральная 2-группа порядка большего, чем 32. Однако, используя стандартный метод, основанный на статье Виландта [29], мы описываем все S-кольца над ней, ранг которых не превосходит 5 (см. §12.2 по поводу связи между S-кольцами и делимыми разностными множествами (divisible difference sets)).

Теорема 1.3. *Пусть* $\mathcal{A}$ – S*-кольцо над диэдральной* 2*-группой. Предположим, что* $\mathrm{rk}(\mathcal{A}) \leqslant 5$*. Тогда справедливо одно из следующих утверждений:*

(1) $\mathcal{A}$ *изоморфно* S*-кольцу над группой* $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$*,*
(2) $\mathcal{A}$ *является собственным произведением или сплетением,*
(3) $\mathrm{rk}(\mathcal{A}) = 5$ *и* $\mathcal{A}$ *получается из делимого разностного множества группы* $\mathbb{Z}_{2^n}$*.*

Все S-кольца из утверждения (1) этой теоремы шуровы по теореме 1.1. По индукции отсюда следует, что и все S-кольца из утверждения (2) шуровы. Таким образом, в силу теоремы 12.4 имеет место следующий результат.

Следствие 1.4. *В условиях теоремы 1.3* S*-кольцо* $\mathcal{A}$ *не является шуровым, только когда оно получается из делимого разностного множества циклической* 2*-группы.*

Неизвестно, существуют ли нетривиальные делимые разностные множества циклической 2-группы, используя которые можно построить S-кольцо $\mathcal{A}$ из утверждения (3) теоремы 1.3. Если их нет, то соответствующая диэдральная 2-группа не является группой Шура. С другой стороны, в §12.2 мы показываем, как с помощью относительных разностных множеств (являющихся частным случаем делимых) можно строить S-кольца ранга 6 (над диэдральной 2-группой). Эти разностные множества, а потому и S-кольца, действительно существуют, но крайне редки. Единственный известный пример – это классическое относительное разностное множество с параметрами $(q+1, 2, q, (q-1)/2)$,

где q – простое число Мерсенна. Таким образом, вопрос о том, является ли группой Шура диэдральная 2-группа, остается открытым.

Статья состоит из четырнадцати параграфов. В §§2, 3 и 4 собраны необходимые обозначения и результаты, касающиеся S-колец, схем Кэли[1], а также основные факты об S-кольцах над циклическими и диэдральными группами. В §§5–10 изучаются S-кольца над группой $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$; главный результат здесь – теорема 10.1, утверждающая, что эта группа является группой Шура. В §11 доказывается, что M_{2^n} не является группой Шура для всех $n \geqslant 4$ (теорема 11.1). В §§12–14 изучаются S-кольца над диэдральной 2-группой: мы начинаем с конструкций, основанных на использовании циклических делимых разностных множеств, и завершаем доказательством теоремы 1.3.

На протяжении статьи мы свободно используем факты и обозначения, связанные с группами перестановок и ассоциативными схемами. Соответствующий материал можно найти в монографии [30] и обзорной статье [11].

Обозначения.

Как обычно, $\mathbb{Z}$ обозначает кольцо целых чисел.

Единица группы D обозначается через e, а множество её неединичных элементов – через $D^{\#}$.

Пусть $X \subseteq D$. Подгруппа группы D, порождённая множеством X, обозначается через $\langle X \rangle$; мы также полагаем $\mathrm{rad}(X) = \{g \in D : \ gX = Xg = X\}$. Элемент $\sum_{x \in X} x$ группового кольца $\mathbb{Z}D$ обозначается через $\underline{X}$. Множество X называется *регулярным*, если порядок $|x|$ элемента $x \in X$ не зависит от его выбора.

Для группы $H \trianglelefteq D$ естественный эпиморфизм из D на D/H обозначается через $\pi_{D/H}$.

Группа всех перестановок множества D обозначается через $\mathrm{Sym}(D)$. Множество всех орбит группы перестановок $G \leqslant \mathrm{Sym}(D)$ обозначается через $\mathrm{Orb}(G) = \mathrm{Orb}(G, D)$. Мы пишем $G \approx_2 G'$, если группа G 2-*эквивалентна* группе $G' \leqslant \mathrm{Sym}(D)$, т.е. если эти группы имеют одни и те же орбиты в покоординатном действии на $D \times D$.

Если $L \trianglelefteq U \leqslant D$, то факторгруппа U/L называется *секцией* группы D. Для множества $\Delta \subseteq \mathrm{Sym}(D)$ и секции $S = U/L$ группы D мы

[1]Мы предполагаем, что читатель знаком с основами теории ассоциативных схем.

полагаем

$$\Delta^S = \{f^S : \ f \in \Delta, \ S^f = S\},$$

где равенство $S^f = S$ означает, что f переставляет правые смежные классы группы U по подгруппе L, и f^S обозначает биекцию множества S, индуцированную биекцией f.

Циклическая группа порядка n обозначается через $\mathbb{Z}_n$.

§2. Основы теории S-колец

Здесь и далее мы используем обозначения и терминологию из работы [2].

Пусть D – конечная группа. Подкольцо $\mathcal{A}$ группового кольца $\mathbb{Z}D$ называется *кольцом Шура* (или, для краткости, S-*кольцом*) над D, если существует разбиение $\mathcal{S} = \mathcal{S}(\mathcal{A})$ группы D такое, что

(S1) $\{e\} \in \mathcal{S}$,
(S2) $X \in \mathcal{S} \ \Rightarrow \ X^{-1} \in \mathcal{S}$,
(S3) $\mathcal{A} = \mathrm{Span}\{\underline{X} : \ X \in \mathcal{S}\}$.

Если $\mathcal{S} = \mathrm{Orb}(K, D)$, где $K \leqslant \mathrm{Aut}(D)$, то S-кольцо $\mathcal{A}$ называется *циклотомическим* и обозначается через $\mathrm{Cyc}(K, D)$. Групповой изоморфизм $f : D \to D'$ называется *изоморфизмом Кэли* S-кольца $\mathcal{A}$ над D на S-кольцо $\mathcal{A}'$ над D', если $\mathcal{S}(\mathcal{A})^f = \mathcal{S}(\mathcal{A}')$.

Из условия (S3) следует, что для любых $X, Y \in \mathcal{S}(\mathcal{A})$ найдутся неотрицательные целые числа c_{XY}^Z, $Z \in \mathcal{S}(\mathcal{A})$, такие, что

$$\underline{X}\,\underline{Y} = \sum_{Z \in \mathcal{S}(\mathcal{A})} c_{XY}^Z \underline{Z}.$$

Легко видеть, что c_{XY}^Z равно числу различных представлений $z = xy$, в которых $(x, y) \in X \times Y$ для фиксированного (а потому и для любого) $z \in Z$. Хорошо известно, что

$$c_{Y^{-1}X^{-1}}^{Z^{-1}} = c_{XY}^Z \quad \text{и} \quad |Z| c_{XY}^{Z^{-1}} = |X| c_{YZ}^{X^{-1}} = |Y| c_{ZX}^{Y^{-1}}$$

для всех X, Y, Z. Кольцевой изоморфизм $\varphi : \mathcal{A} \to \mathcal{A}'$ называется *алгебраическим*, если для каждого $X \in \mathcal{S}(\mathcal{A})$ найдётся $X' \in \mathcal{S}(\mathcal{A}')$ такое, что $\varphi(\underline{X}) = \underline{X'}$.

Классы разбиения $\mathcal{S}$ и число $\mathrm{rk}(\mathcal{A}) = |\mathcal{S}|$ называются соответственно *базисными множествами* и *рангом* S-кольца $\mathcal{A}$. Любое объединение базисных множеств называется $\mathcal{A}$-*подмножеством группы* D или просто $\mathcal{A}$-*множеством*. Совокупность их всех замкнута относительно умножения и взятия обратного. Для $\mathcal{A}$-множества X мы обозначаем

через $\mathcal{A}_X$ подмодуль кольца $\mathcal{A}$, натянутый на элементы $\underline{Y}$, где Y пробегает множество

$$\mathcal{S}(\mathcal{A})_X = \{Y \in \mathcal{S}(\mathcal{A}) : \ Y \subseteq X\}.$$

Каждая подгруппа группы D, являющаяся $\mathcal{A}$-множеством, называется $\mathcal{A}$-*подгруппой* группы D или просто $\mathcal{A}$-*группой*. С любым $\mathcal{A}$-множеством X естественным образом связаны две $\mathcal{A}$-группы: $\langle X\rangle$ и $\mathrm{rad}(X)$ (см. Обозначения). Следующая полезная лемма была доказана в [12, стр.21].[2]

Лемма 2.1. *Пусть $\mathcal{A}$ – S-кольцо над группой D, и пусть $H \leqslant D$ – $\mathcal{A}$-группа. Тогда для каждого $X \in \mathcal{S}(\mathcal{A})$ мощность множества $X \cap xH$ не зависит от выбора $x \in X$.*

Секция $S = U/L$ группы D называется $\mathcal{A}$-*секцией*, если U и L являются $\mathcal{A}$-группами. В этом случае модуль

$$\mathcal{A}_S = \mathrm{Span}\{\pi_S(X) : \ X \in \mathcal{S}(\mathcal{A})_U\}$$

является S-кольцом над группой S, а его базисные величины есть в точности множества $\pi_S(X)$ из правой части последней формулы.

S-кольцо $\mathcal{A}$ называется *примитивным*, если единственными $\mathcal{A}$-группами являются e и D; будем говорить, что $\mathcal{A}$ *импримитивное*, если оно не является примитивным. Легко видеть, что если H – минимальная $\mathcal{A}$-группа, то S-кольцо $\mathcal{A}_H$ примитивно. Классические результаты о примитивных S-кольцах над абелевыми и диэдральными группами были получены в работах [17, 28, 29]. Анализ доказательств показывает, что предположение о шуровости S-колец в этих работах было излишне; см. §3. Поэтому в первой части следующего утверждения мы формулируем соответствующие результаты в чуть более общей форме.

Теорема 2.2. *Пусть D – 2-группа, являющаяся циклической, диэдральной или группой вида $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$. Тогда ранг любого примитивного* S-*кольца над D равен 2. В частности, если $\mathcal{A}$ – S-кольцо над D и $H \leqslant D$ – минимальная $\mathcal{A}$-группа, то $H^\#$ является базисным множеством этого* S-*кольца.*

Пусть $S = U/L$ – $\mathcal{A}$-секция группы D. Тогда S-кольцо $\mathcal{A}$ называется *обобщённым S-сплетением*, [3] если группа L нормальна в D и, кроме

[2] По-видимому, впервые этот результат появляется в [5, предложение 4.5].

[3] В статье [20] использовался термин клинообразное сплетение (wedge product).

того, $L \leqslant \mathrm{rad}(X)$ для всех базисных множеств $X \in D\setminus U$; в этом случае мы пишем

$$\mathcal{A} = \mathcal{A}_U \wr_S \mathcal{A}_{D/L}, \tag{2}$$

опуская S, когда $U = L$. Если явное указание секции S не важно, мы говорим, что $\mathcal{A}$ – *обобщённое сплетение*. Обобщённое S-сплетение называется *собственным*, если $L \neq e$ и $U \neq D$. При $U = L$ обобщённое S-сплетение совпадает с обычным сплетением.

Пусть $D = D_1D_2$, где D_1 и D_2 – подгруппы группы D, пересечение которых тривиально. Если $\mathcal{A}_1$ и $\mathcal{A}_2$ – S-кольца над группами D_1 и D_2 соответственно, то модуль

$$\mathcal{A} = \mathrm{Span}\{\underline{X_1 \cdot X_2} : X_1 \in \mathcal{S}(\mathcal{A}_1),\ X_2 \in \mathcal{S}(\mathcal{A}_2)\}$$

является S-кольцом над группой D при условии, что кольца $\mathcal{A}_1$ и $\mathcal{A}_2$ коммутируют друг с другом. В этом случае $\mathcal{A}$ называется *произведением* S-колец $\mathcal{A}_1$ и $\mathcal{A}_2$, и обозначается через $\mathcal{A}_1 \cdot \mathcal{A}_2$ [20]. Если при этом $D = D_1 \times D_2$, то произведение совпадает с *тензорным призведением* $\mathcal{A}_1 \otimes \mathcal{A}_2$. Следующее утверждение было доказано в [14].

Лемма 2.3. *Пусть $\mathcal{A}$ – S-кольцо над абелевой группой $D = D_1 \times D_2$. Предположим. что D_1 и D_2 – $\mathcal{A}$-группы. Тогда $\mathcal{A} = \mathcal{A}_{D_1} \otimes \mathcal{A}_{D_2}$, если $\mathcal{A}_{D_1} = \mathbb{Z}D_1$ или $\mathcal{A}_{D_2} = \mathbb{Z}D_2$.*

Следующие две важные теоремы восходят к Шуру и Виландту; см. [30, гл. IV]. Первая из них известна как теорема Шура о мультипликаторах; см. [12].

Теорема 2.4. *Пусть $\mathcal{A}$ – S-кольцо над абелевой группой D. Тогда для любого целого числа m, которое взаимно просто с $|D|$, отображение $X \mapsto X^{(m)}$, $X \in \mathcal{S}(\mathcal{A})$, где*

$$X^{(m)} = \{x^m :\ x \in X\}, \tag{3}$$

является биекцией. Более того, отображение $x \mapsto x^m$, $x \in D$, является изоморфизмом Кэли кольца $\mathcal{A}$.

Для подмножества X абелевой группы D обозначим через $\mathrm{tr}(X)$ *след* этого множества; по определению он равен объединению всех $X^{(m)}$, где m пробегает множество всех целых чисел, которые взаимно просты с $|D|$. Будем говорить, что X – *рационально*, если $X = \mathrm{tr}(X)$. Если $\mathrm{tr}(X) = \mathrm{tr}(Y)$ для некоторого $Y \subseteq D$, то X и Y называются *рационально сопряжёнными*. Для S-кольца $\mathcal{A}$ над группой D модуль

$$\mathrm{tr}(\mathcal{A}) = \mathrm{Span}\{\mathrm{tr}(X) :\ X \in \mathcal{S}(\mathcal{A}\}$$

также является S-кольцом; оно называется *рациональным замыканием* кольца $\mathcal{A}$. Наконец, S-кольцо называется *рациональным*, если оно совпадает со своим рациональным замыканием, или, что эквивалентно, если каждое его базисное множество рационально.

В общем случае теорема 2.4 перестает быть верной, если число m не взаимно просто с порядком группы D. Однако, справедливо следующее более слабое утверждение.

Теорема 2.5. *Пусть $\mathcal{A}$ – S-кольцо над абелевой группой D. Тогда для каждого простого делителя p числа $|D|$, отображение $X \mapsto X^{[p]}$, $X \in 2^D$, где*

$$X^{[p]} = \{x^p : \ x \in X, \ |X \cap Hx| \neq 0 \pmod p\} \tag{4}$$

и $H = \{g \in D : \ g^p = 1\}$, переводит любое $\mathcal{A}$-множество в $\mathcal{A}$-множество.

Завершим этот параграф теоремой о разделяющей подгруппе, доказанной в [10].

Теорема 2.6. *Пусть $\mathcal{A}$ – S-кольцо над группой D. Предположим, что $X \in \mathcal{S}(\mathcal{A})$ и $H \leqslant D$ такие, что*

$$X \cap H \neq \varnothing \quad \text{и} \quad X \setminus H \neq \varnothing \quad \text{и} \quad \langle X \cap H \rangle \leqslant \mathrm{rad}(X \setminus H).$$

Тогда $X = \langle X \rangle \setminus \mathrm{rad}(X)$ и $\mathrm{rad}(X) \leqslant H \leqslant \langle X \rangle$.

§3. S-кольца и схемы Кэли

В этом параграфе мы будем свободно использовать язык ассоциативных схем; в нашем изложении мы следуем работам [11, 21].

3.1. Взаимно однозначное соответствие. Для группы D обозначим через $R(D)$ множество всех бинарных отношений на D, которые инвариантны относительно группы D_{right} (она состоит из всех перестановок множества D, индуцированных правыми умножениями в группе D). Тогда отображение

$$2^D \to R(D), \quad X \mapsto R_D(X), \tag{5}$$

где $R_D(X) = \{(g, xg) : \ g \in D, x \in X\}$, является биекцией. Если $\mathcal{A}$ – S-кольцо над группой D, то пара

$$\mathcal{X} = (D, S), \tag{6}$$

где $S = R_D(\mathcal{S}(\mathcal{A}))$, является ассоциативной схемой. Более того, она является *схемой Кэли* над D; по определению последнее означает, что $D_{\mathrm{right}} \leqslant \mathrm{Aut}(\mathcal{X})$. Каждое базисное отношение $s \in S$ этой схемы является (ди)графом Кэли над группой D, определённым множеством $es = \{g \in D : \ (e, g) \in s\}$. Обратно, каждой схеме Кэли (6) отвечает модуль

$$\mathcal{A} = \mathrm{Span}\{\underline{es} : \ s \in S\},$$

который является S-кольцом над группой D.

Теорема 3.1. [4] *Отображения $\mathcal{A} \mapsto \mathcal{X}$, $\mathcal{X} \mapsto \mathcal{A}$ задают взаимно однозначное соответствие между* S*-кольцами и схемами Кэли над группой D.*

Заметим, что указанное выше соответствие сохраняет включения. Более того, отображение (5) индуцирует кольцевой иоморфизм между S-кольцом $\mathcal{A}$ и алгеброй смежности схемы Кэли $\mathcal{X}$, соответствующей $\mathcal{A}$. Отсюда следует, что $c_{XY}^Z = c_{rs}^t$ для всех $X, Y, Z \in \mathcal{S}(\mathcal{A})$, где $r = R_D(X)$, $s = R_D(Y)$ и $t = R_D(Z)$. В частности, число $|X|$ равно валентности n_r отношения r, и S-кольцо $\mathcal{A}$ коммутативно тогда и только тогда, когда коммутативна соответствующая ему схема Кэли $\mathcal{X}$.

3.2. Изоморфизмы и шуровость. Говорят, что S-кольца $\mathcal{A}$ и $\mathcal{A}'$ (комбинаторно) *изоморфны*, если изоморфны соответствующие им схемы Кэли. Любой изоморфизм между ними называется *изоморфизмом* S-колец $\mathcal{A}$ и $\mathcal{A}'$. Группа $\mathrm{Iso}(\mathcal{A})$ всех изоморфизмов S-кольца $\mathcal{A}$ на себя содержит нормальную подгруппу $\mathrm{Aut}(\mathcal{A})$, которая состоит из всех изоморфизмов f таких, что $R_D(X)^f = R_D(X)$ для всех $X \in \mathcal{S}(\mathcal{A})$; каждый такой f называется (комбинаторным) *автоморфизмом* S-кольца $\mathcal{A}$. В частности, если $\mathcal{A} = \mathbb{Z}D$ (соотв. $\mathrm{rk}(\mathcal{A}) = 2$), то $\mathrm{Aut}(\mathcal{A}) = D_{\mathrm{right}}$ (соотв. $\mathrm{Aut}(\mathcal{A}) = \mathrm{Sym}(D)$).

S-кольцо $\mathcal{A}$ называется *шуровым* (соотв. *нормальным*), если таковой является схема Кэли, соответствующая этому кольцу. Таким образом, $\mathcal{A}$ шурово тогда и только тогда, когда $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A})_e, D)$, и нормально тогда и только тогда, когда $D_{\mathrm{right}} \trianglelefteq \mathrm{Aut}(\mathcal{A})$.

Приведённые выше определения показывают, что $\mathcal{A} = \mathcal{A}_1 \wr \mathcal{A}_2$ тогда и только тогда, когда $\mathcal{X} = \mathcal{X}_1 \wr \mathcal{X}_2$, где $\mathcal{X}$, $\mathcal{X}_1$ и $\mathcal{X}_2$ – схемы Кэли, соответствующие S-кольцам $\mathcal{A}$, $\mathcal{A}_1$ и $\mathcal{A}_2$, соответственно. Аналогично, $\mathcal{A} = \mathcal{A}_1 \cdot \mathcal{A}_2$ тогда и только тогда, когда $\mathcal{X} = \mathcal{X}_1 \otimes \mathcal{X}_2$. С другой стороны, тензорное произведение и сплетение ассоциативных схем (и групп перестановок) являются частными случаями операции гребешкового

произведения (crested product), введённой и изученной в статье [6]. Таким образом, сформулированная ниже теорема 3.2, немедленно следует из замечания 23 этой статьи и теорем 21 и 22, доказанных там же.

Теорема 3.2. *Пусть* $\mathcal{A} = \mathcal{A}_1 * \mathcal{A}_2$, *где* $* \in \{\wr, \cdot\}$. *Тогда* S-*кольцо* $\mathcal{A}$ *шурово тогда и только тогда, когда* S-*кольца* $\mathcal{A}_1$ *и* $\mathcal{A}_2$ *шуровы. Более того,*

$$\mathrm{Aut}(\mathcal{A}_1 \wr \mathcal{A}_2) = \mathrm{Aut}(\mathcal{A}_1) \wr \mathrm{Aut}(\mathcal{A}_2) \quad \textit{и} \quad \mathrm{Aut}(\mathcal{A}_1 \cdot \mathcal{A}_2) = \mathrm{Aut}(\mathcal{A}_1) \times \mathrm{Aut}(\mathcal{A}_2).$$

Следующее простое утверждение легко следует из определения сплетения и теоремы 3.2.

Следствие 3.3. *Пусть* $\mathcal{A}$ – S-*кольцо над группой* D, *и пусть* H – $\mathcal{A}$-*группа такая, что* $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}_H) + 1$. *Тогда* $\mathcal{A}$ *изоморфно сплетению* S-*кольца* $\mathcal{A}_H$ *с* S-*кольцом ранга* 2 *над группой* $\mathbb{Z}_{[D:H]}$. *Более того,* $\mathcal{A}$ *шурово тогда и только тогда, когда* $\mathcal{A}_H$ *шурово.*

3.3. Квазитонкие S-кольца. S-кольцо $\mathcal{A}$ называется *квазитонким*, если каждое его базисное множество состоит не более чем из двух элементов. Таким образом, $\mathcal{A}$ – квазитонкое тогда и только тогда, когда квазитонкой является схема Кэли, соответствующая $\mathcal{A}$ (последнее по определению означает, что валентность каждого базисного отношения этой схемы не превосходит двух).

Лемма 3.4. *Пусть* $\mathcal{A}$ – S-*кольцо над абелевой группой* D. *Предположим, что найдется множество* $X \in \mathcal{S}(\mathcal{A})$ *такое, что* $|X| = 2$ *и* $\langle X \rangle = D$. *Тогда* S-*кольцо* $\mathcal{A}$ *квазитонкое.*

Доказательство. В силу абелевости группы D схема Кэли $\mathcal{X}$, соответствующая S-кольцу $\mathcal{A}$, является коммутативной. Более того, её базисное отношение $r = R_D(X)$, отвечающее множеству X, имеет валентность $|X| = 2$. Поэтому из равенства $\langle X \rangle = D$ следует, что $\mathcal{X}$ является 2-циклической схемой, порождённой плотно прикреплённым (tightly attached) отношением r в терминологии статьи [15]. Следовательно, по предложению 3.11 этой статьи схема $\mathcal{X}$ является квазитонкой. Так что, S-кольцо $\mathcal{A}$ также квазитонкое. □

Следуя теории квазитонких схем, развитой в статье [22], будем говорить, что базисное множество $X \neq \{e\}$ квазитонкого S-кольца $\mathcal{A}$ является *ортогоналом*, если $X \subseteq Y\,Y^{-1}$ для некоторого $Y \in \mathcal{S}(\mathcal{A})$.

Лемма 3.5. *Любое квазитонкое коммутативное* S*-кольцо* $\mathcal{A}$ *шурово. Более того, если в нём есть по крайней мере два ортогонала, то группа* $\mathrm{Aut}(\mathcal{A})_e$ *имеет точную регулярную орбиту.*

Доказательство. Первое утверждение является прямым следствием теоремы 1.2 из статьи [22]. Для доказательства второго утверждения обозначим через $\mathcal{X}$ схему Кэли, соответствующую S-кольцу $\mathcal{A}$. Тогда, по следствию 6.4 этой статьи, группа $\mathrm{Aut}(\mathcal{X})_{e,x}$ тривиальна для некоторого элемента $x \in D$. Но это в точности означает, что $x^{\mathrm{Aut}(\mathcal{X})_e}$ – точная регулярная орбита группы $\mathrm{Aut}(\mathcal{A})_e$. □

§4. S-кольца над циклическими и диэдральными группами

4.1. Циклические группы. Пусть C – циклическая группа порядка 2^n, $n \geqslant 1$. Тогда группа $\mathrm{Aut}(C)$ состоит из перестановок $\sigma_m : x \mapsto x^m$, $x \in C$, где m – нечётное целое число. Ниже мы обозначаем через c_1 единственную инволюцию группы C.

Лемма 4.1. *Пусть* $X \in \mathrm{Orb}(K, C)$*, где* $K \leqslant \mathrm{Aut}(C)$*. Тогда*

(1) $\mathrm{rad}(X) = e$ *тогда и только тогда, когда* X *– одноэлементное множество, или* $n \geqslant 3$ *и* $X = \{x, \varepsilon x^{-1}\}$*, где* $x \in X$ *и* $\varepsilon \in \{e, c_1\}$*,*

(2) *если* $K \geqslant \{\sigma_m : \ m = 1 \pmod{2^{n-k}}\}$*, то* 2^k *делит* $|\mathrm{rad}(X)|$*.*

Доказательство. Утверждение (1) следует из [1, лемма 5.1], а утверждение (2) очевидно. □

Пусть $\mathcal{A}$ – S-кольцо над группой C. По теореме Шура о мультипликаторах группа $\mathrm{rad}(X)$ не зависит от множества $X \in \mathcal{S}(\mathcal{A})$, содержащего образующую группы C. Она называется *радикалом* S-кольца $\mathcal{A}$ и обозначается через $\mathrm{rad}(\mathcal{A})$. Поскольку C – 2-группа, из леммы 6.4 статьи [1] следует, что если $\mathrm{rad}(\mathcal{A}) = e$, то либо $n \geqslant 2$ и $\mathrm{rk}(\mathcal{A}) = 2$, или $\mathcal{A} = \mathrm{Cyc}(K, C)$, где $K \leqslant \mathrm{Aut}(C)$ – группа, порождённая автоморфизмом, переводящим образующую x группы C в один из элементов множества $\{x, x^{-1}, c_1 x^{-1}\}$ (см. также утверждение (1) леммы 4.1). В любом случае, S-кольцо $\mathcal{A}$, очевидно, шурово. На самом деле, последнее утверждение справедливо для любого S-кольца над циклической p-группой [13].

Для произвольного базисного множества X S-кольца $\mathcal{A}$ можно образовать $\mathcal{A}$-секцию $S = \langle X \rangle / \mathrm{rad}(X)$. Тогда радикал S-кольца $\mathcal{A}_S$ тривиален. Поскольку в нашем случае S – 2-группа, процитированный выше

результат показывает, что S-кольцо $\mathcal{A}_S$ является циклотомическим, или число $|S|$ – составное и $\mathrm{rk}(\mathcal{A}_S) = 2$. В первом случае множество X является орбитой некоторой группы автоморфизмов группы C, а во втором оно имеет вид $X = \langle X\rangle \setminus \mathrm{rad}(X)$. Таким образом, каждое базисное множество S-кольца $\mathcal{A}$ либо регулярно, либо равно теоретико-множественной разности двух различных $\mathcal{A}$-групп.

Лемма 4.2. *Пусть $\mathcal{A}$ – циклотомическое* S*-кольцо над циклической* 2*-группой. Предположим, что* $\mathrm{rad}(\mathcal{A}) = e$. *Тогда* $\mathrm{rad}(\mathcal{A}_S) = e$ *для любой $\mathcal{A}$-секции S такой, что $|S| \neq 4$.*

Доказательство. Следует из теоремы 7.3 статьи [13]. □

Следующая вспомогательная лемма будет использована в §9.

Лемма 4.3. *Пусть C – циклическая* 2*-группа, и пусть X и Y – орбиты некоторых подгрупп группы* $\mathrm{Aut}(C)$. *Предположим, что $\langle X\rangle \neq \langle Y\rangle$ и* $\mathrm{rad}(X) = \mathrm{rad}(Y) = e$. *Тогда произведение XY не содержит никакого смежного класса по подгруппе $\langle c_1\rangle$.*

Доказательство. Не умаляя общности можно считать, что $\langle Y\rangle$ является собственной подгруппой группы $\langle X\rangle$. Тогда из утверждения (1) леммы 4.1 следует, что $X = \{x\}$ или $\{x, \varepsilon x^{-1}\}$, и $Y = \{y\}$ или $\{y, \varepsilon' y^{-1}\}$, где $|x| > |y|$. Поэтому требуемое утверждение справедливо, когда X или Y является одноэлементным множеством. Таким образом, можно считать, что $|X| = |Y| = 2$, и, значит, $|x| > |y| \geqslant 8$. Кроме того,

$$XY = \{xy, \quad \varepsilon' xy^{-1}, \quad \varepsilon x^{-1}y, \quad \varepsilon'' x^{-1}y^{-1}\},$$

где $\varepsilon'' = \varepsilon\varepsilon'$. Предположим, что это произведение содержит какой-нибудь смежный класс по подгруппе $\langle c_1\rangle$. Тогда легко видеть, что $c_1 xy = \varepsilon' xy^{-1}$ или $c_1\varepsilon x^{-1}y = \varepsilon'' x^{-1}y^{-1}$. В любом случае $y^2 \in \{e, c_1\}$, и, следовательно, $|y| \leqslant 4$. Противоречие. □

4.2. Диэдральные группы. На протяжении этого пункта D обозначает диэдральную группу, а C – её циклическую подгруппу такую, что все элементы в $D \setminus C$ являются инволюциями. Множество $X \subseteq D$ будем называть *смешанным*, если множества $X_0 = X \cap C$ и $X \setminus X_0$ не пусты. Для элемента $s \in D \setminus C$ обозначим через $X_1 = X_{1,s}$ подмножество множества C, для которого $X = X_0 \cup X_1 s$. Следующее утверждение (в других обозначениях) было доказано в работе [29].

Лемма 4.4. *Пусть $\mathcal{A}$ –* S*-кольцо над диэдральной группой D и X – смешанное базисное множество этого кольца. Тогда*

(1) *множества* X_0, $X_1 s$ *и* X *являются симметрическими, и* X_0 *коммутирует с* $X_1 s$,
(2) *для любого целого числа* m, *которое взаимно просто с* $|D|$, *существует единственное базисное множество* Y *кольца* $\mathcal{A}$, *для которого* $(X_0)^{(m)} = Y_0$.

Когда это не приводит к путанице, множество Y из утверждения (2) леммы 4.4 будет также обозначаться через $X^{(m)}$; заметим, что при $X \subseteq C$ это обозначение согласовано с определением (3). Для любого $\mathcal{A}$-множества X с условием $X_0 \neq \varnothing$ можно определить его след $\mathrm{tr}(X)$ как объединение множеств $X^{(m)}$ по всем целым числам m, взаимно простым с $|D|$. Следующее утверждение также было доказано в работе [29].

Лемма 4.5. *Пусть* $\mathcal{A}$ – S-*кольцо над диэдральной группой* D. *Предположим, что* $X_0 \neq \varnothing$ *для всех* $X \in \mathcal{S}(\mathcal{A})$. *Тогда для любого целого числа* m, *которое взаимно просто с* $|D|$, *отображение* $X \mapsto X^{(m)}$ *индуцирует алгебраический изоморфизм* S-*кольца* $\mathcal{A}$; *в частности,* $|X^{(m)}| = |X|$.

Алгебраическое слияние S-кольца $\mathcal{A}$ из леммы 4.5 посредством группы всех определённых в ней алгебраических изоморфизмов представляет собой S-кольцо, каждое базисное множество которого имеет вид $\mathrm{tr}(X)$, где $X \in \mathcal{S}(\mathcal{A})$. Это S-кольцо называется *рациональным замыканием* кольца $\mathcal{A}$ и обозначается через $\mathrm{tr}(\mathcal{A})$. Следует подчеркнуть, что это обозначение имеет смысл только при выполнении условия леммы 4.5.

§5. S-кольца над $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: базисные множества с инволюциями

Ниже $C \leqslant D$ обозначает циклическую группу порядка 2^n и E – подгруппу Клейна группы D. Неединичными элементами этой подгруппы являются инволюция $c_1 \in C$ и две других инволюции: $s \in D \setminus C$ и $c_1 s$. Из теоремы Шура о мультипликаторах (теорема 2.4) следует, что базисное множество X_t произвольного S-кольца над D, содержащее элемент $t \in E$, является рациональным. В этом разделе мы полностью опишем эти множества.

Теорема 5.1. *Пусть* $\mathcal{A}$ – S-*кольцо над группой* D. *Тогда множество* $H = \bigcup_{t \in E} X_t$ *является* $\mathcal{A}$-*группой и для подходящего выбора инволюции* s *справедливо одно из следующих утверждений при* $U = \langle X_{c_1} \rangle$:

(1) $X_{c_1} = X_s = X_{sc_1} = U \setminus e$,
(2) $X_{c_1} = U \setminus e$ *и* $X_s = X_{sc_1} = H \setminus U$,
(3) $X_{c_1} = X_{sc_1} = U \setminus \langle s \rangle$ *и* $X_s = \{s\}$,
(4) $X_{c_1} = U \setminus e$, $X_s = \{s\}$ *и* $X_{sc_1} = sX_{c_1}$.

Доказательство теоремы 5.1 будет приведено позже. Нам понадобится следующее вспомогательное утверждение, которое по сути является следствием теоремы Шура о мультипликаторах. Ниже мы фиксируем S-кольцо $\mathcal{A}$ над группой D.

Лемма 5.2. *Предположим, что $X \in \mathcal{S}(\mathcal{A})$ содержит два элемента x и y таких, что $|x| > |y| \geqslant 2$. Тогда $x\{e, c_1\} \subseteq X$.*

Доказательство. Положим $m = 1 + |x|/2$. Тогда по теореме Шура о мультипликаторах $Y := X^{(m)}$ является базисным множеством кольца $\mathcal{A}$. С другой стороны, $y^m = y$, поскольку $|x| > |y|$. Поэтому $y^m \in X$. Отсюда следует, что $X = Y$, и, значит, $x^m \in X$. Принимая во внимание, что $|x| > 2$ и $x^m = xc_1$, мы заключаем, что $x\{e, c_1\} \subseteq X$. □

В следующей лемме мы используем обозначения из теоремы 5.1.

Лемма 5.3. *Либо $X_{c_1} = U \setminus e$, либо H – $\mathcal{A}$-группа и справедливо утверждение* (3) *теоремы* 5.1.

Доказательство. Утверждение тривиально в случае, когда множество $X := X_{c_1}$ содержится в E. Поэтому можно считать, что X содержит по крайней мере один элемент порядка, большего чем два. Тогда $x\{e, c_1\} \subseteq X$ для каждого такого элемента $x \in X$ (лемма 5.2). Следовательно, $c_1 \in \mathrm{rad}(X \setminus E)$. Заметим, что множество $X \cap E$ равно одному из следующих:

$$\{c_1\} \quad \text{или} \quad \{c_1, s, sc_1\} \quad \text{или} \quad \{c_1, t\},$$

где $t \in \{s, sc_1\}$. В первых двух случаях $c_1 \in \mathrm{rad}(X \setminus \{c_1\})$. По теореме 2.6 при $H = \langle c_1 \rangle$ отсюда следует, что $X = \langle X \rangle \setminus \mathrm{rad}(X)$ и $c_1 \notin \mathrm{rad}(X)$. Однако, в группе D есть лишь две нетривиальных подгруппы, не содержащие элемент c_1, именно $\langle s \rangle$ и $\langle sc_1 \rangle$. Поскольку ни одна из них не равна группе $\mathrm{rad}(X)$, мы заключаем, что $\mathrm{rad}(X) = e$ и $X = U \setminus e$.

В оставшемся случае $X \cap E = \{c_1, t\}$, и потому $|c_1X \cap X| = |X| - 2$. Поскольку $c_1 \in X$, то отсюда следует, что последнее число равно числу c_{XX}^X (см. §2). Таким образом, $|x^{-1}X \cap X| = |X| - 2$ для каждого

$x \in X$. С другой стороны, множество $\{c_1, t\}t = \{c_1 t, e\}$ не пересекается с X. Так что, $t(X \setminus E) = X \setminus E$, и, значит,

$$\mathrm{rad}(X \setminus E) = E.$$

По теореме 2.6 при $H = E$ отсюда следует, что $X = \langle X \rangle \setminus \mathrm{rad}(X)$, и множество $E \setminus \mathrm{rad}(X)$ содержится в X. Поэтому $\mathrm{rad}(X) = \langle t' \rangle$, где t' – отличный от t элемент множества $\{s, sc_1\}$. Таким образом, $X = U \setminus \langle t' \rangle$, и $H = U$ является $\mathcal{A}$-группой. □

Доказательство теоремы 5.1. По лемме 5.3 можно считать, что $X := X_{c_1} = U \setminus e$. Если при этом X содержит s или sc_1, то $H = U$ является $\mathcal{A}$-группой и выполнено утверждение (1) теоремы. Таким образом, можно считать также, что $X \neq X_t$ для каждого $t \in \{s, sc_1\}$. Предположим сначала, что $X_s = X_{sc_1}$; обозначим это множество через Y. Тогда $Y \cap E = \{s, sc_1\}$, и потому $c_1 \in \mathrm{rad}(Y)$ (лемма 5.2). Поскольку $X = U \setminus e$, отсюда следует, что $U \leqslant \mathrm{rad}(Y)$. Следовательно, $H = \langle Y \rangle$ является $\mathcal{A}$-группой, $X_s = X_{sc_1} = Y = H \setminus U$ и выполнено утверждение (2) теоремы.

Пусть теперь $X_s \neq X_{sc_1}$ и $t \in \{s, sc_1\}$. Тогда $Y \cap E = \{t\}$, где $Y = X_t$. Отсюда следует, что $|c_1 Y \cap Y| = |Y| - 1$, и потому

$$\underline{Y}^2 = |Y|e + (|Y| - 1)\underline{X} + \cdots, \tag{7}$$

где опущенные слагаемые в правой части не содержат ни e, ни элементов множества X с ненулевыми коэффициентами. Однако, $|X| c_{YY}^X = |Y| c_{YX}^Y$, поскольку $X = X^{-1}$ и $Y = Y^{-1}$. С учётом равенства $c_{YY}^X = |Y| - 1$, отсюда следует, что $|X|$ делится на $|Y|$. Если при этом $|Y| = 1$, то $\{X_s, X_{sc_1}\} = \{\{t\}, tX_{c_1}\}$, и $H = U \cup tU$ является $\mathcal{A}$-группой. Поэтому выполнено утверждение (4) доказываемой теоремы. Если же $|Y| \neq 1$, то в силу равенства (7) мы имеем $|Y| = |X| = |U| - 1$ и $\underline{Y}^2 = |Y|e + (|Y| - 1)\underline{X}$. Следовательно, $c_{YX}^Y = |X| - 1$. Поэтому

$$|tU \cap Y| = |X| - 1 = |U| - 2.$$

Последнее равенство справедливо для $t = c_1$ и $t = sc_1$. С другой стороны, $sU = sc_1 U$, и множества X_s и X_{sc_1} не пересекаются. Таким образом,

$$|U| = |tU| \geqslant |sU \cap X_s| + |sc_1 U \cap X_{sc_1}| = 2(|U| - 2).$$

Поэтому $|U| = 2$ или $|U| = 4$. В первом случае $H = E$, и утверждение (4) теоремы выполнено тривиально. Во втором случае $|X| = |X_s| = 3$ и $|sU \cap Y| = 2$. Поэтому имеется единственный элемент $x \in X_s$,

не принадлежащий sU. Но тогда $|xU \cap X_s| = 1$, что невозможно по лемме 2.1. $\square$

§6. S-кольца над $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: нерегулярный случай

Множество $X \subseteq D$ называется *старшим* (в D), если оно содержит элемент порядка 2^n. Для S-кольца $\mathcal{A}$ над группой D обозначим через $\mathrm{rad}(\mathcal{A})$ группу, порождённую группами $\mathrm{rad}(X)$, где X пробегает старшие базисные множества этого кольца. Легко видеть, что $\mathrm{rad}(\mathcal{A})$ является $\mathcal{A}$-группой, и она равна e тогда и только тогда, когда каждое старшее базисное множество кольца $\mathcal{A}$ имеет тривиальный радикал. Будем говорить, что S-кольцо $\mathcal{A}$ *регулярно*, если каждое старшее базисное множество кольца $\mathcal{A}$ является регулярным. Во введённых обозначениях и терминологии основной результат этого параграфа можно сформулировать следующим образом.

Теорема 6.1. *Пусть $\mathcal{A}$ – S-кольцо над группой D. Предположим, что $\mathrm{rad}(\mathcal{A}) = e$. Тогда $\mathcal{A}$ либо регулярно, либо рационально. Более того, в последнем случае $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, где $\mathrm{rk}(\mathcal{A}_H) = 2$ и $|L| \leqslant 2 \leqslant |H|$; в частности, $\mathcal{A}$ шурово.*

Доказательство теоремы 6.1 приведено в конце параграфа. В основе доказательства лежит следующее утверждение.

Теорема 6.2. *Пусть $\mathcal{A}$ – S-кольцо над группой D. Тогда каждое нерегулярное базисное множество этого кольца пересекается с E или имеет нетривиальный радикал.*

Доказательство. Пусть X – нерегулярное базисное множество S-кольца $\mathcal{A}$, которое не пересекается с E. Тогда минимальный порядок элемента из X равен 2^m для некоторого $m \geqslant 2$. Обозначим через X_m подмножество множества X, которое состоит из всех элементов порядка 2^m. Ясно, что каждое из множеств $X \setminus X_m$ и X_m непусто. Рассуждая от противного, предположим, что $\mathrm{rad}(X) = e$. Тогда $c_1 \notin \mathrm{rad}(X)$ и $c_1 \in \mathrm{rad}(X \setminus X_m)$ (лемма 5.2). Отсюда следует, что

$$c_1 \notin \mathcal{A}, \tag{8}$$

поскольку в противном случае $c_1 X$ является базисным множеством, которое не совпадает с X, но пересекается с ним.

Обозначим через K стабилизатор множества X в группе $G \cong \mathbb{Z}_{2^n}^*$ всех перестановок $x \mapsto x^m$, $x \in D$, где m – нечётное целое число. Тогда

по теореме Шура о мультипликаторах множество X_m является объединением не более, чем двух K-орбит (одна из них внутри C, а другая снаружи). Радикалы этих орбит должны быть тривиальны, поскольку $\mathrm{rad}(X) = e$ и $c_1 \in \mathrm{rad}(X \setminus X_m)$. Таким образом, по утверждению (1) леммы 4.1 мы имеем

$$X_m = \{x\} \text{ или } \{x, x^{-1}\varepsilon\} \text{ или } \{x, ys\} \text{ или } \{x, x^{-1}\varepsilon, ys, y^{-1}\varepsilon s\}, \quad (9)$$

где элементы $x, y \in X_m$ такие, что $\langle x\rangle = \langle y\rangle$, и $\varepsilon \in \{e, c_1\}$. Следует отметить, что $x \neq \varepsilon y$, поскольку в противном случае $\varepsilon s \in \mathrm{rad}(X)$.

Определим $\mathcal{A}$-группы U и H как в теореме 5.1. Тогда $X \subseteq D \setminus H$, поскольку X не пересекается с E. По определению группы H отсюда следует, что она не содержит элементов порядка 2^m. Принимая во внимание, что $U \leqslant H$, мы заключаем, что $xU \cap X \subseteq X_m$ для каждого $x \in X_m$. Поэтому множество X_m является непересекающимся объединением множеств $xU \cap X$ по таким x. Однако, по лемме 2.1 число $\lambda := |xU \cap X|$ не зависит от выбора элемента $x \in X$. Таким образом, λ делит $|X_m|$. По формуле (9) отсюда следует, что $\lambda \in \{1, 2, 4\}$. Более того, обозначая через Y базисное множество, содержащее элемент c_1, мы получаем равенство

$$c^X_{XY} = \lambda - 1, \quad (10)$$

поскольку $U = Y \setminus e$ или $U = Y \setminus \langle \varepsilon s\rangle$, и $x \neq \varepsilon y$.

Обозначим через α число всех элементов $z \in X_m$, для которых $c_1 z \notin X_m$. Если $\alpha = 1$, то по теореме 2.5 кольцо $\mathcal{A}$ содержит базисное множество $X^{[2]} = \{z^2\}$ для подходящего $z \in X_m$. Поскольку $z \notin E$, отсюда следует, что $c_1 \in \mathcal{A}$ вопреки формуле (8). Таким образом, $\alpha \neq 1$. Поэтому α – чётное число, меньшее или равное $|X_m| \leqslant 4$ (см. (9)). Более того, оно не равно нулю, поскольку иначе $c_1 \in \mathrm{rad}(X)$. Кроме того, из формулы (10) следует, что

$$|X|\,(\lambda - 1) = |X| c^X_{XY} = |Y|\, c^Y_{X X^{-1}} = |Y|\,|c_1 X \cap X| = |Y|\,(|X| - \alpha). \quad (11)$$

Поскольку $|X| > |X_m| \geqslant \alpha$, отсюда следует, что правая часть этого равенства отлична от нуля. Так что, $\lambda \neq 1$, и, значит,

$$\lambda, \alpha \in \{2, 4\}. \quad (12)$$

Лемма 6.3. *Во введённых обозначениях $|X| \geqslant 2|X_m|$, и равенство достигается только, если выполнены следующие утверждения:*

(1) *множество X_m является объединением двух K-орбит и множество $X \setminus X_m$ является K-орбитой,*
(2) *порядок каждого элемента множества $X \setminus X_m$ равен 2^{m+1}.*

Доказательство. По теореме Шура о мультипликаторах стабилизаторы элемента $x \in X$ в группах K и G должны совпадать. Однако, стабилизатор в G состоит из возведений в степень $1 + i|x|$, где $i = 0, 1, \ldots, 2^n/|x| - 1$. Поэтому, $|K_x| = 2^n/|x|$. При $x \in X_m$ и $y \in X \setminus X_m$ отсюда следует, что $|K_x| \geqslant 2|K_y|$, и потому

$$|x^K| = \frac{|G|}{|K_x|} \leqslant \frac{|G|}{2|K_y|} = \frac{|y^K|}{2}.$$

Принимая во внимание, что X_m является непересекающимся объединением не более, чем двух K-орбит, мы получаем требуемое неравенство:

$$|X| - |X_m| \geqslant |y^K| \geqslant 2|x^K| \geqslant |X_m|.$$

Для завершения доказательства достаточно заметить, что равенство здесь выполняется только если второе и третье неравенства в формуле являются равенствами. □

Заметим, что $|Y| \neq \lambda - 1$: действительно, для $\lambda = 2$ это следует из формулы (8), а для $\lambda = 4$ предположение $|Y| = \lambda - 1$ влечёт в силу формулы (11) невозможное равенство $|X| = |X| - \alpha$. Таким образом, по формуле (11) и лемме 6.3 мы имеем

$$\frac{\alpha\,|Y|}{|Y| - (\lambda - 1)} = |X| \geqslant 2|X_m| \geqslant 2\alpha.$$

Далее, если $\lambda = 2$, то $|Y| = 2$ и $|X| = 2\alpha$. С другой стороны, если $\lambda = 4$, то $\lambda - 1 < |Y| \leqslant 6$ и $|Y| \in \{2^a - 1, 2^a - 2\}$ для некоторого a (теорема 5.1); но тогда $|Y| = 6$ и $|T| = 2\alpha$. Таким образом, в силу (12) имеется ровно четыре возможности:

(1) $\alpha = 2,\ \lambda = 2,\ |Y| = 2,\ |X| = 4,\ |X_m| = 2,$
(2) $\alpha = 4,\ \lambda = 2,\ |Y| = 2,\ |X| = 8,\ |X_m| = 4,$
(3) $\alpha = 2,\ \lambda = 4,\ |Y| = 6,\ |X| = 4,\ |X_m| = 2,$
(4) $\alpha = 4,\ \lambda = 4,\ |Y| = 6,\ |X| = 8,\ |X_m| = 4.$

Во всех случаях $|X| = 2|X_m|$. По лемме 6.3 и формуле (9) отсюда следует, что $X_m = \{x, ys\}$ в случаях (1) и (3), и $X_m = \{x, x^{-1}\varepsilon, sy, sy^{-1}\varepsilon\}$ в случаях (2) и (4). Более того, поскольку число $|Y|$ чётно, множество $U \setminus Y$ является группой порядка два. Не умаляя общности будем считать, что она совпадает с группой $\langle s \rangle$.

Пусть π – естественный эпиморфизм из группы D в факторгруппу $D' = D/U$. Тогда группа D' является циклической, S-кольцо $\mathcal{A}' = \mathcal{A}_{D'}$

циркулянтно[4] и $X' = \pi(X)$ – нерегулярное базисное множество этого кольца (порядки элементов множеств $X'_m = \pi(X_m)$ и $X' \setminus X'_m$ различны). Однако, любое нерегулярное базисное множество циркулянтного S-кольца над 2-группой является теоретико-множественной разностью двух её подгрупп (см. пункт 4.1). Поэтому

$$X' = \langle X' \rangle \setminus \mathrm{rad}(X').$$

Поскольку $X' \neq X'_m$, отсюда следует, что $|X'| \geqslant 3$. С другой стороны, $|X'| = |X|/\lambda$ по определению числа λ. Таким образом, можно исключить случаи (1), (3) и (4). В случае (2) пусть $|\mathrm{rad}(X')| = 2^i$ для некоторого $i \geqslant 0$. Тогда $4 = |X'| = 2^{i+2} - 2^i = 3\,2^i$. Противоречие. □

Любое базисное множество S-кольца $\mathcal{A}$ над группой D, которое пересекается с группой E, обязано содержать инволюцию. Следовательно, такое множество всегда рационально. Отсюда по теореме 6.2 мы получаем следующее утверждение.

Следствие 6.4. *Пусть X – базисное множеств* S*-кольца над группой D. Предположим, что* $\mathrm{rad}(X) = e$*. Тогда X регулярно или рационально.*

Доказательство теоремы 6.1. Предположим, что S-кольцо $\mathcal{A}$ не является регулярным. Тогда оно имеет нерегулярное старшее базисное множество X. Поскольку $\mathrm{rad}(X) = e$, из теоремы 6.2 следует, что множество $X \cap E$ непусто. Следовательно, X содержится в $\mathcal{A}$-группе $H \geqslant E$, определённой в теореме 5.1. Но тогда $H = D$, поскольку множество X старшее. Теперь первое из доказываемых утверждений следует из того, что S-кольцо $\mathcal{A}_H = \mathcal{A}$, очевидно, рационально. Более того, утверждения (2) и (3) теоремы 5.1 не выполнены, поскольку $\mathrm{rad}(\mathcal{A}_H) = \mathrm{rad}(\mathcal{A}) = e$. Так что второе утверждение доказываемой теоремы выполнено для $L = e$ (соотв., для $L = \langle s \rangle$), если выполнено утверждение (1) (соотв., утверждение (4)) теоремы 5.1. □

Из доказательства теоремы 6.1 следует, что если одно из старших базисных множеств кольца $\mathcal{A}$ не является регулярным, то все старшие базисные множества рациональны. Это доказывает справедивость следующего утверждения.

[4]Каждое S-кольцо над циклической группой называется циркулянтным.

Следствие 6.5. *Пусть $\mathcal{A}$ – S-кольцо над группой D. Предположим, что* $\mathrm{rad}(\mathcal{A}) = e$. *Тогда либо все старшие базисные множества кольца $\mathcal{A}$ регулярны, либо все старшие базисные множества кольца $\mathcal{A}$ рациональны.*

§7. S-кольца над $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: регулярный случай

В этом параграфе $C = C_n$ обозначает циклическую подгруппу группы $D = D_n$, изоморфную $\mathbb{Z}_{2^n}$. Через c_1, c_2 и s обозначаются соответственно единственная инволюция группы C, один из двух элементов порядка 4, содержащихся в C, и одна из двух инволюций, содержащихся в $D \setminus C$. Основной результат здесь представлен следующей теоремой.

Теорема 7.1. *Пусть $\mathcal{A}$ – регулярное* S-*кольцо над группой D. Предположим, что* $\mathrm{rad}(\mathcal{A}) = e$. *Тогда $\mathcal{A}$ – циклотомическое* S-*кольцо. Более точно, $\mathcal{A} = \mathrm{Cyc}(K, D)$, где $K \leqslant \mathrm{Aut}(D)$ – одна из групп, перечисленных в Таблице 1.*

K	образующие	$\lvert K\rvert$	n	коммент.
K_1	$(x,s) \mapsto (x,s)$	1	$n \geqslant 2$	$X_1 = \varnothing$
K_2	$(x,s) \mapsto (x^{-1},s)$	2	$n \geqslant 3$	$X_1 = \varnothing$
K_3	$(x,s) \mapsto (c_1x^{-1},s)$	2	$n \geqslant 3$	$X_1 = \varnothing$
K_4	$(x,s) \mapsto (x^{-1},sc_1)$	2	$n \geqslant 3$	$X_1 = \varnothing$
K_5	$(x,s) \mapsto (c_1x^{-1},sc_1)$	2	$n \geqslant 3$	$X_1 = \varnothing$
K_6	$(x,s) \mapsto (sc_2x,sc_1)$, $(x,s) \mapsto (x^{-1},s)$	4	$n \geqslant 4$	$X_a \neq \varnothing$
K_7	$(x,s) \mapsto (sc_2x,sc_1)$, $(x,s) \mapsto (c_1x^{-1},s)$	4	$n \geqslant 4$	$X_a \neq \varnothing$
K_8	$(x,s) \mapsto (sx^{-1},s)$	2	$n \geqslant 4$	$X_a \neq \varnothing$
K_9	$(x,s) \mapsto (sc_1x^{-1},s)$	2	$n \geqslant 4$	$X_a \neq \varnothing$
K_{10}	$(x,s) \mapsto (sc_2x,sc_1)$	2	$n \geqslant 3$	$X_a \neq \varnothing$
K_{11}	$(x,s) \mapsto (sc_2x^{-1},sc_1)$	2	$n \geqslant 4$	$X_a \neq \varnothing$

Таблица 1. Группы циклотомических колец с тривиальным радикалом

Следствие 7.2. *В условиях теоремы 7.1 положим $K = K_i$, где $1 \leqslant i \leqslant 11$. Тогда справедливы следующие утверждения:*

(1) $\langle c_1 \rangle$ *является $\mathcal{A}$-группой,*

(2) *C является $\mathcal{A}$-группой тогда и только тогда, когда $i \leqslant 5$,*
(3) *$\langle \varepsilon s \rangle$ при $\varepsilon \in \{e, c_1\}$, является $\mathcal{A}$-группой тогда и только тогда, когда $i \in \{1, 2, 3, 8, 9\}$.*

В дальнейшем для базисного множества $X \in \mathcal{S}(\mathcal{A})$ мы обозначим через X_0 и X_1 однозначно определённые подмножества группы C, для которых $X = X_0 \cup sX_1$.

Доказательство теоремы 7.1. Пусть X – старшее базисное множество S-кольца $\mathcal{A}$. Тогда по условию теоремы оно регулярно. По теореме Шура о мультипликаторах отсюда следует, что если множество X_a непусто для некоторого $a \in \{0, 1\}$, то X_a является орбитой группы $\mathrm{Aut}(C)_{\{X_a\}}$. Поэтому, X_a имеет вид, описанный в утверждении (1) леммы 4.1. Оставшаяся часть доказательства состоит из лемм 7.3, 7.4 и 7.6: в первой из них одно из множеств X_0 или X_1 пусто, а в двух других оба эти множества не пусты и $|X_0| = 2$ или 1, соответственно.

Лемма 7.3. *Пусть $X_0 = \varnothing$ или $X_1 = \varnothing$. Тогда $\mathcal{A} = \mathrm{Cyc}(K_i, D)$, где $i \in \{1, 2, 3, 4, 5\}$.*

Доказательство. Не умаляя общности можно считать, что $n \geqslant 3$ и $X_1 = \varnothing$. Тогда множество $X = X_0$ порождает группу C. Поэтому C – $\mathcal{A}$-группа и X – старшее базисное множество циркулянтного S-кольца $\mathcal{A}_C$. Поскольку $\mathrm{rad}(X) = e$, отсюда следует, что $\mathrm{rad}(\mathcal{A}_C) = e$. Если при этом $\langle s \rangle$ является $\mathcal{A}$-группой, то $\mathcal{A} = \mathcal{A}_C \otimes \mathcal{A}_{\langle s \rangle}$ по лемме 2.3, и потому $\mathcal{A} = \mathrm{Cyc}(K_i, D)$ при $i = 1, 2, 3$. Таким образом, можно считать, что

$$s \notin \mathcal{A}. \tag{13}$$

Докажем индукцией по n, что $\mathcal{A} = \mathrm{Cyc}(K_i, D)$, где $i = 4$ или 5. При $n = 3$ утверждение было проверено на компьютере. Пусть $n > 3$. Обозначим через X' базисное множество кольца $\mathcal{A}$, которое содержит элемент $x' = xs$, где $x \in X$ – образующая группы C. Тогда по условию теоремы X' – регулярное множество с тривиальным радикалом. Поэтому группа $C' = \langle X' \rangle$ совпадает с единственной отличной от C циклической подгруппой группы D порядка 2^n. В частности,

$$\mathrm{rad}(\mathcal{A}_{C'}) = \mathrm{rad}(X') = e.$$

Кроме того, поскольку $C^2 = (C')^2$, базисные множества S-колец $\mathcal{A}_C$ и $\mathcal{A}_{C'}$, содержащиеся в группе C^2, одни и те же; отсюда следует, в частности, что $|X| = |X'|$. Однако, эти S-кольца не являются изоморфными по Кэли. Действительно, в противном случае $X' = sY$,

где $Y = X^{(m)}$ для некоторого нечётного числа m. Тогда s является единственным элементом, который появляется в произведении $\underline{Y^{-1}}\,\underline{X'}$ с кратностью $|X|$. Однако, в этом случае $s \in \mathcal{A}$, что противоречит формуле (13). Таким образом,

$$X = \{x, \varepsilon x^{-1}\} \quad \text{и} \quad X' = \{sx, sc_1\varepsilon x^{-1}\}. \tag{14}$$

Положим $i = 4$ или 5, если соответственно $\varepsilon = e$ или $\varepsilon = c_1$. Тогда из равенств (14) и теоремы Шура о мультипликаторах следует, что S-кольца $\mathcal{A}$ и $\mathrm{Cyc}(K_i, D)$ имеют одни и те же старшие базисные множества. Отметим также, что D_{n-1} является $\mathcal{A}$-группой.

Так как S-кольцо $\mathcal{A}_C$ является циклотомическим, из равенств (14) следует, что $Y = \{x^2, x^{-2}\}$ является базисным множеством кольца $\mathcal{A}$. Обозначим через Y' его базисное множество, содержащее элемент sx^2. Тогда, очевидно,

$$Y' \subseteq X\,X' = \{sx^2, sc_1x^{-2}, s, sc_1\}.$$

Однако, $|sx^2| \geqslant 8$, поскольку $n \geqslant 4$. Следовательно, $Y' \subseteq \{sx^2, sc_1x^{-2}\}$: в противном случае множество $Y \cap E$ непусто, и тогда $|Y'| > 4$ по теореме 5.1. Так что, множество Y' регулярно и $\mathrm{rad}(Y') = e$. Учитывая, что $\mathrm{rad}(Y) = e$ и что Y, Y' – старшие базисные множества S-кольца $\mathcal{A}_{D_{n-1}}$, видим, что последнее удовлетворяет условию леммы 7.3. По индукции отсюда следует, что $\mathcal{A}_{D_{n-1}} = \mathrm{Cyc}(K_4, D_{n-1})$. Таким образом, $\mathcal{A} = \mathrm{Cyc}(K_i, D)$. □

Лемма 7.4. *Пусть* $|X_0| = 2$ *и* $X_1 \neq \varnothing$. *Тогда* $\mathcal{A} = \mathrm{Cyc}(K_i, D)$ *при* $i \in \{6, 7\}$.

Доказательство. По утверждению (1) леммы 4.1 в этом случае мы имеем $X_0 = \{x, \varepsilon x^{-1}\}$. В силу регулярности множества X отсюда следует, что

$$X = \{x, \varepsilon x^{-1}, sy, s\varepsilon y^{-1}\} \tag{15}$$

для некоторой образующей y группы C. Для $n = 3$ мы проверили на компьютере, что ни одно S-кольцо над D не имеет старшего базисного множества X такого, что $X_0 = \{x, \varepsilon x^{-1}\}$ и $X_1 \neq \varnothing$. Предположим, что $n \geqslant 4$. Докажем, что утверждение леммы справедливо для $i = 6$ или $i = 7$, если соответственно $\varepsilon = e$ или $\varepsilon = c_1$. Для $n = 4$ мы проверили это утверждение на компьютере. Поэтому далее считаем, что $n \geqslant 5$.

Лемма 7.5. *В сделанных предположениях справедливы следующие утверждения:*

(1) C_{n-1} *является* $\mathcal{A}$*-группой, а* $\langle s\rangle$ *и* $\langle sc_1\rangle$ *нет,*
(2) $Y_x = \{x^{\pm 2}, c_1x^{\pm 2}\}$ *и* $Z_x = \{sx^{\pm 2}\}$ *являются* $\mathcal{A}$*-множествами,*
(3) $y = xc_2$ *для подходящего выбора* y *и* c_2.[5]

Доказательство. Так как $n \geqslant 5$, выполнены неравенства $x^2 \neq x^{-2}$ и $y^2 \neq y^{-2}$. Кроме того, поскольку ни s, ни sc_1 не принадлежат радикалу множества X, также $x^2 \neq y^{\pm 2} \neq x^{-2}$. Таким образом,

$$|\{x^2, x^{-2}, y^2, y^{-2}\}| = 4. \tag{16}$$

Однако, $X^{[2]} = \{x^2, x^{-2}, y^2, y^{-2}\}$, и это множество является $\mathcal{A}$-множеством по теореме 2.5. Отсюда следует первая часть утверждения (1), поскольку $C_{n-1} = \langle X^{[2]}\rangle$. Для доказательства второй части этого утверждения, предположим, что наоборот $L := \langle s\varepsilon'\rangle$ является $\mathcal{A}$-группой для некоторого $\varepsilon' \in \{e, c_1\}$. Тогда циркулянтное S-кольцо $\mathcal{A}_{D/L}$ имеет базисное множество

$$\pi(X) = \{\pi(x), \pi(\varepsilon x^{-1}), \pi(y), \pi(\varepsilon y^{-1})\},$$

где $\pi : D \to D/L$ – естественный эпиморфизм. Однако, из формулы (16) легко следует, что $|\operatorname{rad}(\pi(X))| \geqslant 2$. Поэтому, одно из частных $\pi(x)/\pi(\varepsilon x^{-1})$, $\pi(x)/\pi(y)$ или $\pi(x)/\pi(\varepsilon y^{-1})$ имеет порядок 2. Отсюда получается, что, соответственно, $|\pi(x)| = 8$, $\pi(x) = \pi(c_1)\pi(y)$ и $\pi(x) = \pi(c_1)\pi(\varepsilon y^{-1})$. Но первый случай невозможен, поскольку $n \geqslant 5$. В двух других получается, что $x \in c_1yL$ и $x \in c_1\varepsilon y^{-1}L$, что также невозможно, но уже в силу (16).

Для доказательства второй части утверждения (2) заметим, что $C_{n-1} \cup \operatorname{tr}(X)$ является $\mathcal{A}$-множеством. Его дополнение в D равно множеству sC_{n-1}. Поэтому оно также является $\mathcal{A}$-множеством. Кроме того,

$$\underline{X}^2 \circ \underline{sC_{n-1}} = 2\,\underline{sX'}, \tag{17}$$

где $X' = \{(xy)^{\pm 1}, \varepsilon(xy^{-1})^{\pm 1}\}$. Поэтому и sX' является $\mathcal{A}$-множеством. Однако, легко видеть, что $|xy| \neq |\varepsilon xy^{-1}|$. Более того, $|xy| = 2^{n-1}$ или $|\varepsilon xy^{-1}| = 2^{n-1}$, поскольку x и y – образующие группы C и $n \geqslant 3$. Таким образом, элементы sxy и $s\varepsilon xy^{-1}$ не могут принадлежать одному и тому же базисному множеству кольца $\mathcal{A}$. Действительно, в противном случае в предположении $|xy| = 2^{n-1}$, мы заключаем по лемме 5.2, что это базисное множество содержит элемент $sxyc_1$. Но тогда $xyc_1 \in X'$, и потому $xyc_1 \in \{(xy)^{-1}, \varepsilon x^{-1}y\}$. Следовательно,

[5]Можно заменить y на y^{-1} и независимо c_2 на c_2^{-1}.

$(xy)^2 = c_1$ или $x^2 = c_1\varepsilon$. В любом случае $n-1 \leqslant 2$. Противоречие. Аналогично получаем противоречие, если $|\varepsilon xy^{-1}| = 2^{n-1}$. Так же можно проверить и то, что никакие два элемента, один из которых принадлежит множеству $\{s(xy)^{\pm 1}\}$, а другой – множеству $\{s\varepsilon(xy^{-1})^{\pm 1}\}$, не могут принадлежать одному и тому же базисному множеству кольца $\mathcal{A}$. Таким образом, sX' является непересекающимся объединением двух $\mathcal{A}$-множеств вида $\{sz^{\pm 1}\}$, где $z \in C$, причём одно из них состоит из элементов порядка 2^{n-1}. Отсюда следует, что Z_x – $\mathcal{A}$-множество.

Для доказательства утверждения (3) предположим от противного, что $x^4 \neq y^{\pm 4}$. Тогда поскольку $Y := X^{[2]}$, то Z_x и Z_y являются $\mathcal{A}$-множествами, и S-кольцо $\mathcal{A}$ содержит элемент

$$(\underline{Y}\,\underline{Z_x}) \circ (\underline{Y}\,\underline{Z_y}) = 2s(2e + x^{\pm 2}y^{\pm 2}).$$

При $n \geqslant 3$ только элемент s появляется в правой части с коэффициентом 4. Поэтому $s \in \mathcal{A}$. Однако, это противоречит второй части утверждения (1).

Для завершения доказательства заметим, что $Y_x = X^{[2]}$ по уже доказанному утверждению (3). Отсюда следует первая часть утверждения (2), поскольку $X^{[2]}$ является $\mathcal{A}$-множеством. □

Продолжим доказательство леммы 7.4. Обозначим через $\mathcal{A}_i$ минимальное S-кольцо над группой D, для которого X является базисным множеством; напомним, что $i = 6$ или $i = 7$, если, соответственно, $\varepsilon = e$ или $\varepsilon = c_1$. Докажем, что

$$\mathcal{A}_i = \mathrm{Cyc}(K_i, D). \tag{18}$$

Действительно, в силу утверждений (2) и (3) леммы 7.5 множества X, Y_x и Z_x являются орбитами группы K_i (см. Таблицу 2, которая содержит описание орбит группы K_i внутри множеств C_{n-1} и sC_{n-1}). По теореме Шура о мультипликаторах отсюда следует, что

$$(\mathcal{A}_i)_{D\setminus D_{n-2}} = \mathrm{Cyc}(K_i, D)_{D\setminus D_{n-2}}. \tag{19}$$

Далее, $C' := \langle Z_x \rangle$ – циклическая $\mathcal{A}$-группа порядка 2^{n-1}, отличная от C_{n-1}. Поэтому, Z_x – старшее базисное множество циркулянтного S-кольца $(\mathcal{A}_i)_{C'}$. Следовательно, радикал этого S-кольца тривиален. Тогда в силу результатов, приведённых после леммы 4.1, оно является циклотомическим S-кольцом $\mathrm{Cyc}(K', C')$ для некоторой группы $K' \leqslant \mathrm{Aut}(C')$, одна из орбит которой совпадает с Z_x. Поскольку

C_{n-1}	sC_{n-1}
$x^{\pm 2}, c_1x^{\pm 2}$	$s\varepsilon x^{\pm 2}$
x^4, x^{-4}	$sx^{\pm 4}, sc_1x^{\pm 4}$
$\cdots$	$\cdots$
c_2, c_2^{-1}	sc_2, sc_2^{-1}
c_1	s, sc_1
e	

Таблица 2. Орбиты групп K_6 и K_7

$\mathrm{Orb}(K_i, C') = \mathrm{Orb}(K', C')$, мы заключаем, что

$$(\mathcal{A}_i)_{C_{n-2}} = \mathrm{Cyc}(K_i, D)_{C_{n-2}}. \tag{20}$$

Завершим доказательство формулы (18). С этой целью, используя равенство $\varepsilon(e + c_1) = e + c_1$, мы получим, что

$$\underline{Y_x}\,\underline{Z_x} = sx^{\pm 4}(e + c_1) + 2s(e + c_1). \tag{21}$$

Более того, поскольку $n \geqslant 5$, элементы $x^{\pm 4}, sx^{\pm 4}c_1$ появляются в правой части с коэффициентом 1. В силу принципа Шура–Виландта, отсюда следует, что $\{s, sc_1\}x^{\pm 4}$ и $\{s, sc_1\}$ являются $\mathcal{A}$-множествами. Таким образом,

$$(\mathcal{A}_i)_{sC_m \setminus sC_{m-1}} = \mathrm{Cyc}(K_i, D)_{sC_m \setminus sC_{m-1}} \text{ и } (\mathcal{A}_i)_{sC_1} = \mathrm{Cyc}(K_i, D)_{sC_1}, \tag{22}$$

где $m = n-2$. Для всех $m = n-3, \ldots, 2$ первое из этих равенств доказывается аналогично индукцией по m; при этом множества Y_x и Z_x в равенстве (21) заменяются на $\mathcal{A}$-множества $\{x^{\pm 2^{m+1}}\}$ и $(e + c_1)\{x^{\pm 2^{m+1}}\}$, соответственно. Так что, формула (18) следует из равенств (19), (20) и (22).

Продолжим доказательство леммы 7.4. Поскольку, очевидно, что $\mathcal{A} \geqslant \mathcal{A}_i$, из формулы (18) следует включение $\mathcal{A} \geqslant \mathrm{Cyc}(K_i, D)$. Для проверки обратного включения надо доказать, что каждая K_i-орбита Z' принадлежит множеству $\mathcal{S}(\mathcal{A})$. Предполагая противное, допустим, что некоторая K_i-орбита Z' собственно содержит множество $Z \in \mathcal{S}(\mathcal{A})$. Тогда

$$Z \subseteq D_{n-1} \setminus D_1. \tag{23}$$

Действительно, в силу формулы (15) и утверждения (3) леммы 7.5, все K_i-орбиты, не лежащие в группе D_{n-1}, являются базисными множествами кольца $\mathcal{A}$. Кроме того, таковыми являются и орбиты $\{e\}$ и $\{c_1\}$, поскольку $\mathcal{A} \geqslant \mathrm{Cyc}(K_i, D)$. Наконец, орбита $\{s, c_1 s\}$ является базисным множеством по второй части утверждения (1) леммы 7.5.

В силу формулы (23) и первой части утверждения (1) леммы 7.5, множество Z является регулярным, а потому и орбитой некоторой группы автоморфизмов группы C. Отсюда следует, что мощность множества Z равна 1, 2 или 4. Последний случай невозможен, поскольку иначе $Z = Z'$. Докажем, что и первый случай невозможен. Действительно, предположим, что $Z = \{z\}$ для некоторого $z \in D_{n-1} \setminus D_1$. Тогда zX – старшее базисное множество кольца $\mathcal{A}$. Однако, в этом случае $(zX)_0 = \{zx, z\varepsilon x^{-1}\}$. Поэтому, $\varepsilon(zx)^{-1} = z\varepsilon x^{-1}$, и, значит, $z = z^{-1}$. Так что, $z \in D_1$. Противоречие.

Для завершения доказательства леммы 7.4 предположим теперь, что $|Z| = 2$. Не умаляя общности можно считать, что порядок элемента множества Z минимальный из возможных. Ясно, что $|Z'| = 4$, и, значит,

$$Z' = \{z^{\pm 1}, c_1 z^{\pm 1}\},$$

где либо $z = x^2$, либо $z = sx^{2^m}$ причём $m \in \{3, \ldots, n-3\}$ (см. Таблицу 2). Выберем $z \in Z$ так, чтобы

$$Z = \{z, c_1 z\} \quad \text{или} \quad Z = \{z, \varepsilon' z^{-1}\},$$

где $\varepsilon' \in \{e, c_1\}$. В первом случае $Z^2 = \{z^2\}$ является базисным множеством кольца $\mathcal{A}$. Используя применённый выше аргумент, легко видеть, что $z^2 \in D_1$. Так что, $z \in D_2$. Противоречие. Во втором случае кольцо $\mathcal{A}$ содержит элемент

$$(sz + sz^{-1})(z + \varepsilon' z^{-1}) = sz^2 + s\varepsilon' z^{-2} + s + s\varepsilon'.$$

Поскольку $s \notin \mathcal{A}$, отсюда следует, что $\varepsilon' = c_1$. Поэтому $\{sz^2, s\varepsilon' z^{-2}\}$ не может быть базисным множеством кольца $\mathcal{A}$, и, значит, $m \neq 3$. Но тогда, $\{sz^2, s\varepsilon' z^{-2}, s, s\varepsilon'\} \in \mathcal{S}(\mathcal{A})$ по минимальности числа $|z|$, что невозможно, в силу того, что $s + sc_1 \in \mathcal{A}$. □

Лемма 7.6. *Пусть* $|X_0| = 1$ *и* $X_1 \neq \varnothing$. *Тогда* $\mathcal{A} = \mathrm{Cyc}(K_i, D)$, *где* $i \in \{8, 9, 10, 11\}$.

Доказательство. В этом случае $X = \{x, ys\}$, где $\langle y \rangle = C$. Поэтому множество X порождает группу D. Более того, $n \geqslant 3$, поскольку

$c_1 \notin \mathrm{rad}(X)$. Отсюда следует, что в S-кольце $\mathcal{A}$ имеется два ортогонала: один из них содержится в множестве $(X\,X^{-1}) \cap Cs$, а другой – в множестве $(X\,X^{-1}) \cap C$. Таким образом, S-кольцо $\mathcal{A}$ является квазитонким (лемма 3.4), и потому шуровым (лемма 3.5). Из последней леммы также следует, что стабилизатор K точки e в группе $\mathrm{Aut}(\mathcal{A})$ имеет точную регулярную орбиту. Поэтому индекс группы D в группе $\mathrm{Aut}(\mathcal{A})$ равен 2. Но тогда $D \trianglelefteq \mathrm{Aut}(\mathcal{A})$, и, значит, $K \leqslant \mathrm{Aut}(D)$. Следовательно, $\mathcal{A} = \mathrm{Cyc}(K, D)$ и группа K порождается инволюцией $\sigma \in \mathrm{Aut}(D)$. Эта инволюция переставляет между собой элементы x и ys. Поэтому автоморфизм σ определён однозначно. Проверку того, что он является одним из автоморфизмов, указанных в строках 8, 9, 10 и 11 Таблицы 1, мы оставляем читателю. □

§8. S-кольца над $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: группы автоморфизмов в регулярном случае

В этом параграфе мы находим группу автоморфизмов регулярного S-кольца с тривиальным радикалом над группой D. С этой целью напомним следующее определение из [3]: группа перестановок называется 2-*изолированной*, если она не 2-эквивалентна никакой другой группе. Следующее утверждение представляет основной результат этого параграфа; оно показывает, в частности, что любое регулярное S-кольцо с тривиальным радикалом над группой D является нормальным.

Теорема 8.1. *Пусть $\mathcal{A}$ – регулярное* S*-кольцо над группой D. Предположим,что* $\mathrm{rad}(\mathcal{A}) = e$. *Тогда для любой $\mathcal{A}$-группы L порядка, не превосходящего* 2, *группа* $\mathrm{Aut}(\mathcal{A}_{D/L})$ *является* 2*-изолированной. В частности, если $\mathcal{A} = \mathrm{Cyc}(K, D)$ для некоторой группы $K \leqslant \mathrm{Aut}(D)$, то* $\mathrm{Aut}(\mathcal{A}) = DK$.

Доказательство этой теоремы приведено в конце параграфа. В следующем утверждении мы устанавливаем достаточное условие 2-изолированности группы перестановок.

Лемма 8.2. *Пусть $\mathcal{A}$ –* S*-кольцо и $G = \mathrm{Aut}(\mathcal{A})$. Предположим, что стабилизатор точки в группе G имеет точную регулярную орбиту. Тогда группа G является* 2*-изолированной.*

Доказательство. По теореме 3.5′ статьи [3] группа G является 2-изолированной, если она 2-замкнута и стабилизатор в ней каких-либо

двух точек тривиален. Однако, последнее в точности означает, что стабилизатор точки в группе G имеет точную регулярную орбиту. $\square$

Для применения леммы 8.2 нам потребуется следующее вспомогательное утверждение, описывающее достаточное условие существования точной регулярной орбиты стабилизатора точки в группе автоморфизмов S-кольца.

Лемма 8.3. *Пусть $\mathcal{A}$ – S-кольцо над абелевой группой H. Предположим, что множество $X \in \mathcal{S}(\mathcal{A})$ удовлетворяет следующим условиям:*

(1) $\langle \mathrm{tr}(X) \rangle = H$,
(2) $c_{XY}^{Z} = 1$ *для каждого* $Z \in \mathcal{S}(\mathcal{A})_{\mathrm{tr}(X)}$ *и некоторого* $Y \in \mathcal{S}(\mathcal{A})$,
(3) $c_{XY}^{X} = 1$ *для каждого* $Y \in \mathcal{S}(\mathcal{A})_{XX^{-1}}$.

Тогда X содержит точную регулярную орбиту группы $\mathrm{Aut}(\mathcal{A})_e$.

Доказательство. Обозначим через $\mathcal{X}$ схему Кэли (над группой H), соответствующую S-кольцу $\mathcal{A}$. Тогда бинарное отношение

$$r = R_H(\mathrm{tr}(X))$$

является объединением базисных отношений этой схемы. Легко видеть, что оно симметрично, а по условию (1) также и связно. Более того, из условий (2) и (3) следует, что когерентная конфигурация $(\mathcal{X}_e)_{er}$ является полурегулярной. Так что, по теореме 3.3 статьи [24] для каждого $x \in X$ двухэлементное множество $\{e, x\}$ является базой схемы $\mathcal{X}$, а, значит, и базой группы $\mathrm{Aut}(\mathcal{X})$. Отсюда следует, что одноэлементное множество $\{x\}$ является базой группы $K = \mathrm{Aut}(\mathcal{X})_e$. Таким образом, $x^K \subseteq X$ – точная регулярная орбита группы K. $\square$

Доказательство теоремы 8.1. По теореме 7.1 справедливо равенство $\mathcal{A} = \mathrm{Cyc}(K, D)$, где $K = K_i$ – одна из групп, перечисленных в Таблице 1, $1 \leqslant i \leqslant 11$. Поэтому с учётом 2-эквивалентности групп DK и $\mathrm{Aut}(\mathcal{A})$ вторая часть утверждения теоремы следует из первой. Для доказательства последней предположим, не умаляя общности, что $i \geqslant 2$ и $n \geqslant 4$.

Пусть $L \leqslant D$ – $\mathcal{A}$-группа. Положим $H = D/L$ и $\pi = \pi_L$. Для доказательства 2-изолированности группы $\mathrm{Aut}(\mathcal{A}_H)$ достаточно проверить, что её стабилизатор точки имеет точную регулярную орбиту (лемма 8.2). Оставшаяся часть доказательства разбивается на три случая.

Случай 1: $L = \langle \varepsilon s \rangle$, где $\varepsilon \in \{e, c_1\}$. Здесь H – циклическая группа и S-кольцо $\mathcal{A}_H = \mathrm{Cyc}(\pi(K), H)$ является циклотомическим. Более того, $i \in \{2, 3, 8, 9\}$ по утверждению (3) следствия 7.2. Поэтому порядок группы $\pi(K) \leqslant \mathrm{Aut}(H)$ не превосходит 2. В силу импликации (3) $\Rightarrow$ (2) теоремы 6.1 из статьи [1], отсюда следует, что группа $\mathrm{Aut}(\mathcal{A}_H)_e$ имеет точную регулярную орбиту. Таким образом, группа $\mathrm{Aut}(\mathcal{A}_H)$ является 2-изолированной по лемме 8.2.

Случай 2: $e \leqslant L \leqslant \langle c_1 \rangle$ и $|K| = 2$. Здесь $i \notin \{1, 6, 7\}$, и мощность любого базисного множества кольца $\mathcal{A}$ не превосходит 2. Поскольку $\mathcal{A}$ коммутативно, последнее верно и для базисных множеств кольца $\mathcal{A}_H$. Поэтому это S-кольцо является квазитонким. Следовательно, по второй части леммы 3.5 достаточно проверить, что в кольце $\mathcal{A}_H$ имеется по крайней мере два ортогонала. Для этого обозначим через X базисное множество кольца $\mathcal{A}$, содержащее образующую группы C. Поскольку S-кольцо$\mathcal{A}$ является циклотомическим, $\pi(X^{(2)})$ и $\pi(X^{(4)})$ – базисные множеств кольца $\mathcal{A}_H$. Более того, они не равны, поскольку $n \geqslant 4$. Наконец, они являются ортогоналами, поскольку $\pi(X^{(2)}) \subseteq \pi(X)\,\pi(X^{-1})$ и $\pi(X)^{(4)} \subseteq \pi(X^{(2)})\,\pi(X^{(-2)})$.

Случай 3: $e \leqslant L \leqslant \langle c_1 \rangle$ и $|K| = 4$. Здесь $i = 6$ или 7. Достаточно проверить, что выполнено условие леммы 8.3 для старшего базисного множества X S-кольца $\mathcal{A}_H$. С этой целью отметим, что каждое из множеств X_0 и X_1 непусто. Поэтому $\mathrm{tr}(X) = D \setminus D_{n-1}$, и условие (1) очевидно выполнено.

Для проверки условий (2) и (3) предположим сначала, что $L = e$. Тогда для любого $x \in X_0$ имеем

$$X = \{x, \varepsilon x^{-1}, sc_2 x, sc_2^{-1} \varepsilon x^{-1}\},$$

где $\varepsilon \in \{e, c_1\}$. Поскольку $n \geqslant 4$, элементы xy^{-1} при $y \in X$ принадлежат различным K-орбитам, мощности которых равны соответственно $1, 2, 2$ и 4. Прямая проверка показывает, что если Y – одна из этих орбит, то

$$|Y| c^Y_{XX^{-1}} = 4.$$

Поэтому $4 = |Y| c^Y_{XX^{-1}} = |X| c^X_{XY^{-1}}$, и условие (3) выполнено, поскольку $|X| = 4$. Пусть теперь $Z \in \mathcal{S}(\mathcal{A})_{\mathrm{tr}(X)}$. Тогда

$$Z = \{xy, \varepsilon(xy)^{-1}, sc_2 xy, sc_2^{-1} \varepsilon (xy)^{-1}\}$$

для некоторого $y \in C_{n-1}$. Пусть Y – то из множеств $\{y^{\pm 1}, c_1 y^{\pm 1}\}$, $\{y^{\pm 1}\}$ или $\{y\}$, для которого y принадлежит множеству $C_{n-1} \setminus C_{n-2}$,

$C_{n-2}\setminus C_1$ или C_1, соответственно. Тогда Y – базисное множество кольца $\mathcal{A}$. Более того, прямое вычисление показывает, что в каждом случае $c^X_{YZ}=1$. Поскольку $c^Z_{XY}=c^{X^{-1}}_{Y^{-1}Z^{-1}}=c^X_{YZ}$, условие (2) также выполнено.

Пусть теперь $L=\langle c_1\rangle$. Для упрощения обозначений отождествим группу $H=D/L$ с группой D_{n-1}, будем писать $\mathcal{A}$ вместо $\mathcal{A}_H$[6] и использовать обозначения x и s для π-образов элементов x и sc_1, соответственно. Таким образом, $\mathcal{A}$ – циклотомическое S-кольцо над группой D_{n-1}, и

$$X=\{x,x^{-1},sx,sx^{-1}\}$$

является старшим базисным множеством этого кольца. Отсюда следует, что C_{n-2} – $\mathcal{A}$-группа и каждое базисное множество внутри C_{n-2} имеет вид $\{z^{\pm1}\}$ для подходящего $z\in C_{n-2}$. Поскольку sC_{n-2} является $\mathcal{A}$-множеством, элементы xy^{-1} при $y\in X$ принадлежат разным базисным множествам кольца $\mathcal{A}$. Следовательно, множество $X\,X^{-1}$ состоит из базисных множеств Y, для которых $c^X_{XY}=1$. Так что, выполнено условие (3). Пусть теперь $Z\in\mathcal{S}(\mathcal{A})_{\mathrm{tr}(X)}$. Тогда

$$Z=\{xy,(xy)^{-1},sxy,s(xy)^{-1}\}$$

для некоторого $y\in C_{n-2}$. Выбирая в качестве Y базисное множество $\{y^{\pm1}\}$, мы получим равенство $c^X_{YZ}=1$. Таким образом, условие (2) также выполнено. □

§9. S-кольца над $D=\mathbb{Z}_2\times\mathbb{Z}_{2^n}$: случай нетривиального радикала

В теоремах 6.1 и 7.1 мы полностью описали структуру S-кольца над группой D, радикал которого тривиален. В этом параграфе мы изучим оставшиеся S-кольца.

Теорема 9.1. *Пусть $\mathcal{A}$ – S-кольцо над группой D. Предположим, что $\mathrm{rad}(\mathcal{A})\neq e$. Тогда $\mathcal{A}$ является собственным обобщённым S-сплетением, где секция $S=U/L$ такая, что*

$$\mathcal{A}_S=\mathbb{Z}S\quad\textit{или}\quad|S|=4\quad\textit{или}\quad\mathrm{rad}(\mathcal{A}_U)=e\ \textit{и}\ |L|=2. \tag{24}$$

Доказательство. Обозначим через U подгруппу группы D, порождённую всеми множествами $X\in\mathcal{S}(\mathcal{A})$, для которых $\mathrm{rad}(X)=e$.

Лемма 9.2. *U является $\mathcal{A}$-группой и $\mathrm{rad}(\mathcal{A}_U)=e$.*

[6] В нашем случае S-кольцо $\mathcal{A}_H$ не зависит от выбора $i\in\{5,6\}$.

Доказательство. Первое утверждение очевидно. Для доказательства второго утверждения предположим, не умаляя общности, что $U=D$. Тогда найдётся старшее множество $X \in \mathcal{S}(\mathcal{A})$ такое, что $\mathrm{rad}(X)=e$. Предположим сначала, что X не является регулярным. Тогда множество $X \cap E$ не пусто по теореме 6.2. Поэтому X – одно из базисных множеств X_{c_1}, X_s или X_{sc_1} из теоремы 5.1. Поскольку $\mathrm{rad}(X) = e$, в утверждениях (2) и (3) этой теоремы мы имеем $X = X_{c_1}$ и $X = X_s$, соответственно. Более того, поскольку множество X старшее, в утверждениях (1), (2), (3) мы имеем $D = \langle X \rangle$. Поэтому, в соответствующих трёх случаях $\mathrm{rk}(\mathcal{A}) = 2$, и, значит, $\mathrm{rad}(\mathcal{A}) = e$. В оставшемся случае (утверждение (4) теоремы 5.1), $D = H$, и, значит, $\mathcal{A} = \mathcal{A}_U \otimes \mathcal{A}_{\langle s \rangle}$. Поскольку каждый сомножитель имеет ранг, равный 2, мы снова получаем, что $\mathrm{rad}(\mathcal{A}) = e$.

Теперь можно считать, что каждое старшее базисное множество с тривиальным радикалом регулярно (следствие 6.4). Более того, если X – одно из таких множеств, причём множества X_0 и X_1 оба не пусты, то все старшие базисные множества рационально сопряжены и, значит, $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(X) = e$. Так что можно считать также, что $\langle X \rangle = C$ – циклическая группа порядка по крайней мере 4, которая имеет индекс 2 в D.

Поскольку $\mathrm{rad}(\mathcal{A}_C) = \mathrm{rad}(X) = e$, циркулянтное S-кольцо $\mathcal{A}_C$ является циклотомическим (см. пункт 4.1). С учётом неравенства $|C| \geqslant 4$ отсюда следует, что $c_1 \in \mathcal{A}$. Докажем, что каждое множество $Y \in \mathcal{S}(\mathcal{A})$ является регулярным, если $\mathrm{rad}(Y) = e$ и $D = \langle X, Y \rangle$. Пусть это не так. Тогда по теореме 6.2 мы имеем $Y = X_h$, где h – неединичный элемент группы E. Однако, $h \neq c_1$: в противном случае получаем, как и выше, что $Y = \{c_1\}$, откуда следует, что $\langle X, Y \rangle = C$, вопреки предположению. Тогда, поскольку $X_{c_1} = \{c_1\}$ и $\mathrm{rad}(Y) = e$, может выполняться лишь утверждение (4) теоремы 5.1. В этом случае Y состоит из одного элемента группы E, и потому регулярен. Противоречие.

Для завершения доказательства возьмём регулярное базисное множество Y с тривиальным радикалом. Будем считать, что $Y \subseteq D \setminus C$; в противном случае, $D = C$ и $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(X) = e$. Если множество Y не является старшим, то старшим является любое базисное множество $Z \subseteq XY$, причём $\langle X, Z \rangle = D$. Более того, тогда $\mathrm{rad}(Z) = e$ по лемме 4.3. Так что, можно считать, что множество Y старшее. Но в этом случае любое старшее базисное множество кольца $\mathcal{A}$ рационально сопряжено с X или Y, и потому $\mathrm{rad}(\mathcal{A}) = e$. □

Из условия теоремы и леммы 9.2 следует, что $U \neq D$. Отметим также, что по теореме 2.2 группа U содержит каждую минимальную $\mathcal{A}$-группу.

Лемма 9.3. *Предположим, что либо имеется единственная минимальная $\mathcal{A}$-группа, либо $c_1 \in \mathrm{rad}(X)$ для всех $X \in \mathcal{S}(\mathcal{A})_{D\setminus U}$. Тогда выполнено утверждение теоремы* 9.1.

Доказательство. Пусть L – единственная минимальная $\mathcal{A}$-группа. Тогда по определению группы U кольцо $\mathcal{A}$ является собственным обобщённым S-сплетением, где $S = U/L$. Если при этом $|L| \leqslant 2$, то по лемме 9.2 выполнено третье утверждение из формулы (24). Пусть теперь $|L| > 2$. Тогда $\langle c_1\rangle$ не является $\mathcal{A}$-группой. По утверждению (1) следствия 7.2, отсюда следует, что S-кольцо $\mathcal{A}_U$ не регулярно. Но тогда оно рационально по первой части теоремы 6.1. Значит, $U = L$ по второй части этой теоремы и единственности группы L. Так что, $|S| = 1$, и выполнено первое утверждение из формулы (24).

Для завершения доказательства предположим, что имеется по крайней мере две минимальные $\mathcal{A}$-группы. Тогда, очевидно, одна из них, скажем H, содержит элемент c_1. Поэтому $c_1 \in H \leqslant U$. С другой стороны, по условию леммы $c_1 \in \mathrm{rad}(X)$ для всех $X \in \mathcal{S}(\mathcal{A})_{D\setminus U}$. Так что, $\mathcal{A}$ – собственное обобщённое S-сплетение, где $S = U/H$. Не умаляя общности можно считать, что $|H| > 2$. Если S-кольцо $\mathcal{A}_U$ рационально, то по второй части теоремы 6.1 найдётся ещё одна минимальная $\mathcal{A}$-группа L порядка 2 такая, что

$$\mathcal{A}_U = \mathcal{A}_H \otimes \mathcal{A}_L.$$

Таким образом, $|S| = |L| = 2$, и выполнено первое утверждение из формулы (24). В оставшемся случае по первой части теоремы 6.1 S-кольцо $\mathcal{A}_U$ регулярно. Но тогда $H = \langle c_1\rangle$ по утверждению (1) следствия 7.2. Значит, $|H| = 2$, и выполнено третье утверждение из формулы (24). □

Обозначим через V объединение всех множеств $X \in \mathcal{S}(\mathcal{A})$, для которых $\mathrm{rad}(X) = e$ или $c_1 \in \mathrm{rad}(X)$. Тогда, очевидно, $U \subseteq V$, и V является $\mathcal{A}$-множеством. По лемме 9.3 можно считать, что $V \neq D$, и что U содержит две различных минимальных $\mathcal{A}$-группы. В этом случае легко видеть, что $E \subseteq V$.

Лемма 9.4. *В сделанных предположениях пусть $X \in \mathcal{S}(\mathcal{A})_{D\setminus V}$. Тогда*

(1) $\mathrm{rad}(X) = \langle s\rangle$ *или* $\langle sc_1\rangle$,

(2) *X регулярно, а X_0 и X_1 не пусты.*

Доказательство. Заметим, что $\mathrm{rad}(X) \neq e$, поскольку $X \not\subseteq U$. Кроме того, $c_1 \notin \mathrm{rad}(X)$ по определению множества V. Таким образом, утверждение (1) выполнено, поскольку $\langle s \rangle$ и $\langle sc_1 \rangle$ – единственные подгруппы группы D, не содержащие элемент c_1. Для доказательства утверждения (2) положим

$$L = \mathrm{rad}(X) \quad \text{и} \quad \pi = \pi_{D/L}.$$

Тогда $\mathrm{rad}(\pi(X)) = e$. Однако, D/L – циклическая 2-группа по утверждению (1). Поэтому $\pi(X)$ – базисное множество циркулянтного S-кольца $\mathcal{A}_{D/L}$. В силу описания базисных множеств такого S-кольца, приведённого в пункте 4.1, множество $\pi(X)$ либо регулярно, либо имеет вид

$$\pi(X) = \pi(H)^{\#}$$

для некоторой $\mathcal{A}$-группы $H \geqslant D_1$ такой, что $|H/L| \geqslant 4$. В последнем случае $X = H \setminus L$, и, значит, L – единственная минимальная $\mathcal{A}$-группа, что противоречит сделанному предположению об U. Следовательно, множество $\pi(X)$ регулярно. Отсюда следует, что регулярно и множество X. Теперь, непустота множеств X_0 и X_1 легко следует из утверждения (1). □

По утверждению (2) леммы 9.4 объединение всех множеств $\mathrm{tr}(X)$ при $X \in \mathcal{S}(\mathcal{A})_{D \setminus V}$, имеет вид $D \setminus D_k$ для некоторого $k \geqslant 1$. Однако, множество V совпадает с дополнением к этому объединению. Таким образом, $V = D_k$ является $\mathcal{A}$-группой. Аналогичные рассуждения показывают, что D_m является $\mathcal{A}$-группой для всех $m \geqslant k$.

Лемма 9.5. *Пусть $m = \max\{2, k\}$. Тогда группа $L := \mathrm{rad}(X)$ не зависит от выбора множества $X \in \mathcal{S}(\mathcal{A})_{D \setminus D_m}$.*

Доказательство. Рассуждая от противного, предположим, что существуют базисные множества X и Y, не пересекающиеся с D_m, для которых $\langle Y \rangle \subsetneq \langle X \rangle$ и $\mathrm{rad}(X) \neq \mathrm{rad}(Y)$. Тогда по утверждению (1) леммы 9.4 не умаляя общности можно считать, что

$$\mathrm{rad}(X) = \langle s \rangle \quad \text{и} \quad \mathrm{rad}(Y) = \langle sc_1 \rangle. \tag{25}$$

По утверждению (2) указанной выше леммы, множество X_0 не пусто и регулярно. Поэтому оно является орбитой некоторой подгруппы группы $\mathrm{Aut}(C)$. Более того, $\mathrm{rad}(X_0) = e$ в силу первого равенства из формулы (25). Пусть теперь $\pi : D \to D/\langle s \rangle$ – естественный

эпиморфизм. Тогда $\pi(X) = X_0$ – базисное множество циркулянтного S-кольца $\mathcal{A}' = \pi(\mathcal{A})$. Отсюда следует, что $\mathcal{A}'_{\langle X_0\rangle}$ – циклотомическое S-кольцо с тривиальным радикалом, $Y' = \pi(Y)$ – базисное множество этого S-кольца и $|\langle Y'\rangle| \geqslant 2^{m+1} \geqslant 8$. Поэтому по лемме 4.2, применённой к $\mathcal{A} = \mathcal{A}'_{\langle X_0\rangle}$ и $S = \langle Y'\rangle/e$, мы получаем, что

$$\mathrm{rad}(\mathcal{A}'_{\langle Y'\rangle}) = e.$$

Следовательно, $\mathrm{rad}(Y') = e$. С другой стороны, $\mathrm{rad}(Y') = \langle c_1\rangle \neq e$ по второму равенству из формулы (25). Противоречие. □

По лемме 9.5 S-кольцо $\mathcal{A}$ является обобщённым S-сплетением, где $S = D_2/L$, если $k = 1$, и $S = V/L$, если $k \geqslant 2$. Единственный случай, когда это обобщённое сплетение не является собственным, возникает при $D = D_2$ и $k = 1$. Однако, тогда кольцо $\mathcal{A}$, очевидно, является собственным E/L-сплетением, и $|E/L| = 2$. Таким образом, если $k \leqslant 2$, то выполнено первое или второе утверждение из формулы (24). Для завершения доказательства теоремы 9.1 достаточно проверить, что при $k \geqslant 3$ выполнено третье утверждение из этой формулы. Однако, это следует из формулируемой ниже леммы.

Лемма 9.6. *Если $k \geqslant 3$, то $\mathrm{rad}(\mathcal{A}_V) = e$. В частности, $V = U$.*

Доказательство. Второе утверждение следует из первого и утверждения (1) леммы 9.4. Докажем, что $\mathrm{rad}(\mathcal{A}_V) = e$. Пусть X – старшее базисное множество S-кольца $\mathcal{A}_V$. Поскольку $V \neq D$, найдётся множество $Y \in \mathcal{S}(\mathcal{A})_{D\setminus V}$ такое, что $X \subseteq Y^2$. По лемме 9.4 имеет место равенство $Y = LY_0$, где Y_0 – орбита подгруппы группы $\mathrm{Aut}(C)$ такая, что $\mathrm{rad}(Y_0) = e$. Однако, $Y_0 = \{y\}$ или $Y_0 = \{y, \varepsilon y^{-1}\}$, где $\varepsilon \in \{e, c_1\}$ (утверждение (1) леммы 4.1). Поэтому

$$Y^2 = LY_0^2 = L \times \begin{cases} \{y^2\}, & \text{если } Y_0 = \{y\}, \\ \{\varepsilon, y^{\pm 2}\}, & \text{если } Y_0 = \{y, \varepsilon y^{-1}\}. \end{cases} \tag{26}$$

С другой стороны, поскольку $X \subset V$, из определения множества V следует, что $\mathrm{rad}(X) = e$ или $c_1 \in \mathrm{rad}(X)$. В первом случае $\mathrm{rad}(\mathcal{A}_V) = e$, как и требуется. Предположим, что $c_1X = X$. Тогда для каждого $x \in X$ множество Y^2 содержит смежный класс $\{x, c_1x\}$ по подгруппе $\langle c_1\rangle$. Поэтому в силу формулы (26) мы получаем включение

$$\{x, c_1x\} \subset \{\varepsilon, y^{\pm 2}\},$$

которое невозможно, так как $|x| = 2^k \geqslant 8$. □

§10. S-кольца над $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: шуровость

В этом параграфе на основе результатов, полученных в §§6–9, мы доказываем следующую теорему.

Теорема 10.1. *Для любого целого числа $n \geqslant 1$ каждое* S*-кольцо над группой $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ является шуровым. В частности, D – группа Шура.*

Доказательство. Докажем теорему индукцией по n. Исчерпывающий компьютерный поиск всех S-колец над небольшими группами показывает, что D является группой Шура при $n \leqslant 4$. Пусть $n \geqslant 5$. Мы должны проверить, что каждое S-кольцо $\mathcal{A}$ над группой D, является шуровым. Однако, если $\mathrm{rad}(\mathcal{A}) = e$, то это следует из теорем 6.1 и 7.1. Далее нам потребуется следующий результат из статьи [2], дающий достаточное условие шуровости обобщённого сплетения S-колец.

Теорема 10.2. [2, следствие 5.7] *Пусть $\mathcal{A}$ – S-кольцо над абелевой группой D. Предположим, что $\mathcal{A}$ является обобщённым S-сплетением шуровых* S*-колец $\mathcal{A}_{D/L}$ и $\mathcal{A}_U$, где $S = U/L$. Тогда* S*-кольцо $\mathcal{A}$ шурово тогда и только тогда, когда существуют группы $\Delta_0 \geqslant (D/L)_{\mathrm{right}}$ и $\Delta_1 \geqslant U_{\mathrm{right}}$ такие, что*

$$\Delta_0 \approx_2 \mathrm{Aut}(\mathcal{A}_{D/L}), \quad \text{и} \quad \Delta_1 \approx_2 \mathrm{Aut}(\mathcal{A}_U), \quad \text{и} \quad (\Delta_0)^{U/L} = (\Delta_1)^{U/L}. \quad (27)$$

Следствие 10.3. *В условиях теоремы* 10.2 S*-кольцо $\mathcal{A}$ шурово, если группа $\mathrm{Aut}(\mathcal{A}_S)$ является 2-изолированной.*

Доказательство. Положим $\Delta_0 = \mathrm{Aut}(\mathcal{A}_{D/L})$ и $\Delta_1 = \mathrm{Aut}(\mathcal{A}_U)$. Тогда справедливы первые два равенства из формулы (27), поскольку S-кольца $\mathcal{A}_{D/L}$ и $\mathcal{A}_U$ шуровы. Далее, в силу 2-изолированности группы $\mathrm{Aut}(\mathcal{A}_S)$, мы получаем равенство $(\Delta_0)^S = \mathrm{Aut}(\mathcal{A}_S) = (\Delta_1)^S$, которое доказывает третье равенство из формулы (27). Так что, S-кольцо $\mathcal{A}$ шурово по теореме 10.2. □

Вернёмся к доказательству теоремы 10.1. Теперь, можно считать, что $\mathrm{rad}(\mathcal{A}) \neq e$. Тогда по теореме 9.1 S-кольцо $\mathcal{A}$ является собственным обобщённым S-сплетением, причём для секции $S = U/L$ справедлива формула (24). Кроме того, по индукции S-кольца $\mathcal{A}_{D/L}$ и $\mathcal{A}_U$ шуровы. Предположим сначала, что $\mathcal{A}_S = \mathbb{Z}S$, или $|S| = 4$, или $|L| = 2$ и $\mathcal{A}_U$ – регулярное S-кольцо с тривиальным радикалом. Тогда группа

$\mathrm{Aut}(\mathcal{A}_S)$ является 2-изолированной: это очевидно в первых двух случаях и следует из теоремы 8.1 (применяемой к $\mathcal{A} = \mathcal{A}_U$) в третьем. Так что, S-кольцо $\mathcal{A}$ шурово по следствию 10.3.

Для завершения доказательства можно считать, что $|S| = |2^m|$, где $m \geqslant 3$, и что $\mathcal{A}_U$ – нерегулярное S-кольцо с тривиальным радикалом. Тогда $\mathcal{A}_U = \mathcal{A}_H \otimes \mathcal{A}_L$, где $|H| \geqslant 4$ и $\mathrm{rk}(\mathcal{A}_H) = 2$ (теорема 6.1). Поэтому

$$\mathrm{Aut}(\mathcal{A}_U)^S = (\mathrm{Sym}(H) \times \mathrm{Sym}(L))^{U/L} = \mathrm{Sym}(S). \tag{28}$$

С другой стороны, $L = \langle s \rangle$ или $L = \langle sc_1 \rangle$, поскольку $c_1 \in H$. Но тогда S-кольцо $\mathcal{A}_{D/L}$ циркулянтно. Кроме того, S является $\mathcal{A}_{D/L}$-секцией составного порядка. По теореме 4.6 статьи [2], отсюда следует, что

$$\mathrm{Aut}(\mathcal{A}_{D/L})^S = \mathrm{Sym}(S). \tag{29}$$

Формулы (28) и (29) показывают, что равенства (27) справедливы для групп $\Delta_0 := \mathrm{Aut}(\mathcal{A}_{D/L})$ и $\Delta_1 := \mathrm{Aut}(\mathcal{A}_U)$. Так что, S-кольцо $\mathcal{A}$ шурово по теореме 10.2. □

§11. Нешурово S-кольцо над группой M_{2^n}

Основным результатом этого параграфа является следующая теорема, в доказательстве которой мы строим нешурово S-кольцо над группой M_{2^n}, определённой формулой (1).

Теорема 11.1. *M_{2^n} не является группой Шура при $n \geqslant 4$.*

Доказательство. По лемме 3.1 статьи [25] группа M_{16} не является группой Шура. Пусть $n \geqslant 5$. Обозначим через e единичный элемент группы $G = M_{2^n}$ и через H – нормальную подгруппу группы G, порождённую элементами $c = a^{2^{n-3}}$ и b. Тогда $H \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ и

$$H = Z_0 \cup Z_1 \cup Z_2, \tag{30}$$

где $Z_0 = \{e\}$, $Z_1 = \{c^2\}$ и $Z_2 = H \setminus \langle c^2 \rangle$; отметим, что эти множества попарно не пересекаются. Далее, зафиксируем два других разложения множества H в непересекающееся объединение подмножеств:

$$H = \underbrace{B \cup Bc^3}_{X_1} \cup \underbrace{Bc^2 \cup Bc}_{Y_1} \quad = \quad \underbrace{B' \cup B'c}_{X_2} \quad \cup \quad \underbrace{B'c^2 \cup B'c^3}_{Y_2}.$$

где B и B' – группы порядка 2, порождённые инволюциями b и $b' := c^2b$. Тогда прямое вычисление показывает, что

$$Ha \cup Ha^{-1} = \underbrace{X_1a \cup X_2a^{-1}}_{Z_3} \cup \underbrace{Y_1a \cup Y_2a^{-1}}_{Z_4}, \tag{31}$$

в частности, множества Z_3 и Z_4 не пересекаются. Более того, $Z_3c^2 = Z_4$, поскольку $Y_1 = X_1c^2$ и $Y_2 = X_2c^2$. Наконец, имеется в точности $m' = 2^{n-3} - 3$ смежных классов по подгруппе H в группе G, отличных от H, Ha и Ha^{-1}. Объединим их в пары следующим образом:

$$Z_{i+3} := Ha^i \cup Ha^{-i}, \quad i = 2, 3, \dots m, \tag{32}$$

где $m = (m'-1)/2+1$ и $Z_{m+1} = Ha^{2^{n-2}}$. Тогда множества $Z_0, \dots, Z_{r-1}$, где $r = m + 5$, образуют разбиение группы G; обозначим его через $\mathcal{S}$. Подмодуль группового кольца $\mathbb{Z}G$, натянутый на элементы $\underline{Z_i}$, $i = 0, \dots, r-1$, обозначим через $\mathcal{A}$.

Лемма 11.2. *Модуль $\mathcal{A}$ является* S*-кольцом над группой G. Более того, $\mathcal{S}(\mathcal{A}) = \mathcal{S}$.*

Доказательство. Определения, сделанные выше, показывают, что $Z_i^{-1} = Z_i$ для всех i. Таким образом, достаточно проверить, что для любых i и j произведение $\underline{Z_i}\,\underline{Z_j}$ раскладывается в линейную комбинацию элементов $\underline{Z_k}$, $k = 0, \dots, r-1$. Однако, легко видеть, что

$$\underline{Ha^i}\,\underline{Ha^j} = \underline{Ha^j}\,\underline{Ha^i} = \underline{Ha^{i+j}} = \underline{a^{i+j}H}$$

для всех i, j, k. Поэтому требуемое утверждение справедливо, когда $i, j \notin \{3, 4\}$. Для завешения доказательства предположим, что $i = 3$ (случай $i = 4$ рассматривается аналогично). Тогда прямое вычисление показывает, что

- $\underline{Z_3}\,\underline{Z_1} = \underline{Z_4}$, $\underline{Z_3}\,\underline{Z_2} = \underline{Z_4}$, $\underline{Z_3}\,\underline{Z_{r-1}} = 4\underline{Z_{r-2}}$,
- $\underline{Z_3}\,\underline{Z_3} = 8\,\underline{Z_0} + 2\,\underline{Z_5} + 4\,\underline{Z_2}$,
- $\underline{Z_3}\,\underline{Z_4} = 8\,\underline{Z_1} + 2\,\underline{Z_5} + 4\,\underline{Z_2}$,
- $\underline{Z_3}\,\underline{Z_5} = 4\underline{Z_3} + 4\underline{Z_4} + 4\underline{Z_6}$,
- $\underline{Z_3}\,\underline{Z_i} = 4\underline{Z_{i-1}} + 4\underline{Z_{i+1}}$, $i = 6, \dots r-2$.

Поскольку $\underline{Z_3}$ коммутирует с $\underline{Z_j}$ для всех j, утверждение доказано. □

По лемме 11.2 утверждение теоремы 11.1 вытекает из нижеследующей леммы.

Лемма 11.3. S*-кольцо $\mathcal{A}$ нешурово.*

Доказательство. Рассуждая от противного, предположим, что $\mathcal{A}$ шурово. Тогда оно совпадает с S-кольцом, соответствующим группе $\Gamma = \mathrm{Aut}(\mathcal{A})$. Следовательно, его базисное множество Z_2 является орбитой стабилизатора точки e в группе Γ. Поскольку $|Z_2| = 6$, найдётся

элемент $\gamma \in \Gamma$ такой, что

$$|\gamma^{Z_2}| = 3. \tag{33}$$

С другой стороны, в силу формулы (31) факторкольцо $\mathcal{A}_{G/H}$ изоморфно S-кольцу, соответствующему диэдральной группе порядка 2^{n-2} в её перестановочном представлении степени 2^{n-3}. Поэтому $\mathrm{Aut}(\mathcal{A}_{G/H})$ является 2-группой. Она содержит подгруппу $\Gamma^{G/H}$ и, следовательно, элемент $\gamma^{G/H}$. По формуле (33) отсюда следует, что перестановка γ оставляет фиксированным (как множество) каждый смежный класс по подгруппе H. Так что,

$$\gamma^{H \cup Ha} \in \mathrm{Aut}(C), \tag{34}$$

где C обозначает двудольный граф с множеством вершин $H \cup Ha$ и рёбрами (h, hax), $x \in X_1$. Однако, этот граф изоморфен лексикографическому произведению пустого графа с 2 вершинами и неориентированного цикла длины 8. Поэтому $\mathrm{Aut}(C)$ является 2-группой. Отсюда следует ввиду (34), что число $|\gamma^H|$ является степенью 2. Но это противоречит формуле (33), поскольку $Z_2 \subset H$. □

§12. S-кольца над $D = D_{2n}$: делимые разностные множества

12.1. Определения. В оставшейся части статьи мы изучаем S-кольца над диэдральной 2-группой $D = D_{2n}$ порядка $2n$. Интересные примеры таких колец получаются из разностных множеств. Для описания этих примеров напомним некоторые определения из монографии [27].

Пусть T – k-подмножество группы G порядка mn такое, что каждый элемент, не принадлежащий группе $N \leqslant G$ порядка n, имеет точно λ_2 представлений в виде частного gh^{-1} элементов $g, h \in G$, и каждый неединичный элемент из N имеет точно λ_1 таких представлений, т.е.

$$\underline{T} \cdot \underline{T}^{-1} = k \cdot e + \lambda_1 \underline{N \setminus e} + \lambda_2 \underline{G \setminus N}. \tag{35}$$

Тогда T называется $(m, n, k, \lambda_1, \lambda_2)$-*делимым разностным множеством* в группе G относительно подгруппы N. Если $\lambda_1 = 0$ (соотв., $n = 1$), то мы говорим, что T – *относительное разностное множество* или *относительное* (m, n, k, λ_2)-*разностное множество* (соотв. разностное множество). Разностное множество T называется *тривиальным*, если оно равно G, $\{x\}$ или $G \setminus \{x\}$, где $x \in G$.

Теорема 12.1. *Пусть C – циклическая 2-группа. Тогда*

(1) *каждое разностное множество в C тривиально,*
(2) *не существует относительного $(2^a, 2, 2^a, 2^{a-1})$-разностного множества в C.*

Доказательство. Утверждение (1) следует из теоремы II.3.17 монографии [7] и теоремы 1.2 статьи [9]. Утверждение (2) следует из теорем 4.1.4 и 4.1.5 монографии [27]. □

12.2. Конструкции. Пусть D – диэдральная группа порядка $2n$, C – её циклическая подгруппа порядка n и $H \leqslant C$. Пусть T – непустое подмножество группы C такое, что число $|T \cap xH|$ не зависит от выбора $x \in T$ (*условие пересечения*, ср. с леммой 2.1). Положим

$$\mathcal{S} := \{e,\ H \setminus e,\ C \setminus H,\ Ts,\ T's\},$$

где $s \in D \setminus C$ и $T' = C \setminus T$. Ясно, что $\mathcal{S}$ является разбиением группы D, для которого выполнено условие (S1). Поскольку все классы этого разбиения симметричны, удовлетворяется также и условие (S2). Положим

$$\mathcal{A} := \mathcal{A}(T, C) = \mathrm{Span}\{\underline{X} :\ X \in \mathcal{S}\}. \tag{36}$$

Теорема 12.2. *Во введённых обозначениях модуль $\mathcal{A}$ является* S*-кольцом над группой D, для которого $\mathcal{S}(\mathcal{A}) = \mathcal{S}$, тогда и только тогда, когда T – делимое разностное множество в группе C относительно подгруппы H.*

Доказательство. Для доказательства необходимости предположим, что $\mathcal{A}$ является S-кольцом таким, что $\mathcal{S}(\mathcal{A}) = \mathcal{S}$. Тогда Ts – базисное множество этого кольца и $Ts\,Ts = T\,T^{-1}$ – подмножество группы C. Поэтому

$$\underline{T} \cdot \underline{T}^{-1} = \underline{Ts}^2 = |T|e + \lambda_1 \underline{H \setminus e} + \lambda_2\, \underline{C \setminus H}, \tag{37}$$

где $\lambda_1 = c_{Ts\,Ts}^{H \setminus e}$ и $\lambda_2 = c_{Ts\,Ts}^{C \setminus H}$. Так что, T является делимым разностным множеством в группе C относительно подгруппы H.

Для доказательства достаточности предположим, что T – делимое разностное множество в группе C относительно подгруппы H. Тогда достаточно проверить, что $\mathcal{A} \cdot \mathcal{A} \subseteq \mathcal{A}$. С этой целью обозначим через $\mathcal{A}'$ модуль, натянутый на элементы e, $\underline{H}$, $\underline{C}$ и $\underline{D}$. Тогда, очевидно, что $\mathcal{A}' \cdot \mathcal{A}' \subseteq \mathcal{A}'$ и $\mathcal{A} = \mathrm{Span}\{\mathcal{A}', \underline{sT}\}$. Так что, остаётся доказать, что

$$\underline{sT}^2 \in \mathcal{A} \quad \text{и} \quad \mathcal{A}' \cdot \underline{sT} \subseteq \mathcal{A}.$$

Первое включение следует из формулы (35), поскольку T является делимым разностным множеством. Простые вычисления показывают,

что второе включение эквивалентно включению $\underline{T} \cdot \underline{H} \in \mathcal{A}$. Однако, последнее легко следует из условия пересечения. $\square$

Мы не знаем, ни одного делимого разностного множества над циклической 2-группой, которое бы удовлетворяло условию пересечения. Однако, можно несколько изменить конструкцию, предполагая, что множество T, удовлетворяющее условию пересечения, на сей раз содержится в $C \setminus H$. Тогда используя аналогичные рассуждения можно построить S-кольцо ранга 6, которое совпадает с $\mathcal{A}$ на C и имеет три базисных множества вне C: Ts, $T's$ и Hs, где $T' = C \setminus (T \cup H)$.

S-кольца такого типа действительно существуют. Достаточно взять классическое относительное $(q+1, 2, q, (q-1)/2)$-разностное множество T, определяемое следующим образом (см. [27, теорема 2.2.13]). Пусть L – аффинная прямая двумерного линейного пространства над конечным полем $\mathbb{F}_q$, которая не проходит через ноль. Тогда L является относительным $(q+1, q-1, q, 1)$-разностным множеством в мультипликативной группе поля $\mathbb{F}_{q^2}$. Пусть π – естественный эпиморфизм этой группы на группу C такой, что $|\ker(\pi)| = m$ для некоторого делителя m числа $q-1$. Тогда $\pi(L)$ – относительное $(q+1, (q-1)/m, q, m)$-разностное множество в группе C. Когда C является 2-группой, число $q+1$ равно степени 2, и поэтому q – число Мерсенна. Если при этом $m = (q-1)/2$, то мы приходим к искомому множеству T.

Следствие 12.3. *Пусть $\mathcal{A}$ – S-кольцо над диэдральной 2-группой D. Предположим, что C является $\mathcal{A}$-группой. Тогда*

(1) *если $\mathrm{rk}(\mathcal{A}_C) = 2$, то $\mathcal{A} \cong \mathcal{A}_C * \mathcal{B}$, где $* \in \{\wr, \cdot\}$ и $\mathcal{B} = \mathbb{Z}\mathbb{Z}_2$,*
(2) *если $\mathrm{rk}(\mathcal{A}_C) = 3$ и $\mathrm{rk}(\mathcal{A}) = 5$, то $\mathcal{A} = \mathcal{A}(T, C)$, где T – делимое разностное множество в группе C.*

Доказательство. Для доказательства утверждения (1) предположим, что $\mathrm{rk}(\mathcal{A}_C) = 2$. Пусть X – базисная величина, не пересекающаяся с группой C. Тогда $X = Ts$ для некоторого $T \subseteq C$. Из формулы (37) при $H = e$ следует, что T является разностным множеством в группе C. Тогда по утверждению (1) теоремы 12.1 либо $T = C$, либо одно из множеств T, $C \setminus T$ одноэлементно. Легко видеть, что S-кольцо $\mathcal{A}$ изоморфно кольцу $\mathcal{A}_C \wr \mathcal{B}$ в первом случае, и кольцу $\mathcal{A}_C \otimes \mathcal{B}$ во втором.

Для доказательства утверждения (2) предположим, что $\mathrm{rk}(\mathcal{A}_C) = 3$ и $\mathrm{rk}(\mathcal{A}) = 5$. Тогда найдётся $\mathcal{A}$-группа $H < C$ такая, что

$$\mathcal{A}_C = \mathrm{Span}\{e, \underline{H}, \underline{C}\}.$$

Далее, каждое множество $X \in \mathcal{S}(\mathcal{A})_{D\setminus C}$ имеет вид $X = Ts$ для некоторого множества $T \subseteq C$, удовлетворяющего условию пересечения (лемма 2.1). Таким образом, $\mathcal{A} = \mathcal{A}(T, C)$. Поэтому T является делимым разностным множеством в группе C по теореме 12.2. □

12.3. Шуровость. В этом пункте мы докажем следующую теорему, которая показывает, что большая часть S-колец, полученных с помощью первой конструкции, не являются шуровыми.

Теорема 12.4. *Пусть T – делимое разностное множество в циклической 2-группе C относительно группы $H \leqslant C$. Предположим, что для него выполнено условие пересечения и, что $HT \neq T$. Тогда* S*-кольцо $\mathcal{A}(T, C)$, определённое формулой* (36)*, не является шуровым.*

Мы выведем эту теорему в конце пункта из общего утверждения о шуровых S-кольцах над диэральной 2-группой. Это утверждение показывает, что если T – делимое разностное множество в циклической 2-группе относительно её подгруппы H и соответствующее ему S-кольцо ранга 6 является шуровым, то либо $|H| = 2$, либо это кольцо – собственное обобщённое сплетение.

Теорема 12.5. *Пусть $\mathcal{A}$ – шурово* S*-кольцо над диэдральной 2-группой D и $H < C$ – минимальная $\mathcal{A}$-группа. Предположим, что $\mathcal{A}$ не является собственным обобщённым сплетением. Тогда $|H| = 2$.*

Доказательство. По условию теоремы $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(G_e, D)$ для некоторой группы $G \leqslant \mathrm{Sym}(D)$, содержащей подгруппу D_{right}. Поскольку H является $\mathcal{A}$-группой, разбиение D/H группы D в правые смежные классы по подгруппе H образует систему импримитивности для G. Обозначим через N стабилизатор этого разбиения в группе G:

$$N = \{g \in G : \ (Hx)^g = Hx \ \text{для всех} \ x \in D\}.$$

Тогда, поскольку $H_{\mathrm{right}} \leqslant N$, группа N^X транзитивна для каждого блока $X \in D/H$. Следующее утверждение может быть также выведено из леммы 2.1 статьи [18].

Лемма 12.6. *Для каждого блока $X \in D/H$ группа N^X дважды транзитивна.*

Доказательство. Пусть $X \in D/H$. Тогда группа G^X дважды транзитивна, поскольку $\mathrm{rk}(\mathcal{A}_H) = 2$. Более того, она содержит регулярную циклическую подгруппу, изоморфную H_{right}. Она, как и H, является

2-группой. Используя классификацию примитивных групп, содержащих регулярную циклическую подгруппу, из статьи [16], мы заключаем, что G^X содержит единственную минимальную подгруппу K, которая тоже дважды транзитивна. Однако, N^X – нетривиальная нормальная подгруппа группы G^X. Так что она содержит K, и поэтому дважды транзитивна. □

Определим отношение эквивалентности $\sim$ на множестве правых смежных классов по подгруппе H, полагая $X \sim Y$ тогда и только тогда, когда действия группы N на X и Y имеют одинаковый перестановочный характер. Тогда по лемме 12.6 и замечанию на стр.2 статьи [8] группа N_e действует транзитивно на каждом классе X, не эквивалентном классу H. Обозначим через U класс отношения эквивалентности $\sim$, который содержит H. Тогда каждая орбита группы G_e, не содержащаяся в U, является объединением N-орбит. Так что, S-кольцо $\mathcal{A}$ является обобщённым U/H-сплетением. По условию теоремы отсюда следует, что $U = D$. Поэтому каждый класс отношения эквивалентности $\sim$ состоит из одного элемента. Но тогда по лемме 12.6 мы имеем

$$|\operatorname{Orb}(N, X \times Y)| = 2 \quad \text{для всех } X, Y \in D/H.$$

Таким образом, мы получаем две симметрических блок-схемы между X и Y, каждая из которых является дополнением к другой. Поскольку группа N содержит циклическую подгруппу H, действующую регулярно на X и на Y, эти блок-схемы циркулянтны, и потому соответствуют циклическим разностным множествам. По утверждению (1) леммы 12.1 они тривиальны. Поэтому для каждого $x \in X$ группа N_x имеет две орбиты на множестве Y, мощности которых равны 1 и $|Y| - 1$.

Для завершения доказательства предположим, что $|H| > 2$. Тогда, очевидно, $|Y| > 2$. Поэтому группа N_e оставляет на месте точно одну точку в каждом смежном классе $Y \in D/H$. Отсюда следует, что множество F всех неподвижных точек этой группы имеет мощность $[D : H]$. С другой стороны, по предложению 5.2 статьи [18] множество F является блоком группы G. Поэтому F – подгруппа группы D. Более того, она является дополнением к H в D, поскольку $F \cap H = e$. Так что, $H = C$. Противоречие. □

Доказательство теоремы 12.4. Рассуждая от противного, предположим, что S-кольцо $\mathcal{A} = \mathcal{A}(T, C)$ шурово. Тогда выполнено условие теоремы 12.5, поскольку H – минимальная $\mathcal{A}$-группа и $HT \neq T$. Таким образом, $|H| = 2$. Обозначим через x единственный элемент порядка 2 в группе H. Тогда $x \in \mathcal{A}$, и потому $x(Ts) = T's$. Отсюда следует, что $|Ts| = |T's| = m$, где $m = |C|/2$, и что x не появляется ни в $\underline{Ts}^2$, ни в $\underline{T's}^2$. Но тогда делимое разностное множество T имеет параметры $(m, 2, m, 0, m/2)$. Поэтому оно является относительным $(m, 2, m, m/2)$-разностным множеством в C. Однако, это противоречит утверждению (2) теоремы 12.1. □

§13. S-кольца над $D = D_{2^{n+1}}$: единственная минимальная $\mathcal{A}$-группа в $D \setminus C$

В этой секции мы изучаем S-кольца над диэдральной группой $D = D_{2^{n+1}}$ порядка 2^{n+1}, сохраняя обозначения пункта 4.2. Основным результатом является следующее утверждение.

Теорема 13.1. *Пусть $\mathcal{A}$ – S-кольцо над диэдральной группой D. Предположим, что имеется единственная минимальная $\mathcal{A}$-группа H, причём $H \not\leqslant C$. Тогда $\mathcal{A}$ изоморфно S-кольцу над группой $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$.*

Доказательство. Из условия на H следует, что каждое базисное множество X, не пересекающееся с H, является смешанным: в противном случае группа $\langle X \rangle$ содержит неединичную $\mathcal{A}$-подгруппу группы C. Более того, легко видеть, что либо $H = \langle s \rangle$ для некоторого $s \in D \setminus C$, либо H – диэдральная группа. Рассмотрим эти два случая по отдельности.

Случай 1: $H = \langle s \rangle$ для некоторого s. В этом случае все базисные множества, за исключением $\{e\}$ и $\{s\}$, являются смешанными. По утверждению (1) леммы 4.4 отсюда следует, что $X_0^{-1} = X_0$ для всех $X \in \mathcal{S}(\mathcal{A})$. Кроме того, $Xs \in \mathcal{S}(\mathcal{A})$, поскольку $s \in \mathcal{A}$, и $(Xs)_0 = X_1$ и $(Xs)_1 = X_0$. Так что, $X_1^{-1} = X_1$ также для всех X.

Обозначим через σ автоморфизм группы D, переводящий пару (c, s) в пару (c^{-1}, s), где c – образующая группы C. Тогда по сказанному выше

$$X^\sigma = (X_0 \cup X_1 s)^\sigma = X_0^{-1} \cup X_1^{-1} = X_0 \cup X_1 s = X$$

для всех $X \in \mathcal{S}(\mathcal{A})$. Поэтому, полупрямое произведение $D \rtimes \langle\sigma\rangle \leqslant \mathrm{Sym}(D)$ является подгруппой группы $\mathrm{Aut}(\mathcal{A})$. Элемент $s\sigma$ этой подгруппы имеет порядок два и коммутирует с c. Так что, группа $D' = \langle s\sigma, c\rangle$ изоморфна группе $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$. С другой стороны, D' – регулярная подгруппа группы $\mathrm{Sym}(D)$. Следовательно, схема Кэли над D, соответствующая S-кольцу $\mathcal{A}$, изоморфна схеме Кэли над D'. Таким образом, $\mathcal{A}$ изоморфно S-кольцу над $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$.

Случай 2: H – диэдральная группа. В этом случае все базисные множества, за исключением $\{e\}$, являются смешанными. Более того, в силу минимальности группы H S-кольцо $\mathcal{A}_H$ примитивно. Поэтому, $\mathrm{rk}(\mathcal{A}_H) = 2$ по теореме 2.2. В частности, $\mathrm{Aut}(\mathcal{A}_H) = \mathrm{Sym}(H)$. Докажем, что

$$H \leqslant \mathrm{rad}(X) \quad \text{для всех } X \in \mathcal{S}(\mathcal{A})_{D\setminus H}. \tag{38}$$

Тогда схема Кэли, соответствующая S-кольцу $\mathcal{A}$, изоморфна сплетению схемы, соответствующей S-кольцу $\mathcal{A}_H$, и циркулянтной схемы на множестве правых смежных классов по подгруппе H. Поэтому группа $\mathrm{Aut}(\mathcal{A})$ содержит подгруппу, изоморфную группе $\mathrm{Sym}(H) \wr \mathbb{Z}_m$, где $m = [D : H]$. Так что, требуемое утверждение следует из того, что последняя группа, очевидно, содержит регулярную подгруппу, изоморфную группе $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$.

Для завершения доказательства мы проверим утверждение (38) за два шага: сначала для рациональных S-колец, и затем – в общем случае.

Лемма 13.2. *Утверждение* (38) *справедливо, если* S*-кольцо* $\mathcal{A}$ *рационально.*

Доказательство. В силу рациональности S-кольцо $\mathcal{A}$ является симметричным, и потому коммутативным. Рассуждая от противного, предположим, что $HX \neq X$ для некоторого базисного множества X, содержащегося в $D \setminus H$. Тогда произведение HX является объединением $m > 1$ базисных множеств $X, Y, \ldots$. Не умаляя общности будем считать, что $|X| \leqslant |Y| \leqslant \cdots$.

Поскольку H является $\mathcal{A}$-группой, из леммы 2.1 следует, что число $\lambda = |X \cap xH|$ не зависит от выбора $x \in X$. Поэтому каждый x появляется λ раз в произведении $\underline{H}\,\underline{X}$, т.е.

$$\underline{H}\,\underline{X} = \lambda(\underline{X} + \underline{Y} + \cdots). \tag{39}$$

В силу минимальности X, отсюда следует, что $|H|\,|X| \geqslant \lambda m|X|$, и потому $|H| \geqslant \lambda m$. С другой стороны, $(H \cap C)X_0 = X_0$ по рациональности X. Так что, элемент $\underline{X}$ появляется в произведении $\underline{H}\,\underline{X}$ по крайней мере $|H \cap C| = |H|/2$ раз. Таким образом, $\lambda \geqslant |H|/2$, и

$$|H| \geqslant \lambda m \geqslant m|H|/2.$$

Пользуясь тем, что $m > 1$, мы заключаем, что $m = 2$ и $\lambda = |H|/2$. Но тогда $H_0 = H_1 = H \cap C$, поскольку группа H диэдральна. Так что,

$$\underline{H}\,\underline{X} = \underline{H_0}(e + s)(\underline{X_0} + s\underline{X_1}) =$$

$$\underline{H_0}\,\underline{X_0} + \underline{H_0}\,\underline{sX_0} + \underline{H_0}\,\underline{X_1} + \underline{H_0}\,\underline{sX_1} = |H_0|\underline{X_0} + \underline{H_0}\,\underline{X_1} + \cdots$$

В силу формулы (39) все коэффициенты в последнем выражении равны $\lambda = |H_0|$. Поэтому множество $H_0X_1 \cap X_0$ должно быть пустым. Но в этом случае, $\underline{H_0}\,\underline{X_1} = |H_0|\underline{H_0X_1}$. Однако, это означает, что $H_0 \leqslant \mathrm{rad}(X_1)$. Поскольку $H_0 \leqslant \mathrm{rad}(X_0)$, отсюда следует, что $H_0 \leqslant \mathrm{rad}(X)$. Принимая во внимание, что подгруппа H_0 диэдральной группы H нетривиальна, мы видим, что нетривиальна и группа $\mathrm{rad}(X)$. Будучи $\mathcal{A}$-группой, она должна содержать единственную минимальную $\mathcal{A}$-группу H. Но тогда $HX = X$. Противоречие. □

Для завершения доказательства формулы (38), рассмотрим базисное множество X, содержащееся в $D \setminus H$. Тогда $Y := \mathrm{tr}(X)$ также содержится в этой разности. По лемме 13.2 отсюда следует, что

$$\underline{Y_0} + \underline{sY_1} = \frac{1}{|H|}\underline{H}\,\underline{Y} = \frac{1}{|H|}(e + s)\,(\underline{H_0Y_0} + \underline{H_0Y_1}).$$

Поэтому, $|Y_0| = |Y_1|$. С другой стороны, $|(X^{(m)})_0| = |X_0|$ для каждого целого числа m, взаимно простого с $|D|$. По лемме 4.5 отсюда следует, что $|(X^{(m)})_1| = |X_1|$. Так что,

$$k|X_0| = |Y_0| = |Y_1| = k|X_1|,$$

где k – число всех различных множеств $X^{(m)}$. Таким образом, $|X_0| = |X_1|$ для всех базисных множеств X, содержащихся в $D \setminus H$.

Обозначим через ρ ограничение на кольцо $\mathcal{A}$ одномерного представления группы D, переводящего элементы s и c в числа -1 и 1, соответственно. Тогда ρ – неприводимое представление кольца $\mathcal{A}$ такое, что $\rho(e) = 1$ и $\rho(\underline{H^{\#}}) = -1$. Более того, отсюда следует, что для каждого

базисного множества $X \subseteq D \setminus H$. мы имеем $\rho(\underline{X}) = -|X_1| + |X_0| = 0$. В частности, $\rho(\underline{X^{-1}}) = 0$. Поэтому

$$0 = \rho(\underline{X}\,\underline{X}^{-1}) = \sum_{Y \in \mathcal{S}(\mathcal{A})} c^{Y}_{XX^{-1}} \rho(\underline{Y}) =$$

$$c^{e}_{XX^{-1}} \rho(e) + c^{H^{\#}}_{XX^{-1}} \rho(H^{\#}) = c^{e}_{XX^{-1}} - c^{H^{\#}}_{XX^{-1}}.$$

Следовательно, $|X| = c^{e}_{XX^{-1}} = c^{H^{\#}}_{XX^{-1}}$. Но тогда $HX = X$ для всех базисных множеств $X \subseteq D \setminus H$, что и требовалось доказать. □

§14. Доказательство теоремы 1.3

Пусть D – диэдральная 2-группа, и C – её циклическая подгруппа индекса 2. Пусть $\mathcal{A}$ – S-кольцо над D. Предположим, что $r := \mathrm{rk}(\mathcal{A})$ не превосходит 5. При $r = 2$ утверждение (1) теоремы 1.3 тривиально. Пусть $r \geqslant 3$. Тогда по теореме 2.2 S-кольцо $\mathcal{A}$ импримитивно; обозначим через H минимальную нетривиальную $\mathcal{A}$-группу. Тогда $\mathrm{rk}(\mathcal{A}_H) = 2$. Теперь, если $r = 3$, то $\mathcal{A}$ является собственным сплетением по следствию 3.3. Так что, можно считать, что $r = 4$ или $r = 5$.

Лемма 14.1. *Если найдётся минимальная $\mathcal{A}$-группа $L \neq H$, то выполнено утверждение* (2).

Доказательство. Из минимальности групп H и L следует, что $H \cap L = e$. Поэтому, по крайней мере одна из них пересекает C тривиально. Более того, если $H \cap C = L \cap C = e$, то $\langle HL \rangle$ – $\mathcal{A}$-подгруппа группы C, и мы заменим H на минимальную $\mathcal{A}$-подгруппу группы $\langle HL \rangle$. Так что, не умаляя общности можно считать, что

$$H \cap C \neq e \quad \text{и} \quad L \cap C = e.$$

Тогда $L = \langle s \rangle$ для некоторой инволюции $s \in D \setminus C$. Более того, $sHs = H$ по минимальности группы H. Таким образом, HL является $\mathcal{A}$-группой и множество $\mathcal{S}(\mathcal{A}_{HL})$ содержит 4 элемента: $\{e\}$, $H^{\#}$, $\{s\}$ и $sH^{\#}$. Следовательно,

$$\mathcal{A}_{HL} = \mathcal{A}_H \cdot \mathcal{A}_L.$$

Это доказывает требуемое утверждение для $r = 4$, а по следствию 3.3 также и для $r = 5$. □

По лемме 14.1 можно считать, что H – единственная минимальная $\mathcal{A}$-группа. Если она не содержится в C, то по теореме 13.1 выполнено утверждение (1). Поэтому будем далее также считать, что $H \leqslant C$.

Обозначим через F объединение всех базисных множеств кольца $\mathcal{A}$, которые не являются смешанными. Ясно, что $H \subseteq F$.

Лемма 14.2. *F является $\mathcal{A}$-группой. Более того, если $r = r(\mathcal{A}_F)+1$, то $\mathcal{A}$ – собственное сплетение.*

Доказательство. Вторая часть утверждения следует из первой и следствия 3.3. Для доказательства первой части обозначим через U и V объединения всех базисных множеств кольца $\mathcal{A}$, содержащихся в C и $D \setminus C$, соответственно. Докажем, что множество $U \cup V$ является группой. Поскольку U, очевидно, является $\mathcal{A}$-группой, не умаляя общности можно считать, что V не пусто. Тогда $V = U's$, где элемент $s \in D \setminus C$ такой, что $U \cap Us$ – подгруппа группы D. Поэтому

$$UU' \subseteq U' \quad \text{и} \quad U'U' \subseteq U.$$

Поскольку $U' \subseteq UU'$, первое из двух включений, указанных выше, показывает, что $U' = UU'$. Следовательно, U' является объединением правых смежных классов группы C по подгруппе U. Отсюда с учётом того, что C – циклическая 2-группа, из второго из двух включений, указанных выше, следует, что $U' = U$. Таким образом, множество $U \cup V = U \cup Us$ является группой. □

Предположим сначала, что $F_0 = C$. Тогда из определения группы F следует, что C является $\mathcal{A}$-группой. Тогда по следствию 3.3 можно считать, что $r_C := \mathrm{rk}(\mathcal{A}_C)$ не равно $r-1$. Поскольку, очевидно, $r_C \geqslant 2$, мы получаем, что

$$(r, r_C) = (4,2),\ (5,2) \text{ или } (5,3).$$

В первых двух случаях требуемое утверждение следует из утверждения (1) следствия 12.3, а в третьем – из утверждения (2). Таким образом, ниже можно считать, что

$$F_0 < C \quad \text{и} \quad H = F \text{ или } r_F = 3,$$

где $r_F = \mathrm{rk}(\mathcal{A}_F)$. В частности, F является объединением двух или трёх базисных множеств (отметим, что все они смешанные).

Лемма 14.3. *Пусть $X \in \mathcal{S}(\mathcal{A})_{D\setminus F}$. Предположим, что множество X рационально или $[V : H] \geqslant 4$, где $V = \langle X_0 \rangle$. Тогда $H \leqslant \mathrm{rad}(X)$.*

Доказательство. Достаточно проверить, что $H \leqslant \mathrm{rad}(X_0)$. Действительно, тогда коэффициент при $\underline{X}$ в произведении $\underline{H}\,\underline{X}$ больше

или равен $|H|$. Отсюда следует требуемое утверждение, поскольку он не может быть больше $|H|$.

Предположим сначала, что множество X рационально. Тогда по утверждению (2) леммы 4.4 рационально множество X_0. Поскольку $X_0 \subseteq C \setminus H$, отсюда следует требуемое включение $H \leqslant \mathrm{rad}(X_0)$.

Пусть теперь $[V : H] \geqslant 4$. Тогда $V \cong \mathbb{Z}_{2^k}$ для некоторого $k \geqslant 2$. Поскольку $r \leqslant 5$, имеется не более двух базисных множеств, рационально сопряженных с X. Поэтому стабилизатор множества X_0 в группе $(\mathbb{Z}_{2^k})^*$ имеет в ней индекс, не больший 2. Отсюда следует, что этот стабилизатор содержит подгруппу, состоящую из всех элементов $x \mapsto x^{1+4m}$, $x \in \mathbb{Z}_{2^k}$, где $m \in \mathbb{Z}_{2^k}$. Но тогда $\mathrm{rad}(X_0) \geqslant V^4 \geqslant H$ по утверждению (2) леммы 4.1. □

Из леммы 14.3 следует, что если рациональны все базисные множества, содержащиеся в $D \setminus F$, то S-кольцо $\mathcal{A}$ является собственным сплетением. Действительно, это очевидно, когда $H = F$. Если же $H \neq F$, то это так, поскольку тогда $F \setminus H$ – базисное множество, радикал которого равен H. Таким образом, можно считать, что два базисных множества, содержащиеся в $D \setminus F$, скажем X и Y, рационально сопряжены, а третье (если есть) рационально. Для завершения доказательства рассмотрим четыре случая.

Случай 1: $F = H$ и $r = 4$. Используя компьютерный пакет COCO [23], мы нашли в точности пять S-колец (соотв. три S-кольца) ранга 4 над группой D_8 (соотв. D_{16}). В обоих случаях только в двух из них минимальная $\mathcal{A}$-группа единственна и содержится в группе C; все эти кольца являются собственными сплетениями. Так что, будем далее считать, что $|D| \geqslant 32$.

В нашем случае нетривиальными базисными множествами являются X, Y и $Z = H^{\#}$. Тогда, как легко видеть, выполнено условие леммы 4.5. Поскольку X и Y рационально сопряжены, найдётся алгебраический изоморфизм S-кольца $\mathcal{A}$, переставляющий X и Y. Поэтому

$$\underline{H}\,\underline{X} = a(\underline{X} + \underline{Y}), \tag{40}$$

где $a = |H|/2$. Следовательно, $c_{ZX}^X = a-1$. С другой стороны, поскольку множества X и Z – симметрические, мы имеем $C_{XX}^Z = \frac{|X|}{|Z|} C_{ZX}^X$. Отсюда следует, что $|Z| = 2a - 1$ делит

$$|X| c_{ZX}^X = \frac{(d-2a)(a-1)}{2},$$

где $d = |D|$. Однако, по лемме 14.3 не умаляя общности можно считать, что $|C : H| = 2$. Поэтому $2a = |H| = d/4$. Следовательно, $2a - 1$ делит $3a(a-1)$. Но a, будучи степенью 2, взаимно просто с $2a - 1$. Значит, $2a-1$ делит $3a-3$. Однако, это возможно только при $a \leqslant 2$, т.е. когда $d \leqslant 16$.

Случай 2: $F = H$ и $r = 5$. Обозначим через Z базисное множество, содержащееся в $D \setminus H$ и отличное от X и Y. Тогда, как легко видеть, выполнено условие леммы 4.5. Поскольку X и Y рационально сопряжены, найдётся алгебраический изоморфизм S-кольца $\mathcal{A}$, переставляющий X и Y и оставляющий Z на месте. Поэтому ранг рационального замыкания S-кольца $\mathcal{A}$ равен 4. Тогда по лемме 14.3 оно совпадает со сплетением $\mathcal{A}_H \wr \mathcal{B}$, где $\mathcal{B}$ изоморфно рациональному замыканию S-кольца $\mathcal{A}_{D/H}$. Но тогда $\mathrm{rk}(\mathcal{B}) = 3$, и потому найдётся нетривиальная $\mathcal{B}$-группа. Обозначим через U её прообраз в $\mathcal{A}$. Тогда, очевидно, $H < U < D$.

Из рациональной сопряжённости X и Y следует, что $X \cup Y \subseteq U$ или $X \cup Y \subseteq D \setminus U$. Однако, $\mathrm{rk}(\mathcal{A}) = r = 5$. Поэтому, $Z = D \setminus U$ в первом случае, и $Z = U \setminus H$ – во втором. В любом случае, $H \leqslant \mathrm{rad}\, Z$. Но тогда по лемме 14.3 из равенства $Z = U \setminus H$ следует, что

$$\mathrm{rad}(X) = \mathrm{rad}(Y) \geqslant H, \tag{41}$$

и, значит, $\mathcal{A}$ – собственное сплетение. Пусть теперь $Z = D \setminus U$. Тогда $\mathrm{rk}(\mathcal{A}_U) = 4$, и $\mathcal{A}_U$ изоморфно сплетению $\mathcal{A}_H \wr \mathcal{A}_{U/H}$. Поэтому снова выполнено равенство (41), и $\mathcal{A}$ – собственное сплетение.

Случай 3: $C \not\geqslant F > H$. В этом случае $F = H \cup Hs$. Следовательно, по лемме 14.3, множества X_0 и Y_0 являются орбитами подгруппы индекса 2 в группе $\mathrm{Aut}(C)$, если только $\mathcal{A}$ не является собственным сплетением. Поэтому группа $\mathrm{rad}(X_0) = \mathrm{rad}(Y_0)$ имеет индекс 2 в H. Отсюда следует равенство (40) при $a = |H|/2$. В точности, как и в случае 2, мы докажем, что $2a - 1$ делит

$$|X| c^X_{ZX} = \frac{(d - 4a)(a-1)}{2},$$

где $Z = H^{\#}$ и $d = |D| = 4|H| = 8a$. Таким образом, $2a - 1$ делит $2a(a-1)$, что невозможно поскольку a является степенью 2.

Случай 4 : $C \geqslant F > H$. В этом случае, из сделанного выше предположения следует, что $F = F_0 < C$. Поэтому X_0 (и потому Y_0) содержит образующую группы C. Тогда

$$[\langle X_0 \rangle : H] = [C : H] \geqslant [C : F][F : H] \geqslant 4.$$

Значит, по лемме 14.3 справедливо равенство (41). Поскольку также $F \setminus H$ является базисным множеством и $H = \mathrm{rad}(F \setminus H)$, группа H содержится в радикале каждого базисного множества, содержащегося в $D \setminus H$. Так что, $\mathcal{A}$ является собственным сплетением. □

Литература

1. С. Евдокимов, И. Пономаренко, *Характеризация циклотомических схем и нормальные кольца Шура над циклической группой.* — Алгебра и Анализ, **14** (2003), no. 2, 189–221.
2. С. Евдокимов, И. Пономаренко, *Шуровость* S*-колец над циклической группой и обобщенное сплетение групп перестановок.* — Алгебра и Анализ, **24** (2012), 3, 84–127.
3. Л. А. Калужнин, М. Х. Клин, *О некоторых числовых инвариантах групп подстановок.* — Латв. матем. ежегодник, **18** (1976), 81–99.
4. М. Х. Клин, *Об аксиоматике клеточных колец.* — В сб.: Исследования по алгебраической теории комбинаторных объектов, М. ВНИИСИ, 6–32, 1985.
5. М. Музычук, *V-кольца групп подстановок с инвариантной метрикой*, Дисс. к.ф.-м.н., Киев (1987).
6. R. A. Bailey, P. J. Cameron, *Crested products of association schemes.* — J. London Math. Soc., **72** (2005), 1, 1–24.
7. T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, 2nd edition, Cambridge Univ. Press, Cambridge, 1999.
8. P. J. Cameron, *On groups with several doubly-transitive permutation representations.* — Math. Z., **128** (1972), 1–14.
9. J. A. Davis, K. Smith, *A construction of difference sets in high exponent 2-groups using representation theory.* — J. Algebraic Combin., **3** (1994), 137–151.
10. S. Evdokimov, I. Ponomarenko, *A new look at the Burnside–Schur theorem.* — Bull. London Math. Soc., **37** (2005), 535–546.
11. S. Evdokimov, I. Ponomarenko, *Permutation group approach to association schemes.* — Europ. J. Combin., **30** (2009), 6, 1456–1476.
12. S. Evdokimov, I. Ponomarenko, *Schur rings over a product of Galois rings.* — Beitr. Algebra Geom., **55** (2014), 1, 105–138.
13. S. Evdokimov, I. Kovács, I. Ponomarenko, *Characterization of cyclic Schur groups.* — Algebra Analysis, **25** (2013), 5, 61–85.
14. S. Evdokimov, I. Kovács, I. Ponomarenko, *On schurity of finite abelian groups*, `arXiv:1309.0989 [math.GR]` (2013), 1–20 (accepted to Commun. Algebra).
15. M. Hirasaka, M. Muzychuk, *Association schemes generated by a non-symmetric relation of valency 2.* — Discrete Math., **244** (2002), 109–135.
16. G. A. Jones, *Cyclic regular subgroups of primitive permutation groups.* — J. Group Theory, **5** (2002), 403–407.
17. R. Kochendörffer, *Untersuchungen über eine Vermutung von W. Burnside.* — Schr. Math. Semin. u. Inst. Angew. Math. Univ. Berlin, **3** (1937), 155–180.
18. I. Kovács, D. Marušič, M. Muzychuk. — *On dihedrants admitting arc-regular group actions*, Journal Algebraic Combin., **35** (2011), 409–426.

19. K. H. Leung, S. L. Ma, *The structure of Schur rings over cyclic groups.* — J. Pure Appl. Algebra, **66** (1990), 287–302.
20. K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups.* — Israel J. Math., **106** (1998), 251–267.
21. M. Muzychuk, I. Ponomarenko, *Schur rings.* — European J. Combin., **30** (2009), 6, 1526–1539.
22. M. Muzychuk, I. Ponomarenko, *On quasi-thin association schemes.* — J. Algebra, **351** (2012), 467–489.
23. Ch. Pech, S. Reichard, M. Ziv-Av, *The COCO share package for* GAP, https://github.com/MatanZ/coco-ii.
24. I. N. Ponomarenko, *Bases of Schurian antisymmetric coherent configurations and an isomorphism test for Schurian tournaments.* — J. Math. Sci. (N. Y.), **192**, No. 3 (2013), 316–338.
25. I. Ponomarenko, A. Vasil'ev, *On non-abelian Schur groups.* — J. Algebra Appl., **13** (2014), 8, 1450055-1–1450055-22.
26. R. Pöschel, *Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen.* — Math. Nachr., **60** (1974), 1–27.
27. A. Pott, *Finite geometry and character theory*, Berlin: Springer-Verlag, 1995.
28. I. Schur, *Zur Theorie der einfach transitiven Permutationgruppen.* — S.-B. Preus Akad. Wiss. phys.-math. Kl., (1933), 598–623.
29. H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen. II.* — Math. Zeitschrift, **52** (1950), 384–393.
30. H. Wielandt, *Finite permutation groups*, Academic Press, New York - London, 1964.

Muzychuk M., Ponomarenko I. On Schur 2-groups.

A finite group G is called a Schur group, if any Schur ring over G is the transitivity module of a point stabilizer in a subgroup of $\mathrm{Sym}(G)$ that contains all right translations. We complete a classification of abelian Schur 2-groups by proving that the group $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ is Schur. We also prove that any non-abelian Schur 2-group of order larger than 32 is dihedral (the Schur 2-groups of smaller orders are known). Finally, in the dihedral case, we study Schur rings of rank at most 5, and show that the unique obstacle here is a hypothetical S-ring of rank 5 associated with a divisible difference set.

Академический Колледж,
Нетанья, Израиль
E-mail: muzy@netanya.ac.il

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова
С.-Петербург. Россия
E-mail: inp@pdmi.ras.ru

Поступило 28 апреля 2015 г.