На конкурс Мёбиуса-2018

ОБ ОТДЕЛИМОСТИ КОЛЕЦ ШУРА НАД АБЕЛЕВЫМИ p-ГРУППАМИ

Г. К. Рябов

Пусть G — конечная группа. Подкольцо группового кольца $\mathbb{Z}G$ называется *S-кольцом* (*кольцом Шура*) над G, если оно является свободным $\mathbb{Z}$-модулем, натянутым на специальное разбиение группы G (точные определения даны в § 1). Элементы разбиения, задающего S-кольцо, принято называть *базисными множествами* этого S-кольца. Понятие S-кольца берет начало из работ Шура и Виланда. Они использовали "метод S-колец" для изучения групп подстановок, содержащих регулярную подгруппу [1, 2].

Изоморфизмом (комбинаторным) колец Шура $\mathcal{A}$ и $\mathcal{A}'$ над группами G и G' соответственно называется биекция $f : G \to G'$ такая, что для любого базисного множества X кольца $\mathcal{A}$ образ графа Кэли $\mathrm{Cay}(G, X)$ под действием отображения f совпадает с графом Кэли $\mathrm{Cay}(G', X')$, где X' — базисное множество кольца $\mathcal{A}'$. *Алгебраический изоморфизм* колец Шура $\mathcal{A}$ и $\mathcal{A}'$ — это кольцевой изоморфизм между ними, индуцирующий биекцию между базисными множествами кольца $\mathcal{A}$ и базисными множествами кольца $\mathcal{A}'$. Несложно понять, что любой комбинаторный изоморфизм индуцирует алгебраический изоморфизм. Кольца Шура, для которых каждый алгебраический изоморфизм индуцируется комбинаторным, принято называть отделимыми. Более точно, пусть $\mathcal{K}$ — некоторый класс S-колец. Будем говорить, что S-кольцо $\mathcal{A}$ *отделимо* относительно класса $\mathcal{K}$, если для любого S-кольца $\mathcal{A}' \in \mathcal{K}$ любой алгебраический изморфизм $\varphi : \mathcal{A} \to \mathcal{A}'$ индуцируется изоморфизмом. Каждое отделимое S-кольцо определяется с точностью до изоморфизма лишь своими структурными константами. Более подробно об отделимых S-кольцах см., например, [3, 4].

Обозначим через $\mathcal{K}_C$ и $\mathcal{K}_A$ классы S-колец над циклическими и абелевыми группами соответственно. Циклическую группу порядка n будем обозначать через C_n. В [3] было доказано, что каждое S-кольцо над циклической p-группой, где p — простое число, отделимо относительно $\mathcal{K}_C$. В [4] были построены бесконечные серии S-колец над циклическими группами, которые не являются отделимыми относительно $\mathcal{K}_C$.

Назовём абелеву группу *отделимой*, если каждое S-кольцо над ней отделимо относительно $\mathcal{K}_A$. Легко проверить, что подгруппа отделимой группы отделима. Из [5, § 3] следует, что группа $H \times H$ не является отделимой, если $|H| \geq 4$. Пусть теперь G — нециклическая абелева p-группа. Если G отделима, то из сказанного выше следует, что G изоморфна $C_p \times C_{p^k}$ или $C_p \times C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$.

В данной работе доказывается отделимость групп $C_p \times C_{p^k}$ при $p \in \{2,3\}$. Вопрос об отделимости групп $C_p \times C_p \times C_{p^k}$ при $p \in \{2,3\}$ остается открытым.

Теорема 1. *Группы $D = C_p \times C_{p^k}$, где $p \in \{2,3\}$ и $k \geq 1$, отделимы.*

Доказательство теоремы 1 основано на классификации всех S-колец над D, которая была получена для $p = 2$ в [6] и для $p = 3$ в [7]. Каждое нетривиальное S-кольцо над D либо строится из S-колец над группами меньшего порядка при помощи операций тензорного произведения и обобщенного сплетения, либо является *циклотомическим*, то есть определяется подходящей подгруппой группы $\mathrm{Aut}(D)$. Детальная классификация S-колец над D приведена в § 6. Вопрос об отделимости тензорных произведений и обобщенных сплетений сводится к вопросу об отделимости операндов. Наиболее трудоемкой является проверка отделимости циклотомических S-колец над D (см. § 7).

Понятие отделимости S-колец тесно связано с проблемой изоморфизма графов Кэли (см, например, [8, пункт 6.2]). В случае, когда все S-кольца над заданной группой отделимы, проблему изоморфизма графов Кэли над этой группой можно решить за полиномиальное от порядка группы время с помощью алгоритма Вейсфейлера-Лемана [9, 10]. Из теоремы 1 мы выводим (см. § 8) следующее утверждение.

Теорема 2. *Пусть группа $D = C_p \times C_{p^k}$, где $p \in \{2,3\}$ и $k \geq 1$, задана своей таблицей Кэли. Тогда для графа Кэли Γ над D и графа Кэли Γ' над произвольной абелевой группой изоморфизм между Γ и Γ' может быть проверен за время $|D|^{O(1)}$.*

Отметим, что проблема изоморфизма в классе графов Кэли над циклическими группами была решена с использованием теории S-колец независимо в [11] и [12].

Для удобства читателя мы приводим в § 1-3 необходимые определения, а также утверждения о кольцах Шура и схемах Кэли. Большинство из них может быть найдено в [13]; перед остальными утверждениями приведена ссылка на источник.

§ 1. S-кольца и схемы Кэли

Пусть G — конечная группа, и $\mathbb{Z}G$ — целочисленное групповое кольцо. Через e будем обозначать единицу группы G. Если $X \subseteq G$, то элемент $\sum_{x \in X} x$ кольца $\mathbb{Z}G$ обозначается через $\underline{X}$, а множество $\{x^{-1} : x \in X\}$ — через X^{-1}.

Кольцо $\mathcal{A} \subseteq \mathbb{Z}G$ называется *S-кольцом* над G, если существует разбиение $\mathcal{S} = \mathcal{S}(\mathcal{A})$ множества G, удовлетворяющее следующим условиям:

1) $\{e\} \in \mathcal{S}$,
2) если $X \in \mathcal{S}$, то $X^{-1} \in \mathcal{S}$,
3) $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : X \in \mathcal{S}\}$.

Элементы множества $\mathcal{S}$ называются *базисными множествами*, а число $|\mathcal{S}|$ — *рангом* S-кольца $\mathcal{A}$. Если $X, Y, Z \in \mathcal{S}$, то через $c_{X,Y}^Z$ обозначается количество представлений $z \in Z$ в виде $z = xy$, где $x \in X, y \in Y$. Заметим, что если X и Y— базисные множества S-кольца $\mathcal{A}$, то $\underline{X}\ \underline{Y} = \sum_{Z \in \mathcal{S}(\mathcal{A})} c_{X,Y}^Z \underline{Z}$. Следовательно, числа $c_{X,Y}^Z$ являются структурными константами S-кольца $\mathcal{A}$ и не зависят от выбора $z \in Z$.

Пара $\mathcal{C} = (G, \mathcal{R})$, где $\mathcal{R}$ — разбиение множества $G \times G$, называется *схемой Кэли* над G, если $\mathcal{R}$ удовлетворяет следующим свойствам:

1) $\mathrm{Diag}(G \times G) = \{(g, g) : g \in G\} \in \mathcal{R}$;

2) $\mathcal{R} = \mathcal{R}^*$, то есть если $R \in \mathcal{R}$, то $R^* = \{(h, g) : (g, h) \in R\} \in \mathcal{R}$;

3) если $R,\ S,\ T \in \mathcal{R}$, то число $c^T_{R,S} = |\{h \in G : (g, h) \in R,\ (h, f) \in S\}|$ не зависит от выбора $(g, f) \in T$;

4) $Rg = \{(hg, fg) : (h, f) \in R\} = R$ для любого $R \in \mathcal{R}$ и любого $g \in G$.

Числа $c^T_{R,S}$ называются *числами пересечений*, элементы множества $\mathcal{R}$ — *базисными отношениями*, мощность множества $\mathcal{R}$ — *рангом* схемы Кэли. Если R — базисное отношение и $g \in G$, то число $n(R) = \{h : (g, h) \in R\}$ не зависит от выбора g и называется *валентностью* отношения R.

Существует взаимно-однозначное соответствие между S-кольцами и схемами Кэли над G. Если $\mathcal{A}$ — S-кольцо над G, то пара $\mathcal{C}(\mathcal{A}) = (G, \mathcal{R}(\mathcal{A}))$, где $\mathcal{R}(\mathcal{A}) = \{R(X) : X \in \mathcal{S}(\mathcal{A})\}$ и $R(X) = \{(g, xg) : g \in G, x \in X\} \subseteq G \times G$, является схемой Кэли над G. И обратно, если $\mathcal{C} = (G, \mathcal{R})$ — схема Кэли над G, то $\mathcal{S}(\mathcal{C}) = \{X(R) : R \in \mathcal{R}\}$, где $X(R) = \{x \in G : (e, x)\} \subseteq G$, является разбиением группы G, задающим S-кольцо $\mathcal{A}(\mathcal{C})$ над G. Если $\mathcal{A}$ — S-кольцо , а $\mathcal{C}(\mathcal{A})$ — соответствующая ему схема Кэли, то

$$c^{R(Z)}_{R(X),R(Y)} = c^Z_{X,Y} \tag{1}$$

для любых $X, Y, Z \in \mathcal{S}(\mathcal{A})$.

§ 2. Изоморфизмы

Пусть $\mathcal{A}$ и $\mathcal{A}'$ — S-кольца, а $\mathcal{C} = (G, \mathcal{R})$ и $\mathcal{C}' = (G', \mathcal{R}')$ — схемы Кэли над группами G и G' соответственно. Положим $\mathcal{S} = \mathcal{S}(\mathcal{A})$ и $\mathcal{S}' = \mathcal{S}(\mathcal{A}')$. Биекция $f : G \to G'$ называется *(комбинаторным) изоморфизмом* схем Кэли $\mathcal{C}$ и $\mathcal{C}'$, если $\mathcal{R}' = \mathcal{R}^f$, где $\mathcal{R}^f = \{R^f :\ R \in \mathcal{R}\}$ и $R^f = \{(g^f,\ h^f) :\ (g,\ h) \in R\}$. Биекция $f : G \to G'$ называется *(комбинаторным) изоморфизмом* S-колец $\mathcal{A}$ и $\mathcal{A}'$, если f является изоморфизмом соответствующих схем Кэли $\mathcal{C}(\mathcal{A})$ и $\mathcal{C}(\mathcal{A}')$.

Группа $\mathrm{Iso}(\mathcal{A})$ всех изоморфизмов S-кольца $\mathcal{A}$ на себя содержит нормальную подгруппу

$$\mathrm{Aut}(\mathcal{A}) = \{f \in \mathrm{Iso}(\mathcal{A}) : R(X)^f = R(X) \text{ для всех } X \in \mathcal{S}(\mathcal{A})\}.$$

Эта группа называется *группой автоморфизмов* S-кольца $\mathcal{A}$ и обозначается $\mathrm{Aut}(\mathcal{A})$; элементы $\mathrm{Aut}(\mathcal{A})$ называются *автоморфизмами* S-кольца $\mathcal{A}$.

Алгебраическим изоморфизмом S-колец $\mathcal{A}$ и $\mathcal{A}'$ называется биекция $\varphi : \mathcal{S} \to \mathcal{S}'$ такая, что $c^Z_{X,Y} = c^{Z^\varphi}_{X^\varphi,Y^\varphi}$ для любых $X, Y, Z \in \mathcal{S}$. Отображение $\underline{X} \to \underline{X}^\varphi$ по линейности продолжатеся до изоморфизма колец $\mathcal{A}$ и $\mathcal{A}'$. *Алгебраическим изоморфизмом* схем Кэли $\mathcal{C}$ и $\mathcal{C}'$ называется биекция $\varphi : \mathcal{R} \to \mathcal{R}'$ такая, что $c^T_{R,S} = c^{T^\varphi}_{R^\varphi,S^\varphi}$ для любых $R, S, T \in \mathcal{R}$. Если φ — алгебраический изоморфизм S-колец $\mathcal{A}$ и $\mathcal{A}'$, то отображение $R(X) \mapsto R(X^\varphi)$ является алгебраическим изоморфизмом соответствующих схем Кэли $\mathcal{C}(\mathcal{A})$ и $\mathcal{C}(\mathcal{A}')$ в силу (1).

Любой изоморфизм S-колец (схем Кэли) сохраняет структурные константы (числа пересечений). Следовательно, любой изоморфизм S-колец (схем Кэли) индуцирует алгебраический изоморфизм.

По аналогии с отделимыми S-кольцами можно определить отделимые схемы Кэли. Схема Кэли $\mathcal{C}$ называется *отделимой* относительно класса схем Кэли $\mathcal{K}$, если для любой схемы Кэли $\mathcal{C}^{'} \in \mathcal{K}$ любой алгебраический изоморфизм $\varphi : \mathcal{C} \to \mathcal{C}^{'}$ индуцируется изоморфизмом. Ясно, что выполнено следующее утверждение.

Предложение 2.1. *Если $\mathcal{A}$ и $\mathcal{C}(\mathcal{A})$ — соответствующие друг другу S-кольцо и схема Кэли, то отделимость S-кольца $\mathcal{A}$ относительно класса S-колец $\mathcal{K}$ равносильна сепарбельности схемы Кэли $\mathcal{C}(\mathcal{A})$ относительно соответствующего $\mathcal{K}$ класса схем Кэли.*

Множество всех изоморфизмов S-колец $\mathcal{A}$ и $\mathcal{A}^{'}$ (схем Кэли $\mathcal{C}$ и $\mathcal{C}^{'}$), индуцирующих заданный алгебраический изоморфизм φ, обозначается через $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)$ $(\mathrm{Iso}(\mathcal{C}, \mathcal{C}^{'}, \varphi))$. Если H — группа, то положим $H_{right} = \{x \mapsto xh,\ x \in H : h \in H\}$. Из определений следует, что

$$G_{right}\,\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)G^{'}_{right} = \mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi). \tag{2}$$

Заметим, что S-кольцо $\mathcal{A}$ отделимо относительно класса S-колец $\mathcal{K}$ тогда и только тогда, когда

$$\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi) \neq \varnothing$$

для любого $\mathcal{A}^{'} \in \mathcal{K}$ и любого алгебраического изморфизма $\varphi : \mathcal{A} \to \mathcal{A}^{'}$. Групповое кольцо $\mathbb{Z}G$ и S-кольцо ранга 2 над G отделимы относительно класса всех S-колец. В первом случае каждое базисное множество одноэлементно, и, следовательно, любой алгебраический изоморфизм естественным образом индуцируется изоморфизмом; во втором случае существует всего один алгебраический изоморфизм, который индуцируется любым изоморфизмом.

Еще один естественный тип изоморфизма S-колец (схем Кэли) происходит из изоморфизма соответствующих групп. *Изоморфизмом Кэли* S-колец $\mathcal{A}$ и $\mathcal{A}^{'}$ (схем Кэли $\mathcal{C}$ и $\mathcal{C}^{'}$) называется изоморфизм групп $f : G \to G^{'}$ такой, что $\mathcal{S}^f = \mathcal{S}^{'}$ $(\mathcal{R}^f = \mathcal{R}^{'})$. Если существует изоморфизм Кэли из $\mathcal{A}$ в $\mathcal{A}^{'}$, то будем писать $\mathcal{A} \cong_{Cay} \mathcal{A}^{'}$. Любой изоморфизм Кэли является изоморфизмом, но не любой изоморфизм является изоморфизмом Кэли.

§ 3. S-кольца: основные конструкции и утверждения

Пусть $\mathcal{A}$ — S-кольцо над группой G. Множество $X \subseteq G$ называется $\mathcal{A}$-*множеством*, если $\underline{X} \in \mathcal{A}$. Подгруппа $H \leq G$ называется $\mathcal{A}$-*подгруппой*, если H является $\mathcal{A}$-множеством. Пусть $L \trianglelefteq U \leq G$. Секция U/L называется $\mathcal{A}$-*секцией*, если U и L являются $\mathcal{A}$-подгруппами.

Если $S = U/L$ — $\mathcal{A}$-секция, то модуль

$$\mathcal{A}_S = Span_{\mathbb{Z}}\left\{\underline{X}^{\pi} :\ X \in \mathcal{S}(\mathcal{A}),\ X \subseteq U\right\},$$

где $\pi : U \to U/L$ — канонический гомоморфизм, является S-кольцом над S.

Если $X \subseteq G$, то множество

$$\mathrm{rad}(X) = \{g \in G :\ Xg = gX = X\}$$

является подгруппой в G, она называется *радикалом* множества X. Если X является $\mathcal{A}$-множеством, то группы $\langle X\rangle$ и $\mathrm{rad}(X)$ являютя $\mathcal{A}$-подгруппами группы G.

Пусть $\mathcal{A}$ и $\mathcal{A}^{'}$ — S-кольца над G и $G^{'}$ соответственно, и $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ — алгебраический изоморфизм. Заметим, что φ продолжается до биекции между $\mathcal{A}$- и $\mathcal{A}^{'}$-множествами, и потому между $\mathcal{A}$- и $\mathcal{A}^{'}$-секциями. Образы $\mathcal{A}$-множества X и $\mathcal{A}$-секции S под действием φ обозначаются через X^{φ} и S^{φ} соответственно. Если S — $\mathcal{A}$-секция, то φ индуцирует алгебраический изоморфизм

$$\varphi_S : \mathcal{A}_S \to \mathcal{A}^{'}_{S'},$$

где $S^{'} = S^{\varphi}$. Поскольку $c^{\{e\}}_{X,Y} = \delta_{Y,X^{-1}}|X|$ и $|X| = c^{\{e\}}_{X,X^{-1}}$, где $\delta_{X,X^{-1}}$ — символ Кронекера, мы заключаем, что $(X^{-1})^{\varphi} = (X^{\varphi})^{-1}$ и $|X| = |X^{\varphi}|$ для любого $\mathcal{A}$-множества X. В частности, $|G| = |G^{'}|$. Можно показать, что

$$\langle X^{\varphi}\rangle = \langle X\rangle^{\varphi},\ \mathrm{rad}(X^{\varphi}) = \mathrm{rad}(X)^{\varphi} \tag{3}$$

для всех $X \in \mathcal{S}^*(\mathcal{A})$ (см. [14, стр.10]).

Назовем S-кольцо $\mathcal{A}$ *симметричным*, если $X = X^{-1}$ для любого $X \in \mathcal{S}(\mathcal{A})$. Ясно, что если $\mathcal{A}$ симметрично и $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ — алгебраический изоморфизм, то $\mathcal{A}^{'}$ тоже симметрично.

Если $X \subseteq G$ и $m \in \mathbb{Z}$, то через $X^{(m)}$ обозначим множество $\{x^m : x \in X\}$. Будем говорить, что множества $X, Y \subseteq G$ *рационально сопряжены*, если существует $m \in \mathbb{Z}$, взаимно простое с $|G|$, для которого $Y = X^{(m)}$.

Далее мы сформулируем два утверждения об S-кольцах над абелевыми группами, которые фактически были доказаны Шуром в [1]. В приведенной ниже формулировке эти утверждения могут быть найдены в [2, §23].

Лемма 3.1. *Пусть $\mathcal{A}$ — S-кольцо над абелевой группой G. Тогда $X^{(m)} \in \mathcal{S}(\mathcal{A})$ для любого $X \in \mathcal{S}(\mathcal{A})$ и любого $m \in \mathbb{Z}$, взаимно простого с $|G|$. Другими словами, отображение $\sigma_m : g \mapsto g^m$ является изоморфизмом Кэли S-кольца $\mathcal{A}$ на себя.*

Лемма 3.2. *Пусть $\mathcal{A}$ — S-кольцо над абелевой группой G, p — простой делитель $|G|$, и $H = \{g \in G : g^p = e\}$. Тогда для любого $\mathcal{A}$-множества X множество $X^{[p]} = \{x^p : x \in X,\ |X \cap Hx| \not\equiv 0 \mod p\}$ является $\mathcal{A}$-множеством.*

Пусть $K \leq \mathrm{Aut}(G)$. Тогда множество орбит $\mathrm{Orb}(K, G)$ действия группы K на G образует разбиение множества G, задающее S-кольцо $\mathcal{A}$ над G. В этом случае S-кольцо $\mathcal{A}$ называется *циклотомическим* и обозначается $\mathrm{Cyc}(K, G)$.

Пусть $\mathcal{A}_1$ и $\mathcal{A}_2$ — S-кольца над G_1 и G_2 соответственно. Тогда множество

$$\mathcal{S} = \mathcal{S}(\mathcal{A}_1) \times \mathcal{S}(\mathcal{A}_2) = \{X_1 \times X_2 :\ X_1 \in \mathcal{S}(\mathcal{A}_1),\ X_2 \in \mathcal{S}(\mathcal{A}_2)\}$$

образует разбиение группы $G = G_1 \times G_2$, которое задает S-кольцо над G. Это S-кольцо называется *тензорным произведением* S-колец $\mathcal{A}_1$ и $\mathcal{A}_2$ и обозначается $\mathcal{A}_1 \otimes \mathcal{A}_2$.

Пусть $\mathcal{A}_1$ и $\mathcal{A}_2$ — S-кольца над G_1 и G_2 соответственно; e_1 и e_2 – единицы групп G_1 и G_2 соответственно. Тогда множество $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, где

$$\mathcal{S}_1 = \{X_1 \times \{e_2\} : \ X_1 \in \mathcal{S}(\mathcal{A}_1)\}, \ \mathcal{S}_2 = \{G_1 \times \{X_2\} : \ X_2 \in \mathcal{S}(\mathcal{A}_2) \setminus \{e_2\}\}$$

образует разбиение группы $G = G_1 \times G_2$, которое задает S-кольцо над G. Это S-кольцо называется *сплетением* S-колец $\mathcal{A}_1$ и $\mathcal{A}_2$ и обозначается $\mathcal{A}_1 \wr \mathcal{A}_2$.

Лемма 3.3. *S-кольца $\mathcal{A}_1 \otimes \mathcal{A}_2$ и $\mathcal{A}_1 \wr \mathcal{A}_2$ отделимы тогда и только тогда, когда S-кольца $\mathcal{A}_1$ и $\mathcal{A}_2$ отделимы.*

Доказательство. Следует из, например, [15, теорема 1.20]. □

Лемма 3.4. [3, лемма 2.1] *Пусть $\mathcal{A}$ и $\mathcal{A}^{'}$ — S-кольца над G и $G^{'}$ соответственно. Пусть $\mathcal{B}$— S-кольцо, порожденное $\mathcal{A}$ и элементом $\xi \in \mathbb{Z}G$, $\mathcal{B}^{'}$ — S-кольцо, порожденное $\mathcal{A}^{'}$ и элементом $\xi^{'} \in \mathbb{Z}G^{'}$. Тогда для заданного алгебраического изоморфизма $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ существует не более одного алгебраического изоморфизма $\psi : \mathcal{B} \to \mathcal{B}^{'}$, продолжающего φ и такого, что $\psi(\xi) = \xi^{'}$.*

Следуя [16], назовем S-кольцо $\mathcal{A}$ *квазитонким*, если $|X| \leq 2$ для любого $X \in \mathcal{S}(\mathcal{A})$.

Лемма 3.5. *Пусть $\mathcal{A}$ — квазитонкое S-кольцо над G. Предположим, что в G нет $\mathcal{A}$-подгрупп H таких, что $H \cong C_2 \times C_2$, $\mathcal{A}_H = \mathbb{Z}H$ и $\mathcal{A}_{G/H} = \mathbb{Z}(G/H)$. Тогда $\mathcal{A}$ отделимо относительно класса всех S-колец.*

Доказательство. Квазитонкому S-кольцу $\mathcal{A}$ соответствует квазитонкая схема Кэли $\mathcal{C}(\mathcal{A})$, валентность каждого базисного отношения которой не превосходит 2. Из [16, теорема 1.1] следует, что каждая квазитонкая схема Кэли, не являющаяся схемой Клейна (см. [16, стр.2]), отделима относительно класса всех схем Кэли. Если $\mathcal{C}(\mathcal{A})$ является схемой Клейна, то в G найдется $\mathcal{A}$-подгруппа H такая, что $H \cong C_2 \times C_2$, $\mathcal{A}_H = \mathbb{Z}H$ и $\mathcal{A}_{G/H} = \mathbb{Z}(G/H)$, что противоречит предположению леммы. Следовательно, $\mathcal{C}(\mathcal{A})$ и $\mathcal{A}$ отделимы относительно класса всех схем Кэли и класса всех S-колец соответственно. □

§ 4. Обобщенное сплетение S-колец

Пусть $\mathcal{A}$ — S-кольцо над G, и U/L — $\mathcal{A}$-секция. Будем говорить, что $\mathcal{A}$ является *обобщенным сплетением* или *U/L-сплетением*, если $L \trianglelefteq G$ и $L \leq \mathrm{rad}(X)$ для любого $X \in \mathcal{S}(\mathcal{A})$, лежащего вне U. Обобщенное сплетение называется *нетривиальным* или *собственным*, если $L \neq 1$ и $U \neq G$. Если $U = L$, то $\mathcal{A}$ является обычным сплетением S-колец $\mathcal{A}_L$ и $\mathcal{A}_{G/L}$.

Далее мы докажем достаточное условие отделимости обобщенного сплетения S-колец над абелевыми группами, но прежде сформулируем необходимые для доказательства утверждения.

Если $f : G \to G^{'}$ — биекция и $X \subseteq G$, то сужение f на X обозначается через f^X. Пусть $H \leq G$. Для заданных $X, Y \in G/H$ положим

$$G_{X \to Y} = \{f^X : f \in G_{right}, X^f = Y\}.$$

В следующих трех леммах $\mathcal{A}$ и $\mathcal{A}^{'}$ — S-кольца над группами G и $G^{'}$ соответственно, и $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ — алгебраический изоморфизм.

Лемма 4.1. [14, лемма 3.4] *Если $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$, H является $\mathcal{A}$-подгруппой группы G и $H' = H^{\varphi}$, то*

$$hf^X h' \in \mathrm{Iso}(\mathcal{A}_H, \mathcal{A}'_{H'}, \varphi_H)$$

для всех $X \in G/H$, $h \in G_{H \to X}$ и $h' \in G'_{X' \to H'}$, где $X' = X^f$.

Лемма 4.2. [14, теорема 3.3, 1] *Пусть группы G и G' абелевы, и U/L — $\mathcal{A}$-секция группы G. Предположим, что $\mathcal{A}$ является U/L-сплетением, $U' = U^{\varphi}$ и $L' = L^{\varphi}$. Тогда $\mathcal{A}'$ является U'/L'-сплетением.*

Лемма 4.3. [14, теорема 3.5] *В условиях леммы 4.2 множество $\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$ состоит из всех биекций $f : G \to G'$, обладающих следующими свойствами:*

1) $(G/U)^f = G'/U'$, $(G/L)^f = G'/L'$,

2) $f^{G/L} \in \mathrm{Iso}(\mathcal{A}_{G/L}, \mathcal{A}'_{G'/L'}, \varphi_{G/L})$,

3) *если $X \in G/U$ и $X' = X^f$, то найдутся $g \in G_{U \to X}$ и $g' \in G'_{X' \to U'}$ такие, что $gf^X g' \in \mathrm{Iso}(\mathcal{A}_U, \mathcal{A}'_{U'}, \varphi_U)$.*

Лемма 4.4. *Пусть $\mathcal{A}$ — U/L-сплетение над абелевой группой G. Предположим, что $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ отделимы относительно $\mathcal{K}_A$ и $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Тогда $\mathcal{A}$ отделимо относительно $\mathcal{K}_A$.*

Доказательство. Пусть $\mathcal{A}'$ — S-кольцо над абелевой группой G', $\varphi : \mathcal{A} \to \mathcal{A}'$ — алгебраический изоморфизм, и $U' = U^{\varphi}, L' = L^{\varphi}$. Тогда из леммы 4.2 следует, что $\mathcal{A}'$ является U'/L'-сплетением. Поскольку $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ отделимы, алгебраические изоморфизмы

$$\varphi_U : \mathcal{A}_U \to \mathcal{A}'_{U'}, \ \varphi_{G/L} : \mathcal{A}_{G/L} \to \mathcal{A}'_{G'/L'}$$

индуцируются некоторыми изоморфизмами f_1 и f_2 соответственно. Пусть $X \in G/U$. Множество X можно рассматривать как подмножество множества G/L, так как X является объединением смежных классов по L. Положим $X' = X^{f_2}$. Выберем $g \in G_{U \to X}$ и $g' \in G'_{X' \to U'}$. В силу леммы 4.1, примененной к $\mathcal{A}_{G/L}$-подгруппе U/L группы G/L, биекция $g^{U/L} f_2^{X/L} {g'}^{X'/L'}$ индуцирует алгебраический изоморфизм $\varphi_{U/L}$. Положим

$$f_0 = g^{U/L} f_2^{X/L} {g'}^{X'/L'} (f_1^{U/L})^{-1}.$$

Поскольку $f_1^{U/L}$ также индуцирует $\varphi_{U/L}$, мы заключаем, что $f_0 \in \mathrm{Aut}(\mathcal{A}_{U/L})$. Так как $\mathrm{Aut}(\mathcal{A}_{U/L}) = \mathrm{Aut}(\mathcal{A}_U)^{U/L}$, существует $h_X \in \mathrm{Aut}(\mathcal{A}_U)$ такой, что $h_X^{U/L} = f_0$. Положим

$$f_X = g^{-1} h_X f_1 (g')^{-1}.$$

Пусть $f : G \to G'$ — биекция, для которой ограничение f на X совпадает с f_X для любого $X \in G/U$. Проверим, что f обладает свойствами 1-3 из леммы 4.3. Ясно, что $(G/U)^f = G'/U'$ и $(G/L)^f = G'/L'$ и, следовательно, f обладает свойством 1. По определению f мы имеем $gf^X g' = gf_X g' = h_X f_1$. Значит, из (2) следует, что для каждого $X \in G/U$ биекция $gf^X g'$ индуцирует алгебраический изоморфизм φ_U. Это доказывает, что f обладет свойством 3. Прямые вычисления показывают, что

$$f^{X/L} = (g^{-1}h_X f_1(g^{'})^{-1})^{X/L} = (g^{U/L})^{-1} g^{U/L} f_2^{X/L} g^{'X^{'}/L^{'}} (f_1^{U/L})^{-1} f_1^{U/L} (g^{'X^{'}/L^{'}})^{-1} = f_2^{X/L}$$

для любого $X \in G/U$. Следовательно, $f^{G/L} = f_2$ и $f^{G/L}$ индуцирует $\varphi_{G/L}$. Поэтому f обладет свойством 2. Таким образом, $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)$ по лемме 4.3.

Заметим, что приведенные рассуждения похожи на рассуждения, использовавшиеся при доказательстве отделимости S-колец смежных классов над циклическими группами ([14, стр.33]). □

§ 5. S-кольца над циклическими группами

Лемма 5.1. *Пусть G — циклическая группа порядка $n \neq 4$, и $\mathcal{A}$ — S-кольцо над G такое, что $\mathcal{A} = \mathbb{Z}G$ или $\mathcal{A} = \mathrm{Cyc}(K, G)$, где $K = \{\varepsilon, \sigma\}$, $\sigma : x \to x^{-1}$. Предположим, что φ — алгебраический изоморфизм из $\mathcal{A}$ в S-кольцо $\mathcal{A}^{'}$ над абелевой группой $G^{'}$. Тогда $G^{'} \cong G$.*

Доказательство. Из свойств алгебраического изоморфизма следует, что $|G| = |G^{'}| = n$. Пусть $X \in \mathcal{S}(\mathcal{A})$ — порождающее множество группы G. Тогда X^{φ} в силу (3) является порождающим множеством группы $G^{'}$. Если $|X| = 1$, то $|X^{\varphi}| = 1$ и, следовательно, $G^{'}$ циклическая. Если $|X| = 2$, то $X = X^{-1}$. Значит, по свойствам алгебраического изоморфизма $|X^{\varphi}| = 2$ и $(X^{\varphi})^{-1} = X^{\varphi}$. Поэтому либо $X^{\varphi} = \{x, x^{-1}\}$ для некоторого $x \in G^{'}$, либо $X^{\varphi} = \{x, y\}$ для некоторых $x, y \in G^{'}$ таких, что $|x| = |y| = 2$. В первом случае $G^{'}$ циклическая и, значит, изоморфна G; во втором случае $|G| = |G^{'}| = 4$, что противоречит предположению леммы. □

Пусть $\mathcal{A}$ — S-кольцо над циклической группой G. Положим $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(X)$, где X — базисное множество S-кольца $\mathcal{A}$, содержащее порождающий элемент группы G. Заметим, что $\mathrm{rad}(\mathcal{A})$ не зависит от выбора X. В самом деле, если $Y \in \mathcal{S}(\mathcal{A})$, $\langle Y \rangle = G$, и $Y \neq X$, то X и Y рационально сопряжены по теореме 3.1, и, следовательно, $\mathrm{rad}(X) = \mathrm{rad}(Y)$.

Лемма 5.2. *Пусть p — простое число, и $\mathcal{A}$ — S-кольцо над циклической p-группой G. Предположим, что $\mathrm{rad}(\mathcal{A}) > e$. Тогда найдется $\mathcal{A}$-секция U/L такая, что $\mathcal{A}$ является собственным U/L-сплетением и $\mathrm{rad}(\mathcal{A}_U) = e$.*

Доказательство. Пусть X — объединение всех базисных множеств S-кольца $\mathcal{A}$ с тривиальным радикалом. Тогда $U = \langle X \rangle$ — собственная $\mathcal{A}$-подгруппа, и $\mathrm{rad}(\mathcal{A}_U) = e$. Существует наименьшая нетривиальная $\mathcal{A}$-подгруппа L, так как G — циклическая p-группа. Все базисные множества вне U имеют нетривиальный радикал. Поскольку радикал каждого базисного множества является $\mathcal{A}$-подгруппой, мы заключаем, что $L \leq \mathrm{rad}(X)$ для любого $X \in \mathcal{S}(\mathcal{A})$, лежащего вне U. Таким образом, $\mathcal{A}$ является собственным U/L-сплетением. □

Пусть $p \in \{2, 3\}$ и $k \geq 1$. Положим $A = \langle a \rangle$ и $a_1 = a^{p^{k-1}}$, где $|a| = p^k$. Эти обозначения действуют до конца параграфа.

Лемма 5.3. *Пусть $\mathcal{A}$ — S-кольцо над A. Предположим, что $\mathrm{rad}(\mathcal{A}) = e$. Тогда выполнено одно из следующих утверждений:*

1) $\mathrm{rk}(\mathcal{A}) = 2$;
2) $\mathcal{A} = \mathbb{Z}A$;
3) $\mathcal{A} = \mathrm{Cyc}(K, A)$, *где* $K = \{\varepsilon, \sigma\}$, $\sigma : x \to x^{-1}$;
4) $p = 2$ *и* $\mathcal{A} = \mathrm{Cyc}(K, A)$, *где* $K = \{\varepsilon, \sigma\}$, $\sigma : x \to a_1 x^{-1}$.

Во всех случаях $\mathcal{A}$ отделимо относительно класса всех S-колец.

Доказательство. Из [17, теорема 4.1] и [17, теорема 4.2] следует, что любое S-кольцо с тривиальным радикалом над циклической группой является тензорным произведением циклотомических S-колец с тривиальным радикалом и S-колец ранга 2. Поскольку A — p-группа, мы заключаем, что либо $\mathrm{rk}(\mathcal{A}) = 2$, либо $\mathcal{A} = \mathrm{Cyc}(K, A)$ для некоторой $K \leq \mathrm{Aut}(A)$. В первом случае ясно, что $\mathcal{A}$ отделимо. Во втором случае из [18, лемма 5.1] вытекает, что для $\mathcal{A}$ выполнено одно из утверждений 2-4. В частности, $\mathcal{A}$ квазитонкое. Группа A циклическая и, очевидно, не содержит $\mathcal{A}$-подгрупп H таких, что $H \cong C_2 \times C_2$. Следовательно, $\mathcal{A}$ отделимо по лемме 3.5. □

Через $\mathrm{Sym}(V)$ обозначим симметрическую группу множества V. Группы подстановок Γ, $\Gamma' \leq \mathrm{Sym}(V)$ называются 2-*эквивалентными*, если множество орбит покомпонентного действия группы Γ на V^2 совпадает с множеством орбит покомпонентного действия группы Γ' на V^2. Группа подстановок $\Gamma \leq \mathrm{Sym}(V)$ называется 2-*изолированной*, если не существует групп подстановок, отличных от Γ и 2-эквивалентных Γ.

Лемма 5.4. *Пусть $\mathcal{A}$ — собственное U/L-сплетение над A, и $\mathrm{rad}(\mathcal{A}_U) = e$. Тогда $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$.*

Доказательство. Для того, чтобы доказать лемму, достаточно доказать, что группа $\mathrm{Aut}(\mathcal{A}_{U/L})$ — 2-изолированная. В самом деле, орбиты покомпонентного действия групп $\mathrm{Aut}(\mathcal{A}_{U/L})$ и $\mathrm{Aut}(\mathcal{A}_U)^{U/L}$ на множестве $(U/L)^2$ совпадают с базисными отношениями схемы Кэли, соответствующей S-кольцу $\mathcal{A}_{U/L}$. Поэтому $\mathrm{Aut}(\mathcal{A}_{U/L})$ и $\mathrm{Aut}(\mathcal{A}_U)^{U/L}$ являются 2-эквивалентными. Из этого следует, что если $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной, то $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$.

Поскольку $\mathrm{rad}(\mathcal{A}_U) = e$, для $\mathcal{A}_U$ выполнено одно из утверждений леммы 5.3. Если $\mathrm{rk}(\mathcal{A}_U) = 2$, то $U = L$, и $\mathrm{Aut}(\mathcal{A}_{U/L})$, очевидно, 2-изолированная. Если для $\mathcal{A}_U$ выполнено одно из утверждений 2-4 леммы 5.3, то $\mathcal{A}_{U/L} = \mathbb{Z}(U/L)$, или каждое базисное множество $\mathcal{A}_{U/L}$ имеет вид $\{x, x^{-1}\}$, $x \in U/L$. Следовательно, стабилизатор точки L в группе $\mathrm{Aut}(\mathcal{A}_{U/L})$ имеет точную регулярную орбиту, и $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной по [6, лемма 8.2]. □

Заметим, что для циклических p-групп, где $p > 3$, лемма, вообще говоря, неверна.

В [3] было доказано, что каждое S-кольцо над циклической p-группой, где p — простое число, отделимо относительно $\mathcal{K}_C$. Далее мы докажем, что все S-кольца над циклическими 2- и 3-группами отделимы относительно $\mathcal{K}_A$.

Лемма 5.5. *Пусть $\mathcal{A}$ — S-кольцо над A. Тогда $\mathcal{A}$ отделимо относительно $\mathcal{K}_A$.*

Доказательство. Будем вести доказательство индукцией по k. Если $k = 1$, то утверждение леммы выполнено, так как либо $\mathrm{rk}(\mathcal{A}) = 2$, либо $\mathcal{A} = \mathbb{Z}A$. Пусть теперь $k \geq 2$. Если $\mathrm{rad}(\mathcal{A}) = e$, то $\mathcal{A}$ отделимо по лемме 5.3. Предположим, что $\mathrm{rad}(\mathcal{A}) > e$. Тогда из леммы 5.2 следует, что $\mathcal{A}$ является собственным U/L-сплетением таким, что $\mathrm{rad}(\mathcal{A}_U) = e$. По предположению индукции S-кольца $\mathcal{A}_U$ и $\mathcal{A}_{A/L}$ отделимы относительно $\mathcal{K}_A$. В силу леммы 5.4 мы заключаем, что $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Таким образом, для $\mathcal{A}$ выполнены все условия леммы 4.4 и, следовательно, $\mathcal{A}$ отделимо относительно $\mathcal{K}_A$. □

§ 6. S-кольца над $C_p \times C_{p^k}$

Пусть $p \in \{2,3\}$ и $k \geq 1$. Положим $D = A \times B$, где $A = \langle a \rangle,\ |a| = p^k,\ B = \langle b \rangle,\ |b| = p$. Пусть $a_1 = a^{p^{k-1}}$ и $a_2 = a^{p^{k-2}}$. Если $l \leq k$, то обозначим подгруппы $\{g \in A : |g| \leq p^l\}$ и $\{g \in D : |g| \leq p^l\}$ группы D через A_l и D_l соответственно. В этих обозначениях $A = A_k$ и $D = D_k$.

В следующей лемме дается описание секций группы D, которыми она полностью определяется.

Лемма 6.1. *Пусть q — простое число, $m \geq 3$, и D' — абелева группа порядка q^{m+1}. Предположим, что выполнены следующие утверждения:*

1) D' содержит как минимум две подгруппы порядка q^{m-1}, и одна из этих подгрупп, скажем A', циклическая;

2) A' содержит подгруппу A'_1 порядка q такую, что D'/A'_1 изоморфна $C_q \times C_{q^{m-1}}$.

Тогда D' изоморфна $C_q \times C_{q^m}$ или $C_{q^2} \times C_{q^{m-1}}$. Более того, если $m \geq 4$ или D' содержит нециклическую подгруппу W' порядка q^2 такую, что $|W' \cap A'| = q$ и D'/W' циклическая, то $D' \cong C_q \times C_{q^m}$.

Доказательство. Поскольку D' абелева, она является прямым произведением циклических групп. Более того, D' изоморфна одной из следующих групп

$$C_{q^{m+1}}, C_q \times C_{q^m}, C_{q^2} \times C_{q^{m-1}}, C_q \times C_q \times C_{q^{m-1}},$$

потому что A' — циклическая группа порядка q^{m-1}. Заметим, что D' нециклическая, так как D' содержит как минимум две подгруппы порядка q^{m-1}. Предположим, что $D' \cong C_q \times C_q \times C_{q^{m-1}}$. Тогда $D' = H' \times A'$, где $H' \cong C_q \times C_q$. Если $A'_1 \leq A'$ имеет порядок q, то D'/A'_1 содержит подгруппу, изоморфную $C_q \times C_q \times C_q$, так как $m \geq 3$. Мы получаем противоречие, потому что $D'/A'_1 \cong C_q \times C_{q^{m-1}}$. Таким образом, $D' \cong C_q \times C_{q^m}$ или $D' \cong C_{q^2} \times C_{q^{m-1}}$.

Если $X \subseteq G \times H$, то проекции X на G и H мы будем обозначать через $\mathrm{pr}_G(X)$ и $\mathrm{pr}_H(X)$ соответственно. Докажем вторую часть леммы. Предположим, что $D' = H' \times A'$, где $H' \cong C_{q^2}$. Если $m \geq 4$, то D'/A'_1 содержит подгруппу, изоморфную $C_{q^2} \times C_{q^2}$ и мы получаем противоречие с тем, что $D'/A'_1 \cong C_q \times C_{q^{m-1}}$. Если в D' найдется нециклическая подгруппа W' порядка q^2 такая, что $|W' \cap A'| = q$ и D'/W' — циклическая, то $|\,\mathrm{pr}_{H'}(W')| = q$, потому что $|W' \cap A'| = q$. Поскольку W' нециклическая, $|\,\mathrm{pr}_{A'}(W')| = q$. Следовательно, $W' = \mathrm{pr}_{H'}(W') \times \mathrm{pr}_{A'}(W') \cong C_q \times C_q$. Поэтому D'/W' нециклическая, противоречие. Таким образом, $D' \cong C_q \times C_{q^m}$. □

Пусть $\mathcal{A}$ — S-кольцо над D. Базисное множество $X \in \mathcal{S}(\mathcal{A})$ называется *старшим*, если оно содержит элемент порядка p^k. Радикалом S-кольца $\mathrm{rad}(\mathcal{A})$ назовем подгруппу, порожденную подгруппами $\mathrm{rad}(X)$, где X пробегает все старшие базисные множества. Подмножество группы D называется *регулярным*, если оно состоит из элементов одного и того же порядка.

Классификация всех S-колец над D была получена для $p = 2$ в [6] и для $p = 3$ в [7].

Лемма 6.2. *Если $\mathcal{A}$ — S-кольцо над D и $k = 1$, то выполнено одно из следующих утверждений:*

1) $\mathrm{rk}(\mathcal{A}) = 2$;

2) *$\mathcal{A}$ является тензорным произведением двух S-колец над циклическими группами порядка p;*

3) *$\mathcal{A}$ является сплетением двух S-колец над циклическими группами порядка p;*

4) *$p = 3$ и $\mathcal{A} = \mathrm{Cyc}(K, D)$, где $K = \{e,\ \delta\},\ \delta : x \to x^{-1}$;*

5) *$p = 3$ и $\mathcal{A} \cong_{Cay} \mathrm{Cyc}(K, D)$, где K порождается элементом $(a_1, b) \to (b, a_1^2)$.*

Доказательство. Легко проверяется компьютерным вычислением с использованием пакета COCO2P [19]. □

Лемма 6.3. *Пусть $\mathcal{A}$ — S-кольцо над D и $k \geq 2$. Тогда выполнено одно из следующих утверждений:*

1) $\mathrm{rad}(\mathcal{A}) = e$, *и найдутся $\mathcal{A}$-подгруппы $L, H \leq D$ такие, что $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, $\mathrm{rk}(\mathcal{A}_H) = 2$, и $|L| \leq p \leq |H|$;*

2) $\mathrm{rad}(\mathcal{A}) > e$, *и найдется $\mathcal{A}$-секция U/L такая, что $\mathcal{A}$ — собственное U/L-сплетение. Более того, $\mathcal{A}_{U/L} = \mathbb{Z}(U/L)$, или $|U/L| \leq 4$, или $\mathrm{rad}(\mathcal{A}_U) = e$ и $|L| = p$;*

3) $\mathrm{rad}(\mathcal{A}) = e$, *и $\mathcal{A} \cong_{Cay} \mathrm{Cyc}(K, D)$, где $K \leq \mathrm{Aut}(D)$ — одна из групп, представленных в таблице 1 для $p = 2$ и в таблице 2 для $p = 3$.*

группа	действие на порождающих элементах	порядок группы	k
K_0	$(a, b) \to (a, b)$	1	$k \geq 2$
K_1	$(a, b) \to (a^{-1}, b)$	2	$k \geq 3$
K_2	$(a, b) \to (a_1 a^{-1}, b)$	2	$k \geq 3$
K_3	$(a, b) \to (a^{-1}, b a_1)$	2	$k \geq 3$
K_4	$(a, b) \to (a_1 a^{-1}, b a_1)$	2	$k \geq 3$
K_5	$(a, b) \to (b a_2 a, b a_1),\ (a, b) \to (a^{-1}, b)$	4	$k \geq 4$
K_6	$(a, b) \to (b a_2 a, b a_1),\ (a, b) \to (a_1 a^{-1}, b)$	4	$k \geq 4$
K_7	$(a, b) \to (b a^{-1}, b)$	2	$k \geq 4$
K_8	$(a, b) \to (b a_1 a^{-1}, b)$	2	$k \geq 4$
K_9	$(a, b) \to (b a_2 a, b a_1)$	2	$k \geq 3$
K_{10}	$(a, b) \to (b a_2 a^{-1}, b a_1)$	2	$k \geq 4$

Таблица 1.

группа	действие на порождающих элементах	порядок группы	k
K_0	$(a,b)\to(a,b)$	1	$k\geq 2$
K_1	$(a,b)\to(a,b^2)$	2	$k\geq 2$
K_2	$(a,b)\to(a^{-1},b)$	2	$k\geq 2$
K_3	$(a,b)\to(a^{-1},b),\ (a,b)\to(a,b^2)$	4	$k\geq 2$
K_4	$(a,b)\to(a^{-1},b^2)$	2	$k\geq 2$
K_5	$(a,b)\to(ba^{-1},b)$	2	$k\geq 2$
K_6	$(a,b)\to(ba,ba_1)$	3	$k\geq 3$
K_7	$(a,b)\to(ba,ba_1),\ (a,b)\to(a,b^2a_1)$	6	$k\geq 3$
K_8	$(a,b)\to(ba,ba_1^2),\ (a,b)\to(a^{-1},ba_1)$	6	$k\geq 3$
K_9	$(a,b)\to(ba,ba_1^2),\ (a,b)\to(a^{-1},b^2)$	6	$k\geq 3$

Таблица 2.

Доказательство. Утверждения леммы представляют собой утверждения [6, теорема 6.1, теорема 7.1, теорема 9.1] в случае $p=2$ и утверждения [7, теорема 4.1, теорема 5.1, теорема 6.1] в случае $p=3$. $\square$

Лемма 6.4. *Пусть $\mathcal{A}$ — S-кольцо над D, для которого выполнено утверждение* 2 *леммы* 6.3. *Тогда* $\mathrm{Aut}(\mathcal{A}_U)^{U/L}=\mathrm{Aut}(\mathcal{A}_{U/L})$.

Доказательство. Для доказательства леммы покажем, что либо $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной, либо $\mathrm{Aut}(\mathcal{A}_{U/L})=\mathrm{Sym}(U/L)=\mathrm{Aut}(\mathcal{A}_U)^{U/L}$. В первом случае $\mathrm{Aut}(\mathcal{A}_U)^{U/L}=\mathrm{Aut}(\mathcal{A}_{U/L})$, потому что $\mathrm{Aut}(\mathcal{A}_{U/L})$ и $\mathrm{Aut}(\mathcal{A}_U)^{U/L}$ являются 2-эквивалентными (см. доказательство леммы 5.4).

Если $\mathcal{A}_{U/L}=\mathbb{Z}(U/L)$ или $|U/L|\leq 4$, то, очевидно, что $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной. Далее по лемме 6.3 можно считать, что $\mathrm{rad}(\mathcal{A}_U)=e$ и $|L|=p$. Предположим, что U циклическая. Тогда $L=A_1$ — единственная $\mathcal{A}$-подгруппа порядка p, и для $\mathcal{A}_U$ выполнено одно из утверждений леммы 5.3. Если $\mathrm{rk}(\mathcal{A}_U)=2$, то $U=L$ и $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной. Если для $\mathcal{A}_U$ выполнено одно из утверждений 2-4 леммы 5.3, то $\mathcal{A}_{U/L}=\mathbb{Z}(U/L)$ или каждое базисное множество $\mathcal{A}_{U/L}$ имеет вид $\{x,x^{-1}\}$, $x\in U/L$. Значит, стабилизатор точки L в группе $\mathrm{Aut}(\mathcal{A}_{U/L})$ имеет точную регулярную орбиту, и $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной по [6, лемма 8.2].

Предположим теперь, что U нециклическая. Тогда $U\cong D_l$ для некоторого $l\leq k$. Если $\mathcal{A}_U$ регулярно, то $\mathrm{Aut}(\mathcal{A}_{U/L})$ — 2-изолированная по [6, теорема 8.1] для $p=2$ и по [7, следствие 5.2] для $p=3$. Если $\mathcal{A}_U$ нерегулярно, то из леммы 6.3 вытекает, что $\mathcal{A}_U=\mathcal{A}_H\otimes\mathcal{A}_L$, где $\mathrm{rk}(\mathcal{A}_H)=2$. Заметим, что $\mathrm{rk}(\mathcal{A}_L)=2$ или $\mathcal{A}_L=\mathbb{Z}L$, потому что $|L|=p$ и $p\in\{2,3\}$. Если $\mathrm{rk}(\mathcal{A}_L)=2$, то

$$\mathrm{Sym}(U/L)\geq\mathrm{Aut}(\mathcal{A}_{U/L})\geq\mathrm{Aut}(\mathcal{A}_U)^{U/L}=(\mathrm{Sym}(H)\times\mathrm{Sym}(L))^{U/L}=\mathrm{Sym}(U/L);$$

если $\mathcal{A}_L=\mathbb{Z}L$, то

$$\mathrm{Sym}(U/L)\geq\mathrm{Aut}(\mathcal{A}_{U/L})\geq\mathrm{Aut}(\mathcal{A}_U)^{U/L}=(\mathrm{Sym}(H)\times L_{right})^{U/L}=\mathrm{Sym}(U/L).$$

Таким образом, в обоих случаях $\mathrm{Aut}(\mathcal{A}_{U/L})=\mathrm{Sym}(U/L)=\mathrm{Aut}(\mathcal{A}_U)^{U/L}$. $\square$

§ 7. Доказательство теоремы 1

В данном параграфе сохраняются все обозначения, введенные в предыдущем параграфе.

Пусть $\mathcal{A}$ — произвольное S-кольцо над D. Покажем, что $\mathcal{A}$ отделимо относительно $\mathcal{K}_A$. Далее на протяжении данного параграфа для краткости будем писать "отделимо" вместо "отделимо относительно $\mathcal{K}_A$". Пусть $\mathcal{A}'$ — S-кольцо над абелевой группой D', и $\varphi : \mathcal{A} \to \mathcal{A}'$ — алгебраический изоморфизм. Будем вести доказательство индукцией по k. Пусть $k = 1$. Тогда для $\mathcal{A}$ выполнено одно из утверждений леммы 6.2. Если $\mathrm{rk}(\mathcal{A}) = 2$, то $\mathcal{A}$, очевидно, отделимо. Если $\mathcal{A}$ является тензорным произведением или сплетением двух S-колец над циклическими группами порядка p, то $\mathcal{A}$ отделимо по лемме 3.3. Если для $\mathcal{A}$ выполнено утверждение 4 леммы 6.2, то $\mathcal{A}$ удовлетворяет условиям леммы 3.5 и, следовательно, отделимо.

Предположим теперь, что для $\mathcal{A}$ выполнено утверждение 5 леммы 6.2. Тогда $|D'| = |D| = 9$ и $\mathrm{rk}(\mathcal{A}') = \mathrm{rk}(\mathcal{A}) = 3$. Из (3) следует, что $\mathrm{rad}(\mathcal{A}')$ тривиален, поскольку $\mathrm{rad}(\mathcal{A}) = e$. Если D' циклическая, то по лемме 5.3 либо $\mathrm{rk}(\mathcal{A}') = 2$, либо $\mathcal{A}'$ и $\mathcal{A}$ должны быть квазитонкими, что неверно. Значит, D' нециклическая и, следовательно, $D' \cong D$. Далее считаем, что $D' = D$. Из леммы 6.2 следует, что $\mathcal{A}$ — единственное с точностью до изоморфизма Кэли S-кольцо ранга 3 над D с базисными множествами мощностей $1, 4, 4$. Поэтому $\mathcal{A}' \cong_{Cay} \mathcal{A}$. Пусть $X = \{x, x^{-1}, y, y^{-1}\}$ — нетривиальное базисное множество $\mathcal{A}$ и $X^{\varphi} = \{x', (x')^{-1}, y', (y')^{-1}\}$. Тогда изоморфизм Кэли

$$\sigma : (x, y) \to (x', y') \in \mathrm{Aut}(D)$$

индуцирует φ.

Пусть теперь $k \geq 2$. Тогда для $\mathcal{A}$ выполнено одно из утверждений 1-3 леммы 6.3. Каждое S-кольцо над группой порядка p, где $p \in \{2, 3\}$, очевидно, отделимо. Поэтому если $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, где $\mathrm{rk}(\mathcal{A}_H) = 2$ и $|L| \leq p$, то $\mathcal{A}$ отделимо по лемме 3.3.

Преположим, что для $\mathcal{A}$ выполнено утверждение 2 леммы 6.3. Из леммы 6.4 следует, что $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Тогда по лемме 4.4 для того, чтобы доказать отделимость $\mathcal{A}$, достаточно доказать отделимость $\mathcal{A}_U$ и $\mathcal{A}_{D/L}$. Если $U = D_l$ для некоторого $l < k$, то $\mathcal{A}_U$ отделимо по предположению индукции. Если U циклическая, то $\mathcal{A}_U$ отделимо по лемме 5.5. Аналогично, $\mathcal{A}_{D/L}$ отделимо по предположению индукции, если D/L нециклическая, и по по лемме 5.5, если D/L циклическая.

Предположим, что для $\mathcal{A}$ выполнено утверждение 3 леммы 6.3. Тогда $\mathcal{A} \cong_{Cay} \mathrm{Cyc}(K, D)$, где $K \leq \mathrm{Aut}(D)$ — одна из групп, представленных в таблице 1 для $p = 2$ и в таблице 2 для $p = 3$. Если $K = K_0$, то $\mathcal{A} = \mathbb{Z}D$ отделимо. Если $p = 2$ и $K \in \{K_1, K_2, K_3, K_4, K_7, K_8, K_9, K_{10}\}$ или $p = 3$ и $K \in \{K_1, K_2, K_4, K_5\}$, то $\mathcal{A}$ квазитонкое, и легко напрямую проверить, что в D нет $\mathcal{A}$-подгрупп H, таких что $H \cong C_2 \times C_2$ и $\mathcal{A}_{D/H} = \mathbb{Z}(D/H)$. Значит, в этих случаях $\mathcal{A}$ отделимо по лемме 3.5. Если $p = 3$ и $K = K_3$, то $\mathcal{A}$ является тензорным произведением двух квазитонких S-колец над циклическими 3-группами. Следовательно, $\mathcal{A}$ отделимо по лемме 3.5 и лемме 3.3.

Таким образом, нам осталось рассмотреть следующие случаи: $K \in \{K_5, K_6\}$, если $p = 2$, и $K \in \{K_6, K_7, K_8, K_9\}$, если $p = 3$.

Лемма 7.1. $D^{'} \cong D$.

Доказательство. Проверим, что для $D^{'}$ выполнены условия леммы 6.1. Рассмотрим сначала случай $p=2$.

1. Неравенство $k \geq 4$ выполняется, потому что $K \in \{K_5, K_6\}$ (см. таблицу 1).

2. Заметим, что $\{bu, bu^{-1}\} \in \mathcal{S}(\mathcal{A})$ для любого $u \in A_{k-1} \setminus A_{k-2}$, так как $K \in \{K_5, K_6\}$. Выберем базисное множество $Y \subseteq b(A_{k-1} \setminus A_{k-2})$. Группа $F = \langle Y \rangle$ является циклической $\mathcal{A}$-подгруппой порядка 2^{k-1} и $\mathcal{A}_F = \mathrm{Cyc}(M, F)$, где $M = \{\varepsilon, \sigma\}$ и $\sigma : x \to x^{-1}$. Поскольку $k \geq 4$, мы заключаем, что $|F| > 4$. Ясно, что φ индуцирует алгебраический изоморфизм

$$\varphi_F : \mathcal{A}_F \to \mathcal{A}_{F^\varphi}.$$

Из леммы 5.1 вытекает, что F^φ — циклическая подгруппа $D^{'}$ порядка 2^{k-1}.

3. Из того, что D_{k-2} —$\mathcal{A}$-подгруппа порядка 2^{k-1}, отличная от F, следует, что D_{k-2}^φ — $\mathcal{A}^{'}$-подгруппа порядка 2^{k-1}, отличная от F^φ.

4. Группа A_1 является $\mathcal{A}$-подгруппой порядка 2. Поэтому A_1^φ — $\mathcal{A}^{'}$-подгруппа порядка 2. Пусть $\pi : D \to D/A_1$ — естественный гомоморфизм и X — старшее базисное множество $\mathcal{A}$. Если $K = K_5$, то $X = \{x, x^{-1}, ba_2x, ba_2^{-1}x^{-1}\}$, а если $K = K_6$, то $X = \{x, a_1x^{-1}, ba_2x, ba_2x^{-1}\}$, где x — порождающий элемент группы A. Множество $\pi(X)$ является порождающим для D/A_1 и выполнены следующие свойства

$$|\pi(X)| = 4,\ \pi(X) = \pi(X)^{-1},\ |\operatorname{rad}(\pi(X))| = 2. \tag{4}$$

Пусть

$$\varphi_{D/A_1} : \mathcal{A}_{D/A_1} \to \mathcal{A}_{D^{'}/A_1^\varphi}$$

— алгебраический изоморфизм, индуцированный φ. Из (3) следует, что $\pi(X)^{\varphi_{D/A_1}}$ — порождающее множество группы $D^{'}/A_1^\varphi$ и (4) также выполнено для $\pi(X)^{\varphi_{D/A_1}}$. Пусть $\pi(X)^{\varphi_{D/A_1}} = \{x^{'}, b^{'}x^{'}, y^{'}, b^{'}y^{'}\}$, где $\{e, b^{'}\} = \operatorname{rad}(\pi(X)^{\varphi_{D/A_1}})$. Если $(x^{'})^{-1} = bx^{'}$, то $(x^{'})^2 = (y^{'})^2 = b^{'}$ и, следовательно, $|D^{'}/A_1^\varphi| = 8$. Значит, $|D| = |D^{'}| = 16$. Мы получаем противоречие, потому что $k \geq 4$ и $|D| \geq 32$. Поэтому мы можем считать, что $y^{'} = (x^{'})^{-1}$. Из этого следует, что $D^{'}/A_1^\varphi$ порождается не более, чем двумя элементами, один из которых имеет порядок 2. Заметим, что $D^{'}/A_1^\varphi$ нециклическая, потому что она содержит как минимум две подгруппы A_2^φ/A_1^φ и D_1^φ/A_1^φ порядка 2. Мы заключаем, что $D^{'}/A_1^\varphi \cong C_2 \times C_{2^{k-1}}$. Таким образом $D^{'} \cong D \cong C_2 \times C_{2^k}$ по лемме 6.1.

Проверим, что для $D^{'}$ выполнятеся лемма 6.1 в случае $p = 3$.

1. Поскольку $K \in \{K_6, K_7, K_7, K_8\}$, группа A_{k-1} является циклической $\mathcal{A}$- подгруппой порядка 3^{k-1}. Более того, $\mathcal{A}_{A_{k-1}} = \mathbb{Z}A_{k-1}$, если $K \in \{K_6, K_7\}$, и $\mathcal{A}_{A_{k-1}} = \mathrm{Cyc}(M, A_{k-1})$, где $M = \{\varepsilon, \sigma\}$, $\sigma : x \to x^{-1}$, если $K \in \{K_8, K_9\}$. Ясно, что φ индуцирует алгебраический изоморфизм

$$\varphi_{A_{k-1}} : \mathcal{A}_{A_{k-1}} \to \mathcal{A}_{(A_{k-1})^\varphi}.$$

Из леммы 5.1 вытекает, что A_{k-1}^φ — циклическая $\mathcal{A}^{'}$-подгруппа порядка 3^{k-1}.

2. Группа D_{k-2}^φ — $\mathcal{A}^{'}$-подгруппа порядка 3^{k-1}, отличная от A_{k-1}^φ.

3. Заметим, что A_1^φ — $\mathcal{A}^{'}$-подгруппа порядка 3. Пусть $\pi : D \to D/A_1$ — естественный гомоморфизм и X — старшее базисное множество $\mathcal{A}$. Если $K \in \{K_6, K_7\}$, то

$X=\{x,bx,b^2a_1x\}$; если $K\in\{K_8,K_9\}$, то $X=\{x,x^{-1},bx,b^2x^{-1},b^2a_1^2x,ba_1x^{-1}\}$. Множество $\pi(X)$ является порождающим для D/A_1,

$$|\pi(X)|=3,\ |\operatorname{rad}(\pi(X))|=3, \tag{5}$$

если $K\in\{K_6,K_7\}$, и

$$|\pi(X)|=6,\ \pi(X)=\pi(X)^{-1},\ |\operatorname{rad}(\pi(X))|=3, \tag{6}$$

если $K\in\{K_8,K_9\}$. Пусть

$$\varphi_{D/A_1}:\mathcal{A}_{D/A_1}\to\mathcal{A}_{D'/A_1^\varphi}$$

— алгебраический изоморфизм, индуцированный φ. Из свойств алгебраического изоморфизма вытекает, что $\pi(X)^{\varphi_{D/A_1}}$ — порождающее множество D'/A_1^φ, (5) выполняется для $\pi(X)^{\varphi_{D/A_1}}$, если $K\in\{K_6,K_7\}$, и (6) выполняется для $\pi(X)^{\varphi_{D/A_1}}$, если $K\in\{K_8,K_9\}$. Поскольку $k\geq 3$, мы заключаем, что $\pi(X)^{\varphi_{D/A_1}}=x'B'$ или $\pi(X)^{\varphi_{D/A_1}}=x'B'\cup(x')^{-1}B'$, где $B'=\operatorname{rad}(\pi(X)^{\varphi_{D/A_1}})$. Таким образом, D'/A_1^φ порождается максимум двумя элементами, один из которых имеет порядок 3. Заметим, что D'/A_1^φ нециклическая, потому что она содержит как минимум две подгруппы A_2^φ/A_1^φ и D_1^φ/A_1^φ порядка 3. Из этого следует, что $D'/A_1^\varphi\cong C_3\times C_{3^{k-1}}$.

В силу леммы 6.1 группа D' изоморфна $C_3\times C_{3^k}$ или $C_9\times C_{3^{k-1}}$. Если $k\geq 4$, то $D'\cong C_3\times C_{3^k}$ по лемме 6.1. Пусть теперь $k=3$. Положим $D_1'=\{x\in D':|x|=3\}$. Ясно, что $|D_1'|=9$. Предположим, что D_1' — $\mathcal{A}'$-подгруппа. Тогда $D_1'=D_1^\varphi$ или $D_1'=A_2^\varphi$, так как только D_1 и A_2 являются $\mathcal{A}$-подгруппами порядка 9. Однако, A_2^φ циклическая по лемме 5.1. Значит, $D_1'=D_1^\varphi$. Группа D/D_1 циклическая, $\mathcal{A}_{D/D_1}=\mathbb{Z}(D/D_1)$ или $\mathcal{A}_{D/D_1}=\operatorname{Cyc}(M,D/D_1)$, где $M=\{\varepsilon,\sigma\}$, $\sigma:x\to x^{-1}$. В силу леммы 5.1 группа D'/D_1' также циклическая. Заметим, что $|D_1\cap A_2|=3$ и, следовательно, $|D_1'\cap A_2^\varphi|=3$. Таким образом, $D'\cong D\cong C_3\times C_9$ по лемме 6.1.

Предположим, что $D'\cong C_9\times C_9$. Тогда по доказанному выше D_1' не является $\mathcal{A}'$-подгруппой. Группа D_2 — $\mathcal{A}$-подгруппа, так как $\mathcal{A}$ регулярно. Следовательно, D_2^φ — $\mathcal{A}'$-подгруппа и $D'\setminus D_2^\varphi$ — $\mathcal{A}'$-множество. Поскольку $|D_2|=|D_2^\varphi|=27$, выполняется включение $D_1'\subset D_2^\varphi$. Пусть $X\subseteq D\setminus D_2$ — старшее базисное множество $\mathcal{A}$. Тогда $|X|\in\{3,6\}$, $\operatorname{rad}(X)$ тривиален, $\langle X\rangle=D$, и, если $|X|=6$, то $X=X^{-1}$. Эти свойства также выполняются для X^φ.

Предположим, что $|xD_1'\cap X^\varphi|=3$, где $x'\in X^\varphi$. Если $|X^\varphi|=3$, то $Y'=X^\varphi(X^\varphi)^{-1}$ является $\mathcal{A}'$-множеством, и $Y'\subseteq D_1'$. Более того, $Y'\nsubseteq A_1^\varphi$, так как иначе $\operatorname{rad}(X^\varphi)=A_1^\varphi$. Следовательно, $D_1'=\langle A_1^\varphi,Y'\rangle$ является $\mathcal{A}'$-подгруппой, противоречие с предположением. Пусть $|X^\varphi|=6$. Если $((x')^2\cup(x')^{-2})D_1'\cap D_2^\varphi\neq\varnothing$, то $((x')^2\cup(x')^{-2})D_1'\subset D_2^\varphi$ и, следовательно, $x'\in D_2^\varphi$. С другой стороны, $x'\in D'\setminus D_2^\varphi$, противоречие. Таким образом, $((x')^2\cup(x')^{-2})D_1'\cap D_2^\varphi=\varnothing$. Из этого вытекает, что $Y'=X^2\cap D_2^\varphi$ является $\mathcal{A}'$-множеством, и $Y'\subseteq D_1'$. Заметим, что $Y'\nsubseteq A_1^\varphi$, потому что иначе $\operatorname{rad}(X^\varphi)=A_1^\varphi$. Мы заключаем, что $D_1'=\langle A_1^\varphi,Y'\rangle$ — $\mathcal{A}'$-подгруппа, противоречие. Значит, $|xD_1'\cap X^\varphi|\neq 3$ для любого старшего базисного множества $X\in\mathcal{S}(\mathcal{A})$. Тогда $Y'=(X^\varphi)^{[3]}$ является $\mathcal{A}'$-множеством по лемме 3.2. Так как $D'\cong C_9\times C_9$, мы получаем, что $Y'\subseteq D_1'$. Если $Y'\nsubseteq A_1^\varphi$, то $D_1'=\langle A_1^\varphi,Y'\rangle$ — $\mathcal{A}'$-подгруппа, противоречие с предположением. Поэтому $(X^\varphi)^{[3]}\subseteq A_1^\varphi$ для любого старшего базисного множества X. Объединение всех старших базисных множеств $\mathcal{A}$ имеет мощность 54. Значит, $|\{x \in D' : x^3 \in A_1^{\varphi}\}| \geq 54$, что невозможно, если $D' \cong C_9 \times C_9$. Таким образом, D' не изоморфна $C_9 \times C_9$ и, следовательно, $D' \cong D \cong C_3 \times C_9$. □

Далее без ограничения общности мы можем считать, что $D = D'$.

Лемма 7.2. *$\mathcal{A}' \cong_{Cay} \mathcal{A}$.*

Доказательство. Для $\mathcal{A}'$ выполняется одно из утверждений леммы 6.3. Поскольку $\mathrm{rad}(\mathcal{A})$ тривиален, из (3) следует, что $\mathrm{rad}(\mathcal{A}')$ также тривиален. Значит, утверждение 2 леммы 6.3 для $\mathcal{A}'$ не выполняется. Ясно, что $|\mathcal{S}(\mathcal{A}')| = |\mathcal{S}(\mathcal{A})| > 6$. Следовательно, утверждение 1 леммы 6.3 для $\mathcal{A}'$ тоже не выполняется. Таким образом, для $\mathcal{A}'$ выполняется утверждение 3 леммы 6.3, то есть $\mathcal{A}' \cong_{Cay} \mathrm{Cyc}(K', D)$, где $K' \leq \mathrm{Aut}(D)$ — одна из групп, представленных в таблице 1 для $p = 2$ и в таблице 2 для $p = 3$.

Рассмотрим сначала случай $p = 2$. У $\mathcal{A}$, а значит и у $\mathcal{A}'$, есть базисные множества мощности 4. Следовательно, $\mathcal{A}'$ не является квазитонким. Из этого вытекает, что $K' \in \{K_5, K_6\}$. Заметим, что $\mathrm{Cyc}(K_5, D)$ симметрично, а $\mathrm{Cyc}(K_6, D)$ не является симметричным. Если $\mathcal{A}$ симметрично, то по свойствам алгебраического изоморфизма $\mathcal{A}'$ тоже симметрично и, следовательно, $\mathcal{A}' \cong_{Cay} \mathrm{Cyc}(K_5, D) \cong_{Cay} \mathcal{A}$. Если $\mathcal{A}$ несимметрично, то $\mathcal{A}'$ тоже несимметрично и $\mathcal{A}' \cong_{Cay} \mathrm{Cyc}(K_6, D) \cong_{Cay} \mathcal{A}$.

Пусть теперь $p = 3$. Для заданного S-кольца $\mathcal{B}$ положим

$$\mathcal{N}(\mathcal{B}) = \{|X| : X \in \mathcal{S}(\mathcal{B})\}.$$

Ясно, что $\mathcal{N}(\mathcal{B})$ является инвариантом относительно алгебраических изоморфизмов. Поэтому утверждение леммы следует из следующего замечания: $\mathcal{B} = \mathrm{Cyc}(K_i, D)$ является единственным с точностью до изоморфизма Кэли циклотомическим S-кольцом над D таким, что

1) $\mathcal{N}(\mathcal{B}) = \{1, 3\}$, если $i = 6$;
2) $\mathcal{N}(\mathcal{B}) = \{1, 3, 6\}$, если $i = 7$;
3) $\mathcal{N}(\mathcal{B}) = \{1, 2, 3, 6\}$, если $i = 8$;
4) $\mathcal{N}(\mathcal{B}) = \{1, 2, 6\}$, если $i = 9$. □

Пусть $X \in \mathcal{S}(\mathcal{A})$ — старшее базисное множество. Если $p = 3$ и $K \in \{K_6, K_8\}$, то положим $Z = bA_1$ и $Y = X \cup Z$; иначе положим $Y = X$.

Лемма 7.3. *$\mathcal{A} = \langle \underline{Y} \rangle$ и $\mathcal{A}' = \langle \underline{Y^{\varphi}} \rangle$.*

Доказательство. Положим $\mathcal{A}_1 = \langle \underline{Y} \rangle$. Из леммы 6.3 следует, что X содержит некоторый порождающий элемент x группы A и

$$X = \{x, x^{-1}, ba_2x, ba_2^{-1}x^{-1}\},$$

если $p = 2$ и $K = K_5$;

$$X = \{x, a_1x^{-1}, ba_2x, ba_2x^{-1}\},$$

если $p = 2$ и $K = K_6$;

$$X = \{x, bx, b^2a_1x\},$$

если $p = 3$ и $K \in \{K_6, K_7\}$;

$$X = \{x, x^{-1}, bx, b^2x^{-1}, b^2a_1^2x, ba_1x^{-1}\},$$

если $p = 3$ и $K \in \{K_8, K_9\}$.

Для $\mathcal{A}_1$ не выполняется утверждение 1 леммы 6.3, так как иначе каждый элемент порядка p^k лежал бы в базисном множестве мощности как минимум p^k-1, где $k \geq 4$, если $p = 2$, и $k \geq 3$, если $p = 3$. Легко проверить, что каждое подмножество множества Y, состоящее из элементов порядка p^k, имеет тривиальный радикал. Следовательно, $\mathcal{A}_1$ имеет старшее базисное множество с тривиальным радикалом, и утверждение 2 леммы 6.3 не выполняется для $\mathcal{A}_1$. Таким образом, $\mathcal{A}_1$ циклотомическое. Из описания всех циклотомических S-колец над D, которое представлено в лемме 6.3, вытекает, что $\mathcal{A}_1 = \mathcal{A}$. Стоит отметить, что если $p = 3$, то $\mathrm{Cyc}(K_6, D)$ и $\mathrm{Cyc}(K_7, D)$, а также $\mathrm{Cyc}(K_8, D)$ и $\mathrm{Cyc}(K_9, D)$ имеют одинаковые старшие базисные множества. В случаях, когда $K \in \{K_7, K_9\}$, порождающим множеством для $\mathcal{A}$ является старшее базисное множество X, а в случаях, когда $K \in \{K_6, K_8\}$, порождающим множеством для $\mathcal{A}$ является $X \cup Z$.

Из (3) следует, что X^φ является старшим базисным множеством $\mathcal{A}'$. Если $p = 3$, то имеется ровно две подгруппы порядка 9 в D: A_2 и D_1. Они являются $\mathcal{A}$-подгруппами. Группа A_2^φ циклическая $\mathcal{A}'$-подгруппа по лемме 5.1, и, следовательно, $A_2^\varphi = A_2$. Значит, $D_1^\varphi = D_1$. Если $K \in \{K_6, K_8\}$, то $Z^\varphi \in \{Z, Z^{-1}\}$, так как только Z и Z^{-1} являются базисными множествами мощности 3, лежащими в D_1. Таким образом, если $Y = X \cup Z$, то $Y^\varphi = X^\varphi \cup Z$ или $Y^\varphi = X^\varphi \cup Z^{-1}$. Поскольку $\mathcal{A}' \cong_{Cay} \mathcal{A}$, рассуждениями, аналогичными проведенным выше, можно показать, что $\mathcal{A}' = \langle \underline{Y^\varphi} \rangle$. □

Лемма 7.4. *Алгебраический изоморфизм φ индуцируется изоморфизмом Кэли.*

Доказательство. По лемме 7.2 найдется изоморфизм Кэли f из $\mathcal{A}$ в $\mathcal{A}'$. Множества X^φ и X^f являются старшими базисными множествами $\mathcal{A}'$. Если $p = 2$, то каждое старшее базисное множество кольца $\mathcal{A}'$ имеет вид

$$X_0 \cup bX_1,$$

где $X_i \subseteq A,\ X_i \neq \varnothing,\ i \in \{0, 1\}$. Это следует из того, что $K \in \{K_5, K_6\}$. Аналогично, если $p = 3$, то каждое старшее базисное множество кольца $\mathcal{A}'$ имеет вид

$$X_0 \cup bX_1 \cup b^2X_2,$$

где $X_i \subseteq A,\ X_i \neq \varnothing,\ i \in \{0, 1, 2\}$. Значит, по лемме 3.1 множества X^φ и X^f рационально сопряжены и найдется изоморфизм Кэли g из $\mathcal{A}'$ в $\mathcal{A}'$ такой, что $X^{fg} = X^\varphi$. Изоморфизм Кэли fg из $\mathcal{A}$ в $\mathcal{A}'$ индуцирует алгебраический изоморфизм φ_{fg}. Если $p = 2$ или $p = 3$ и $K \in \{K_7, K_9\}$, то $\mathcal{A} = \langle \underline{X} \rangle$ и $\mathcal{A}' = \langle \underline{X^\varphi} \rangle$ по лемме 7.3. В этих случаях из леммы 3.4 следует, что $\varphi = \varphi_{fg}$.

Пусть теперь $p = 3$ и $K \in \{K_6, K_8\}$. Из леммы 7.3 следует, что $\mathcal{A} = \langle \underline{Y} \rangle$ и $\mathcal{A}' = \langle \underline{Y^\varphi} \rangle$. Если $Z^{fg} = Z^\varphi$, то $Y^{fg} = Y^\varphi$. По лемме 3.4 мы заключаем, что $\varphi = \varphi_{fg}$. Предположим, что $Z^{fg} \neq Z^\varphi$. Без ограничения общности мы считаем, что $Z^{fg} = \{b, ba_1, ba_1^2\}$ и $Z^\varphi = \{b^2, b^2a_1, b^2a_1^2\}$. Если $K = K_6$, то $X^\varphi = \{y, by, b^2a_1y\}$ или

$X^\varphi = \{y, ba_1^2 y, b^2 y\}$; если $K = K_8$, то $X^\varphi = \{y, y^{-1}, by, ba_1 y^{-1}, b^2 a_1^2 y, b^2 y^{-1}\}$, где y — порождающий элемент A. Положим

$$h : (y, b) \to (y, b^2 a_1) \in \mathrm{Aut}(D)$$

если $K = K_6$ и

$$h : (y, b) \to (y, b^2 a_1^2) \in \mathrm{Aut}(D)$$

если $K = K_8$. Прямая проверка показывает, что $X^{fgh} = (X^\varphi)^h = X^\varphi$ и $Z^{fgh} = Z^\varphi$. Поскольку X^φ — старшее базисное множество циклотомического S-кольца $(\mathcal{A}')^h$, мы имеем, что $(\mathcal{A}')^h = \mathcal{A}'$. Таким образом, fgh — изоморфизм Кэли из $\mathcal{A}$ в $\mathcal{A}'$ такой, что $Y^{fgh} = Y^\varphi$. Из леммы 3.4 следует, что $\varphi = \varphi_{fgh}$, где φ_{fgh} — алгебраический изоморфизм, индуцированный fgh. $\square$

Таким образом, в случаях, когда $\mathcal{A} = \mathrm{Cyc}(K, D)$, где $K \in \{K_5, K_6\}$, если $p = 2$, и $K \in \{K_6, K_7, K_8, K_9\}$, если $p = 3$, любой алгебраический изоморфизм $\mathcal{A}$ индуцируется изоморфизмом Кэли. Следовательно, $\mathcal{A}$ отделимо, и доказательство теоремы 1 завершено.

§ 8. Связь отделимости с проблемой изоморфизма графов Кэли

Пусть $\Gamma = Cay(G, X)$ и $\Gamma' = Cay(G', X')$ — графы Кэли над группами G и G' соответственно. Обозначим множество всех изоморфизмов Γ и Γ' через $\mathrm{Iso}(\Gamma, \Gamma')$. Фиксируем классы групп $\mathcal{K}$ и $\mathcal{K}'$. Проблема изоморфизма графов Кэли может быть сформулирована следующим образом

ISO. Для заданных графов Кэли Γ над $G \in \mathcal{K}$ и Γ' над $G' \in \mathcal{K}'$ определить верно ли, что $\mathrm{Iso}(\Gamma, \Gamma') \neq \varnothing$.

Далее мы рассмотрим сведение ISO к следующей проблеме:

ALISO. Для заданных схем Кэли $\mathcal{C}$ над $G \in \mathcal{K}$ и $\mathcal{C}'$ над $G' \in \mathcal{K}'$ и алгебраического изоморфизма $\varphi : \mathcal{C} \to \mathcal{C}'$ определить верно ли, что $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) \neq \varnothing$.

Предложение 8.1. *Проблема ISO сводится к ALISO за время $|G|^{O(1)}$.*

Доказательство. Предположим, что существует алгоритм Al_1 для решения ALISO. Считаем, что $|G| = |G'| = n$, в противном случае, Γ и Γ', очевидно, не изоморфны. Обозначим через E и E' множества ребер Γ и Γ' соответственно. Пусть

$$\mathcal{T} = (\mathrm{Diag}(G \times G), E, G \times G \setminus (E \cup \mathrm{Diag}(G \times G))$$

и

$$\mathcal{T}' = (\mathrm{Diag}(G' \times G'), E', G' \times G' \setminus (E' \cup \mathrm{Diag}(G' \times G'))$$

— соответствующие Γ и Γ' упорядоченные разбиения множеств $G \times G$ и $G' \times G'$. С помощью алгоритма Вейсфейлера-Лемана ([9, 10]) по $\mathcal{T}$ и $\mathcal{T}'$ можно построить за время $n^{O(1)}$ упорядоченные разбиения $\mathcal{R} = (P_1, P_2, \ldots, P_k)$ и $\mathcal{R}' = (Q_1, Q_2, \ldots, Q_l)$, задающие схемы Кэли $\mathcal{C}$ и $\mathcal{C}'$ над G и G' соответственно. Это будут наименьшие схемы, в которых E и E' являются объединениями базисных отношений.

Если $f \in \mathrm{Iso}(\Gamma, \Gamma')$, то по свойствам алгоритма Вейсфейлера-Лемана $k = l$, f является изоморфизмом $\mathcal{C}$ и $\mathcal{C}'$ таким, что $P_i^f = Q_i,\ i = 1, \ldots, k$, и, следовательно, отображение $\varphi : P_i \to Q_i,\ i = 1, \ldots, k$ является алгебраическим изоморфизмом. Обратно, если $\varphi : P_i \to Q_i$ является алгебраическим изоморфизмом и $f \in \mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi)$, то $E^f = E'$ и $f \in \mathrm{Iso}(\Gamma, \Gamma')$. Таким образом, $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) = \mathrm{Iso}(\Gamma, \Gamma')$.

Проверить, является ли отображение $\varphi : P_i \to Q_i,\ i = 1, \ldots, k$, алгебраическим изоморфизмом можно за время $n^{O(1)}$, так как чисел пересечения у схемы $\mathcal{C}$ не больше, чем n^3. Если φ не является алгебраическим изоморфизмом, то Γ и Γ' неизоморфны. Если же φ является алгебраическим изоморфизмом , то, применяя Al_1, можно проверить непустоту множества $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) = \mathrm{Iso}(\Gamma, \Gamma')$. □

Пусть теперь $\mathcal{K}$ — класс групп, изоморфных группе $D = C_p \times C_{p^k}$ для $p \in \{2, 3\}$ и $k \geq 1$, а $\mathcal{K}'$ — класс всех абелевых групп. Если $\mathcal{C}$ — схема Кэли над $G \in \mathcal{K}$, являющаяся отделимой относительно класса схем Кэли над группами из $\mathcal{K}'$, и $\mathcal{C}' \in \mathcal{K}'$, то ALISO становится тривиальной, так как для любого алгебраического изоморфизма $\varphi : \mathcal{C} \to \mathcal{C}'$ множество $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi)$ непусто. Следовательно, ISO разрешима за время $|G|^{O(1)}$. Таким образом, теорема 2 следует из теоремы 1, предложения 2.1 и предложения 8.1, примененного к классам $\mathcal{K}$ и $\mathcal{K}'$.

Стоит отметить, что представленный в данном параграфе материал основан на идеях, предложенных в [9] и развитых в [8].

Литература

1. *I. Schur*, Zur theorie der einfach transitiven Permutationgruppen, S.-B. Preus Akad. Wiss. Phys.-Math. Kl., **18**, No. 20 (1933), 598-623.
2. *H. Wielandt*, Finite permutation groups, Academic Press, New York - London, 1964.
3. *S. Evdokimov, I. Ponomarenko*, On separability problem for circulant S-rings, Алгебра и анализ, **28**, № 1 (2016), 32-51.
4. *С. Евдокимов, И. Пономаренко*, Об одном семействе колец Шура над конечной циклической группой, Алгебра и анализ, **13**, № 3 (2001), 139–154.
5. *Я.Гольфанд, М.Клин*, Аморфные клеточные кольца I, Исследования по алгебраической теории комбинаторных объектов: труды семинара, ВНИИСИ, Институт системных исследований, Москва, 1985, 32-38.
6. *М. Музычук, И. Пономаренко*, О 2-группах Шура, Зап. научн. сем. ПОМИ, **435** (2015), 113–162.
7. *G. Ryabov*, On Schur p-groups of odd order, J. Algebra Appl., **16**, No. 3 (2017), 1750045-1-1750045-29.
8. *S. Evdokimov, I. Ponomarenko*, Permutation group approach to association schemes, Eur. J. Comb., **30** (2009), 1456-1476.
9. *B. Yu. Weisfeiler*, On the construction and identification of graphs, Lecture Notes in Math., vol. 558, Springer-Verlag, Berlin etc., 1976.
10. *Б. Ю. Вейсфейлер, А. А. Леман*, Приведение графа к каноническому виду и возникающая при этом алгебра, Научно-техн. информ. Сб. ВИНИТИ. **2**, № 9 (1968), 12–16.
11. *С. Евдокимов, И. Пономаренко*, Распознавание и проверка изоморфизма циркулянтных графов за полиномиальное время, Алгебра и анализ, **15**, № 6 (2003), 1–34.
12. *M. Muzychuk*, A solution of the isomorphism problem for circulant graphs, Proc. Lond. Math. Soc., **88**, No. 1 (2004), 1-41.
13. *M. Muzychuk, I. Ponomarenko*, Schur rings, European Journal of Combinatorics, **30** (2009), 1526-1539.
14. *S. Evdokimov, I. Ponomarenko*, Coset closure of a circulant S-ring and schurity problem, J. Algebra Appl., **15**, No. 4 (2016), 1650068-1-1650068-49.

15. *С. Евдокимов*, Шуровость и отделимость ассоциативных схем, Дис. на соиск. учен. ст. докт. физ.-мат. наук, СПбГУ, СПб., 2004.
16. *M. Muzychuk, I. Ponomarenko*, On quasi-thin association schemes, J. Algebra, **351** (2012), 467-489.
17. *С. Евдокимов, И. Пономаренко*, Шуровость S-колец над циклической группой и обобщенное сплетение групп перестановок, Алгебра и анализ, **24**, № 3 (2012), 84–127.
18. *С. Евдокимов, И. Пономаренко*, Характеризация циклотомических схем и нормальные кольца Шура над циклической группой, Алгебра и анализ, **14**, № 2 (2002), 11–55.
19. *M. Klin, C. Pech, S. Reichard*, COCO2P — a GAP package, 0.14, 07.02.2015, http://www.math.tu-dresden.de/ pech/COCO2P.

Рябов Григорий Константинович, Новосибирский Государственный Университет, ул.Пирогова, 2, г. Новосибирск, 630090, Россия

E-mail address: gric2ryabov@gmail.com