Федеральное государственное автономное
образовательное учреждение высшего образования
«Новосибирский национальный исследовательский
государственный университет»

На правах рукописи

Рябов Григорий Константинович

ШУРОВОСТЬ И ОТДЕЛИМОСТЬ КОЛЕЦ ШУРА НАД КОНЕЧНЫМИ p-ГРУППАМИ

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация на соискание ученой степени кандидата
физико-математических наук

Научный руководитель
доктор физико-математических наук
Васильев Андрей Викторович

Новосибирск – 2019

Оглавление

Введение

Постановка задачи и цели исследования. В 1933 г. Шур доказал, что каждая примитивная группа подстановок, содержащая регулярную циклическую подгруппу составного порядка, является дважды транзитивной. В отличие от Бернсайда, использовавшего при доказательстве аналогичного утверждения для p-групп теорию характеров, Шур свел задачу к изучению специальных подколец целочисленного группового кольца. Пусть G — конечная группа и $G_{right} = \{x \mapsto xg,\ x \in G : g \in G\}$ — подгруппа правых сдвигов группы подстановок множества G. В [25] Шур показал, что для любой группы подстановок K на множестве G, содержащей G_{right}, подмодуль целочисленного группового кольца группы G, натянутый на орбиты стабилизатора единицы группы G в K, является подкольцом последнего. Это подкольцо очевидным образом замкнуто относительно покомпонентного умножения и инволюции, индуцированной взятием обратного элемента в G, а также содержит единицы по обоим умножениям. Позднее каждое подкольцо целочисленного группового кольца, обладающее этими свойствами, стали называть *кольцом Шура* или S-*кольцом* над заданной группой.

В [28] Виланд писал: «Шур длительное время полагал, что каждое S-кольцо определяется подходящей группой подстановок». Однако, предположение Шура оказалось неверным, и первые контрпримеры к его предположению были найдены Виландом [27]. Позднее Пёшель предложил называть S-кольца, происходящие из групп подстановок, *шуровыми* [24].

В работе [24] Пёшель предложил следующее определение: конечная группа называется *шуровой*, если каждое S-кольцо над ней шурово. В этой же работе он доказал, что циклические p-группы нечетного порядка шуровы, а если p — простое число, большее 3, то p-группа шурова тогда и только тогда, когда она циклическая. Стоит отметить, что описание S-колец над циклическими p-группами нечетного порядка, полученное Пёшелем при доказательстве упомянутого выше результата, было использовано Клином и Пёшелем в дальнейшем для решения проблемы изоморфизма графов Кэли над циклическими p-группами нечетного порядка [16].

Следующая проблема, исследованию которой посвящена диссертация, также была предложена Пёшелем в [24].

Проблема 1. Определить все шуровы группы.

Изоморфизмом (комбинаторным) S-колец $\mathcal{A}$ и $\mathcal{A}'$ над группами G и G' соответственно

называется биекция $f : G \to G'$, являющаяся изоморфизмом соотвествующих схем Кэли. *Алгебраический изоморфизм* S-колец $\mathcal{A}$ и $\mathcal{A}'$ — это кольцевой изоморфизм между ними. Несложно проверить, что любой комбинаторный изоморфизм индуцирует алгебраический. Однако, обратное утверждение неверно. Соответствующие примеры были найдены Евдокимовым и Пономаренко в [3]. Пусть $\mathcal{K}$ — класс групп. Следуя работе [9] Евдокимова и Пономаренко, назовем S-кольцо $\mathcal{A}$ *отделимым* относительно $\mathcal{K}$, если каждый алгебраический изоморфизм из $\mathcal{A}$ в S-кольцо над группой из $\mathcal{K}$ индуцируется комбинаторным изоморфизмом. Заметим, что если $\mathcal{A}$ отделимо относительно $\mathcal{K}$, то $\mathcal{A}$ определяется с точностью до изоморфизма в классе S-колец над группами из $\mathcal{K}$ лишь тензором своих структурных констант относительно базиса, соответствующего разбиению группы. Таким образом, вопрос об отделимости S-колец является частным случаем общего вопроса о том, когда комбинаторная структура определяется с точностью до изоморфизма своими параметрами.

Назовем конечную группу *отделимой* относительно класса групп $\mathcal{K}$, если каждое S-кольцо над ней отделимо относительно $\mathcal{K}$. Если группа G является отделимой относительно некоторого класса групп, то изоморфизм двух графов Кэли над G может быть проверен за полиномиальное время от порядка G с помощью алгоритма Вейсфейлера-Лемана [1, 26].

Ещё одна проблема, которая исследуется в диссертации, может быть сформулирована следующим образом.

Проблема 2. Определить все абелевы группы, отделимые относительно класса абелевых групп.

Степень проработанности темы исследования. Заметим, что для доказательства шуровости данной группы необходимо доказать, что все S-кольца над ней шуровы. Однако, задача описания всех S-колец над заданной группой зачастую является трудной. К примеру, эта задача не решена даже для элементарной абелевой группы порядка p^2, где p — произвольное простое число. В свою очередь, для доказательства того, что группа не является шуровой, достаточно найти хотя бы одно нешурово S-кольцо над этой группой.

Обозначим циклическую группу порядка n через C_n, а элементарную абелеву группу порядка n — через E_n. Пёшель и Клин доказали, что группы C_{pq}, где p и q —различные простые числа, шуровы [17]. Шуровость циклических 2-групп была доказана Гольфандом, Наймарком и Пёшелем в [15]. Позднее Клином была высказана гипотеза о том, что все циклические группы шуровы. Однако, эта гипотеза была опровергнута в работе [3] Евдокимова и Пономаренко, где были найдены первые примеры нешуровых циклических групп. Все циклические и элементарные абелевы шуровы группы были классифицированы Евдокимовым,

Ковачем и Пономаренко в [13] и [14] соответственно. В [14] ими также были получены сильные необходимые условия шуровости для абелевых нециклических групп, не являющихся элементарными абелевыми. Более точно, ими была доказана следующая теорема.

Теорема А. Пусть G — абелева нециклическая шурова группа, не являющаяся элементарной абелевой. Тогда G принадлежит одному из следующих семейств групп:

1) $C_2 \times C_{2^k}$, $C_{2p} \times C_{2^k}$, $E_4 \times C_{p^k}$, $E_4 \times C_{pq}$, $E_{16} \times C_p$,

2) $C_3 \times C_{3^k}$, $C_6 \times C_{3^k}$, $E_9 \times C_q$, $E_9 \times C_{2q}$,

где p и q — различные простые числа, $p \neq 2$ и $k \geq 1$.

Шуровость групп $E_4 \times C_p$, где p — простое число, была доказана Евдокимовым, Ковачем и Пономаренко в [14]. Музычук и Пономаренко доказали, что группы $C_2 \times C_{2^k}$, где $k \geq 1$, шуровы [7]. Вопрос о шуровости остальных групп из теоремы А к началу диссертационного исследования оставался открытым.

С помощью компьютерных вычислений с использованием пакета COCO2P [18] были получены примеры шуровых неабелевых групп небольших порядков. Вопрос о шуровости неабелевых групп изучался в статье Васильева и Пономаренко [23]. В ней было доказано, что каждая шурова группа является метабелевой и множество простых делителей порядка шуровой группы содержит не более семи элементов.

Обозначим группу диэдра порядка $2n$ и группу кватернионов через D_{2n} и Q_8 соответственно. Положим $G_{16} = \langle a, b, c : a^4 = b^2 = c^2 = [a, b] = [a, c] = e,\ [b, c] = a^2 \rangle$ и $M_{p^k} = \langle a, b : a^{p^{k-1}} = b^p = e, a^b = a^{p^{k-2}+1} \rangle$, где p — простое число. Одним из ключевых шагов на пути к определению всех шуровых групп является определение всех шуровых p-групп. В работе [23] Васильев и Пономаренко доказали следующую теорему о неабелевых шуровых p-группах.

Теорема Б. Если неабелева p-группа G шурова, то $p \in \{2, 3\}$ и G изоморфна одной из следующих групп:

1) Q_8, G_{16}, M_{2^k}, $k > 5$, D_{2^k}, $k > 2$, если $p = 2$,

2) M_{3^k}, $k > 2$, если $p = 3$.

Более того, группы Q_8, G_{16}, D_{2^k}, где $2 < k < 6$, шуровы.

Музычук и Пономаренко доказали, что группы M_{2^k}, $k > 5$, нешуровы [7]. Вопрос о шуровости групп D_{2^k} при $k > 5$ и M_{3^k} при $k > 2$ к началу диссертационного исследования оставался открытым.

В [3] Евдокимовым и Пономаренко было показано существование циклических групп, не отделимых относительно класса циклических групп. С другой стороны, в [11] они доказали, что циклические p-группы отделимы относительно класса циклических групп. До начала диссертационного исследования циклические p-группы были единственным известным примером бесконечной серии групп, отделимых относительно некоторого класса. Оставался открытым вопрос о том, существуют ли бесконечные серии нециклических групп, отделимых относительно некоторого класса.

Как уже говорилось ранее, если группа G отделима относительно некоторого класса групп, то проблема изоморфизма в классе графов Кэли над G может быть решена за полиномиальное время от порядка G. Таким образом, любой результат об отделимости конечных групп влечет за собой результат о решении проблемы изоморфизма для графов Кэли над этими группами. Проблема изоморфизма для графов Кэли над циклическими группами была решена независимо Евдокимовым и Пономаренко в [5] и Музычуком в [19]. В 2018 г. Недела и Пономаренко решили проблему изоморфизма для графов Кэли над группами $E_4 \times C_p$, где p — простое число [22].

Основные результаты диссертации.

1. Доказано, что группы $M_{3^k} = \langle a, b : a^{3^{k-1}} = b^3 = e, a^b = a^{3^{k-2}+1} \rangle$, где $k \geq 3$, не являются шуровыми (теорема 1). Как следствие установлено, что шурова p-группа нечетного порядка должна быть абелевой (следствие 1). Опубликовано в статье [30].

2. Получено описание всех S-колец над группами $C_3 \times C_{3^k}$, где $k \geq 1$ (теорема 2). Доказано, что эти группы шуровы (теорема 3). Как следствие получено полное описание всех шуровых p-групп нечетного порядка (теорема 4). Опубликовано в статье [31].

3. Доказано, что группы $C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$, и $E_4 \times C_p$, где p — простое число, отделимы относительно класса абелевых групп (теоремы 5,6). Тем самым получены первые примеры бесконечных серий нециклических групп, отделимых относительно класса абелевых групп. Как следствие решена проблема изоморфизма для графов Кэли над этими группами (следствия 2,3). Опубликовано в статьях [32, 33].

Научная новизна и значимость работы. В диссертации сделан существенный шаг в изучении проблем шуровости и отделимости для S-колец и конечных групп, а также в изучении проблемы изоморфизма для графов Кэли. Теоремы 1, 3, 4 завершают классификацию шуровых p-групп нечетного порядка. Теоремы 5 и 6 дают первые примеры бесконечных серий нециклических групп, отделимых относительно класса абелевых групп. Кроме того, в диссертации были предложены новые методы работы с S-кольцами. В частности, было

получено достаточное условие отделимости обобщенного сплетения S-колец над абелевыми группами (предложение 1.6.9).

Работа носит теоретический характер. Все полученные результаты являются новыми. Результаты работы могут быть использованы в дальнейших исследованиях по алгебраической комбинаторике и теории групп, связанных с S-кольцами и проблемой изоморфизма графов, а также могут быть включены в спецкурсы для студентов и аспирантов, специализирующихся в области алгебры и комбинаторики.

Методы исследования. Для работы с S-кольцами над абелевыми группами применяются классические результаты Шура и Виланда об S-кольцах и группах подстановок (см. [25, 27]), а также результаты о структуре S-колец над абелевыми группами, полученные в работах Евдокимова, Музычука, Пономаренко (см. [6,7,12]). При работе с S-кольцами над группами малых порядков используются компьютерные вычисления в GAP с использованием пакета COCO2P [18]. Получение описания всех S-колец над группами $C_3 \times C_{3^k}$, $k \geq 1$, основано на подходе, предложенном Музычуком и Пономаренко в [7]. Ключевым инструментом доказательства шуровости этих групп является достаточное условие шуровости обобщенного сплетения S-колец над абелевыми группами, полученное в работе [6] Евдокимова и Пономаренко. Доказательство отделимости групп относительно класса абелевых групп базируется на описании всех S-колец над исследуемыми группами, которое было получено для различных групп в диссертации, работе [7] Музычука и Пономаренко и работе [14] Евдокимова, Ковача и Пономаренко. Также одним из основных инструментов доказательства отделимости является достаточное условие отделимости обобщенного сплетения S-колец над абелевыми группами, полученное в диссертации (предложение 1.6.9). Результаты о решении проблемы изоморфизма для графов Кэли над исследуемыми группами являются следствием теорем об отделимости этих групп и предложения 1.9.2 диссертации. В свою очередь, предложение 1.9.2 является прямым следствием идей, предложенных Вейсфейлером и Леманом в [1, 26] и развитых Евдокимовым и Пономаренко в [9].

Апробация работы. Результаты диссертации докладывались на Международной молодёжной школе-конференции «Алгоритмические вопросы теории групп и смежных областей» (Новосибирск, 2014, 2016), Международной школе-конференции «Coherent Configurations, Permutation Groups and Applications in Algebraic Graph Theory» (Новый Смоковец, Словакия, 2014), Международной конференции «Мальцевские чтения» (Новосибирск, 2015, 2016, 2018), Международной конференции «8th Slovenian Conference on Graph Theory» (Краньска Гора, Словения, 2015), Международной конференции «Дискретная математика, алгебра и их

приложения» (Минск, Беларусь, 2015), Международной конференции «Graphs and Groups, Spectra and Symmetries» (Новосибирск, 2016), Международной конференции «Workshop on Group Theory and Algebraic Combinatorics» (Новосибирск, 2017), Международной конференции «Groups and Graphs, Metrics and Manifolds» (Екатеринбург, 2017), XII школе-конференции по теории групп, посвященной 65-летию А.А. Махнева (Геленджик, 2018), Международной конференции «Symmetry vs. Regularity» (Пльзень, Чехия, 2018), Международной конференции «Graphs and Groups, Representations and Relations» (Новосибирск, 2018), а также обсуждались на семинарах «Теория групп» и «Алгебра и логика» Института математики СО РАН и Новосибирского государственного университета, «Algebraic combinatorics», Central China Normal University, Ухань, Китай, «Discrete mathematics», University of Primorska, Копер, Словения. Кроме того, результаты диссертации были представлены на финальном туре конкурса Мёбиуса-2018, МЦНМО, Москва.

Публикации. Результаты работы опубликованы в [30–44]. Основные результаты диссертации опубликованы в [30–33] в изданиях, входящих в перечень ВАК рецензируемых научных журналов, в которых должны быть опубликованы основные результаты диссертаций на соискание учёных степеней доктора и кандидата наук.

Структура и объем диссертации. Диссертация состоит из введения, 5 глав, заключения и списка литературы. Она изложена на 86 страницах, включает 3 таблицы. Главы диссертации подразделяются на параграфы. Основные результаты глав сформулированы в виде теорем и следствий и имеют сквозную нумерацию. Вспомогательные утверждения (леммы, предложения) имеют тройную нумерацию: номер главы, номер параграфа в главе и номер утверждения в текущем параграфе. Формулы имеют двойную нумерацию: номер главы и номер формулы внутри главы. Список литературы содержит 44 наименования. Работы автора по теме диссертации приведены отдельным списком.

Основное содержание диссертации

Во **введении** приводятся постановка и описание задачи, аргументируется актуальность темы исследования и описывается степень ее проработанности. Излагаются цели и задачи исследования, приводятся основные результаты диссертации и методы, применяемые в исследовании. Также здесь отражается теоретическая значимость и новизна полученных результатов. В конце приводятся данные об апробации и публикации полученных результатов, а также краткое содержание диссертации.

Глава 1 содержит необходимые предварительные сведения. В параграфе 1.1 данной главы перечисляются обозначения, используемые в диссертации. Параграфы 1.2-1.6 содер-

жат основные сведения об S-кольцах, схемах Кэли и группах подстановок. В параграфе 1.6 определяются кострукции тензорного произведения и обобщенного сплетения S-колец, приводятся результаты об их шуровости и отделимости. На основании идей, предложенных в [12], доказывается достаточное условие отделимости обобщенного сплетения S-колец над абелевыми группами.

Предложение 1.6.9. *Пусть $\mathcal{A}$ — U/L-сплетение над абелевой группой G. Предположим, что S-кольца $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ отделимы относительно класса всех конечных абелевых групп и $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Тогда $\mathcal{A}$ отделимо относительно класса всех конечных абелевых групп.*

Параграф 1.7 содержит результаты об S-кольцах над циклическими p-группами, полученные в [4, 6]. Кроме того, в этом параграфе доказывается, что циклические 2- и 3-группы отделимы относительно класса всех конечных абелевых групп (лемма 1.7.9). В параграфе 1.8 приведено описание S-колец над группами $C_2 \times C_{2^k}$, $k \geq 1$, полученное в [7]. Параграф 1.9 посвящен проблеме изоморфизма для графов Кэли и ее связи с проблемой отделимости для S-колец. В этом параграфе формулируется и доказывается следующее предложение, являющееся прямым следствием идей, предложенных в [1, 26] и развитых в [9].

Предложение 1.9.2. *Пусть группа G порядка n отделима относительно класса групп $\mathcal{K}$. Предположим, что G задана своей таблицей Кэли. Тогда для графа Кэли Γ над G и графа Кэли Γ' над произвольной группой из $\mathcal{K}$ изоморфизм между Γ и Γ' может быть проверен за полиномиальное время от n.*

Основным результатом **главы 2** является следующая теорема.

Теорема 1. *Группы $M_{3^k} = \langle a, b : a^{3^{k-1}} = b^3 = e, a^b = a^{3^{k-2}+1} \rangle$, где $k \geq 3$, нешуровы.*

Для доказательства теоремы 1 достаточно найти хотя бы одно нешурово S-кольцо над M_{3^k}. Пример нешурового S-кольца над M_{27} был найден с помощью компьютерных вычислений, проведенных в GAP с использованием пакета COCO2P [18]. В параграфе 2.1 описывается конструкция S-кольца над M_{3^k}, где $k \geq 4$, а в параграфе 2.2 доказывается, что это S-кольцо нешурово. Ключевым этапом доказательства является вычисление порядка группы автоморфизмов построенного S-кольца. Напрямую из теоремы 1 и теоремы Б вытекает

Следствие 1. *Если p — нечетное простое число, то шурова p-группа абелева.*

Глава 3 посвящена описанию S-колец над группой $D = C_3 \times C_{3^k}$, где $k \geq 1$. В параграфе 3.1 описывается структура базисных множеств S-колец над D. В параграфе 3.2 доказывается, что каждое нерегулярное S-кольцо с тривиальным радикалом над D либо имеет ранг 2, либо является тензорным произведением двух S-колец над циклическими группами. Параграф 3.3 посвящен доказательству того, что каждое регулярное S-кольцо с тривиальным

радикалом над D является циклотомическим, то есть определяется подходящей подгруппой группы $\mathrm{Aut}(D)$. В параграфе 3.4 показывается, что каждое S-кольцо с нетривиальным радикалом над D является обобщенным сплетением S-колец над меньшими группами. Полное описание всех S-колец над D приводится в теореме 2. В параграфе 3.5 проверяется шуровость всех S-колец из теоремы 2. Тем самым доказывается

Теорема 3. *Группы $C_3 \times C_{3^k}$, где $k \geq 1$, шуровы.*

Отметим, что наибольшую сложность представляет проверка шуровости обобщенных сплетений над D, для которой используются леммы 1.6.4 и 1.6.5, доказанные в [7].

Из следствия 1, теоремы 3 и [14, теоремы 1.1-1.3] вытекает полное описание шуровых p-групп нечетного порядка, приведенное в следующей теореме.

Теорема 4. *Конечная p-группа G, где p — нечетное простое число, шурова тогда и только тогда, когда G циклическая или $p = 3$ и G изоморфна одной из следующих групп:*

1) E_{27};

2) $C_3 \times C_{3^k}$, $k \geq 1$.

В **главе 4** исследуется отделимость S-колец над группами $C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$. Основным результатом главы 4 является

Теорема 5. *Группы $D = C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$, отделимы относительно класса всех конечных абелевых групп.*

В параграфе 4.1 доказываются вспомогательные утверждения, необходимые для доказательства теоремы 5. В частности, проверяется, что для обобщенного сплетения S-колец над D выполнены условия предложения 1.6.9. Само доказательство теоремы 5 приведено в параграфе 4.2. Оно основано на описании всех S-колец над D, приведенном в лемме 1.8.1 (доказана в [7]) для $p = 2$ и в теореме 2 для $p = 3$. 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. Вопрос об отделимости тензорных произведений и обобщенных сплетений сводится к вопросу об отделимости операндов с помощью леммы 1.6.3 и предложения 1.6.9. Наиболее трудоемкой является проверка отделимости циклотомических S-колец над D (леммы 4.2.1-4.2.4).

Из теоремы 5 и предложения 1.9.2 вытекает

Следствие 2. *Пусть группа $D \cong C_p \times C_{p^k}$ порядка n, 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 полиномиальное время от n.*

Глава 5 посвящена исследованию вопроса об отделимости S-колец над абелевыми группами порядка $4p$, где p — простое число. В параграфе 5.1 доказываются утверждения о стро-

ении S-колец над абелевыми группами порядка $4p$. Материал этого параграфа основан на результатах, полученных в [14]. Основным результатом главы 5 является

Теорема 6. *Абелева группа порядка $4p$ отделима относительно класса всех конечных абелевых групп для каждого простого числа p.*

Доказательство теоремы 6 приведено в параграфе 5.2. Основной сложностью при доказательстве теоремы 6, как и в случае теоремы 5, является проверка отделимости циклотомических S-колец (леммы 5.2.2-5.2.3). Из теоремы 6 и предложения 1.9.2 вытекает

Следствие 3. *Пусть абелева группа G порядка $n = 4p$, где p — простое число, задана своей таблицей Кэли. Тогда для графа Кэли Γ над G и графа Кэли Γ' над произвольной абелевой группой изоморфизм между Γ и Γ' может быть проверен за полиномиальное время от n.*

В **заключении** приводятся основные результаты диссертации. Изложение работы завершается **списком литературы**.

Благодарности

Автор выражает искреннюю благодарность своему научному руководителю А.В. Васильеву за поставленные задачи и всестороннюю помощь в работе. Автор глубоко признателен И. Н. Пономаренко за плодотворные дискуссии, неизменную поддержку и научное сотрудничество. Автор благодарен коллективам лаборатории теории групп ИМ СО РАН и кафедры алгебры и математической логики ММФ НГУ за сотрудничество и атмосферу, в которой выполнялась диссертационная работа.

1. Предварительные сведения

В изложении материала данной главы мы следуем работам [7, 8, 20].

§ 1.1. Обозначения

Множество нетривиальных элементов группы G обозначается через $G^{\#}$.

Порядок элемента $g \in G$ обозначается через $|g|$.

Группа правых сдвигов $\{x \mapsto xg,\ x \in G : g \in G\}$ группы G обозначается через G_{right}.

Полупрямое произведение группы G на группу K, где K действует на G автоморфизмами, обозначается через $G \rtimes K$.

Пусть $X \subseteq G$. Элемент $\sum_{x \in X} x$ группового кольца $\mathbb{Z}G$ обозначается через $\underline{X}$.

Множество $\{x^{-1} : x \in X\}$ обозначается через X^{-1}.

Подгруппа группы G, порожденная множеством $X \subseteq G$, обозначается через $\langle X \rangle$.

Если $X \subseteq G$, то положим $\mathrm{rad}(X) = \{g \in G :\ gX = Xg = X\}$.

Если $m \in \mathbb{Z}$, то множество $\{x^m : x \in X\}$ обозначается через $X^{(m)}$.

Проекции множества $X \subseteq G \times H$ на G и H обозначаются через X_G и X_H соответственно.

Если $R \subseteq \Omega \times \Omega$, то положим $R^* = \{(\beta, \alpha) : (\alpha, \beta) \in R\}$.

Симметрическая группа множества Ω обозначается через $\mathrm{Sym}(\Omega)$.

Если $K \leq \mathrm{Sym}(\Omega)$, то стабилизаторы точки $\alpha \in \Omega$ и множества $\Delta \subseteq \Omega$ в K обозначаются через K_α и K_Δ соответственно

Если группа K действует на множестве Ω, то множество всех орбит этого действия обозначается через $\mathrm{Orb}(K, \Omega)$.

Если $f : \Omega \to \Omega'$ — биекция и $\Delta \subseteq \Omega$, то сужение f на Δ обозначается через f^Δ.

Для заданных множества $X \subseteq \mathrm{Sym}(G)$ и секции $S = U/L$ группы G положим

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

где равенство $S^f = S$ означает, что f переставляет смежные классы по L в U, и f^S обозначает подстановку на множестве S, индуцированную действием f.

Если $H \leq G$, то для заданных $X, Y \in G/H$ положим $G_{X \to Y} = \{f^X : f \in G_{right}, X^f = Y\}$.

Циклическая группа порядка n обозначается через C_n.

Элементарная абелева группа порядка n обозначается через E_n.

Класс всех конечных абелевых групп обозначается через $\mathcal{K}_A$.

Функция, являющаяся полиномом от n, обозначается через $\mathrm{poly}(n)$.

§ 1.2. S-кольца и схемы Кэли

Пусть G — конечная группа, и $\mathbb{Z}G$ — целочисленное групповое кольцо. Через e будем обозначать единицу группы G. 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 $\mathcal{A}$. Будем обозначать ранг S-кольца $\mathcal{A}$ через $\mathrm{rk}(\mathcal{A})$. Если $X, Y, Z \in \mathcal{S}$, то через $c^Z_{X,Y}$ 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 $\underline{X}\ \underline{Y} = \sum_{Z \in \mathcal{S}(\mathcal{A})} c^Z_{X,Y} \underline{Z}$. Следовательно, числа $c^Z_{X,Y}$ 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 $R^* \in \mathcal{R}$;

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*, число $|\mathcal{R}|$ — *рангом* схемы Кэли. Будем обозначать ранг схемы Кэли $\mathcal{C}$ через $\mathrm{rk}(\mathcal{C})$. 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

$$c^{R(Z)}_{R(X),R(Y)} = c^Z_{X,Y} \tag{1.1}$$

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

§ 1.3. Изоморфизмы и шуровость

Пусть $\mathcal{A}$ и $\mathcal{A}'$ — S-кольца, а $\mathcal{C} = \mathcal{C}(\mathcal{A}) = (G, \mathcal{R})$ и $\mathcal{C}' = \mathcal{C}(\mathcal{A}') = (G', \mathcal{R}')$ — схемы Кэли над группами G и G', отвечающие $\mathcal{A}$ и $\mathcal{A}'$ 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 $\mathcal{C}(\mathcal{A}')$. Если существует изоморфизм из $\mathcal{A}$ в $\mathcal{A}'$, то будем говорить, что $\mathcal{A}$ и $\mathcal{A}'$ *изоморфны*, и писать $\mathcal{A} \cong \mathcal{A}'$.

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

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

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

Пусть K — подгруппа группы $\mathrm{Sym}(G)$, содержащая G_{right}. В [25] Шур доказал, что $\mathbb{Z}$-подмодуль

$$V(K, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathrm{Orb}(K_e, \ G)\},$$

является S-кольцом над G. S-кольцо $\mathcal{A}$ над G называется *шуровым*, если $\mathcal{A} = V(K, G)$ для некоторой группы K такой, что $G_{right} \leq K \leq \mathrm{Sym}(G)$. Первый пример нешурового S-кольца был построен Виландом в [27]. Заметим, что если $\mathcal{A} = \mathbb{Z}G$ или $\mathrm{rk}(\mathcal{A}) = 2$, то $\mathcal{A}$ — шурово. Действительно, в первом случае $\mathcal{A} = V(G_{right}, G)$, во втором случае $\mathcal{A} = V(\mathrm{Sym}(G), G)$.

Схема Кэли $\mathcal{C}$ называется *шуровой*, если $\mathcal{R} = \mathrm{Orb}(K, G^2)$ для некоторой группы K такой, что $G_{right} \leq K \leq \mathrm{Sym}(G)$. Заметим, что S-кольцо $\mathcal{A}$ шурово тогда и только тогда, когда соответствующая схема Кэли $\mathcal{C}$ шурова. Следующая лемма непосредственно вытекает из определений.

Лемма 1.3.1. *S-кольцо $\mathcal{A}$ (схема Кэли $\mathcal{C}$) шурово (шурова) тогда и только тогда, когда $\mathcal{S} = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A})_e, G)$ ($\mathcal{R} = \mathrm{Orb}(\mathrm{Aut}(\mathcal{C}), G^2)$).*

В [24] было предложено следующее определение. Конечная группа называется *шуровой*, если каждое S-кольцо над ней шурово.

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 говорить, что $\mathcal{A}$ и $\mathcal{A}'$ *Кэли изоморфны*, и писать $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}'$. Любой изоморфизм Кэли является изоморфизмом, но не любой изоморфизм является изоморфизмом Кэли.

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 над G. S-кольцо $\mathcal{A}$ над G называется *циклотомическим*, если $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(K, G)$ для некоторой $K \leq \mathrm{Aut}(G)$. В этом случае будем писать $\mathcal{A} = \mathrm{Cyc}(K, G)$. Каждое циклотомическое S-кольцо шурово, так как если $\mathcal{A} = \mathrm{Cyc}(K, G)$ для некоторой $K \leq \mathrm{Aut}(G)$, то $\mathcal{A} = V(G_{right} \rtimes K, G)$.

§ 1.4. Алгебраические изоморфизмы и отделимость

Алгебраическим изоморфизмом S-колец $\mathcal{A}$ и $\mathcal{A}'$ называется биекция $\varphi : \mathcal{S} \to \mathcal{S}'$ такая, что $c_{X,Y}^Z = c_{X^\varphi,Y^\varphi}^{Z^\varphi}$ 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 $c_{R,S}^T = c_{R^\varphi,S^\varphi}^{T^\varphi}$ 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 (1.1). Если существует алгебраический изоморфизм из $\mathcal{A}$ в $\mathcal{A}'$, то будем говорить, что $\mathcal{A}$ и $\mathcal{A}'$ *алгебраически изоморфны*, и писать $\mathcal{A} \cong_{\mathrm{alg}} \mathcal{A}'$.

Любой изоморфизм S-колец (схем Кэли) сохраняет структурные константы (числа пересечений). Следовательно, любой изоморфизм S-колец (схем Кэли) индуцирует алгебраический изоморфизм. Однако, не любой алгебраический изоморфизм индуцируется изоморфизмом. Соответствующие примеры могут быть найдены в [3].

Пусть $\mathcal{K}$ — класс групп. Следуя [9], будем говорить, что S-кольцо $\mathcal{A}$ *отделимо* относительно $\mathcal{K}$, если каждый алгебраический изоморфизм из $\mathcal{A}$ в S-кольцо над группой из $\mathcal{K}$ индуцируется комбинаторным изоморфизмом. Отделимое S-кольцо определяется с точностью до изоморфизма лишь тензором своих структурных констант относительно базиса, соответствующего разбиению множества G на базисные множества. Назовем конечную группу *отделимой* относительно $\mathcal{K}$, если каждое S-кольцо над этой группой отделимо относительно $\mathcal{K}$.

По аналогии с отделимыми S-кольцами можно определить отделимые схемы Кэли. Схе-

ма Кэли $\mathcal{C}$ называется *отделимой* относительно класса $\mathcal{K}$, если для каждый алгебраический изоморфизм из $\mathcal{C}$ в схему Кэли над группой из $\mathcal{K}$ индуцируется комбинаторным изоморфизмом. Ясно, что выполнено следующее утверждение.

Лемма 1.4.1. *Если $\mathcal{A}$ и $\mathcal{C}(\mathcal{A})$ — соответствующие друг другу S-кольцо и схема Кэли, то отделимость S-кольца $\mathcal{A}$ относительно класса групп $\mathcal{K}$ равносильна отделимости схемы Кэли $\mathcal{C}(\mathcal{A})$ относительно $\mathcal{K}$.*

Множество всех изоморфизмов S-колец $\mathcal{A}$ и $\mathcal{A}'$ (схем Кэли $\mathcal{C}$ и $\mathcal{C}'$), индуцирующих заданный алгебраический изоморфизм φ, обозначается через $\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$ ($\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi)$) . Из определений следует, что

$$G_{right}\,\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)G'_{right} = \mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi). \tag{1.2}$$

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

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

для любого S-кольца $\mathcal{A}'$ над группой из $\mathcal{K}$ и любого алгебраического изморфизма $\varphi : \mathcal{A} \to \mathcal{A}'$.

Для каждой группы G S-кольцо ранга 2 над G и $\mathbb{Z}G$ отделимы относительно класса всех конечных групп. В первом случае каждое базисное множество одноэлементно и, значит, каждый алгебраический изоморфизм естественным образом индуцируется изоморфизмом. Во втором случае существует единственный алгебраический изоморфизм из S-кольца ранга 2 над G в S-кольцо ранга 2 над заданной группой порядка $|G|$, который индуцируется любым изоморфизмом.

§ 1.5. 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 K — транзитивная подгруппа группы $\mathrm{Sym}(\Omega)$. Напомним, что множество $\Delta \subseteq \Omega$ называется *блоком* группы K, если для любого $g \in K$ либо $\Delta^g = \Delta$, либо $\Delta^g \cap \Delta = \varnothing$. Если $1 < |\Delta| < |\Omega|$, то блок Δ называется нетривиальным. Группа K называется *imprимитивной*, если у нее есть нетривиальные блоки, иначе она называется *примитивной*. Если K imprимитивна, то множество Ω распадается в объединение попарно непересекающихся блоков одинаковой мощности. Такое множество блоков называется *системой imprимитивности* группы K. Следующее утверждение легко следует из определений.

Лемма 1.5.1. *Пусть $\mathcal{A}$ — шурово S-кольцо над группой G. Тогда* $\mathrm{Aut}(\mathcal{A})$ *импримитивна, если и только если существует нетривиальная собственная $\mathcal{A}$-подгруппа H группы G. В этом случае правые смежные классы по подгруппе H образуют нетривиальную систему импримитивности группы* $\mathrm{Aut}(\mathcal{A})$.

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

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

где $\pi : U \to U/L$ — естественный гомоморфизм, является S-кольцом над S. Непосредственно проверяется, что если $\mathcal{A} = V(K, G)$ для некоторой $K \leq \mathrm{Sym}(G)$ такой, что $K \geq G_{right}$, то $\mathcal{A}_S = V(K^S, S)$. Из этого вытекает следующее утверждение.

Лемма 1.5.2. *Каждая секция шуровой группы шурова.*

Если X является $\mathcal{A}$-множеством, то группы $\langle X \rangle$ и $\mathrm{rad}(X)$ являютя $\mathcal{A}$-подгруппами группы G такими, что $\langle X \rangle \geq \mathrm{rad}(X)$.

Пусть $\varphi : \mathcal{A} \to \mathcal{A}'$ — алгебраический изоморфизм. Легко видеть, что φ продолжается до биекции между $\mathcal{A}$- и $\mathcal{A}'$-множествами и, следовательно, между $\mathcal{A}$- и $\mathcal{A}'$-секциями. Образы $\mathcal{A}$-множества X и $\mathcal{A}$-секции S под действием алгебраического изоморфизма 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 $S' = S^{\varphi}$. Для каждого $\mathcal{A}$-множества X верно, что

$$\langle X^{\varphi} \rangle = \langle X \rangle^{\varphi} \text{ и } \mathrm{rad}(X^{\varphi}) = \mathrm{rad}(X)^{\varphi}. \tag{1.3}$$

Соотношения (1.3) могут быть найдены в [12, с.10]. Поскольку $c_{X,Y}^{\{e\}} = \delta_{Y,X^{-1}}|X|$, где $X, Y \in \mathcal{S}(\mathcal{A})$ и $\delta_{X,X^{-1}}$ — символ Кронекера, мы заключаем, что $(X^{-1})^{\varphi} = (X^{\varphi})^{-1}$ и $|X| = |X^{\varphi}|$ для каждого $\mathcal{A}$-множества X. В частности, $|G| = |G'|$.

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.

Лемма 1.5.3. [11, лемма 2.1] *Пусть $\mathcal{A}$ и $\mathcal{A}'$ — S-кольца над группами 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 $\psi(\xi) = \xi'$.*

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 [25].

Лемма 1.5.4. [7, теорема 2.4] *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 1.5.5. [7, теорема 2.5] *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.*

Следующая лемма представляет известные свойства базисных множеств S-кольца.

Лемма 1.5.6. *Пусть $\mathcal{A}$ — S-кольцо над G. Тогда для всех $X, Y, Z \in \mathcal{S}(\mathcal{A})$ выполнены следующие утверждения:*

1) $|Z|c_{X,Y}^{Z^{-1}} = |X|c_{Y,Z}^{X^{-1}} = |Y|c_{Z,X}^{Y^{-1}}$;

2) *если $|X| = 1$ или $|Y| = 1$, то $XY \in \mathcal{S}(\mathcal{A})$.*

Лемма 1.5.7. [7, лемма 2.1] *Пусть H — $\mathcal{A}$-подгруппа G и $X \in \mathcal{S}(\mathcal{A})$. Тогда число $|X \cap Hg|$ не зависит от выбора $g \in G$ такого, что $X \cap Hg \neq \varnothing$.*

Лемма 1.5.8. [7, теорема 2.6] *Пусть X — базисное множество S-кольца $\mathcal{A}$ над группой G. Предположим, что $H \leq \mathrm{rad}(X \setminus H)$ для некоторой группы H такой, что $X \cap H \neq \varnothing$ и $X \setminus H \neq \varnothing$. Тогда $X = \langle X \rangle \setminus \mathrm{rad}(X)$, причем $\mathrm{rad}(X) \leq H \cap \langle X \rangle$.*

Группы подстановок $K_1, K_2 \leq \mathrm{Sym}(\Omega)$ называются 2-*эквивалентными*, если

$$Orb(K_1, \Omega^2) = Orb(K_2, \Omega^2).$$

Если K_1 и K_2 являются 2-эквивалентными, то будем писать $K_1 \approx_2 K_2$. Группа подстановок $K \leq \mathrm{Sym}(\Omega)$ называется 2-*изолированной*, если не существует групп подстановок, отличных от K и 2-эквивалентных K.

Лемма 1.5.9. [7, лемма 8.2] *Пусть $\mathcal{A}$ — S-кольцо над G. Предположим, что $\mathrm{Aut}(\mathcal{A})_e$ имеет точную регулярную орбиту. Тогда $\mathrm{Aut}(\mathcal{A})$ является 2-изолированной.*

Следуя [21], назовем S-кольцо $\mathcal{A}$ *квазитонким*, если $|X| \leq 2$ для любого $X \in \mathcal{S}(\mathcal{A})$. Базисное множество $X \neq \{e\}$ квазитонкого S-кольца $\mathcal{A}$ называется *ортогональю*, если существует $Y \in \mathcal{S}(\mathcal{A})$ такое, что $X \subseteq YY^{-1}$.

Лемма 1.5.10. [7, лемма 3.5] *Каждое коммутативное квазитонокое S-кольцо $\mathcal{A}$ шуково. Более того, если $\mathcal{A}$ имеет как минимум две ортогонали, то группа $\mathrm{Aut}(\mathcal{A})_e$ имеет точную регулярную орбиту.*

Лемма 1.5.11. *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 конечных групп.*

Доказательство. Квазитонкому S-кольцу $\mathcal{A}$ соответствует квазитонкая схема Кэли $\mathcal{C}(\mathcal{A})$, валентность каждого базисного отношения которой не превосходит 2. Из [21, теорема 1.1] следует, что каждая квазитонкая схема Кэли, не являющаяся схемой Клейна (см. [21, с.2]), отделима относительно класса всех конечных групп. 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 конечных групп. □

§ 1.6. Тензорное произведение и обобщенное сплетение

Если $\mathcal{A}_1$ и $\mathcal{A}_2$ — S-кольца над группами G_1 и G_2 соответственно, то разбиение

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

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

Лемма 1.6.1. [14, лемма 2.3] *Пусть $\mathcal{A}$ — S-кольцо над абелевой группой $G = G_1 \times G_2$. Предположим, что G_1 и G_2 являются $\mathcal{A}$-подгруппами. Тогда*

1) *$X_{G_i} \in \mathcal{S}(\mathcal{A})$ для всех $X \in \mathcal{S}(\mathcal{A})$ и $i \in \{1, 2\}$;*

2) *$\mathcal{A} \geq \mathcal{A}_{G_1} \otimes \mathcal{A}_{G_2}$, и равенство достигается, если $\mathcal{A}_{G_i} = \mathbb{Z}G_i$ для некоторого $i \in \{1, 2\}$.*

Лемма 1.6.2. *Тензорное произведение двух S-колец шуково тогда и только тогда, когда каждое из них шуково.*

Доказательство. Утверждение леммы непосредственно следует из [7, теорема 3.2] □

Лемма 1.6.3. *Пусть $\mathcal{K}$ — класс групп, замкнутый относительно взятия подгрупп. Тогда тензорное произведение двух S-колец отделимо относительно $\mathcal{K}$, если и только если каждое из них отделимо относительно $\mathcal{K}$.*

Доказательство. Утверждение леммы следует из [2, теорема 1.20]. См. также [8, следствие 3.2.24]. □

Пусть $\mathcal{A}$ — S-кольцо над группой G и U/L — $\mathcal{A}$-секция. Будем говорить, что $\mathcal{A}$ является *U/L-сплетением*, если $L \trianglelefteq G$ и $L \leq \mathrm{rad}(X)$ для каждого базисного множества X вне U. В случае, когда явное указание секции U/L не важно, будем говорить, что $\mathcal{A}$ является *обобщенным сплетением*. Назовем U/L-сплетение *нетривиальным* или *собственным*, если $e \neq L$ и $U \neq G$. Если $U = L$, то $\mathcal{A}$ называется *сплетением* S-колец $\mathcal{A}_L$ и $\mathcal{A}_{G/L}$ и обозначается $\mathcal{A} = \mathcal{A}_L \wr \mathcal{A}_{G/L}$.

Лемма 1.6.4. [7, теорема 10.2] *Пусть $\mathcal{A}$ — S-кольцо над абелевой группой G. Предположим, что $\mathcal{A}$ является U/L-сплетением и S-кольца $\mathcal{A}_U$, $\mathcal{A}_{G/L}$ шуровы. Тогда $\mathcal{A}$ шурово, если и только если существуют группы $\Delta_0 \geq (G/L)_{right}$ и $\Delta_1 \geq U_{right}$ такие, что $\Delta_0 \approx_2 \mathrm{Aut}(\mathcal{A}_{G/L})$, $\Delta_1 \approx_2 \mathrm{Aut}(\mathcal{A}_U)$ и $(\Delta_0)^{U/L} = (\Delta_1)^{U/L}$.*

Лемма 1.6.5. [7, следствие 10.3] *В условиях леммы 1.6.4 если группа $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной, то S-кольцо $\mathcal{A}$ шурово.*

Далее мы докажем достаточное условие отделимости обобщенного сплетения S-колец над абелевыми группами, но прежде сформулируем необходимые для доказательства утверждения. 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 1.6.6. [12, 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 1.6.7. [12, 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 1.6.8. [12, теорема 3.5] *В условиях леммы 1.6.7 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 $gf^X g' \in \mathrm{Iso}(\mathcal{A}_U, \mathcal{A}'_{U'}, \varphi_U)$.*

Предложение 1.6.9. *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 $U^{'} = U^{\varphi}, L^{'} = L^{\varphi}$. Докажем, что φ индуцируется изоморфизмом. Из леммы 1.6.7 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 1.6.6, 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 $f_0 \in \mathrm{Aut}(\mathcal{A}_{U/L})$. Ввиду того, что $\mathrm{Aut}(\mathcal{A}_{U/L}) = \mathrm{Aut}(\mathcal{A}_U)^{U/L}$, 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 1.6.8. Ясно, что $(G/U)^f = G^{'}/U^{'}$ и $(G/L)^f = G^{'}/L^{'}$ и, следовательно, f обладает свойством 1. По определению f мы имеем $g f^X g^{'} = g f_X g^{'} = h_X f_1$. Значит, из (2) следует, что для каждого $X \in G/U$ биекция $g f^X g^{'}$ 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 1.6.8.

Заметим, что приведенные рассуждения похожи на рассуждения, использовавшиеся при доказательстве отделимости S-колец смежных классов над циклическими группами ([12, с.33]). □

§ 1.7. S-кольца над циклическими p-группами

На протяжении данного параграфа A — циклическая p-группа порядка p^k, где p — простое число и $k \geq 1$, и $\mathcal{A}$ — S-кольцо над A. Пусть a — порождающий элемент группы A и $a_1 = a^{p^{k-1}}$. Положим $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(X)$, где X — базисное множество S-кольца $\mathcal{A}$, содержащее произвольный порождающий элемент группы A. Заметим, что $\mathrm{rad}(\mathcal{A})$ не зависит от выбора X. В самом деле, если $Y \in \mathcal{S}(\mathcal{A})$, $\langle Y \rangle = A$, и $Y \neq X$, то X и Y рационально сопряжены по лемме 1.5.4, и, следовательно, $\mathrm{rad}(X) = \mathrm{rad}(Y)$.

Лемма 1.7.1. *Циклические p-группы шуровы.*

Доказательство. Утверждение леммы для $p = 2$ было доказано в [15] и для $p \geq 3$ в [24]. □

Лемма 1.7.2. *Если p — нечетное простое число, то для любого $X \in \mathcal{S}(\mathcal{A})$ выполнено одно из следующих утверждений:*

1) $X \in \mathrm{Orb}(K, A)$ *для некоторой группы* $K \leq \mathrm{Aut}(A)$*;*
2) $X = \langle X \rangle \setminus \mathrm{rad}(X)$.

Доказательство. Если $X = \{e\}$, то $X \in \mathrm{Orb}(K, A)$, где K тривиальна. Пусть $X \neq \{e\}$. Группы $\langle X \rangle$ и $\mathrm{rad}(X)$ являются $\mathcal{A}$-подгруппами и $\langle X \rangle \geq \mathrm{rad}(X)$. Положим $S = \langle X \rangle / \mathrm{rad}(X)$. Заметим, что $\mathrm{rad}(\mathcal{A}_S)$ тривиален, так как $\mathrm{rad}(X)$ наибольшая подгруппа такая, что $X\,\mathrm{rad}(X) = X$. Тогда из [6, теорема 4.1, теорема 4.2] следует, что либо $\mathcal{A}_S = \mathrm{Cyc}(K', S)$ для некоторой группы $K' \leq \mathrm{Aut}(S)$, либо $\mathrm{rk}(\mathcal{A}_S) = 2$. Ясно, что $\mathrm{Aut}(A)^S = \mathrm{Aut}(S)$. Поэтому в первом случае $X \in \mathrm{Orb}(K, A)$, где K — полный прообраз группы K' при эпиморфизме $\psi : \mathrm{Aut}(A)_{\langle X \rangle} \to \mathrm{Aut}(S)$ таком, что $\psi : f \mapsto f^S$, и утверждение 1 леммы выполнено. Во втором случае X — единственное базисное множество S-кольца $\mathcal{A}_{\langle X \rangle}$, лежащее вне $\mathrm{rad}(X)$. Следовательно, утверждение 2 леммы выполнено. □

Лемма 1.7.3. *Пусть $X \in \mathrm{Orb}(K, A)$, где $K \leq \mathrm{Aut}(A)$. В этом случае $\mathrm{rad}(X) = e$ тогда и только тогда, когда Kтривиальна или $K = \langle \delta \rangle$, где $\delta : x \to x^{-1}$. Это означает, что найдется $x \in A$ такой, что $X = \{x\}$ или $X = \{x,\ x^{-1}\}$.*

Доказательство. Утверждение леммы следует из [4, лемма 5.1]. □

Лемма 1.7.4. *Пусть p — нечетное простое число, $\mathcal{A}$ — циклотомическое и S — $\mathcal{A}$-секция группы A. Предположим, что $|\mathrm{rad}(\mathcal{A})| = 1$. Тогда $|\mathrm{rad}(\mathcal{A}_S)| = 1$.*

Доказательство. Утверждение леммы непосредственно следует из [13, теорема 7.3]. □

Лемма 1.7.5. *Пусть* $\mathcal{A} = \mathbb{Z}A$ *или* $\mathcal{A} = \mathrm{Cyc}(K, A)$, *где* $K = \{\varepsilon, \sigma\}$, $\sigma : x \to x^{-1}$. *Предположим, что* $|A| \neq 4$ *и* φ — *алгебраический изоморфизм из* $\mathcal{A}$ *в* S*-кольцо* $\mathcal{A}'$ *над абелевой группой* A'. *Тогда* $A' \cong A$.

Доказательство. Из свойств алгебраического изоморфизма следует, что $|A| = |A'|$. Пусть $X \in \mathcal{S}(\mathcal{A})$ — порождающее множество группы A. Тогда X^φ в силу (1.3) является порождающим множеством группы A'. Если $|X| = 1$, то $|X^\varphi| = 1$. Поэтому A' циклическая и, следовательно, $A' \cong A$. 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 $x \in A'$, либо $X^\varphi = \{x, y\}$ для некоторых $x, y \in A'$ таких, что $|x| = |y| = 2$. В первом случае A' циклическая и, значит, изоморфна A; во втором случае $|A| = |A'| = 4$, что противоречит предположению леммы. □

Лемма 1.7.6. *Пусть* $\mathrm{rad}(\mathcal{A}) > e$. *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 A — 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. □

Лемма 1.7.7. *Пусть* $p \in \{2, 3\}$. *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 конечных групп.*

Доказательство. Из [6, теорема 4.1, 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 группы $K \leq \mathrm{Aut}(A)$. В первом случае ясно, что $\mathcal{A}$ отделимо. Во втором случае из [4, 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 1.5.10. □

Лемма 1.7.8. *Если $\mathcal{A}$ — собственное U/L-сплетение над A и $\mathrm{rad}(\mathcal{A}_U) = e$, то $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$.*

Доказательство. Для доказательства леммы достаточно доказать, что группа $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной. 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 $\mathcal{A}_{U/L}$, так как $\mathcal{A}_{U/L}$ — шурово S-кольцо по лемме 1.7.1. Поэтому $\mathrm{Aut}(\mathcal{A}_{U/L}) \approx_2 \mathrm{Aut}(\mathcal{A}_U)^{U/L}$. 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 1.7.7. 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 1.7.7, 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 лемме 1.5.9. □

В [11] было доказано, что каждое S-кольцо над циклической p-группой, где p — простое число, отделимо относительно класса всех конечных циклических групп. Далее мы докажем, что все S-кольца над циклическими 2- и 3-группами отделимы относительно $\mathcal{K}_A$.

Лемма 1.7.9. *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 1.7.7. Предположим, что $\mathrm{rad}(\mathcal{A}) > e$. Тогда из леммы 1.7.6 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 1.7.8 мы заключаем, что $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Таким образом, для $\mathcal{A}$ выполнены все условия предложения 1.6.9 и, следовательно, $\mathcal{A}$ отделимо относительно $\mathcal{K}_A$. □

§ 1.8. S-кольца над $C_2 \times C_{2^k}$

В данном параграфе мы приводим описание все S-колец над $C_2 \times C_{2^k}$, полученное в [7]. Пусть $k \geq 1$. Положим $D = A \times B$, где $A = \langle a \rangle,\ |a| = 2^k,\ B = \langle b \rangle,\ |b| = 2$. Пусть $a_1 = a^{2^{k-1}}$ и $a_2 = a^{2^{k-2}}$.

Лемма 1.8.1. *Пусть $\mathcal{A}$ — S-кольцо над D. 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* $|L| \leq 2 \leq |H|$;

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 $|U/L| = 4$, или* $\mathrm{rad}(\mathcal{A}_U) = e$ *и* $|L| = 2$;

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

группа	действие на порождающих элементах	порядок группы	k
K_0	$(a,b) \to (a,b)$	1	$k \geq 1$
K_1	$(a,b) \to (a^{-1},b)$	2	$k \geq 3$
K_2	$(a,b) \to (a_1a^{-1},b)$	2	$k \geq 3$
K_3	$(a,b) \to (a^{-1},ba_1)$	2	$k \geq 3$
K_4	$(a,b) \to (a_1a^{-1},ba_1)$	2	$k \geq 3$
K_5	$(a,b) \to (ba_2a,ba_1),\ (a,b) \to (a^{-1},b)$	4	$k \geq 4$
K_6	$(a,b) \to (ba_2a,ba_1),\ (a,b) \to (a_1a^{-1},b)$	4	$k \geq 4$
K_7	$(a,b) \to (ba^{-1},b)$	2	$k \geq 3$
K_8	$(a,b) \to (ba_1a^{-1},b)$	2	$k \geq 4$
K_9	$(a,b) \to (ba_2a,ba_1)$	2	$k \geq 3$
K_{10}	$(a,b) \to (ba_2a^{-1},ba_1)$	2	$k \geq 4$

Таблица 1.

Доказательство. Утверждения предложения представляют собой утверждения [7, теорема 6.1, теорема 7.1, теорема 9.1]. □

Лемма 1.8.2. [7, теорема 10.1] *Группы $C_2 \times C_{2^k}$, где $k \geq 1$, шуровы.*

§ 1.9. Проблема изоморфизма графов Кэли

Пусть $\Gamma = \mathrm{Cay}(G, X)$ и $\Gamma' = \mathrm{Cay}(G', X')$ — графы Кэли над группами G и G' соответственно. Обозначим множество всех изоморфизмов из Γ в 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 1.9.1. *Проблема ISO сводится к ALISO за время* $\mathrm{poly}(n)$*, где* $n = |G|$.

Доказательство. Предположим, что существует алгоритм Al_1 для решения ALISO. Считаем, что $|G'| = n$, 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 ([1, 26]) по $\mathcal{T}$ и $\mathcal{T}'$ можно построить за время $\mathrm{poly}(n)$ 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 $\mathrm{poly}(n)$, 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 $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) = \mathrm{Iso}(\Gamma, \Gamma')$. □

Предложение 1.9.2. *Пусть группа* G *порядка* n *отделима относительно класса групп* $\mathcal{K}$*. Предположим, что* G *задана своей таблицей Кэли. Тогда для графа Кэли* Γ *над* G *и графа Кэли* Γ' *над произвольной группой из* $\mathcal{K}$ *изоморфизм между* Γ *и* Γ' *может быть проверен за время* $\mathrm{poly}(n)$.

Доказательство. Пусть $\mathcal{C}$ и $\mathcal{C}'$ — схемы Кэли, построенные из Γ и Γ' соответственно с помощью алгоритма Вейсфейлера-Лемана. Из леммы 1.4.1 следует, что $\mathcal{C}$ отделима относительно класса $\mathcal{K}$. Поэтому $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) \neq \varnothing$ для любого алгебраического изоморфизма из $\mathcal{C}$ в $\mathcal{C}'$ и

проблема ALISO тривиальна для $\mathcal{C}$ и $\mathcal{C}'$. Значит, ввиду предложения 1.9.1, проблема ISO для Γ и Γ' разрешима за время $\mathrm{poly}(n)$. □

Стоит отметить, что представленный в данном параграфе материал основан на идеях, предложенных в [26] и развитых в [9, § 6.2].

2. Нешуровость групп M_{3^k}

Основным результатом данной главы является следующая теорема.

Теорема 1. Группы $M_{3^k} = \langle a, b : a^{3^{k-1}} = b^3 = e, a^b = a^{3^{k-2}+1} \rangle$, где $k \geq 3$, нешуровы.

Непосредственно из теоремы Б и теоремы 1 вытекает

Следствие 1. *Если p — нечетное простое число, то шурова p-группа абелева.*

§ 2.1. Конструкция нешурового S-кольца

Пусть $G = M_{3^k} = \langle a, b : a^{3^{k-1}} = b^3 = e, a^b = a^{3^{k-2}+1} \rangle$ и $k \geq 4$. Положим $A = \langle a \rangle$, $B = \langle b \rangle$, $c = a^{3^{k-2}}$, $C = \langle c \rangle$, и $H = C \times B$. Ясно, что $Z(G) = \langle a^3 \rangle$, $[G, G] = C$, $|C| = 3$, и $|H| = 9$. Кроме того, H нормальна в G, так как $H \geq [G, G] = C$.

Рассмотрим множества

$$Z_0 = \{e\},$$

$$Z_1 = \{b, b^2\},$$

$$Z_2 = \{c, c^2\},$$

$$Z_3 = \{cb, cb^2, c^2b, c^2b^2\} = H \setminus (Z_0 \cup Z_1 \cup Z_2).$$

$$Z_4 = a\{e, cb, c^2b^2\} \cup a^{-1}\{e, c^2b, cb^2\},$$

$$Z_5 = (Ha \cup Ha^{-1}) \setminus Z_4,$$

$$X_i = Ca^{3i} \cup Ca^{-3i},\ Y_i = (Ha^{3i} \cup Ha^{-3i}) \setminus X_i,\ i = 1, \ldots, \frac{3^{k-3} - 1}{2},$$

$$T_j = Ha^j \cup Ha^{-j},\ j = 2, 4, 5, \ldots, \frac{3^{k-2} - 1}{2},\ j \not\equiv 0 \mod 3.$$

Заметим, что множества $Z_m,\ X_i,\ Y_i,\ T_j$ образуют разбиение группы G. Обозначим это разбиение через $\mathcal{S}$. Легко видеть, что $Z_m = Z_m^{-1},\ X_i = X_i^{-1},\ Y_i = Y_i^{-1},\ T_j = T_j^{-1}$. Положим $\xi_m = \underline{Z_m},\ \theta_i = \underline{X_i},\ \psi_i = \underline{Y_i},\ \varphi_j = \underline{T_j}$.

Лемма 2.1.1. *$\mathbb{Z}$-модуль $\mathcal{A}$, натянутый на элементы $\xi_m,\ \theta_i,\ \psi_i,\ \varphi_j$, является коммутативным S-кольцом над группой G.*

Доказательство. Коммутативность S-кольца $\mathcal{A}$ следует из того, что каждое его базисное множество замкнуто относительно взятия обратного элемента. Прямые вычисления в групповом кольце группы G показывают, что

$$\xi_0\xi_m = \xi_m,\ \xi_0\theta_i = \theta_i,\ \xi_0\psi_i = \psi_i,\ \xi_0\varphi_j = \varphi_j;$$

$$\xi_1\xi_1 = 2\xi_0 + \xi_1,$$

$$\xi_1\xi_2 = \xi_2\xi_1 = \xi_3,$$

$$\xi_1\xi_3 = \xi_3\xi_1 = \xi_3 + 2\xi_2,$$

$$\xi_1\xi_4 = \xi_4\xi_1 = \xi_5,$$

$$\xi_1\xi_5 = \xi_5\xi_1 = \xi_5 + 2\xi_4,$$

$$\xi_1\theta_i = \theta_i\xi_1 = \psi_i,$$

$$\xi_1\psi_i = \psi_i\xi_1 = \psi_i + 2\theta_i,$$

$$\xi_1\varphi_j = \varphi_j\xi_1 = 2\varphi_j;$$

$$\xi_2\xi_2 = 2\xi_0 + \xi_2,$$

$$\xi_2\xi_3 = \xi_3\xi_2 = \xi_3 + 2\xi_1,$$

$$\xi_2\xi_4 = \xi_4\xi_2 = \xi_5,$$

$$\xi_2\xi_5 = \xi_5\xi_2 = 2\xi_4 + \xi_5,$$

$$\xi_2\theta_i = \theta_i\xi_2 = 2\theta_i,$$

$$\xi_2\psi_i = \psi_i\xi_2 = 2\psi_i,$$

$$\xi_2\varphi_j = \varphi_j\xi_2 = 2\varphi_j;$$

$$\xi_3\xi_3 = \xi_3 + 2\xi_1 + 2\xi_2 + 4\xi_0,$$

$$\xi_3\xi_4 = \xi_4\xi_3 = \xi_5 + 2\xi_4,$$

$$\xi_3\xi_5 = \xi_5\xi_3 = 3\xi_5 + 2\xi_4,$$

$$\xi_3\theta_i = \theta_i\xi_3 = 2\psi_i,$$

$$\xi_3\psi_i = \psi_i\xi_3 = 2\psi_i + 4\theta_i,$$

$$\xi_3\varphi_j = \varphi_j\xi_3 = 4\varphi_j;$$

$$\xi_4\xi_4 = \varphi_2 + 6\xi_0 + 3\xi_3,$$

$$\xi_4\xi_5 = \xi_5\xi_4 = 2\varphi_2 + 6\xi_1 + 6\xi_2 + 3\xi_3,$$

$$\xi_4\theta_i = \theta_i\xi_4 = \varphi_{3i+1} + \varphi_{3i-1},$$

$$\xi_4\psi_i = \psi_i\xi_4 = 2\varphi_{3i+1} + 2\varphi_{3i-1},$$

$$\xi_4\varphi_j = \varphi_j\xi_4 = 3\varphi_{j+1} + 3\theta_l + 3\psi_l,\ j-1 = 3l,$$

$$\xi_4\varphi_j = \varphi_j\xi_4 = 3\varphi_{j-1} + 3\theta_l + 3\psi_l,\ j+1 = 3l;$$

$$\xi_5\xi_5 = 4\varphi_2 + 6\xi_1 + 6\xi_2 + 9\xi_3 + 12\xi_0,$$

$$\xi_5\theta_i = \theta_i\xi_5 = 2\varphi_{3i+1} + 2\varphi_{3i-1},$$

$$\xi_5\psi_i = \psi_i\xi_5 = 4\varphi_{3i+1} + 4\varphi_{3i-1},$$

$$\xi_5\varphi_j = \varphi_j\xi_5 = 6\varphi_{j+1} + 6\theta_l + 6\psi_l,\ j-1 = 3l,$$

$$\xi_5\varphi_j = \varphi_j\xi_5 = 6\varphi_{j-1} + 6\theta_l + 6\psi_l,\ j+1 = 3l;$$

$$\theta_i\theta_l = \theta_l\theta_i = \theta_{i+l} + \theta_{i-l},\ i \neq l,$$

$$\theta_i\theta_i = 3\theta_{2i} + 6\xi_0 + 6\xi_2,$$

$$\theta_i\psi_l = \psi_l\theta_i = \psi_{i+l} + \psi_{i-l},\ i \neq l,$$

$$\theta_i\psi_i = \psi_i\theta_i = 3\psi_{2i} + 6\xi_1 + 6\xi_3,$$

$$\theta_i\varphi_j = \varphi_j\theta_i = 3\varphi_{3i+j} + 3\varphi_{3i-j};$$

$$\psi_i\psi_l = \psi_l\psi_i = 2\theta_{i+l} + 2\theta_{i-l} + \psi_{i+l} + \psi_{i-l},\ i \neq l,$$

$$\psi_i\psi_i = 3\psi_{2i} + 6\theta_{2i} + 6\xi_1 + 12\xi_2 + 6\xi_3 + 12\xi_0,$$

$$\psi_i\varphi_j = \varphi_j\psi_i = 6\varphi_{3i+j} + 6\varphi_{3i-j};$$

$$\varphi_i\varphi_j = \varphi_j\varphi_i = 9\varphi_{i+j} + 9\theta_l + 9\psi_l,\ i-j = 3l,$$

$$\varphi_i\varphi_j = \varphi_j\varphi_i = 9\varphi_{i-j} + 9\theta_l + 9\psi_l,\ i+j = 3l,$$

$$\varphi_j\varphi_j = 9\varphi_{2j} + 18\xi_0 + 18\xi_1 + 18\xi_2 + 18\xi_3.$$

Проверим, к примеру, что $\varphi_j\varphi_j = 9\varphi_{2j}+18\xi_0+18\xi_1+18\xi_2+18\xi_3$. Поскольку H нормальна в G, мы имеем $gH = Hg$ для каждого $g \in G$. Значит, $\varphi_j\varphi_j = (\underline{H}a^j + \underline{H}a^{-j})^2 = (\underline{H})^2a^{2j} + (\underline{H})^2a^{-2j} + 2(\underline{H})^2 = 9\underline{H}a^{2j} + 9\underline{H}a^{-2j} + 18\underline{H} = 9\varphi_{2j} + 18\xi_0 + 18\xi_1 + 18\xi_2 + 18\xi_3$. □

§ 2.2. Доказательство теоремы 1

Утверждение теоремы для $k = 3$ следует из компьютерных вычислений с использованием пакета COCO2P [18] (см. также [29]). Далее мы считаем, что $k \geq 4$. Пусть $\mathcal{A}$ — S-кольцо над $G = M_{3^k}$, построенное в § 2.1. Для доказательства теоремы 1 достаточно показать, что $\mathcal{A}$ нешурово. Предположим противное. Тогда из леммы 1.3.1 следует, что $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A})_e, G)$. Положим $K = \mathrm{Aut}(\mathcal{A})_e$.

Лемма 2.2.1. *Группы C, B, H являются $\mathcal{A}$-подгруппами. Правые смежные классы по подгруппам C, B, H являются блоками группы K.*

Доказательство. Заметим, что $B = Z_0 \cup Z_1,\ C = Z_0 \cup Z_2,\ H = Z_0 \cup Z_1 \cup Z_2 \cup Z_3$. Тогда $\underline{C},\ \underline{B},\ \underline{H} \in \mathcal{A}$. Поэтому C, B, H — $\mathcal{A}$-подгруппы. Поскольку $\mathrm{Aut}(\mathcal{A}) = KG_{right}$, из леммы 1.5.1 вытекает, что правые смежные классы по подгруппами C, B, H являются блоками группы K. □

Ввиду того, что H — нормальная $\mathcal{A}$-подгруппа, можно определить S-кольцо $\mathcal{A}_{G/H}$ над G/H.

Лемма 2.2.2. *Группа $\mathrm{Aut}(\mathcal{A}_{G/H})_H$ имеет порядок 2. Её нетривиальный элемент меняет местами Ha^i и Ha^{-i}.*

Доказательство. Базисные множества S-кольца $\mathcal{A}_{G/H}$ имеют вид

$$\{H\}, \left\{Ha^i, Ha^{-i}\right\}, i = 1, \ldots, \frac{3^{k-2}-1}{2}.$$

Пусть $\mathcal{C}(\mathcal{A}_{G/H})$ — схема Кэли, соответствующая $\mathcal{A}_{G/H}$. Базисное отношение схемы Кэли $\mathcal{C}(\mathcal{A}_{G/H})$, соответствующее базисному множеству $\{Ha, Ha^{-1}\}$ — цикл длины 3^{k-2}. Утверждение леммы является прямым следствием того факта, что группа автоморфизмов неориентированного цикла является диэдральной и стабилизатор точки в этой группе имеет порядок 2. □

Рассмотрим действие группы K на множестве Z_3. Элементы группы K не содержат в их циклическом строении циклов длины 3 и 4, состоящих из элементов из Z_3, потому что в силу леммы 2.2.1 правые смежные классы $Bc,\ Bc^2$ b $Cb,\ Cb^2$ — блоки группы K. Поскольку

Z_3 — орбита группы K, группа K действует на Z_3 как группа Клейна. Поскольку Z_1 и Z_2 — орбиты группы K длины 2, каждая подстановка из K может быть записана одним из следующих образов:

$$\gamma, \tag{2.1}$$

$$(b,\ b^2)(cb,\ cb^2)(c^2b,\ c^2b^2)\gamma, \tag{2.2}$$

$$(c,\ c^2)(cb,\ c^2b)(cb^2,\ c^2b^2)\gamma, \tag{2.3}$$

$$(c,\ c^2)(b,\ b^2)(cb,\ c^2b^2)(cb^2,\ c^2b)\gamma, \tag{2.4}$$

где $\gamma \in K$ действует на H тривиально.

Пусть $\mathcal{C}(\mathcal{A})$ — схема Кэли, соответствующая $\mathcal{A}$. Ниже мы выпишем все элементы, смежные с $e,\ b,\ b^2,\ c,\ c^2$ в отношении $R(Z_4)$:

$$e : a,\ cab,\ c^2ab^2,\ a^{-1},\ ca^{-1}b^2,\ c^2a^{-1}b;$$

$$b : ab,\ cab^2,\ c^2a,\ a^{-1}b,\ ca^{-1},\ c^2a^{-1}b^2;$$

$$b^2 : ab^2,\ ca,\ c^2ab,\ a^{-1}b^2,\ ca^{-1}b,\ c^2a^{-1};$$

$$c : ab^2,\ ca,\ c^2ab,\ a^{-1}b,\ ca^{-1},\ c^2a^{-1}b^2;$$

$$c^2 : ab,\ cab^2,\ c^2a,\ a^{-1}b^2,\ ca^{-1}b,\ c^2a^{-1}.$$

Обозначим множество всех элементов, смежных с $q \in G$ в $R(Z_4)$, через L_q. Пусть $\alpha \in K$ имеет вид (2.4). Тогда $b^\alpha = b^2$ и $(c^2)^\alpha = c$. Элемент ab смежен с b и c^2 в $R(Z_4)$. Значит, $(ab)^\alpha$ смежен с b^2 и c в $R(Z_4)$. Мы заключаем, что $(ab)^\alpha \in L_{b^2} \cap L_c = \{ab^2,\ ca,\ c^2ab\}$. Аналогично элемент группы K вида (2.2) переводит ab в один из элементов $ca^{-1}b,\ a^{-1}b^2,\ c^2a^{-1}$; элемент группы K вида (2.3) переводит ab в один из элементов $a^{-1}b,\ ca^{-1},\ c^2a^{-1}b^2$. Это означает, что $(ab)^\alpha \in Ha \cap (Ha)^\alpha$ для $\alpha \in K$ видов (2.1) и (2.4) и $(ab)^\alpha \in Ha^{-1} \cap (Ha)^\alpha$ для $\alpha \in K$ видов (2.2) и (2.3). Смежные классы по H являются блоками группы K и, следовательно, $Ha = (Ha)^\alpha$ для каждого $\alpha \in K$ видов (2.1) и (2.4) и $Ha^{-1} = (Ha)^\alpha$ для каждого $\alpha \in K$ видов (2.2) и (2.3). Применяя лемму 2.2.2, мы получаем, что элементы видов (2.1) и (2.4) действуют тривиально на G/H в то время, как элементы видов (2.2) и (2.3) меняют местами смежные классы Ha^i и Ha^{-i}.

Пусть $\alpha \in K$ такой, что $(a^2)^\alpha = a^2$. Элементы

$$a^3,\ a,\ a^{3^{k-2}+3}b^2,\ a^{2\cdot 3^{k-2}+3}b,\ ab^2,\ ab$$

смежны с a^2 в $R(Z_4)$. Элемент a — единственный среди них из Z_4, элемент a^3 — единственный среди них из X_1. Следовательно, $a^\alpha = a$ и $(a^3)^\alpha = a^3$.

Далее мы докажем, что $(a^i)^\alpha = a^i$ для каждого $i = 1, \dots, 3^{k-1} - 1$. Будем вести доказательство индукцией по i. Предположим, что $(a^j)^\alpha = a^j$ для всех $j \leq i$. Элементы

$$a^{i+1},\ a^{i-1},\ a^{k_1}b^{l_1},\ a^{k_2}b^{l_2},\ a^{k_3}b^{l_3},\ a^{k_4}b^{l_4},\ l_m \neq 0,\ m = 1, \dots, 4,$$

смежны с a^i в $R(Z_4)$. Они переставляются между собой под действием α, так как $(a^i)^\alpha = a^i$. Элементы

$$a^{i+1},\ a^{i+1+3^{k-2}},\ a^{i+1+2\cdot 3^{k-2}},\ a^{i-5+3^{k-2}},\ a^{i-5+2\cdot 3^{k-2}},\ a^{i-5}$$

смежны с a^{i-2} в $R(X_1)$. Они также переставляются между собой под действием α, так как $(a^{i-2})^\alpha = a^{i-2}$. Заметим, что $(a^{i+1})^\alpha \neq a^{i-1}$, потому что $(a^{i-1})^\alpha = a^{i-1}$. Таким образом,

$$\left(a^{i+1}\right)^\alpha \in M \cap N,$$

где

$$M = \{a^{i+1},\ a^{k_1}b^{l_1},\ a^{k_2}b^{l_2},\ a^{k_3}b^{l_3},\ a^{k_4}b^{l_4},\ l_m \neq 0,\ m = 1, \dots, 4\},$$

$$N = \{a^{i+1},\ a^{i+1+3^{k-2}},\ a^{i+1+2\cdot 3^{k-2}},\ a^{i-5+3^{k-2}},\ a^{i-5+2\cdot 3^{k-2}},\ a^{i-5}\}.$$

Поскольку $C \cap D = \{a^{i+1}\}$, мы получаем, что $\left(a^{i+1}\right)^\alpha = a^{i+1}$.

Элемент α может действовать нетривиально только переставляя ba^i and b^2a^i для некоторого i, потому что правые смежные классы по B являются блоками группы K. Значит, α действует тривиально на G/H. Поэтому α не видов (2.2) и (2.3). Кроме того, α не вида (2.4), так как α оставляет неподвижными элементы $c = a^{3^{k-2}}$ и $c^2 = a^{2\cdot 3^{n-2}}$. Таким образом, α имеет вид (2.1). Поэтому α действует на H тривиально. В частности, $b^\alpha = b$ и $(b^2)^\alpha = b^2$. Заметим также, что α действует тривиально на Z_4, так как все элементы из Z_4 лежат в попарно различных правых смежных классах по B, и на X_i для каждого $i \in \{1, \dots, \frac{3^{k-3}-1}{2}\}$, так как $X_i \subseteq A$.

Элемент α может действовать нетривиально на Z_5 только переставляя ba и b^2a или ba^{-1} и b^2a^{-1}, так как α оставляет неподвижным как множество каждый правый смежный класс по B. Однако, элемент ba^l, $l \in \{-1, 1\}$, смежен с ac^2a^l в $R(Z_4)$ в то время, как b^2a^l, $l \in \{-1, 1\}$, не смежен с ac^2a^l в $R(Z_4)$. Ввиду того, что $(ac^2a^l)^\alpha = ac^2a^l \in A$, мы заключаем, что α действует тривиально на Z_5. Элементы вида $a^{3l}b$ из Y_i смежны с b в $R(X_i)$ в то время, как элементы вида $a^{3l}b^2$ из Y_i не смежны с b в $R(X_i)$. Следовательно, α действует тривиально на Y_i для каждого $i \in \{1, \dots, \frac{3^{k-3}-1}{2}\}$.

Два элемента из T_j, где $j \in \{2, 4, 5, \ldots, \frac{3^{k-2}-1}{2}\}$ и $j \not\equiv 0 \mod 3$, которые могут переставляться между собой под действием α, должны быть вида ba^j и b^2a^j. Элемент ba^j смежен с ac^2a^i в $R(Z_4)$, а элемент b^2a^j не смежен. Поскольку $(ac^2a^i)^\alpha = ac^2a^i \in A$, мы заключаем, что $(ba^j)^\alpha = ba^j$ и $(b^2a^j)^\alpha = b^2a^j$. Значит, α действует тривиально T_j, где $j \in \{2, 4, 5, \ldots, \frac{3^{k-2}-1}{2}\}$ и $j \not\equiv 0 \mod 3$.

Поскольку α действует тривиально на всех базисных множествах, α — тривиальная подстановка. Следовательно, стаблизатор K_{a^2} тривиален. Тогда $|K| = |K_{a^2}| \cdot |a^2K| = |K_{a^2}| \cdot |T_2| = 18$. Мы получаем противоречие, так как длины орбит Z_5 и Y_k группы K, равные 12, не делят порядок группы K, равный 18. Таким образом, $\mathcal{A}$ — нешурово S-кольцо над G и, следовательно, G нешурова. Теорема доказана.

3. S-кольца над $C_3 \times C_{3^k}$

Данная глава посвящена изучению S-колец над группами $C_3 \times C_{3^k}$, где $k \geq 1$. Пусть $D = A \times B$, где $A = \langle a \rangle,\ |a| = 3^k,\ k \geq 1,\ B = \langle b \rangle,\ |b| = 3$. Положим $a_1 = a^{3^{k-1}}$ и $A_1 = \langle a_1 \rangle$. Описание всех S-колец над D приведено в следующей теореме.

Теорема 2. Пусть $\mathcal{A}$ — S-кольцо над D. 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 $|L| \leq 3 \leq |H|$;

2) $\mathrm{rad}(\mathcal{A}) > e$, и найдется $\mathcal{A}$-секция U/L такая, что $\mathcal{A}$ — собственное U/L-сплетение. Более того, $|U/L| \leq 3$, или $\mathrm{rad}(\mathcal{A}_U) = e$ и $|L| = 3$;

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

группа	действие на порождающих элементах	порядок группы	k
K_0	$(a,b) \to (a,b)$	1	$k \geq 1$
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	$k \geq 1$
K_5	$(a,b) \to (ba^{-1},b)$	2	$k \geq 2$
K_6	$(a,b) \to (ba,ba_1)$	3	$k \geq 2$
K_7	$(a,b) \to (ba,ba_1),\ (a,b) \to (a,b^2a_1)$	6	$k \geq 2$
K_8	$(a,b) \to (ba,ba_1^2),\ (a,b) \to (a^{-1},ba_1)$	6	$k \geq 2$
K_9	$(a,b) \to (ba,ba_1^2),\ (a,b) \to (a^{-1},b^2)$	6	$k \geq 2$
K_{10}	$(a,b) \to (b,a^{-1})$	4	$k = 1$

Таблица 2.

Теорема 2 для $k = 1$ легко проверяется компьютерным вычислением с использованием пакета COCO2P [18], а для $k \geq 2$ является прямым следствием предложений 3.2.1, 3.3.1, и 3.4.1, доказываемых в § 3.2, § 3.3, и § 3.4 соответственно. Используя теорему 2, мы доказываем следующую теорему, являющуюся основным результатом данной главы.

Теорема 3. Группы $C_3 \times C_{3^k}$, где $k \geq 1$, шуровы.

Из [14, теоремы 1.1-1.3], следствия 2 и теоремы 3 вытекает классификация шуровых p-групп нечетного порядка.

Теорема 4. Конечная p-группа G, где p — нечетное простое число, шурова тогда и только тогда, когда G циклическая или $p = 3$ и G изоморфна одной из следующих групп:

1) E_{27};

2) $C_3 \times C_{3^k}$, $k \geq 1$.

§ 3.1. Структура базисных множеств

Любое множество $X \subseteq D$ может быть единственным образом представлено в виде объединения

$$X = X_{0e} \cup bX_{1b} \cup b^2X_{2b^2},$$

где $X_{0e},\ X_{1b},\ X_{2b^2} \subseteq A$. Обозначим через E элементарную абелеву группу $A_1 \times B$. Если $T \subseteq D$ и $m \leq k$, то множество $\{t \in T : |t| \leq 3^m\}$ обозначается через T_m. В этих обозначениях $D = D_k$, $A = A_k$, $E = D_1$. Пусть $\mathcal{A}$ — S-кольцо над D. Если $x \in D$, то через T_x обозначим базисное множество S-кольца $\mathcal{A}$, содержащее x.

Лемма 3.1.1. *Пусть $k \geq 2$ и $\mathcal{A}$ — S-кольцо над группой G, где $G \in \{A, D\}$. Предположим, что не существует нетривиальных собственных $\mathcal{A}$-подгрупп группы G. Тогда* $\mathrm{rk}(\mathcal{A}) = 2$.

Доказательство. Утверждение леммы напрямую следует из [27, теорема 25.3, теорема 25.5]. □

Лемма 3.1.2. *Пусть T — базисное множество S-кольца $\mathcal{A}$ над D, содержащее элементы x и y такие, что $|x| > |y| \geq 3$. Тогда $xA_1 \subseteq T$*

Доказательство. Положим $m = 1 + \frac{|x|}{3},\ l = 1 + \frac{2|x|}{3}$. Тогда $y^m = y^l = y$. По лемме 1.5.4 множества $T^{(m)},\ T^{(l)}$ являются базисными. Поскольку $y \in T^{(m)} \cap T^{(l)} \cap T$, мы заключаем, что $T^{(m)} = T^{(l)} = T$. Значит, $\{x^m,\ x^l\} = \{xx^{\frac{|x|}{3}},\ xx^{\frac{2|x|}{3}}\} = \{xa_1,\ xa_1^2\} \subseteq T$. □

Лемма 3.1.3. *Пусть T — базисное множество S-кольца $\mathcal{A}$ над D и $3^m = \min\limits_{t \in T} |t|$. Предположим, что* $\mathrm{rad}(T) = e$. *Тогда существуют множества*

$$X, Y, Y_1, Z, Z_1 \subseteq A$$

такие, что

$$T_m = X \cup bY \cup b^2Y_1 \cup bZ \cup b^2Z_1,\ Y \cap Y_1 = Z \cap Z_1 = \varnothing,$$

и выполнено одно из следующих утверждений:

1) *каждое непустое множество* $U \in \{X, Y \cup Y_1, Z \cup Z_1\}$ *одноэлементно;*

2) *каждое непустое множество* $U \in \{X, Y \cup Y_1, Z \cup Z_1\}$ *имеет вид* $\{u, u^{-1}\},\ u \in A$.

Доказательство. Представим T_m как объединение $T_m = T_{0e,m} \cup bT_{1b,m} \cup b^2T_{2b^2,m}$, где $T_{0e,m}$, $T_{1b,m}$, $T_{2b^2,m}$ — подмножества множества A. Положим $K = \{\sigma_m : m \not\equiv 0 \mod 3\}$, где $\sigma_m : x \to x^m$, и $M = K_T$. Если $x \in T_{0e,m}$ и $\alpha \in M$, то $x^\alpha \in T_{0e,m}$. Значит, $T_{0e,m}$ является объединением некоторого множества орбит группы M. Предположим, что $T_{0e,m} \neq \varnothing$. Поскольку все элементы в $T_{0e,m}$ имеют одинаковый порядок, $T_{0e,m}$ является орбитой группы M.

Если $x \in bT_{1b,m} \cup b^2T_{2b^2,m}$ и $\alpha \in M$, то $x^\alpha \in bT_{1b,m} \cup b^2T_{2b^2,m}$. Следовательно, $bT_{1b,m} \cup b^2T_{2b^2,m}$ является объединением некоторого множества орбит группы M. Более того, легко проверить, что $bT_{1b,m} \cup b^2T_{2b^2,m}$ явялется объединением не более, чем двух орбит группы M. Таким образом, T_m может быть представлено в виде

$$T_m = X \cup bY \cup b^2Y_1 \cup bZ \cup b^2Z_1,$$

где каждое множество $X,\ Y \cup Y_1,\ Z \cup Z_1$ пусто или является орбитой группы M.

Хотя бы одно из множеств $X,\ Y \cup Y_1,\ Z \cup Z_1$ имеет тривиальный радикал, потому что иначе $a_1 \in \mathrm{rad}(T_m)$ и, следовательно, $a_1 \in \mathrm{rad}(T)$ по лемме 3.1.2. Без ограничения общности можно считать, что $X \neq \varnothing$ и $\mathrm{rad}(X) = e$. Тогда из леммы 1.7.3 следует, что M тривиальна или $M = \langle\delta\rangle$, где $\delta : x \to x^{-1}$, и мы получаем требуемое. □

Множество $X \subset D$ называется *старшим* (в D), если оно содержит элемент порядка 3^k. Если $\mathcal{A}$ — S-кольцо над D, то $\mathrm{rad}(\mathcal{A})$ — это группа, порожденная группами $\mathrm{rad}(X)$, где X пробегает все старшие базисные множества S-кольца $\mathcal{A}$. Ясно, что $\mathrm{rad}(\mathcal{A}) = e$ тогда и только тогда, когда каждое старшее базисное множество S-кольца $\mathcal{A}$ имеет тривиальный радикал. Множество $X \subset D$ называется *регулярным*, если оно состоит из элементов одного и того же порядка. Если каждое базисное множество S-кольца $\mathcal{A}$ над D регулярно, то $\mathcal{A}$ называется *регулярным*. Множество $X \subset D$ называется *рациональным*, если $X = \bigcup\limits_m X^{(m)}$, где m пробегает все целые числа, не кратные 3. Если каждое базисное множество S-кольца $\mathcal{A}$ над D рационально, то $\mathcal{A}$ называется *рациональным*.

Далее до конца параграфа $\mathcal{A}$ — S-кольцо над D и $T_x \in \mathcal{S}(\mathcal{A})$ — базисное множество, содержащее элемент $x \in D$.

Лемма 3.1.4. *Пусть* T_{a_1} *нерегулярно. Тогда* T_{a_1} *рационально.*

Доказательство. Предположим противное. Пусть $T_{a_1} \cap E = Y$, $|T_{a_1}| = l$, и $r = |Y| - |a_1Y \cap Y|$. Заметим, что $r \geq 1$, так как $a_1 \in Y$ и $a_1 \notin a_1Y$. Поскольку T_{a_1} нерационально, $|Y| \leq 4$ и если

$|Y| = 4$, то $|a_1 Y \cap Y| \geq 1$. Поэтому $r \leq 3$. Из леммы 3.1.2 следует, что $A_1 \leq \mathrm{rad}(T_{a_1}) \setminus Y$. Следовательно,

$$c_{T_{a_1} T_{a_1}^{-1}}^{T_{a_1}} = |a_1 T_{a_1} \cap T_{a_1}| = l - r.$$

Таким образом, каждый элемент из $T_{a_1} \cup T_{a_1}^{-1}$ входит в элемент $\underline{T_{a_1}}\ \underline{T_{a_1}}^{-1}$ с коэффициентом $l-r$. Так как e входит в $\underline{T_{a_1}}\ \underline{T_{a_1}}^{-1}$ с коэффициентом l, мы получаем, что как минимум $2l^2 - 2lr + l$ элементов входят в $\underline{T_{a_1}}\ \underline{T_{a_1}}^{-1}$. С другой стороны, в точности l^2 элементов входят в этот элемент. Следовательно, чтобы получить противоречие, достаточно доказать неравенство $2l^2 - 2lr + l > l^2$, которое в свою очередь эквивалентно неравенству $l > 2r - 1$. Последнее неравенство выполнено для $r = 1$, потому что T_{a_1} нерегулярно; если $r = 2$, то $l > 4$ по лемме 3.1.2; если $r = 3$, то $l > 5$ по лемме 3.1.2. □

Лемма 3.1.5. *Выполнено ровно одно из следующих утверждений:*

1) *T_{a_1} рационально, нерегулярно, и $T_{a_1} \cup L$ является $\mathcal{A}$-подгруппой для некоторой $\mathcal{A}$-подгруппы $L \leq E$ такой, что $L \cap A_1 = \{e\}$;*

2) *T_{a_1} регулярно. В этом случае A_1 или E является $\mathcal{A}$-подгруппой.*

Доказательство. Если T_{a_1} нерационально, то T_{a_1} регулярно по лемме 3.1.4. В этом случае $A_1 = \langle T_{a_1} \rangle$ или $E = \langle T_{a_1} \rangle$ и утверждение 2 леммы выполнено. Если T_{a_1} регулярно и рационально, то, очевидно, утверждение 2 леммы тоже выполнено. Предположим, что T_{a_1} рационально и нерегулярно. Тогда из леммы 3.1.2 следует, что $A_1 \leq \mathrm{rad}(T_{a_1} \setminus E)$. В силу рациональности множества T_{a_1}, множество $T_{a_1} \cap E$ является объединением 1, 2, 3 или 4 подгрупп порядка 3 без $\{e\}$. Таким образом, имеется четыре возможности для $T_{a_1} \cap E$:

1) $T_{a_1} \cap E = \{a_1, a_1^2\}$;

2) $T_{a_1} \cap E = \{a_1, a_1^2, q, q^2\}$, где $|q| = 3$;

3) $T_{a_1} \cap E = \{a_1, a_1^2, q, q^2, f, f^2\}$, где $|q| = |f| = 3$;

4) $T_{a_1} \cap E = \{a_1, a_1^2, b, b^2, ba_1, b^2a_1, ba_1^2, b^2a_1^2\} = E \setminus \{e\}$.

Если $T_{a_1} = \langle T_{a_1} \rangle \setminus \mathrm{rad}(T_{a_1})$ и $|\mathrm{rad}(T_{a_1})| \in \{1, 3\}$, то утверждение 1 леммы выполнено для $L = \mathrm{rad}(T_{a_1})$. Покажем, что во всех случаях

$$T_{a_1} = \langle T_{a_1} \rangle \setminus \mathrm{rad}(T_{a_1}) \text{ и } |\mathrm{rad}(T_{a_1})| \in \{1, 3\}.$$

Заметим, что $T_{a_1} \cap A_1 \neq \varnothing$ и $T_{a_1} \setminus A_1 \neq \varnothing$. В первом и четвертом случаях лемма 3.1.2 влечет, что $A_1 \leq \mathrm{rad}(T \setminus A_1)$. Из леммы 1.5.8 для $H = A_1$ следует, что $T_{a_1} = \langle T_{a_1} \rangle \setminus \mathrm{rad}(T_{a_1})$. В первом случае $\mathrm{rad}(T_{a_1})$ не содержит a_1. Если $\mathrm{rad}(T_{a_1})$ содержит элемент x порядка $m > 3$, то $x^{\frac{m}{3}} = a_1 \in \mathrm{rad}(T_{a_1})$ или $x^{\frac{2m}{3}} = a_1 \in \mathrm{rad}(T_{a_1})$. Следовательно, $\mathrm{rad}(T_{a_1}) = e$ или $|\mathrm{rad}(T_{a_1})| = 3$.

В четвертом случае $\mathrm{rad}(T_{a_1}) = e$. Во втором случае

$$|a_1T_{a_1} \cap T_{a_1}| = |T_{a_1}| - 3 = c_{T_{a_1}T_{a_1}}^{T_{a_1}} = |qT_{a_1} \cap T_{a_1}|. \tag{3.1}$$

Заметим, что $q\{a_1, a_1^2, q, q^2\} \cap T_{a_1} = \{q^2\}$. Поэтому $|q(T_{a_1} \setminus E) \cap T_{a_1}| = |T_{a_1}| - 4 = |T_{a_1} \setminus E|$, и мы получаем, что $q, q^2 \in \mathrm{rad}(T_{a_1} \setminus E)$. Кроме того, $a_1, a_1^2 \in \mathrm{rad}(T_{a_1} \setminus E)$ по лемме 3.1.2 и $T_{a_1} \cap E \neq \varnothing,\ T_{a_1} \setminus E \neq \varnothing$. Таким образом, из леммы 1.5.8 для $H = E$ следует, что $T_{a_1} = \langle T_{a_1} \rangle \setminus \mathrm{rad}(T_{a_1})$. Поскольку $\mathrm{rad}(T_{a_1})$ не содержит a_1, группа $\mathrm{rad}(T_{a_1})$ тривиальна или имеет порядок 3. В третьем случае $|q\{a_1, a_1^2, q, q^2, f, f^2\} \cap T_{a_1}| = 3$, потому что $\{f, f^2\} = \{qa_1, q^2a_1^2\}$ или $\{f, f^2\} = \{q^2a_1, qa_1^2\}$, и (3.1) выполнено. Значит, $|q(T_{a_1} \setminus E) \cap T_{a_1}| = |T_{a_1}| - 6 = |T_{a_1} \setminus E|$ и $q,\ q^2 \in \mathrm{rad}(T_{a_1} \setminus E)$. Из леммы 1.5.8 для $H = E$ следует, что $T_{a_1} = \langle T_{a_1} \rangle \setminus \mathrm{rad}(T_{a_1})$. Так как $\mathrm{rad}(T_{a_1})$ не содержит a_1, $\mathrm{rad}(T_{a_1})$ тривиален или имеет порядок 3. □

Лемма 3.1.6. *Пусть множество T_{a_1} рационально и нерегулярно. Обозначим множество всех базисных множеств, содержащих элемент порядка 3, через I. Тогда выполнено ровно одно из следующих утверждений:*

1) $I = \{T_{a_1}, \{q, q^2\}, \{q, q^2\}T_{a_1}\}$, *где* $q \in E \setminus A_1$ *и* $T_{a_1} \cup \{e\}$ — *циклическая $\mathcal{A}$-подгруппа;*
2) $I = \{T_{a_1}, \{q, q^2\}\}$, *где* $q \in E \setminus A_1$ *и* $T_{a_1} \cup \{e, q, q^2\}$ — *$\mathcal{A}$-подгруппа;*
3) $I = \{T_{a_1}\}$ *;*
4) $I = \{T_{a_1}, \{q\}, \{q^2\}, qT_{a_1}, q^2T_{a_1}\}$, *где* $q \in E \setminus A_1$ *и* $T_{a_1} \cup \{e\}$ — *циклическая $\mathcal{A}$-подгруппа;*
5) $A_1 \leq \mathrm{rad}(T)$ *для любого* $T \in I \setminus \{T_{a_1}\}$.

Прежде, чем доказать лемму 3.1.6, докажем вспомогательное утверждение.

Лемма 3.1.7. *Предположим, что в условиях леммы 3.1.6 все базисные множества, лежащие в $I \setminus \{T_{a_1}\}$, рациональные с тривиальным радикалом. Тогда выполнено одно из утверждений $1 - 3$ леммы 3.1.6.*

Доказательство. Утверждение 2 леммы 3.1.6, очевидно, выполнено, если $T_{a_1} \cup \{e, q, q^2\} \leq D$, где $q, q^2 \in E \setminus A_1$. По лемме 3.1.5 мы можем считать, что $U = T_{a_1} \cup \{e\} \leq D$. Утверждение 3 леммы выполнено, если U — нециклическая группа. Далее без ограничения общности мы считаем, что U — циклическая группа и $U \leq A$.

Если $X \in I \setminus \{T_{a_1}\}$, то $|X \cap E| \in \{2, 4, 6\}$, так как X рационально по условию. Если $|X \cap E| = 6$, то $A_1 \leq \mathrm{rad}(X)$, что противоречит предположению леммы. Значит, $I \setminus \{T_{a_1}\} = \{X, Y, Z\}$, где $|X \cap E| = |Y \cap E| = |Z \cap E| = 2$, или $I \setminus \{T_{a_1}\} = \{X, Y\}$, где $|X \cap E| = 2$, $|Y \cap E| = 4$. В обоих случаях существует $X \in I \setminus \{T_{a_1}\}$ такое, что $X \cap E = \{q, q^2\}$. Заметим,

что $|a_1X \cap X| = |X| - 2$. Это очевидно, если X регулярно и следует из леммы 3.1.2 иначе. Поэтому утверждение 1 леммы 1.5.6 влечет

$$(|X| - 2)|T_{a_1}| = c_{XX}^{T_{a_1}}|T_{a_1}| = c_{T_{a_1}X}^{X}|X|. \tag{3.2}$$

Поскольку $(|X|, |X| - 2) \leq 2$, мы заключаем, что $|X| = 2$ или $|T_{a_1}| = \frac{l}{2}|X|$, где $l \geq 1$— целое число. Более того, $l \neq 1$, потому что $|T_{a_1}| \equiv |X| \equiv 2 \mod 3$. Каждый элемент из T_{a_1} входит в элемент $\underline{X}^2$ с коэффициентом $|X| - 2$, потому что $|a_1X \cap X| = |X| - 2$; каждый элемент из X входит в $\underline{X}^2$, потому что $|qX \cap X| \geq 1$; элемент e входит в $\underline{X}^2$ с коэффициентом $|X|$, потому что $X = X^{-1}$. Таким образом, если $|X| > 2$ и $|T_{a_1}| \geq \frac{3}{2}|X|$, то как минимум $\frac{3}{2}|X|^2 - |X|$ элементов входят в элемент $\underline{X}^2$. Однако, в точности $|X|^2$ элементов входят в $\underline{X}^2$ и если $|X| > 2$, то $|X|^2 < \frac{3}{2}|X|^2 - |X|$, противоречие. Следовательно, $|X| = 2$ или $|T_{a_1}| = |X|$, и

$$\underline{X}^2 = |X|e + (|X| - 2)\underline{T_{a_1}} + \underline{X}. \tag{3.3}$$

Если для $Y \in I \setminus \{T_{a_1}\}$ выполнено $Y \cap E = \{q, q^2, f, f^2\}$, то $|a_1Y \cap Y| = |Y| - 2$. Поэтому лемма 1.5.6 влечет, что (3.2) верно для Y. Значит, $|T_{a_1}| = \frac{l}{2}|Y|$, где $l \geq 1$ — целое число. Заметим, что $l < 3$, так как иначе не меньше $\frac{3}{2}|Y|^2 - |Y|$ элементов входят в элемент $\underline{Y}^2$, что невозможно. Более того, $l \neq 2$, потому что $|T_{a_1}| \equiv 2 \mod 3$, $|Y| \equiv 1 \mod 3$. Таким образом, $|Y| = 2|T_{a_1}|$.

Пусть $3^m = \max\limits_{t \in T_{a_1}} |t|$ и $D_m = \{g \in D : |g| \leq 3^m\}$. Предположим, что X содержит l элементов $x_1, \ldots, x_l$ порядка больше, чем 3^m. Тогда как минимум $2l$ элементов $qx_1, \ldots, qx_l$, $q^2x_1, \ldots, q^2x_l$ порядка больше, чем 3^m, входят в элемент $\underline{X}\ \underline{X}$. С другой стороны, в соответствии с (3.3), в точности l элементов $x_1, \ldots, x_l$ порядка больше, чем 3^m, входят в элемент $\underline{X}\ \underline{X}$, противоречие. Следовательно, X не содержит элементов порядка больше, чем 3^m, и

$$T_{a_1} \cup X \cup T_{a_1}X = D_m \setminus \{e\}. \tag{3.4}$$

Предположим, что $I \setminus \{T_{a_1}\} = \{X, Y, Z\}$, где $|X \cap E| = |Y \cap E| = |Z \cap E| = 2$ и $|X| > 2$, $|Y| > 2$, $|Z| > 2$. Тогда $|X| = |Y| = |Z| = |T_{a_1}| = j$. Поэтому $|a_1X \cap X| = |qX \cap T_{a_1}| = j - 2$ и $\underline{T_{a_1}}\ \underline{X} = (j-2)\underline{X} + \underline{Y} + \underline{Z}$. В соответствии с (3.4), мы имеем $D_m \setminus \{e\} = T_{a_1} \cup X \cup Y \cup Z$. Однако, $3j + 2 = |D_m \setminus \{e\}| = |T_{a_1}| + |X| + |Y| + |Z| = 4j$. Поскольку $j > 2$, мы получаем противоречие. Таким образом, в этом случае хотя бы одно из множеств X, Y, Z имеет мощность 2.

Предположим, что $I \setminus \{T_{a_1}\} = \{X, Y\}$, где $|X \cap E| = 2$, $|Y \cap E| = 4$ и $|X| > 2$. Тогда $|X| = |T_{a_1}| = j$, $|Y| = 2|T_{a_1}| = 2j$, и $\underline{T_{a_1}}\ \underline{X} = (j-2)\underline{X} + \underline{Y}$. Снова, из (3.4) следует, что $D_m \setminus \{e\} = T_{a_1} \cup X \cup Y \cup Z$, и мы получаем противоречие. Следовательно, в любом случае существует базисное множество $X \in I \setminus \{T_{a_1}\}$, имеющее вид $\{q, q^2\}$, $q \in E$.

Покажем, что $\{q, q^2\}T_{a_1}$ является базисным множеством. Если элементы

$$qa_1, q^2a_1^2, q^2a_1, qa_1^2$$

лежат в одном базисном множестве Y, то $|Y| = 2|T_{a_1}|$ и $Y = \{q, q^2\}T_{a_1}$. Иначе имеется два базисных множества

$$Y = qF \cup q^2(T_{a_1} \setminus F),\ Z = q(T_{a_1} \setminus F) \cup q^2F,$$

где $F \subseteq T_{a_1},\ T_{a_1} \setminus F = F^{-1}$. Тогда лемма 3.1.2 влечет, что

$$a_1 \in \mathrm{rad}(F \setminus A_1) \cap \mathrm{rad}(F^{-1} \setminus A_1).$$

Предположим, что $yz = a_1,\ y, z \in F$ и $|y| = |z| > 3$. Тогда $z = a_1y^{-1} \in F^{-1}$ по лемме 3.1.2, противоречие. Таким образом, элемент a_1 входит в элемент $\underline{Y}\ \underline{Z} = (q+q^2)\underline{F}\ \underline{F}^{-1} + \underline{F}^2 + (\underline{F}^{-1})^2$ с коэффициентом 1 (только как произведение элементов порядка 3). С другой стороны, существует элемент из T_{a_1}, входящий в элемент $\underline{Y}\ \underline{Z}$ с коэффициентом не меньше, чем 2, противоречие. Следовательно, $X = \{q, q^2\}T_{a_1}$ — базисное множество $\mathcal{A}$ и утверждение 1 леммы 3.1.6 выполнено. □

Доказательство леммы 3.1.6. Если $\mathrm{rad}(T) > e$ для некоторого $T \in I \setminus \{T_{a_1}\}$, то $A_1 \leq \mathrm{rad}(T)$ для любого $T \in I \setminus \{T_{a_1}\}$ и утверждение 5 леммы выполнено. Поэтому в соответствии с леммой 3.1.7 мы можем считать, что существует нерациональное $T \in I \setminus \{T_{a_1}\}$ такое, что $\mathrm{rad}(T) = e$. Тогда T содержит один, два или три элемента порядка 3. Предположим, что T содержит в точности один элемент q порядка 3. В этом случае $c_{TT^{-1}}^{T_{a_1}} = |a_1T \cap T| = |T| - 1$. Это очевидно, если T регулярно и следует из леммы 3.1.2 иначе. Из утверждения 1 леммы 1.5.6 вытекает, что

$$|T_{a_1}|(|T| - 1) = c_{TT^{-1}}^{T_{a_1}}|T_{a_1}| = c_{T_{a_1}T}^{T}|T|.$$

Значит, $|T|$ делит $(|T|-1)|T_{a_1}|$. Если $|T_{a_1}| = l|T|$, где $l > 1$, то как минимум $|T| + l|T|(|T|-2) > |T|^2$ элементов входят в элемент $\underline{T}\ \underline{T}^{-1}$, противоречие. Следовательно, $|T| = 1$ или $|T_{a_1}| = |T|$. В первом случае $T = \{q\}$ и выполнено утверждение 4 леммы.

Во втором случае $|T_{a_1}| = |T| \equiv 1 \mod 3$ по лемме 3.1.2. Из этого следует, что T_{a_1} содержит четыре элемента $a_1,\ a_1^2,\ qa_1\ , q^2a_1^2$ порядка 3. Предположим, что $a_1 = tx,\ t \in T_{a_1},\ x \in T$. Если $|t| > |x| \geq 3$, то $|tx| = |t| > 3$. Это же верно, если $|x| > |t| \geq 3$. Значит, $|x| = |t|$. Если $|t| > 3$, то $x = a_1t^{-1} \in T_{a_1}$ по лемме 3.1.2. Таким образом, $|x| = |t| = 3$. Тогда a_1^2 входит в элемент $\underline{T}\ \underline{T_{a_1}}$, в то время, как a_1 не входит, противоречие с рациональностью T_{a_1}.

Предположим, что T содержит ровно три элемента порядка 3. Мы рассмотрим случай, когда $b, ba_1, b^2a_1 \in T,\ b^2,\ b^2a_1^2,\ ba_1^2 \in T^{-1}$. В остальных случаях таких, что $|T \cap E| = 3$

рассуждения аналогичны. Заметим, что $|a_1T \cap T| = |T| - 2$ и $(|T| - 2)|T_{a_1}|$ делится на $|T|$. Лемма 3.1.2 влечет, что $|T|$ делится на 3. Однако, $(|T| - 2)|T_{a_1}|$ не делится на 3, потому что T_{a_1} содержит два элемента порядка 3, противоречие.

Предположим, что T содержит ровно два элемента порядка 3.

Случай 1. Пусть $b,\ b^2a_1^2 \in T,\ b^2,\ ba_1 \in T^{-1}$. Обозначим базисное множество, содержащее ba_1^2 через X. Заметим, что a_1 и a_1^2 появляются в $\underline{X}\ \underline{T}$ только как произведение двух элементов порядка 3, так как иначе $X \cap T^{-1} \neq \varnothing$ по лемме 3.1.2. Поэтому a_1 входит в элемент $\underline{X}\ \underline{T}$, в то время как a_1^2 не входит, противоречие с тем, что $T_{a_1} = T_{a_1^2}$.

Случай 2. Пусть $b,\ ba_1 \in T,\ b^2,\ b^2a_1^2 \in T^{-1}$. Тогда $b^2a_1 \in X$, так как иначе X содержит ровно один элемент порядка 3. Следовательно, $|X| = 1$ и утверждение 4 леммы выполнено. Элемент ba_1^2 входит в элемент $\underline{T_{a_1}}\ \underline{T}$ как произведение b и a_1^2. Поскольку $sc_1^2, s^2c_1 \in X$, элемент s^2c_1 также входит в $\underline{T_{c_1}}\ \underline{T}$. Поэтому существуют элементы $r \in T_{a_1}$ и $t \in T$ такие, что $|r| > 3$, $|t| > 3$, и $rt = a_1b^2$. Из леммы 3.1.2 следует, что $r^{-1}a_1 \in T_{a_1}$. Лемма 3.1.5 влечет, что $T_{a_1} \cup \{e\} \leq D$ или $T_{a_1} \cup \{e, q, q^2\} \leq D,\ |q| = 3$. Последний случай невозможен, потому что тогда $T_{a_1} = T$. Значит, $U = T_{a_1} \cup \{e\}$ — $\mathcal{A}$-подгруппа. С одной стороны, $|bU \cap T| \equiv 1 \mod 3$ и $|b^2U \cap T| \equiv 0 \mod 3$. Значит, из леммы 1.5.7 вытекает, что $b^2U \cap T = \varnothing$. С другой стороны, $t = r^{-1}a_1b^2 \in b^2U \cap T$, противоречие.

Остальные случаи, в которых $|T \cap E| = 2$, аналогичны случаю 1 или случаю 2. Таким образом, T не может содержать в точности два элемента порядка 3. □

Лемма 3.1.8. *Пусть* $3^m = \max\limits_{t \in T_{a_1}} |t|$, $D_m = \{g \in D : |g| \leq 3^m\}$, T_{a_1} *нерегулярно и рационально, и* R *— объединение всех базисных множеств, содержащих элемент порядка 3. Тогда* $(D_m \setminus \{e\}) \subseteq R$. *Более того, если* $\mathrm{rad}(T) = e$ *для любого* $T \in I \setminus \{T_{a_1}\}$, *то* $R = D_m \setminus \{e\}$.

Доказательство. Утверждение следствия, очевидно, следует из утверждений $1 - 4$ леммы 3.1.6. Предположим, что выполнено утверждение 5 леммы 3.1.6. Тогда $U = T_{a_1} \cup \{e\}$ — циклическая группа. Пусть $T \in I \setminus \{T_{a_1}\}$ и $q \in T \cap E$. Поскольку $\mathrm{rad}(T)$ является $\mathcal{A}$-подгруппой, мы заключаем, что $T_{a_1} = U \setminus \{e\} \subseteq \mathrm{rad}(T)$. Таким образом $qU \subseteq T$, $q^2U \subseteq T^{-1}$, и $R = T_{a_1} \cup T \cup T^{-1} \supseteq T_{a_1} \cup bU \cup b^2U = D_m \setminus \{e\}$. □

§ 3.2. Нерегулярные S-кольца с тривиальным радикалом

Основной результат данного параграфа может быть сформулирован следующим образом.

Предложение 3.2.1. *Пусть $\mathcal{A}$ — S-кольцо над D. Предположим, что* $\mathrm{rad}(\mathcal{A}) = e$. *Тогда выполнено одно из следующих утверждений:*

1) *$\mathcal{A}$ регулярно;*

2) *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 $|L| \leq 3 \leq |H|$.*

Доказательство предложения 3.2.1 будет дано в конце параграфа.

Лемма 3.2.2. *Пусть T — нерегулярное базисное множество S-кольца $\mathcal{A}$ над D. Предположим, что A_1 является $\mathcal{A}$-подгруппой. Тогда* $A_1 \leq \mathrm{rad}(T)$.

Доказательство. Пусть $3^m = \min\limits_{t \in T} |t|$. Из леммы 3.1.2 следует, что $A_1 \leq \mathrm{rad}(T \setminus T_m)$. Предположим, что существует $t \in T_m$ такое, что $ta_1 \notin T$. Тогда $X = T_{ta_1}$ отлично от T. Пусть $\pi : D \to D/A_1$ — естественный гомоморфизм. Множества $\pi(T)$ и $\pi(X)$ являются базисными множествами S-кольца $\mathcal{A}_{D/A_1}$ и $\pi(t) \in \pi(T) \cap \pi(X)$. Поэтому $\pi(T) = \pi(X)$. Значит, найдется $y \in T \setminus T_m$ такой, что $ya_1 \in X$ или $ya_1^2 \in X$. Однако, $ya_1,\ ya_1^2 \in T$ по лемме 3.1.2, противоречие. Таким образом, $ta_1 \in T$ для любого $t \in T_m$ и $A_1 \leq \mathrm{rad}(T)$. □

Лемма 3.2.3. *Пусть T — нерегулярное базисное множество S-кольца $\mathcal{A}$ над D. Предположим, что T не содержит элементов порядка 3. Тогда* $\mathrm{rad}(T) > e$.

Доказательство. Предположим противное. Пусть $3^m = \min\limits_{t \in T} |t|$. Тогда $m > 1$, $a_1 \notin \mathrm{rad}(T_m)$, $T_m \neq \varnothing$, и $T \setminus T_m \neq \varnothing$. Из леммы 3.1.3 следует, что $|T_m| \leq 6$. По лемме 3.2.2 группа A_1 не является $\mathcal{A}$-подгруппой. Лемма 3.1.5 влечет, что T_{a_1} рационально и нерегулярно или E — $\mathcal{A}$-подгруппа. Определим группы K и M как в доказательстве леммы 3.1.3:

$$K = \{\sigma_m : m \not\equiv 0 \mod 3\},\ \sigma_m : x \to x^m,\ M = K_T.$$

Лемма 3.2.4. *Выполнено неравенство $|T \setminus T_m| \geq |T_m|$, причем равенство достигается тогда и только тогда, когда*

1) *T_m является объединением трех орбит группы M;*

2) *$T \setminus T_m$ является орбитой группы M;*

3) *любой элемент из $T \setminus T_m$ имеет порядок 3^{m+1}.*

Доказательство. Из леммы 1.5.4 вытекает, что $M = K_{T_m}$ и $K_t \leq M$ для любого $t \in T$. Поэтому

$$M_t = K_t = \{1 + |t|l : l = 0, \ldots, \frac{3^k}{|t|} - 1\}.$$

Таким образом, $|M_t| = \frac{3^k}{|t|}$. Из этого следует, что если $|t_1| = |t_2|$, то $|t_1M| = |t_2M|$. Пусть $x \in T_m$. Тогда $|T_m| = |T_m/M||xM|$. Пусть $z \in T \setminus T_m,\ |z| > |x|$. Тогда

$$|M_z| = |M_x|\frac{|x|}{|z|}.$$

Множество T_m является дизъюнктным объединением не более трех орбит группы M. Поэтому $|M_z| \leq \frac{|M_x|}{3}$ и

$$|T| - |T_m| \geq |zM| \geq 3|xM| \geq |T_m/M||xM| = |T_m|.$$

Поскольку равенство $|T \setminus T_m| = |T_m|$ выполнено тогда и только тогда, когда все неравенства в цепочке являются равенствами, мы получаем требуемое. □

Положим $H = \langle T_{a_1} \rangle$ и $3^l = \exp(H)$. Пусть R — объединение всех базисных множеств, содержащих элемент порядка 3. Тогда R — рациональное $\mathcal{A}$-множество и $R \cap T = \varnothing$. Более того, $l < m$. В самом деле, если T_{a_1} рационально и нерегулярно, то это следует из леммы 3.1.8; иначе $T_{a_1} \subseteq E$ и, следовательно, $l = 1 < m$. Таким образом, $|th| = |t|$ для любого $t \in T$ и любого $h \in H$. Из этого вытекает, что $tH \cap T \subseteq T_m$ для любого $t \in T_m$. Поэтому T_m является дизъюнктным объединением нескольких множеств вида $tH \cap T$, где $t \in T_m$. По лемме 1.5.7 число $\lambda = |tH \cap T|$ не зависит от выбора $t \in T$. Значит, λ делит $|T_m|$. Из леммы 3.1.3 вытекает, что $|T_m| \in \{1, 2, 3, 4, 6\}$ и, следовательно,

$$\lambda \in \{1, 2, 3, 4, 6\}.$$

Покажем, что T_{a_1} регулярно. Предположим противное. Тогда $H = T_{a_1} \cup \{e\}$ или $H = T_{a_1} \cup \{e, q, q^2\},\ q \in E \setminus A_1$ по лемме 3.1.5. В первом случае $c^T_{TT_{a_1}} = \lambda - 1$. Во втором случае существует $t \in T$ такой, что $qt \notin T$ или $q^2t \notin T$, потому что иначе $tq, tq^2 \in T$ для любого $t \in T$ и, следовательно, $q \in \mathrm{rad}(T) > e$, противоречие. Значит, $c^T_{TT_{a_1}} = \lambda - 1$ или $c^T_{TT_{a_1}} = \lambda - 2$. Утверждение 1 леммы 1.5.6 влечет, что

$$c^T_{TT_{a_1}}|T| = c^{T_{a_1}}_{TT^{-1}}|T_{a_1}| = |a_1T \cap T||T_{a_1}| = (|T| - \alpha)|T_{a_1}|, \tag{3.5}$$

где $\alpha = |T_m| - |a_1T_m \cap T_m|$. Мы заключаем, что $\alpha > 0$, потому что $a_1 \notin \mathrm{rad}(T_m)$. Из леммы 3.2.4 вытекает, что $|T| - \alpha > 0$. Число $|T_{a_1}| - c^T_{TT_{a_1}}$ не равно 0, так как иначе $\alpha = 0$. Таким образом, из (3.5) и леммы 3.2.4 следует, что

$$\frac{\alpha|T_{a_1}|}{|T_{a_1}| - c^T_{TT_{a_1}}} = |T| \geq 2|T_m| \geq 2\alpha.$$

Поскольку $c^T_{TT_{a_1}} \leq \lambda - 1 \leq 5$, мы получаем, что $|T_{a_1}| \leq 2c^T_{TT_{a_1}} \leq 10$. Значит, $|H| = 9$ и, следовательно, $H = E$ или H — циклическая группа. Покажем, что последнее невозможно.

Если H циклическая, то можно считать, что $H \leq A$. С одной стороны, $|tH \cap T| \geq 3$ для $t \in T \backslash T_m$ по лемме 3.1.2. С другой стороны, лемма 3.1.3 влечет, что $0 < |tH \cap T| \leq |tC \cap T_m| \leq 2$ для любого $t \in T_m$. Мы получаем противоречие с леммой 1.5.7. Таким образом, $H = E$ и T_{a_1} регулярно.

Из леммы 3.1.2 следует, что $tA_1 \subseteq tH \cap T$ для любого $t \in T \setminus T_m$. Поэтому $\lambda = 3$ или $\lambda = 6$. Для завершения доказательства леммы 3.2.3 мы покажем, что оба эти случая невозможны. Поскольку λ делит $|T_m|$ и $|T_m| \leq 6$, мы имеем $|T_m| = 3$ или $|T_m| = 6$. Кроме того, из леммы 3.1.3 вытекает, что $|a_1 T_m \cap T_m| = 0$ (иначе $A_1 \leq \mathrm{rad}(T)$) и $\alpha = |T_m|$. Предположим, что $\lambda = 6$. Тогда $|tH \cap T_m| = 6$ для любого $t \in T_m$. Следовательно, $T_m \subseteq tH$ и $|a_1 T_m \cap T_m| > 0$, противоречие. Значит, $\lambda = 3$. Тогда регулярность T_{a_1} влечет, что $|T_{a_1}| \in \{2, 3, 4, 6, 8\}$. Если $|T_{a_1}| \in \{4, 6, 8\}$, то T_{a_1} рационально и $c^T_{TT_{a_1}} = \lambda - 1 = 2$, потому что для любого $t \in T \setminus T_m$ выполнено $a_1 t, a_1^2 t \in tT_{a_1} \cap T$ по лемме 3.1.2. Если $|T_{a_1}| \in \{2, 3\}$, то $c^T_{TT_{a_1}} = \lambda - 2 = 1$, так как $t, a_1^2 t \in tH \cap T$, но $t, a_1^2 t \notin tT_{a_1} \cap T$ для любого $t \in T \setminus T_m$. С другой стороны, из (3.5) следует, что

$$|T| = \alpha + \frac{2\alpha}{|T_{a_1}| - 2} \leq 2\alpha$$

для $|T_{a_1}| \in \{4, 6, 8\}$ и

$$|T| = \alpha + \frac{\alpha}{|T_{a_1}| - 1} \leq 2\alpha$$

для $|T_{a_1}| \in \{2, 3\}$. Мы заключаем, что $|T| = 2\alpha = 2T_m \in \{6, 12\}$, потому что $|T| \geq 2\alpha$ по лемме 3.2.4.

Пусть $\pi : D \to D/E$ — естественный гомоморфизм и $T' = \pi(T)$. Тогда T' является нерегулярным базисным множеством с тривиальным радикалом циркулянтного S-кольца над D/E. Лемма 1.7.2 влечет, что $|T'| \geq 4$. С другой стороны, $|T'| = \frac{|T|}{\lambda} = \frac{|T|}{3}$ по определению числа λ. Значит, $|T| \neq 6$. Поэтому $|T| = 12$. Тогда $|T'| = 4$. Поскольку T' является нерегулярным множеством с тривиальным радикалом, из леммы 1.7.2 следует, что $T' = \langle T' \rangle \setminus \mathrm{rad}(T') = \langle T' \rangle \setminus \{e\}$ и $4 = |T'| = 3^i - 1$ для некоторого целого i, противоречие. □

Лемма 3.2.5. *Предположим, что у S-кольца $\mathcal{A}$ на D найдется нерегулярное старшее базисное множество X с тривиальным радикалом. Тогда выполнено утверждение* 2 *предложения 3.2.1. В частности,* $\mathrm{rad}(\mathcal{A}) = e$.

Доказательство. Поскольку X нерегулярное и $\mathrm{rad}(X) = e$, мы заключаем по лемме 3.2.3, что множество $X \cap E$ непусто. Значит, ни A_1, ни E не является $\mathcal{A}$-подгруппой (первое следует из леммы 3.2.2). Таким образом, T_{a_1} нерегулярно и рационально по утверждению 2 леммы 3.1.5.

Покажем, что T_{a_1} старшее. Это очевидно, если $T_{a_1} = X$. Если $T_{a_1} \neq X$, то каждое базисное множество T такое, что $T \cap E \neq \varnothing$ и $T \neq T_{a_1}$, имеет тривиальный радикал (иначе $a_1 \in \mathrm{rad}(X)$). Из леммы 3.1.8 следует, что $D_m \setminus \{e\} = R$, где $3^m = \max\limits_{t \in T_{a_1}} |t|$, и R — объединение всех базисных множеств, содержащих элемент порядка 3. Поскольку $X \subseteq R$ и X — старшее, $D_m = D$ и T_{a_1} — старшее.

Из леммы 3.1.5 следует, что $H = T_{a_1} \cup \{e\}$ является $\mathcal{A}$-подгруппой или $H = T_{a_1} \cup \{e, q, q^2\}$ является $\mathcal{A}$-подгруппой, где $q \in E \setminus A_1$. В последнем случае $H = D$, потому что T_{a_1} старшее. Значит, $T_{a_1} = X$ — единственное старшее базисное множество и $q \in \mathrm{rad}(T_{a_1})$, что невозможно. Таким образом, $H = T_{a_1} \cup \{e\}$. Если H нециклическая, то $H = D$ и $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$ для $L = \{e\}$. Если H циклическая, то $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$ для L порядка 3 по утверждениям 1 и 4 леммы 3.1.6. □

Доказательство предложения 3.2.1. Предположим, что $\mathcal{A}$ нерегулярно. Тогда найдется хотя бы одно нерегулярное старшее базисное множество X и мы получаем требуемое по лемме 3.2.5. □

§ 3.3. Регулярные S-кольца с тривиальным радикалом

Основным результатом данного параграфа является

Предложение 3.3.1. *Пусть $k \geq 2$ и $\mathcal{A}$ — регулярное S-кольцо над D. Предположим, что $\mathrm{rad}(\mathcal{A}) = e$. Тогда $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K, D)$, где $K \leq \mathrm{Aut}(D)$ — одна из групп $K_0 - K_9$, представленных в таблице 2.*

Прежде, чем приступить к доказательству предложения 3.3.1, мы сформулируем в удобной для нас форме техническую лемму об S-кольцах над $E = A_1 \times B$.

Лемма 3.3.2. *Пусть $\mathcal{A}$ — S-кольцо над E. Предположим, что A_1 является $\mathcal{A}$-подгруппой. Тогда $\mathcal{A}$ Кэли изоморфно одному из следующих S-колец:*

1) $\mathcal{A} = \mathbb{Z}A_1 \wr \mathcal{A}_B$, *где* $\mathrm{rk}(\mathcal{A}_B) = 2$;
2) $\mathcal{A} = \mathbb{Z}E$;
3) $\mathcal{A} = \mathbb{Z}A_1 \wr \mathbb{Z}B$;
4) $\mathcal{A} = \mathbb{Z}A_1 \otimes \mathcal{A}_B$, *где* $\mathrm{rk}(\mathcal{A}_B) = 2$;
5) $\mathcal{A} = \mathcal{A}_{A_1} \otimes \mathbb{Z}B$, *где* $\mathrm{rk}(\mathcal{A}_{A_1}) = 2$;
6) $\mathcal{A} = \mathcal{A}_{A_1} \wr \mathbb{Z}B$, *где* $\mathrm{rk}(\mathcal{A}_{A_1}) = 2$;
7) $\mathcal{A} = \mathrm{Cyc}(M, E)$, *где* $M = \{e,\ \delta\},\ \delta : x \to x^{-1}$;
8) $\mathcal{A} = \mathcal{A}_{A_1} \otimes \mathcal{A}_B$, *где* $\mathrm{rk}(\mathcal{A}_B) = \mathrm{rk}(\mathcal{A}_{A_1}) = 2$;
9) $\mathcal{A} = \mathcal{A}_{A_1} \wr \mathcal{A}_B$, *где* $\mathrm{rk}(\mathcal{A}_B) = \mathrm{rk}(\mathcal{A}_{A_1}) = 2$;

и $\mathcal{S}(\mathcal{A}) \setminus \{e\}$ *устроено (с точностью до изоморфизма Кэли) одним из следующих способов :*

1) $\mathcal{S}(\mathcal{A}) = \{\{a_1\},\ \{a_1^2\},\ \{b, ba_1, ba_1^2, b^2, b^2a_1, b^2a_1^2\}\}$;

2) $\mathcal{S}(\mathcal{A}) = \{\{a_1\},\ \{a_1^2\},\ \{b\},\ \{b^2\},\ \{ba_1\},\ \{b^2a_1\},\ \{ba_1^2\},\ \{b^2a_1^2\}\}$;

3) $\mathcal{S}(\mathcal{A}) = \{\{a_1\},\ \{a_1^2\},\ \{b, ba_1, ba_1^2\},\ \{b^2, b^2a_1, b^2a_1^2\}\}$;

4) $\mathcal{S}(\mathcal{A}) = \{\{a_1\},\ \{a_1^2\},\ \{b, b^2\},\ \{ba_1, b^2a_1\},\ \{ba_1^2, b^2a_1^2\}\}$;

5) $\mathcal{S}(\mathcal{A}) = \{\{a_1, a_1^2\},\ \{b\},\ \{b^2\},\ \{ba_1, ba_1^2\},\ \{b^2a_1, b^2a_1^2\}\}$;

6) $\mathcal{S}(\mathcal{A}) = \{\{a_1, a_1^2\},\ \{b, ba_1, ba_1^2\},\ \{b^2, b^2a_1, b^2a_1^2\}\}$;

7) $\mathcal{S}(\mathcal{A}) = \{\{a_1, a_1^2\},\ \{b, b^2\},\ \{ba_1, b^2a_1^2\},\ \{ba_1^2, b^2a_1\}\}$;

8) $\mathcal{S}(\mathcal{A}) = \{\{a_1, a_1^2\},\ \{b, b^2\},\ \{ba_1, b^2a_1^2, ba_1^2, b^2a_1\}\}$;

9) $\mathcal{S}(\mathcal{A}) = \{\{a_1, a_1^2\},\ \{b, b^2, ba_1, b^2a_1^2, ba_1^2, b^2a_1\}\}$.

Заметим, что S-кольца 4 и 5 Кэли изоморфны, но их ограничения на A_1 не являются Кэли изоморфными.

Доказательство. Утверждение леммы следует из вычислений в групповом кольце группы E, которые выполнены при помощи пакета COCO2P [18]. □

Доказательство предложения 3.3.1. Пусть X — старшее базисное множество и $x \in X$. Без ограничения общности можно считать, что $\langle x \rangle = A$. Из леммы 3.1.3 следует, что $|X| \in \{1, 2, 3, 4, 6\}$. Рассмотрим все эти случаи.

Случай 1: $|X| = 1$. В этом случае $X = \{x\}$. Ясно, что $A = \langle X \rangle$ является $\mathcal{A}$-подгруппой. Кроме того, $\mathcal{A}_A = \mathbb{Z}A$ по утверждению 2 леммы 1.5.6. Предположим, что базисное множество T_b, содержащее элемент b, нерегулярно. Тогда из леммы 3.2.2 следует, что $A_1 \leq \mathrm{rad}(T_b)$. Поэтому $|T_b| \geq 6$. Пусть Y — старшее базисное множество, содержащее bx^{-1}. Предположим, что $|Y| = 6$. Тогда $Y_{0e} \neq \varnothing$, $Y_{1b} \neq \varnothing$, $Y_{2b^2} \neq \varnothing$, и $Y = Y^{-1}$. Значит, каждое старшее базисное множество рационально сопряжено с Y, что неверно для X. Поэтому $|Y| \leq 4$. По утверждению 2 леммы 1.5.6, множество $x^{-1}Y$ является базисным множеством, содержащим b. Следовательно, $x^{-1}Y = T_b$. Однако, $|x^{-1}Y| \leq 4$ и $|T_b| \geq 6$, противоречие. Таким образом, T_b регулярно. Из этого вытекает, что E является $\mathcal{A}$-подгруппой. Поскольку также $a_1, a_1^2 \in \mathcal{A}$, мы заключаем, что $\mathcal{S}(\mathcal{A}_E)$ имеет (с точностью до изоморфизма Кэли) одну из форм $1 - 4$ из леммы 3.3.2.

Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 1, то множество

$$X_1 = x\{b, ba_1, ba_1^2, b^2, b^2a_1, b^2a_1^2\}$$

является старшим базисным множеством таким, что $a_1 \in \mathrm{rad}(X_1)$, противоречие. Если $\mathcal{S}(\mathcal{A}_E)$

имеет форму 3, то множество

$$X_1 = x\{b, ba_1, ba_1^2\}$$

старшее и $a_1 \in \mathrm{rad}(X_1)$, противоречие. Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 2 или 4, то $\mathcal{A}_A = \mathbb{Z}A$ и B — $\mathcal{A}$-подгруппа. В силу утверждения 2 леммы 1.6.1, $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B$. В первом случае $\mathcal{A} = \mathbb{Z}D = \mathrm{Cyc}(K_0, D)$; во втором случае $\mathcal{A} = \mathrm{Cyc}(K_1, D)$.

Случай 2: $|X| = 2$. Пусть $X = \{x, x_1\}$. Если $x_1 \notin A$, то без ограничения общности можно считать, что $x_1 \in bA$. Если $x_1 \in A$, то лемма 3.1.3 влечет, что $x_1 = x^{-1}$. В первом случае положим $y = b^2x_1$. Заметим, что $y \in A$.

Пусть $X = \{x\} \cup b\{y\}$. Поскольку A — циклическая, найдется $l \in \mathbb{Z}$ такое, что $y = x^l$. По лемме 1.5.4 множество $X^{(2)} = \{x^2\} \cup b^2\{y^2\}$ является базисным. Из равенства $2\underline{bxy} = \underline{X}^2 - \underline{X}^{(2)}$ следует, что $Y = \{bxy\} \in \mathcal{S}(\mathcal{A})$. Если $l \equiv 1 \mod 3$, то Y — старшее базисное множество мощности 1, и мы приходим к предыдущему случаю. Значит, можно считать, что $l \equiv 2 \mod 3$. Из леммы 1.5.4 вытекает, что множество $Z = X^{(-l)} = \{x^{-l}\} \cup b\{x^{-l^2}\}$ является базисным.

Рассмотрим элемент

$$\xi = \underline{X}\ \underline{Z} = x^{-l+1} + bx^{-l^2+1} + b + b^2x^{-l^2+k}. \tag{3.6}$$

Элементы x^{-l+1} и $b^2x^{-l^2+l}$ имеют порядок 3^k, потому что $l \equiv 2 \mod 3$. Следовательно, $T_b = \{b\}$ или $T_b = \{b, bx^{-l^2+1}\}$. В последнем случае $|bx^{-l^2+1}| = 3$ и T_b регулярно, потому что иначе $|T_b| \geq 4$ по лемме 3.1.2. Если $T_b = \{b, bx^{-l^2+1}\}$, то $2\underline{b^2x}^{-l^2+1} = \underline{T_b}^2 - \underline{T_b}^{(2)}$ и $\{b^2x^{-l^2+1}\} \in \mathcal{S}(\mathcal{A})$. Поэтому в каждом из случаев существует базисное множество вида $\{q\},\ q \in E \setminus A_1$. Без ограничения общности можно считать, что $T_b = \{b\}$. Тогда множества

$$bX = b\{x\} \cup b^2\{y\},\ b^2X = b^2\{x\} \cup \{y\}$$

являются базисными. Последнее влечет, что $X^{(l)} = b^2X$. Значит, $x^{l^2} = y^l = x$ и, следовательно, 3^k делит $l^2 - 1 = (l-1)(l+1)$. Поэтому 3^k делит $l + 1$. Это показывает, что $y = x^{-1}$. Поскольку A — циклическая, из леммы 1.5.4 следует, что каждое старшее базисное множество рационально сопряжено с X или с bX. Таким образом, каждое старшее базисное множество имеет одну из следующих форм

$$\{x\} \cup b\{x^{-1}\},\ b\{x\} \cup b^2\{x^{-1}\},\ b^2\{x\} \cup \{x^{-1}\},\ x \in A,\ |x| = 3^k.$$

Из леммы 1.5.5 следует, что множество $\{u, u^{-1}\}$ базисное для любого $u \in A,\ |u| < 3^k$. Поскольку $\{b\} \in \mathcal{S}(\mathcal{A})$, множества $b\{u, u^{-1}\},\ b^2\{u, u^{-1}\}$ являются базисными для любого $u \in A,\ |u| < 3^k$. Значит,

$$\mathcal{A} = \mathrm{Cyc}(K_5, D).$$

Пусть теперь $X = \{x, x^{-1}\}$. Тогда A является $\mathcal{A}$-подгруппой. Базисные множества $\mathcal{A}_A$ имеют вид $\{x^l, x^{-l}\},\ l \in \mathbb{Z}$, по лемме 1.5.4 и лемме 1.5.5. Покажем, что

$$\mathrm{rad}(T_b) = e. \tag{3.7}$$

Предположим противное. Тогда $ba_1, ba_1^2 \in T_b$. Пусть Y — старшее базисное множество, содержащее bx. Заметим, что $|Y| \in \{2, 4\}$, потому что иначе лемма 1.5.4 влечет, что каждое старшее базисное множество имеет мощность 3 или 6. Значит, $Y = b\{x\} \cup b^2\{x^{-1}\}$ или $Y = b\{x, y\} \cup b^2\{x^{-1}, y^{-1}\},\ y \in A$. Элемент b входит в элемент $\psi = \underline{X}\ \underline{Y}$. Поэтому ba_1 и ba_1^2 входят в ψ. Если $|Y| = 2$, то только элементы b и bx^2 из bA входят в ψ, противоречие. Если $|Y| = 4$, то только элементы $b, bx^2, bxy, bx^{-1}y$ из bA входят в ψ. Однако, bx^2 и один из элементов $bxy, bx^{-1}y$ имеют порядок 3^k, противоречие. Полученное противоречие доказывает (3.7). Более того, T_b регулярно, так как иначе $A_1 \leq \mathrm{rad}(T_b)$ по лемме 3.2.2. Следовательно, $E = \langle T_{a_1}, T_b\rangle$ является $\mathcal{A}$-подгруппой и $\mathcal{S}(\mathcal{A}_E)$ имеет (с точностью до изоморфизма Кэли) одну из форм $5, 7, 8$ из леммы 3.3.2.

Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 5, то $\mathcal{A}_B = \mathbb{Z}B$ и A является $\mathcal{A}$ - подгруппой. Поэтому $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B = \mathrm{Cyc}(K_2, D)$ по утверждению 2 леммы 1.6.1. Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 7 или 8, то множество $\{b, b^2\}$ является базисным и, следовательно, каждое базисное множество вне A имеет форму $b\{y\} \cup b^2\{y^{-1}\}$ или $b\{y, y^{-1}\} \cup b^2\{y, y^{-1}\}$, где $y \in A$. Предположим, что существуют базисные множества

$$Y = b\{y\} \cup b^2\{y^{-1}\},\ y \in A,\ Z = b\{z, z^{-1}\} \cup b^2\{z, z^{-1}\},\ z \in A.$$

Тогда элементы bz и b^2z^{-1} входят в элемент $(zy^{-1}+yz^{-1})\underline{Y}$, в то время как элементы bz^{-1} и b^2z не входят, противоречие. Таким образом, все базисные множества вне A имеют форму $b\{y\} \cup b^2\{y^{-1}\},\ y \in A$, или все базисные множества вне A имеют форму $b\{y, y^{-1}\} \cup b^2\{y, y^{-1}\},\ y \in A$. Значит, $\mathcal{A} = \mathrm{Cyc}(K_4, D)$ или $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B = \mathrm{Cyc}(K_3, D)$, где $\mathcal{A}_B$ — S-кольцо ранга 2 над B.

Случай 3: $|X| = 4$. Из леммы 3.1.3 следует, что $X = \{x, x^{-1}\} \cup b\{y\} \cup b^2\{y^{-1}\},\ y \in A$, так как $x \in A$. Очевидно, $\underline{X}^2$ совпадает с

$$x^2 + x^{-2} + b^2y^2 + by^{-2} + 4e + 2bxy + 2b^2xy^{-1} + 2bx^{-1}y + 2b^2x^{-1}y^{-1}. \tag{3.8}$$

Поскольку $X^{(2)} \in \mathcal{S}(\mathcal{A})$ и ровно два элемента из

$$bxy, b^2xy^{-1}, bx^{-1}y, b^2x^{-1}y^{-1}$$

имеют порядок 3^k, существует старшее базисное множество Y такое, что $|Y| \leq 2$, и мы приходим к случаю 1 или случаю 2.

Случай 4: $|X| = 3$. В этом случае $X = \{x\} \cup b^i\{y\} \cup b^j\{z\},\ x, y, z \in A,\ i, j \in \{1, 2\}$. Поскольку A — циклическая, существуют $m, l \in \mathbb{Z}$ такие, что $y = x^m, z = x^l$. Заметим, что $T = \{b^i x^{m+1}, b^j x^{l+1}, b^{i+j} x^{m+l}\}$ — $\mathcal{A}$-множество, потому что

$$2(b^i x^{l+1} + b^j x^{l+1} + b^{i+j} x^{m+l}) = \underline{X}^2 - \underline{X}^{(2)}.$$

Если $m \equiv 2 \mod 3$ или $l \equiv 2 \mod 3$, то T содержит ровно один элемент порядка 3^k и мы приходим к случаю 1. Значит, можно считать, что $m \equiv 1 \mod 3$ и $l \equiv 1 \mod 3$. Предположим, что $i = j$. Тогда $b^i y, b^j z \in \langle b^i x \rangle$. Лемма 3.1.3 влечет $b^j z = (b^i y)^{-1}$. Поэтому $X = X^{-1}$ и $|X|$ — четное число. Противоречие с $|X| = 3$. Следовательно, $i \neq j$. Без ограничения общности можно считать, что $i = 1,\ j = 2$.

Покажем, что

$$\underline{A_1},\ \underline{E} \in \mathcal{A}. \tag{3.9}$$

Предположим сначала, что $|xE \cap X| = 3$. Тогда

$$X = x\{e, b\varepsilon_1, b^2\varepsilon_2\},\ \varepsilon_1, \varepsilon_2 \in A_1.$$

Заметим, что $\varepsilon_2 \neq \varepsilon_1^{-1}$, так как иначе $\mathrm{rad}(X) = A_1 > e$. Прямые вычисления показывают, что

$$\underline{E \setminus A_1} = \underline{X}\ \underline{X}^{-1} - 3e.$$

Значит, $E \setminus A_1$ — $\mathcal{A}$-множество. Следовательно, $E = \langle E \setminus A_1 \rangle$ и $A_1 = E \setminus (E \setminus A_1)$ — $\mathcal{A}$-подгруппы. Если $|xE \cap X| < 3$, то из леммы 1.5.5 следует, что $X^{[3]} = \{x^3, y^3, z^3\} \subseteq A$ является $\mathcal{A}$-множеством. Предположим, что $\{x^3\}$ — базисное множество. Тогда множество $x^3 X^{(-2)}$ также базисное. Следовательно, $x^3 X^{(-2)} = X$. Это означает, что $x^3 y^{-2} = x^3 x^{-2m} = x^m = y$ и $x^3 z^{-2} = x^3 x^{-2l} = x^l = z$. Поэтому $y, z \in xE$ и, значит, $|xE \cap X| = 3$, противоречие. Аналогично ни $\{y^3\}$, ни $\{z^3\}$ не являются базисными множествами. Значит, $X^{[3]}$ — базисное множество. Из леммы 1.7.2 вытекает, что $X^{[3]} \in \mathrm{Orb}(K, A_{k-1})$ для некоторой $K \leq \mathrm{Aut}(A_{k-1})$. Если $|X^{[3]}| = 2$, то $\mathrm{rad}(X^{[3]}) = e$ и по лемме 1.7.3 без ограничения общности $x^{3m} = y^3 = x^3,\ x^{3l} = z^3 = x^{-3}$. Это противоречит тому, что $m \equiv 1 \mod 3$ и $l \equiv 1 \mod 3$. Поэтому $|X^{[3]}| = 3$ и это множество имеет нетривиальный радикал по лемме 1.7.3. Значит, $X^{[3]} = x^3 A_1$ и $A_1 = \mathrm{rad}(X^{[3]})$ — $\mathcal{A}$-подгруппа. Теперь для доказательства того, что E — $\mathcal{A}$-подгруппа, достаточно проверить, что T_b регулярно. Действительно, если T_b регулярно, то $E = \langle T_b, A_1 \rangle$ — $\mathcal{A}$-подгруппа. Предположим, что T_b нерегулярно. Тогда $A_1 \leq \mathrm{rad}(T_b)$ по лемме 3.2.2 и, следовательно, $|T_b| \geq 6$. Поскольку $X^{[3]} = x^3 A_1$ — базисное множество, $A_{k-1} = \langle X^{[3]} \rangle$ — $\mathcal{A}$-подгруппа. Пусть $\pi : G \to G/A_1$ — естественный гомоморфизм. Тогда $\{\pi(x^3)\}$ — старшее базисное множество $\mathcal{A}_{A_{k-1}/A_1}$ и, следовательно, $\mathcal{A}_{A_{k-1}/A_1} = \mathbb{Z}(A_{k-1}/A_1)$ по утверждению 2

леммы 1.5.6. Множество $\pi(T_b)$ нерегулярно. Поэтому из леммы 3.2.2 следует, что $\mathrm{rad}(\pi(T_b)) > e$ и $|\pi(T_b)| \geq 6$. Значит, $|T_b| \geq 18$. Ровно 9 элементов входят в элемент $\theta_1 = \underline{X}\ \underline{Y}$, где Y — старшее базисное множество, содержащее y^{-1}. С другой стороны, b входит в θ_1, и мы заключаем, что как минимум 18 элементов входят в θ_1, противоречие. Таким образом, T_b регулярно и E является $\mathcal{A}$-подгруппой.

Далее мы покажем, что

$$\{a_1\} \in \mathcal{S}(\mathcal{A}).$$

Без ограничения общности можно предполагать, что $x^{3^{k-1}} = a_1$. Поскольку $m \equiv 1 \mod 3$ и $l \equiv 1 \mod 3$, мы получаем, что $y^{3^{k-1}} = z^{3^{k-1}} = a_1$ и множество $X^{(3^{k-1}+1)} = a_1 X$ базисное. Элемент a_1 входит в элемент $\underline{a_1 X}\ \underline{X}^{-1}$ в то время, как элемент a_1^2 не входит. Поэтому a_1 и a_1^2 лежат в разных базисных множествах.

Проверим, что не существует $\mathcal{A}$-подгрупп порядка 3, отличных от A_1. Предположим противное. Без ограничения общности пусть B — $\mathcal{A}$-подгруппа порядка 3, отличная от A_1. Пусть π_1 — естественный гомоморфизм из D в D/B. Множество $\pi_1(X)$ имеет тривиальный радкиал, так как иначе $\mathrm{rad}(\pi_1(X)) = A_1$ и, следовательно, $\mathrm{rad}(X) = \langle ba_1 \rangle$ или $\mathrm{rad}(X) = \langle b^2 a_1 \rangle$. Значит, $\pi_1(X) \in \mathrm{Orb}(K, A)$ для некоторой $K \leq \mathrm{Aut}(A)$ по лемме 1.7.2. Лемма 1.7.3 влечет, что $\pi_1(X) = \{u\}$ или $\pi_1(X) = \{u, u^{-1}\}$. Первый случай невозможен, потому что тогда $B \leq \mathrm{rad}(X)$. Во втором случае $y = x^m = x^{-1}$ или $z = x^l = x^{-1}$. Это противоречит тому, что $m \equiv 1 \mod 3$ и $l \equiv 1 \mod 3$. Таким образом не существует $\mathcal{A}$-подгрупп порядка 3, отличных от A_1 и из (3.9) вытекает, что $\mathcal{S}(\mathcal{A}_E)$ имеет (с точностью до изоморфизма Кэли) форму 1 или 3 из леммы 3.3.2.

Пусть Y и Z — базисные множества, содержащие элементы y и z соответственно. Пусть $Y^{-1} = \{y^{-1}\} \cup b\{u\} \cup b^2\{v\},\ u, v \in A$, и $Z^{-1} = \{z^{-1}\} \cup b\{u_1\} \cup b^2\{v_1\},\ u_1, v_1 \in A$. Элемент b входит в элемент $\underline{X}\ \underline{Y}^{-1}$. Значит, элементы ba_1 и ba_1^2 тоже входят в $\underline{X}\ \underline{Y}^{-1}$. Поэтому без ограничения общности можно считать, что $u = a_1 x^{-1},\ v = a_1^2 z^{-1}$. Элемент b^2 входит в элемент $\underline{X}\ \underline{Z}^{-1}$. Значит, элементы $s^2 c_1$ и $s^2 c_1^2$ тоже входят в $\underline{X}\ \underline{Z}^{-1}$. Поэтому без ограничения общности можно считать, что $u_1 = a_1 y^{-1},\ v_1 = a_1^2 x^{-1}$. Таким образом,

$$Y = \{y\} \cup b\{a_1 z\} \cup b^2\{a_1^2 x\},\ Z = \{z\} \cup s\{a_1 x\} \cup b^2\{a_1^2 y\}.$$

По лемме 1.5.4 мы имеем $Y = X^{(m)},\ Z = X^{(l)}$. Поскольку $m \equiv 1 \mod 3$ и $l \equiv 1 \mod 3$, мы заключаем, что $y^m = a_1 z,\ z^m = a_1^2 x,\ y^l = a_1 x,\ z^l = a_1^2 y$. Эти равенства влекут $x^{m^3} = y^{m^2} = x,\ x^{l^3} = z^{l^2} = x$. Значит, 3^k делит $m^3 - 1$ и $l^3 - 1$. Пусть $m = 3^r p + 1$, где 3 не делит p и $r \geq 1$. Тогда

$$m^3 - 1 = 3^{r+1} p (3^{2r-1} p^2 + 3^r p + 1).$$

Заметим, что $r+1 \geq k$, так как 3 не делит $(3^{2r-1}p^2+3^rp+1)$. Следовательно, $y = x^m = q_1x$, где $q_1 \in A_1$. Аналогично $z = q_2x,\ q_2 \in A_1$. Поскольку $\mathrm{rad}(X) = e$, мы имеем $q_2 \neq q_1^{-1}$. Каждое старшее базисное множество рационально сопряжено с X, потому что $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$. Из этого следует, что если X — орбита некоторой $K \leq \mathrm{Aut}(D)$, то каждое старшее базисное множество является орбитой K.

Прямые вычисления показывают, что $q_1q_2x^3$ — единственный элемент, который входит в элемент $\underline{X}\ \underline{X}^{(3)}$ с коэффициентом 3. Значит, множество $\{x^3\}$ — базисное. Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 3 из леммы 3.3.2, то базисные множества $\mathcal{A}_{D_{k-1}}$ имеют вид

$$\{u\},\ buA_1,\ b^2uA_1,\ u \in A_{k-1}$$

по утверждению 2 леммы 1.5.6, и, следовательно, $\mathcal{A}$ Кэли изоморфно $\mathrm{Cyc}(K_6, D)$; если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 1 из леммы 3.3.2, то базисные множества $\mathcal{A}_{D_{k-1}}$ имеют вид

$$\{u\},\ buA_1 \cup b^2uA_1,\ u \in A_{k-1}$$

по утверждению 2 леммы 1.5.6, и, следовательно, $\mathcal{A}$ Кэли изоморфно $\mathrm{Cyc}(K_7, D)$.

Случай 5: $|X| = 6$. Из леммы 3.1.3 следует, что

$$X = \{x, x^{-1}\} \cup b\{y, z\} \cup b^2\{y^{-1}, z^{-1}\},\ x, y, z \in A.$$

Лемма 1.5.4 влечет, что для любого старшего базисного множества Y существует $s \in \mathbb{Z}$ такое, что $Y = X^{(s)}$. Поскольку A — циклическая, существуют $m, l \in \mathbb{Z}$ такие, что $y = x^m, z = x^l$. Без ограничения общности можно считать, что

$$m \equiv 1 \mod 3,\ l \equiv 2 \mod 3.$$

Действительно, предположим, что $m \equiv l \mod 3$. Тогда элемент b^2yz имеет порядок 3^k и входит в элемент $\theta_2 = \underline{X}^2 - \underline{X}^{(2)}$. Значит, существует $v \in C,\ |v| = 3^k$, входящее в θ_2, так как каждое старшее базисное множество нетривиально пересекается с A. Однако, только элементы $yz^{-1},\ y^{-1}z,\ e$ из A входят в θ_2. Все эти элементы имеют порядок меньше, чем 3^k, противоречие. Следовательно, $m \not\equiv l \mod 3$.

Докажем (3.9). Доказательство аналогично случаю, когда $|X| = 3$. Если $|xE \cap X| = 3$, то

$$X = x\{e, b\varepsilon_1, b^2\varepsilon_2\} \cup x^{-1}\{e, b^2\varepsilon_1^2, b\varepsilon_2^2\},\ \varepsilon_1, \varepsilon_2 \in A_1,$$

потому что $X = X^{-1}$. Заметим, что $\varepsilon_2 \neq \varepsilon_1^{-1}$, так как иначе $\mathrm{rad}(X) > e$. Значит, все элементы из $E \setminus A_1$ входят в $\underline{X}^2$ и только эти элементы из D_{k-1} входят в $\underline{X}^2$. Поскольку $\mathcal{A}$ регулярно,

D_{k-1} является $\mathcal{A}$-подгруппой. Следовательно, $E \setminus A_1$ — $\mathcal{A}$-множество. Тогда $E = \langle E \setminus A_1 \rangle$ — $\mathcal{A}$-подгруппа, что и требовалось.

Если $|xE \cap X| < 3$, то из леммы 1.5.5 следует, что

$$X^{[3]} = \{x^3, y^3, z^3, x^{-3}, y^{-3}, z^{-3}\} \subseteq A$$

— $\mathcal{A}$-множество. Все базисные множества, содержащиеся в $X^{[3]}$, сопряжены и , следовательно, имеют один и тот же радикал. Предположим, что каждое базисное множество в $X^{[3]}$ имеет тривиальный радикал. Тогда из леммы 1.7.2 и леммы 1.7.3 следует, что $T_{x^3} = \{x^3\}$ или $T_{x^3} = \{x^3, x^{-3}\}$. В первом случае $x^3X^{(2)}$ является базисным множеством по утверждению 2 леммы 1.5.6. Значит, $x^3X^{(2)} = X$ и $x^5 = x$, противоречие с $|x| > 3$. Во втором случае $(x^3 + x^{-3})\underline{X}^{(2)}$ содержит 12 элементов, включая x и x^5. Из этого следует, что

$$(x^3 + x^{-3})\underline{X}^{(2)} = \underline{X} + \underline{X}^{(5)}. \tag{3.10}$$

Прямые вычисления показывают, что $b\{x^3y^{-2}, x^3z^{-2}, x^{-3}y^{-2}, x^{-3}z^{-2}\}$ — множество всех элементов из bA, которые содержатся в левой части (3.10). Поэтому

$$\{x^3y^{-2}, x^3z^{-2}, x^{-3}y^{-2}, x^{-3}z^{-2}\} = \{y, z, y^{-5}, z^{-5}\}.$$

Поскольку $m \equiv 1 \mod 3$, $l \equiv 2 \mod 3$, мы заключаем, что $y^3, z^3 \in \{x^3, x^{-3}\}$. Из этого вытекает $|xE \cap X| = 3$, что противречит предположению. Значит, $\mathrm{rad}(X^{[3]}) > e$. Более того, $\mathrm{rad}(X^{[3]}) = A_1$, потому что $|X^{[3]}| \leq 6$. Поэтому A_1 — $\mathcal{A}$-подгруппа. Если T_b нерегулярно, то как и в случае, когда $|X| = 3$, мы имеем, что $|T_b| \geq 18$. Это противречит тому, что ровно 16 элементов, включая b, из bA входят в $\underline{X}^2$. Таким образом, T_b регулярно и E — $\mathcal{A}$-подгруппа.

Теперь покажем, что $\{a_1, a_1^2\} \in \mathcal{S}(\mathcal{A})$. Предположим противное. Тогда $\{a_1\}$ является базисным множеством. Следовательно, a_1X тоже является базисным множеством. Без ограничения общности можно считать, что $x^{3^{k-1}} = a_1$. Поскольку $m \equiv 1 \mod 3$ и $l \equiv 2 \mod 3$, мы заключаем, что $y^{3^{k-1}} = a_1$ и $z^{3^{k-1}} = a_1^2$. С одной стороны,

$$X^{(3^{k-1}+1)} = \{a_1x, a_1^2x^{-1}\} \cup b\{a_1y, a_1^2z\} \cup b^2\{a_1^2y^{-1}, a_1z^{-1}\}$$

— базисное множество, содержащее a_1x. С другой стороны, $X^{(3^{k-1}+1)} \neq a_1X$, потому что $ba_1z \in a_1X$, $ba_1z \notin X^{(3^{k-1}+1)}$, противоречие. Таким образом, $\{a_1, a_1^2\} \in \mathcal{S}(\mathcal{A})$.

Покажем, что не существует $\mathcal{A}$-подгрупп порядка 3, отличных от A_1. Предположим противное. Без ограничения общности пусть B — $\mathcal{A}$-подгруппа порядка 3, отличная от A_1. Пусть π_1 — естественный гоморфизм из D в D/B. Предположим, что $\mathrm{rad}(\pi_1(X)) > e$. Тогда $\mathrm{rad}(\pi_1(X)) = A_1$, потому что $|\pi_1(X)| \leq 6$. Из этого следует, что $\pi_1(X) = xA_1 \cup x^{-1}A_1$. Значит,

$$X = x\{e, f_1, f_2\} \cup x^{-1}\{e, f_1^{-1}, f_2^{-1}\},$$

где $f_1, f_2 \in \{ba_1, ba_1^2, b^2a_1, b^2a_1^2\}$. Предположим, что $f_2 \neq f_1^{-1}$. Тогда $f_2 = ff_1$, где $f \in \{b, b^2, a_1, a_1^2\}$. Заметим, что $\{f, f^2\}$ является $\mathcal{A}$-множеством. Элемент f_2x входит в $(f+f^2)\underline{X}$ в то время, как x не входит. Получаем противоречие, так как x и f_2x лежат в одном базисном множестве X. Поэтому $f_2 = f_1^{-1}$ и $\mathrm{rad}(X) = \{e, f_1, f_1^{-1}\}$, что неверно. Значит, $\mathrm{rad}(\pi_1(X)) = e$. Следовательно, лемма 1.7.2 и лемма 1.7.3 влекут, что $\pi_1(X) = \{u, u^{-1}\}$. Тогда $B \leq \mathrm{rad}(X)$, противоречие. Таким образом, не существует $\mathcal{A}$-подгрупп порядка 3, отличных от A_1. Так как $\{a_1, a_1^2\}$ — $\mathcal{A}$-множество, $\mathcal{S}(\mathcal{A}_E)$ имеет форму 6 или 9 из леммы 3.3.2.

Далее мы докажем, что $y = q_1x,\ z = q_2x^{-1},\ q_1, q_2 \in A_1$. Используя предположения на l и m, перечислим все элементы из bA порядка меньше, чем 3^k, входящие в $\underline{X}^{-1}\ \underline{X}^{(m)}$

$$b,\ bz^mx,\ by^mx^{-1},\ byz,\ bz^{-m}y^{-1},\ by^{-m}z^{-1}. \tag{3.11}$$

и все элементы из bA порядка меньше, чем 3^k, входящие в $\underline{X}^{-1}\ \underline{X}^{(l)}$

$$b,\ bx^{-1}y^{-l},\ byz,\ bz^ly^{-1},\ by^lz^{-1},\ bxz^{-l}. \tag{3.12}$$

Каждый элемент из (3.11) имеет вид bx^i, где

$$i \in I = \{ml+1,\ m^2-1,\ m+l,\ ml+m,\ m^2+l\},$$

потому что $y = x^m,\ z = x^l$. Поскольку $a_1 \in \mathrm{rad}(T_b)$ и T_b входит в $\underline{X}^{-1}\ \underline{X}^{(k)}$, мы заключаем, что sc_1 и sc_1^2 встречаются в (11). Поэтому два числа из I делятся на 3^{k-1}. Покажем, что 3^{k-1} делит $m-1$. Это очевидно следует из предположения на m, если m^2-1 делится на 3^{k-1}. Если $m+l$ и $ml+m$ делятся на 3^{k-1}, то 3^{k-1} делит $l(m-1) = ml+m-m-l$, следовательно, 3^{k-1} делит $m-1$ по предположению на l. Если $m+l$ и $ml+1$ делятся на 3^{k-1}, то $(m-1)(l-1) = ml+1-m-l$ делится на 3^{k-1}, следовательно, $m-1$ делится на 3^{k-1}. Если $m+l$ и m^2+l делятся на 3^{k-1}, то $m(m-1) = m^2+l-l-m$ делятся на 3^{k-1} и, значит, $m-1$ делится на 3^{k-1}. Если 3^{k-1} делит $ml+m$ и $ml+1$, то 3^{n-1} делит $k-1 = kl+k-kl-l$. Если $kl+k$ и k^2+l делятся на 3^{n-1}, то $(k-1)(k-l) = k^2+l-ml-m$ делится на 3^{k-1} и, значит, $m-1$ делится на 3^{k-1}. Если $ml+1$ и m^2+l делятся на 3^{k-1}, то без ограничения общности $z^mx = x^{ml+1} = a_1,\ y^{-m}z^{-1} = x^{-m^2-l} = a_1^2$. Заметим, что $x^{-m^3+1} = (x^{-m^2-l})^m x^{ml+1} = a_1^2a_1 = e$. Поэтому m^3-1 делится на 3^k и, следовательно, $m-1$ делится на 3^{k-1}. Таким образом, во всех случаях $m-1$ делится на 3^{k-1}. Из этого следует, что $y = q_1x,\ q_1 \in A_1$.

Каждый элемент из (3.12) имеет вид bx^j, где

$$j \in J = \{ml+1,\ l^2-1,\ m+l,\ ml-l,\ l^2-m\},$$

потому что $y = x^m,\ z = x^l$. Снова ba_1 и ba_1^2 встречаются в (3.12), так как T_b входит в $\underline{X}^{-1}\ \underline{X}^{(l)}$. Из этого вытекает, что 3^{k-1} делит два элемента из J. Применяя рассуждения,

подобные приведенным выше, мы получаем, что $l+1$ делится на 3^{k-1} и $z = x^{l+1}x^{-1} = q_2x^{-1}$, где $q_2 \in A_1$. Заметим, что $q_1 \neq q_2$, так как иначе $bq_1 \in \mathrm{rad}(X)$. Каждое старшее базисное множество рационально сопряжено с X, потому что $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$. Поэтому если X — орбита некоторой $K \leq \mathrm{Aut}(D)$, то каждое старшее базисное множество также является орбитой K.

Прямые вычисления показывают, что только элементы $q_1q_2^2x^3$ и $q_1^2q_2x^{-3}$ входят в элемент $\underline{X}^{(3)}$ с коэффициентом 3. Если $\{q_1q_2^2x^3\}$ является базисным множеством, то $\{a_1\}$ является базисным множеством по утверждению 2 леммы 1.5.6, что неверно. Поэтому $\{q_1q_2^2x^3,\ q_1^2q_2x^{-3}\}$ — базисное множество и каждое базисное множество $\mathcal{A}_{A_{k-1}}$ имеет вид $\{u, u^{-1}\},\ u \in A_{k-1}$, по лемме 1.5.4 и лемме 1.5.5. Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 6 из леммы 3.3.2, то прямая проверка показывает, что каждое нестаршее базисное множество вне A имеет один из двух видов

$$\{bu, ba_1u, ba_1^2u, bu^{-1}, ba_1u^{-1}, ba_1^2u^{-1}\},$$

$$\{b^2u, b^2a_1u, b^2a_1^2u, b^2u^{-1}, b^2a_1u^{-1}, b^2a_1^2u^{-1}\}, u \in A.$$

Значит, $\mathcal{A}$ Кэли изоморфно $\mathrm{Cyc}(K_8, D)$. Если $\mathcal{S}(\mathcal{A}_E)$ имеет форму 9 из леммы 3.3.2, то прямая проверка показывает, что каждое нестаршее базисное множество вне A имеет вид

$$\{bu, ba_1u, ba_1^2u, b^2u^{-1}, b^2a_1u^{-1}, b^2a_1^2u^{-1}\},\ u \in A.$$

Значит, $\mathcal{A}$ Кэли изоморфно $\mathrm{Cyc}(K_9, D)$. □

Непосредственно из описания всех регулярных S-колец с тривиальным радикалом над D вытекает

Лемма 3.3.3. *Пусть $k \geq 2$ и $\mathcal{A}$ — регулярное S-кольцо с тривальным радикалом над D. Тогда A_1 и A_{k-1} являются $\mathcal{A}$-подгруппами.*

Лемма 3.3.4. *Пусть $k \geq 2$ и $\mathcal{A}$ — регулярное S-кольцо с тривальным радикалом над D. Если L — $\mathcal{A}$-подгруппа порядка 3 и $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_i, D)$, где $i \in \{0,1,2,3,4,5\}$, то группа $\mathrm{Aut}(\mathcal{A}_{D/L})$ является 2-изолированной.*

Доказательство. Для $k \leq 3$ утверждение следует из вычислений в групповом кольце группы D, выполненных при помощи пакета COCO2P [18]. Далее мы считаем, что $k \geq 4$. Ввиду леммы 1.5.9, достаточно проверить, что $\mathrm{Aut}(\mathcal{A}_{D/L})_L$ имеет точную регулярную орбиту. Если $L \neq A_1$, то D/L циклическая и предложение 3.3.1 влечет, что $\mathcal{A}_{D/L} = \mathbb{Z}(D/L)$ или каждое базисное множество $\mathcal{A}_{D/L}$ имеет вид $\{x, x^{-1}\},\ x \in A/L$. В обоих случаях, очевидно, группа $\mathrm{Aut}(\mathcal{A}_{D/L})_L$ имеет точную регулярную орбиту.

Пусть $L = A_1$ и $\pi : D \to D/L$ — естественный гомоморфизм. Если $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_0, D)$, то $|\operatorname{Aut}(\mathcal{A}_{D/L})_L| = 1$ и, очевидно, $\operatorname{Aut}(\mathcal{A}_{D/L})_L$ имеет точную регулярную орбиту. Если $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_1, D) = \mathbb{Z}A \otimes \mathcal{A}_B$, где $\mathcal{A}_B$ имеет ранг 2, то $\mathcal{A}_{D/L} = \mathbb{Z}A_{k-1} \otimes \mathcal{A}_B$. Следовательно, $|\operatorname{Aut}(\mathcal{A}_{D/L})_L| = 2$ и $\pi(\{bx, b^2x\})$ является точной регулярной орбитой $\operatorname{Aut}(\mathcal{A}_{D/L})_L$. Если $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_i, D),\ i \in \{2, 4, 5\}$, то $\mathcal{A}_{D/L}$ — квазитонкое S-кольцо с как минимум двумя ортогоналями. В самом деле, $\{\pi(y^2), \pi(y^{-2})\}$ и $\{\pi(y^4), \pi(y^{-4})\}$, где y — порождающий группы A_{k-1}, являются ортогоналями. Эти ортогонали различны, так как $k \geq 4$. Таким образом, $\operatorname{Aut}(\mathcal{A}_{D/L})_L$ имеет точную регулярную орбиту по лемме 1.5.10. Если $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_3, D)$, то базисные множества $\mathcal{A}_{D/L}$ имеют вид

$$\{\pi(b), \pi(b^2)\},\ \{\pi(y), \pi(y^{-1})\},\ \pi(b)\{\pi(y), \pi(y^{-1})\} \cup \pi(b^2)\{\pi(y), \pi(y^{-1})\},\ y \in A.$$

Заметим, что $\pi(B)$ и $\pi(A)$ — $\mathcal{A}_{D/L}$-подгруппы, $\mathcal{A}_{D/L} = \mathcal{A}_{\pi(A)} \otimes \mathcal{A}_{\pi(B)}$, и $\operatorname{Aut}(\mathcal{A}_{D/L})_L^{\pi(A)} \cong \operatorname{Aut}(\mathcal{A}_{D/L})_L^{\pi(B)} \cong C_2$. Поэтому $\operatorname{Aut}(\mathcal{A}_{D/L})_L \cong C_2 \times C_2$ и $\pi(b)\{\pi(y), \pi(y^{-1})\} \cup \pi(b^2)\{\pi(y), \pi(y^{-1})\}$ является точной регулярной орбитой $\operatorname{Aut}(\mathcal{A}_{D/L})_L$. □

Лемма 3.3.5. *Пусть $k \geq 2$ и $\mathcal{A}$ — S-кольцо над D. Предположим, что для любого старшего базисного множества X с тривиальным радикалом выполнены следующие утверждения:*

1) *X регулярно;*

2) *$\langle X \rangle = D$.*

Тогда каждое старшее базисное множество $\mathcal{A}$ имеет тривиальный радикал.

Доказательство. Из леммы 3.1.3 следует, что $|X| \leq 6$. Если $|X| = 1$, то условие 2 леммы не выполнено. Утверждение леммы следует из леммы 1.5.4, если $|X| \in \{3, 6\}$. В этих случаях каждое старшее базисное множество рационально сопряжено с X, потому что $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$. Предположим, что $|X| = 2$. Тогда без ограничения общности можно считать, что $X = \{x\} \cup b\{y\},\ x, y \in A$. Из леммы 1.5.5 вытекает, что A_1 является $\mathcal{A}$-подгруппой. Из (3.6) (см. доказательство предложения 3.3.1) следует, что T_b регулярно (иначе $|T_b| \geq 6$ по лемме 3.2.2), $|T_b| \leq 2$, и $T_b \neq T_{b^2}$. Таким образом, E является $\mathcal{A}$-подгруппой и лемма 3.3.2 влечет, что существует базисное множество вида $\{q\},\ q \in E \setminus A_1$. Из утверждения 2 леммы 1.5.6 следует, что qX — базисное множество. Значит,

$$\bigcup_m (X^{(m)} \cup (qX)^{(m)}) = D \setminus D_{k-1},$$

где m пробегает все целые числа, не делящиеся на 3. Получаем требуемое, так как $\operatorname{rad}(X) = e$.

Покажем, что условие 2 леммы не выполнено, если $|X| = 4$. В этом случае без ограничения общности можно считать, что $X = \{x, x^{-1}\} \cup b\{y\} \cup b^2\{y^{-1}\},\ x, y \in A$. Из леммы 1.5.5 следует, что A_1 — $\mathcal{A}$-подгруппа. Ровно один из элементов $bxy, bx^{-1}y$, например первый, имеет порядок 3^k. Если T_{bxy} нерегулярно, то $|T_{bxy}| \geq 6$ по лемме 3.2.2, что противоречит (3.8) (см. доказательство предложения 3.3.1). В самом деле, ровно четыре различных элемента, включая bxy, входят в $\underline{X}^2 - \underline{X}^{(2)}$. Значит, T_{bxy} регулярно и из (3.8) следует, что $T_{bxy} = \{bxy\}$ или $T_{bxy} = \{bxy, b^2x^{-1}y^{-1}\}$. В обоих случаях $\langle T_{bxy}\rangle$ является циклической группой. □

§ 3.4. S-кольца с нетривиальным радикалом

Основным результатом данного параграфа является

Предложение 3.4.1. *Пусть $k \geq 2$ и $\mathcal{A}$ — S-кольцо над D такое, что $\mathrm{rad}(\mathcal{A}) > e$. Тогда найдется $\mathcal{A}$-секция U/L такая, что $\mathcal{A}$ — собственное U/L-сплетение. Более того, $|U/L| \leq 3$, или $\mathrm{rad}(\mathcal{A}_U) = e$ и $|L| = 3$.*

Доказательство. Положим $U = \langle X : X \in \mathcal{S}(\mathcal{A}),\ \mathrm{rad}(X) = e\rangle$.

Лемма 3.4.2. *Подгруппа U — $\mathcal{A}$-подгруппа группы D, и $\mathrm{rad}(\mathcal{A}_U) = e$.*

Доказательство. Первое утверждение выполнено, так как U порождается базисными множествами. Покажем, что

$$\mathrm{rad}(\mathcal{A}_U) = e.$$

Без ограничения общности можно считать, что $U = D$. Тогда существует старшее базисное множество X такое, что $\mathrm{rad}(X) = e$. Если X нерегулярно, то оно содержит элемент порядка 3 по лемме 3.2.3 и по лемме 3.2.5 мы имеем, что $\mathrm{rad}(\mathcal{A}) = e$. Поэтому можно считать, что каждое старшее базисное множество с тривиальным радикалом регулярно. Хотя бы одно из множеств X_{0e}, X_{1b}, X_{2b^2} непусто. Без ограничения общности считаем, что $X_{0e} \neq \varnothing$. Если $\langle Z\rangle = D$ для любого старшего базисного множества Z с тривиальным радикалом, то каждое старшее базисное множество имеет тривиальный радикал по лемме 3.3.5. Значит, можно считать, что $\langle X\rangle = A$. Тогда лемма 1.7.3 влечет, что $X = \{x\}$ или $X = \{x, x^{-1}\}$, где $x \in A$. Поскольку $\langle X\rangle = A$, существует базисное множество Y такое, что $D = \langle X, Y\rangle$ и $\mathrm{rad}(Y) = e$. Если Y нерегулярно, то из леммы 3.2.2 следует, что $A_1 \leq \mathrm{rad}(Y)$. Поэтому Y регулярно. Пусть без ограничения общности $Y_{1b} \neq \varnothing$ и $y \in Y_{1b}$. Заметим, что $|Y_{1b}| \leq 2$ по лемме 3.1.3.

Покажем, что $\mathrm{rad}(T_b) = e$, где T_b — базисное множество, содержащее b. Это очевидно, если $T_b = Y$. Пусть теперь $T_b \neq Y$. Предположим противное, что $\mathrm{rad}(T_b) > e$. Тогда $A_1 \leq$

$\mathrm{rad}(T_b)$. Если $|Y_{1b}| = 1$, то ровно два элемента b и by^2 из bA входят в элемент $\alpha = (y + y^{-1})\underline{Y}$, противоречие. Предположим, что $Y_{1b} = \{y, z\}$. Тогда ровно четыре элемента b, byz, $by^{-1}z$, и by^2 из bA входят в α. Поскольку $ba_1, ba_1^2 \in T_b$, мы заключаем, что $\{a_1, a_1^2\} \subseteq \{y^2, yz, y^{-1}z\}$. Если $y^2 \in A_1$, то $ba_1 \in Y$ или $ba_1^2 \in Y$, и, значит, $Y = T_b$, противоречие. Таким образом, $\{a_1, a_1^2\} = \{yz, y^{-1}z\}$. Следовательно, $z^2 = e$, противоречие.

Из рассуждений, приведенных в предыдущем абзаце, следует, что T_b регулярно, потому что иначе $A_1 \leq \mathrm{rad}(T_b)$ по лемме 3.2.2. Поскольку A_1 — $\mathcal{A}$-подгруппа, из леммы 3.3.2 следует, что существует $\mathcal{A}$-подгруппа $Q \neq A_1$ порядка 3. Каждое базисное множество внутри A имеет вид $\{x\}$ или $\{x, x^{-1}\}$. Следовательно, $\{qx, qx^{-1}, q^2x, q^2x^{-1}\}$ — $\mathcal{A}$-множество для любого $x \in A$. Таким образом, каждое базисное множество $\mathcal{A}$ имеет тривиальный радикал, что и требовалось. □

Лемма 3.4.3. *Пусть H — минимальная нетривиальная $\mathcal{A}$-подгруппа. Тогда $\mathrm{rk}(\mathcal{A}_H) = 2$, или $|H| = 3$ и $\mathcal{A}_H = \mathbb{Z}H$, или $H = E$ и $\mathcal{A}_H \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_{10}, H)$, где K_{10} — группа из таблицы 2. Во всех случаях радикал всякого базисного множества $\mathcal{A}_H$ тривиален.*

Доказательство. В силу минимальности, у H нет нетривиальных собственных $\mathcal{A}$-подгрупп. Если $H \not\leq E$, то $\mathrm{rk}(\mathcal{A}_H) = 2$ по лемме 3.1.1. Если $H = E$, то компьютерные вычисления с использованием пакета COCO2P [18] показывают, что либо $\mathrm{rk}(\mathcal{A}_H) = 2$, либо для $\mathcal{A}_H \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_{10}, H)$, где K_{10} — группа из таблицы 2. Если $H < E$, то $|H| = 3$. Тогда, очевидно, либо $\mathrm{rk}(\mathcal{A}_H) = 2$, либо $\mathcal{A}_H = \mathbb{Z}H$. Второе утверждение леммы непосредственно вытекает из первого. □

Поскольку по предположению предложения $\mathrm{rad}(\mathcal{A}) > e$, лемма 3.4.2 влечет, что $U < D$. Кроме того, из леммы 3.4.3 следует, что U содержит каждую минимальную $\mathcal{A}$-подгруппу.

Лемма 3.4.4. *Если существует единственная минимальная нетривиальная $\mathcal{A}$-подгруппа группы D или $A_1 \leq \mathrm{rad}(X)$ для любого базисного множества X, лежащего вне U, то выполнено утверждение предложения 3.4.1.*

Доказательство. Пусть L — единственная минимальная нетривиальная $\mathcal{A}$-подгруппа. Тогда $L \leq \mathrm{rad}(X)$ для любого $X \in \mathcal{S}(\mathcal{A})$, лежащего вне U, потому что группа $\mathrm{rad}(X)$ является нетривиальной $\mathcal{A}$-подгруппой. Значит, $\mathcal{A}$ является U/L-сплетением. Если $|L| = 3$, то предложение 3.4.1 выполнено. Предположим, что $|L| > 3$. Если $|U| = 9$, то $U = L$ и предложение 3.4.1 выполнено. Если $U > 9$, то из леммы 3.3.3 следует, что $\mathcal{A}_U$ нерегулярно (иначе A_1 — $\mathcal{A}$-подгруппа порядка 3). Следовательно, из предложения 3.2.1 вытекает, что $\mathrm{rk}(\mathcal{A}_U) = 2$ (в

противном случае найдется две минимальные нетривиальные $\mathcal{A}$-подгруппы). Поэтому $U = L$, что и требовалось.

Для завершения доказательства предположим, что существует хотя бы две различные минимальные нетривиальные $\mathcal{A}$-подгруппы и $A_1 \leq \mathrm{rad}(X)$ для любого $X \in \mathcal{S}(\mathcal{A})$, лежащего вне U. Предположим, что $A_1 \not\leq U$. Тогда $|U| = 3$ и U — единственная минимальная нетривиальная $\mathcal{A}$-подгруппа, так как U содержит каждую минимальную $\mathcal{A}$-подгруппу, противоречие. Поэтому $A_1 \leq U$. Обозначим через H минимальную $\mathcal{A}$-подгруппу, содержащую A_1. Тогда $\mathcal{A}$ является U/H-сплетением. Если $H = A_1$, то $|H| = 3$ и предложение 3.4.1 выполнено. Если $|U| = 9$, то $|U/L| \leq 3$ и предложение 3.4.1 выполнено. Далее считаем, что $H > A_1$ и $|U| > 9$. Тогда $\mathcal{A}_U$ нерегулярно по лемме 3.3.3. Таким образом, предложение 3.2.1 влечет, что $\mathcal{A}_U = \mathcal{A}_H \otimes \mathcal{A}_L$, где $|L| \leq 3$. Значит, $|U/H| \in \{1, 3\}$. □

Объединение всех базисных множеств X таких, что $\mathrm{rad}(X) = e$ или $A_1 \leq \mathrm{rad}(X)$, обозначим через V. Тогда $U \subset V$ и V — $\mathcal{A}$-множество. По лемме 3.4.4 можно считать, что $V \neq D$ и существует хотя бы две минимальных нетривиальных $\mathcal{A}$-подгруппы. Пусть X — базисное множество, содержащее элемент порядка 3. Предположим, что $\mathrm{rad}(X) > e$ и $A_1 \not\leq \mathrm{rad}(X)$. Тогда $|\mathrm{rad}(X)| = 3$ и $\mathrm{rad}(X)$ — единственная минимальная нетривиальная $\mathcal{A}$-подгруппа, противоречие. Значит, $X \subseteq V$ и $E \subseteq V$.

Для заданного $\mathcal{A}$-множества X положим $\mathcal{S}(\mathcal{A})_X = \{Y \in \mathcal{S}(\mathcal{A}) : Y \subseteq X\}$.

Лемма 3.4.5. *Пусть $X \in \mathcal{S}(\mathcal{A})_{D\setminus V}$. Тогда выполнены следующие утверждения:*

1) $\mathrm{rad}(X) = \{e, q, q^2\},\ q \in E \setminus A_1$;

2) *X регулярно и $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$.*

Доказательство. Заметим, что $\mathrm{rad}(X) > e$, так как $X \not\subseteq U$. Группа $\mathrm{rad}(X)$ не содержит элементов порядка больше, чем 3, потому что $a_1 \notin \mathrm{rad}(X)$. Поэтому $\mathrm{rad}(X)$ является группой порядка 3, отличной от A_1, и утверждение 1 леммы выполнено. Обозначим $\mathrm{rad}(X) = \{e, q, q^2\}$ через L. Тогда $\mathrm{rad}(\pi(X)) = e$, где $\pi : D \to D/L$ — естественный гомоморфизм. Группа D/L циклическая. Значит, по лемме 1.7.2 множество $\pi(X)$ регулярно или $\pi(X) = H \setminus \{e\}$ для некоторой $H \leq D/L$. Если $\pi(X) = H \setminus \{e\}$, то X содержит все элементы порядка 3, отличные от q и q^2. Следовательно, L — единственная минимальная $\mathcal{A}$-подгруппа, противоречие. Таким образом, $\pi(X)$ и X регулярны. Поскольку $LX = X$, мы заключаем, что $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$ и утверждение 2 леммы выполнено. □

Из утверждения 2 леммы 3.4.5 вытекает, что

$$\bigcup_{X\in\mathcal{S}(\mathcal{A})_{D\setminus V}} tr(X) = D \setminus D_m$$

для некоторого $m \geq 1$. Поэтому $V = D_m$ — $\mathcal{A}$-подгруппа.

Лемма 3.4.6. *Пусть* $X, Y \in \mathcal{S}(\mathcal{A})_{D\setminus V}$. *Тогда* $\mathrm{rad}(X) = \mathrm{rad}(Y)$.

Доказательство. Предположим противное. Тогда по лемме 3.4.5 без ограничения общности можно считать, что $\mathrm{rad}(X) = \{e, b, b^2\} = B$ и $\mathrm{rad}(Y) = \{e, ba_1, ba_1^2\}$. Значит,

$$X = X_{0e} \cup bX_{0e} \cup b^2X_{0e},\ Y = Y_{0e} \cup ba_1Y_{0e} \cup b^2a_1^2Y_{0e}.$$

Множества X_{0e} и Y_{0e} регулярны и непусты по утверждению 2 леммы 3.4.5. Следовательно, X_{0e} и Y_{0e} являются орбитами некоторой группы $K \leq \mathrm{Aut}(A)$ по лемме 1.7.2. Более того, $\mathrm{rad}(X_{0e}) = \mathrm{rad}(Y_{0e}) = e$, так как иначе $\mathrm{rad}(X)$ или $\mathrm{rad}(Y)$ содержит как минимум девять элементов, что противоречит утверждению 1 леммы 3.4.5. Рассмотрим базисные множества $\pi(X)$ и $\pi(Y)$ циркулянтного S-кольца $\mathcal{A}_{D/B}$, где $\pi : D \to D/B$ — естественный гомоморфизм. Радикал множества $\pi(X) = X_{0e}$ тривиален, радикал множества $\pi(Y)$ содержит $\pi(ba_1)$. Это противоречит лемме 1.7.4, примененной к S-кольцу $\pi(\mathcal{A}_{\langle X\rangle})$ и $\mathcal{A}$-секции $\pi(\langle Y\rangle)$. □

Лемма 3.4.7. *Радикал S-кольца $\mathcal{A}_V$ тривиален. В частности, $U = V$.*

Доказательство. Пусть X — старшее базисное множество S-кольца $\mathcal{A}_V$. Поскольку $V \neq D$, существует $Y \in \mathcal{S}(\mathcal{A})_{D\setminus V}$ такое, что $X \cap Y^3 \neq \varnothing$. Более того, $X \subset Y^3$, потому что Y^3 — $\mathcal{A}$-множество. По лемме 3.4.5 без ограничения общности можно считать, что $Y = Y_{0e} \cup bY_{0e} \cup b^2Y_{0e},\ \mathrm{rad}(Y) = B,\ \mathrm{rad}(Y_{0e}) = e$. Тогда $Y^3 = BY_{0e}^3$. Поскольку Y_{0e} непусто и регулярно по лемме 3.4.5, из леммы 1.7.2 следует, что множество Y_{0e} является орбитой некоторой $K \leq \mathrm{Aut}(A)$. Поэтому лемма 1.7.3 влечет, что $Y_{0e} = \{y\}$ или $Y_{0e} = \{y, y^{-1}\}$. Значит, Y^3 имеет один из двух видов:

$$\{y^3, by^3, b^2y^3\},$$

$$\{y, by, b^2y, y^{-1}, by^{-1}, b^2y^{-1}, y^3, by^3, b^2y^3, y^{-3}, by^{-3}, b^2y^{-3}\}.$$

Поскольку $X \subset V$, мы заключаем, что $\mathrm{rad}(X) = e$ или $a_1 \in \mathrm{rad}(X)$. Покажем, что последнее невозможно. Это очевидно, если Y^3 имеет первый вид. Если Y^3 имеет второй вид и $a_1 \in \mathrm{rad}(X)$, то легко проверить, что $y = a_1$ или $y = a_1^2$. Однако, $y \notin V$. Это противоречит тому, что $E \subseteq V$. Таким образом, $\mathrm{rad}(X) = e$ и $\mathrm{rad}(\mathcal{A}_V) = e$. □

Для завершения доказательства предложения 3.4.1 предположим, что $L = \mathrm{rad}(X),\ X \in \mathcal{S}(\mathcal{A})_{D\setminus V}$. По лемме 3.4.5 группа L не зависит от выбора X. Тогда $\mathcal{A}$ является V/L-сплетением. Поскольку $\mathrm{rad}(\mathcal{A}_V) = e$ и $|L| = 3$, предложение 3.4.1 выполнено. □

§ 3.5. Доказательство теоремы 3

Будем вести доказательство теоремы индукцией по k. Утверждение теоремы для $k \leq 3$ следует из вычислений в групповом кольце группы D, выполненных при помощи пакета COCO2P [18]. Пусть $k \geq 4$ и $\mathcal{A}$ — S-кольцо над D. Покажем, что $\mathcal{A}$ шурово. Если $\mathrm{rad}(\mathcal{A}) = e$, то по предложениям 3.2.1 и 3.3.1 либо $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, где $\mathrm{rk}(\mathcal{A}_H) = 2$ и $|L| \leq 3 \leq |H|$, либо $\mathcal{A}$ циклотомическое. В первом случае шуровость S-кольца $\mathcal{A}$ следует из шуровости S-колец $\mathcal{A}_H$ и $\mathcal{A}_L$ и леммы 1.6.2; во втором случае шуровость $\mathcal{A}$ очевидна.

Предположим, что $\mathrm{rad}(\mathcal{A}) > e$. Тогда из предложения 3.4.1 следует, что $\mathcal{A}$ является собственным U/L-сплетением для некоторой $\mathcal{A}$-секции U/L, и выполнено одно из следующих утверждений:

1) $|U/L| = 1$,

2) $|U/L| = 3$,

3) $\mathrm{rad}(\mathcal{A}_U) = e$ и $|L| = 3$.

Покажем, что во всех этих случаях $\mathcal{A}$ шурово. Если U — циклическая группа, то $\mathcal{A}_U$ шурово по лемме 1.7.1, иначе $\mathcal{A}_U$ шурово по предположению индукции. Аналогично $\mathcal{A}_{D/L}$ шурово по лемме 1.7.1, если D/L — циклическая группа, и по предположению индукции иначе. Значит, по лемме 1.6.5 достаточно доказать, что $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной. Очевидно, $\mathrm{Aut}(\mathcal{A}_{U/L})$ является 2-изолированной, если $|U/L| = 1$ или $|U/L| = 3$. Следовательно, можно считать, что $|U/L| \geq 9$. Пусть $\mathrm{rad}(\mathcal{A}_U) = e$ и $|L| = 3$. Если U циклическая, то из леммы 1.7.2 и из леммы 1.7.3 вытекает, что каждое базисное множество $\mathcal{A}_U$ имеет вид $\{x\}$ или каждое базисное множество $\mathcal{A}_U$ имеет вид $\{x, x^{-1}\}$. В этих случаях $\mathrm{Aut}\left(\mathcal{A}_{U/L}\right)_L$ имеет точную регулярную орбиту. Значит, $\mathrm{Aut}\left(\mathcal{A}_{U/L}\right)$ является 2-изолированной по лемме 1.5.9. Таким образом, можно считать, что $U = D_m$, где $m < k$. Поскольку L — $\mathcal{A}$-подгруппа порядка 3, мы заключаем, что $\mathrm{rk}(\mathcal{A}_U) > 2$.

Предположим, что $\mathcal{A}_U$ нерегулярно. Тогда предложение 3.2.1 влечет, что $\mathcal{A}_U = \mathcal{A}_H \otimes \mathcal{A}_L$, где H — $\mathcal{A}_U$-подгруппа и $\mathrm{rk}(\mathcal{A}_H) = 2$. Если $\mathrm{rk}(\mathcal{A}_L) = 2$, то

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

Если $\mathrm{rk}(\mathcal{A}_L) = 3$, то

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

Заметим, что D/L циклическая и U/L — $\mathcal{A}_{D/L}$-секция составного порядка. Из [6, теорема 4.6] следует, что $\mathrm{Aut}(\mathcal{A}_{D/L})^{U/L} = \mathrm{Sym}(U/L)$. Значит, $\mathcal{A}$ шурово по лемме 1.6.4 примененной к $\Delta_0 = \mathrm{Aut}(\mathcal{A}_{D/L})$ и $\Delta_1 = \mathrm{Aut}(\mathcal{A}_U)$. Таким образом, по предложению 3.2.1 можно считать, что $\mathcal{A}_U$ регулярно.

Из предложения 3.3.1 следует, что $\mathcal{A}_U \cong_{\mathrm{Cay}} \mathrm{Cyc}(K, U)$, где K — одна из групп $K_0 - K_9$ из таблицы 2. Если $\mathcal{A}_U \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_i, U),\ i \in \{0, 1, 2, 3, 4, 5\}$, то группа $\mathcal{A}_{U/L}$ является 2-изолированной по лемме 3.3.4.

Лемма 3.5.1. *Пусть $\mathcal{A}_U \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_i, U)$, где $i \in \{6, 7, 8, 9\}$. Тогда найдется $\mathcal{A}$-секция U_1/L_1 такая, что $\mathcal{A}$ —собственное U_1/L_1-сплетение и $\mathrm{Aut}(\mathcal{A}_{U_1/L_1})$ — 2-изолированная.*

Доказательство. Если $\mathcal{A}_U \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_i, U),\ i \in \{6, 7, 8, 9\}$, то A_1 — единственная минимальная $\mathcal{A}$-подгруппа порядка 3 и, следовательно, $L = A_1$. Кроме того, для любого множества $X \in \mathcal{S}(\mathcal{A}_U)$ выполнено $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$. Покажем, что группа $H = \mathrm{rad}(\mathcal{A})$ нециклическая. Предположим противное. Заметим, что $A_1 \leq H < U$. Первое неравенство выполнено, потому что иначе H является $\mathcal{A}$-подгруппой порядка 3, отличной от A_1. Второе неравенство выполнено, потому что иначе $X \subseteq H$ для некоторого старшего базисного множества $X \in \mathcal{S}(\mathcal{A}_U)$ и H не может быть циклической, так как $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$. Далее, группа D/H изоморфна D_l, где $l < k$. Заметим, что $\mathcal{A}_{D/H}$ имеет тривиальный радикал, потому что иначе H не является радикалом S-кольца $\mathcal{A}$. Группа $\widetilde{E} = \{x \in D/H : |x| = 3\}$ является $\mathcal{A}_{D/H}$-подгруппой, так как каждое базисное множество $\mathcal{A}_{U/H}$ регулярно и U/H содержит все элементы порядка 3. Поэтому из предложения 3.2.1, примененной к $D/H \cong D_l$, следует, что $\mathcal{A}_{D/H}$ регулярно. Тогда по лемме 3.3.3 существует циклическая $\mathcal{A}_{D/H}$-подгруппа порядка 3^{l-1}. Это противоречит тому, что $X_{0e} \neq \varnothing,\ X_{1b} \neq \varnothing,\ X_{2b^2} \neq \varnothing$ для всех старших базисных множеств $\mathcal{A}_{U/H}$. Таким образом, H нециклическая и, следовательно, D/H циклическая.

Поскольку H нециклическая, существует старшее базисное множество $X \in \mathcal{S}(\mathcal{A})$ такое, что $b \in \mathrm{rad}(X)$. По лемме 1.5.4 каждое базисное множество $\mathcal{A}$ рационально сопряжено с X и $\mathrm{rad}(Y) = H$ для любого старшего базисного множества $Y \in \mathcal{S}(\mathcal{A})$. Значит, $\mathcal{A}_{D/H}$ циркулянтно и $|\mathrm{rad}(\mathcal{A}_{D/H})| = 1$. Из [6, теорема 4.1, теорема 4.2] следует, что либо $\mathrm{rk}(\mathcal{A}_{D/H}) = 2$, либо $\mathcal{A}_{D/H}$ циклотомическое. В первом случае $\mathcal{A} = \mathcal{A}_H \wr \mathcal{A}_{D/H}$ и утверждение леммы выполнено для $U_1 = L_1 = H$. Во втором случае $\mathcal{A}_{D/H}$ регулярно, а потому D_{k-1} — $\mathcal{A}$-подгруппа, и

из леммы 1.7.7 вытекает, что каждое базисное множество $\mathcal{A}_{D/H}$ имеет вид $\{x\}$ или каждое базисное множество $\mathcal{A}_{D/H}$ имеет вид $\{x, x^{-1}\}$.

Поскольку $H \leq D_{k-1}$ и $\mathrm{rad}(Y) = H$ для любого старшего базисного множества $Y \in \mathcal{S}(\mathcal{A})$, мы заключаем, что $\mathcal{A}$ является D_{k-1}/H-сплетением. Базисные множества циркулянтного S-кольца $\mathcal{A}_{D_{k-1}/H}$ имеют вид $\{x\}$ или $\{x, x^{-1}\}$. Таким образом, $\mathrm{Aut}(\mathcal{A}_{D_{k-1}/H})_H$ имеет точную регулярную орбиту. Следовательно, $\mathrm{Aut}(\mathcal{A}_{D_{k-1}/H})$ является 2-изолированной по лемме 1.5.9. Утверждение леммы выполнено для $U_1 = D_{k-1}$ и $L_1 = H$. □

Поскольку $\mathcal{A}$ — собственное U_1/L_1-сплетение, S-кольца $\mathcal{A}_{U_1}$ и $\mathcal{A}_{D/L_1}$ шуровы по лемме 1.7.1 или по предположению индукции. В силу того, что $\mathrm{Aut}(\mathcal{A}_{U_1/L_1})$ 2-изолированная, $\mathcal{A}$ шурово по лемме 1.6.5. Теорема 3 доказана.

4. Отделимость S-колец над $C_2 \times C_{2^k}$ и $C_3 \times C_{3^k}$

В данной главе изучается вопрос об отделимости S-колец над группами $C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$. Основным результатом данной главы является следующая теорема.

Теорема 5. Группы $D = C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$, отделимы относительно класса всех конечных абелевых групп.

Из теоремы 5 и предложения 1.9.2 вытекает

Следствие 2. *Пусть группа $D \cong C_p \times C_{p^k}$ порядка n, 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* $\mathrm{poly}(n)$.

§ 4.1. Вспомогательные результаты

Пусть $p \in \{2, 3\}$ и $k \geq 1$. На протяжении данной главы используются следующие обозначения. 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 $a_2 = a^{p^{k-2}}$. Положим $A_1 = \langle a_1 \rangle$ и $A_2 = \langle a_2 \rangle$. Обозначим через E элементарную абелеву группу $A_1 \times B$. Если $T \subseteq D$ и $m \leq k$, то множество $\{t \in T : |t| \leq p^m\}$ обозначается через T_m. В этих обозначениях $D = D_k$, $A = A_k$, $E = D_1$.

Лемма 4.1.1. *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 $D' \cong C_{q^2} \times C_{q^{m-1}}$.

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 $|W'_{H'}| = q$, потому что $|W' \cap A'| = q$. Поскольку W' нециклическая, $|W'_{A'}| = q$. Следовательно, $W' = W'_{H'} \times W'_{A'} \cong C_q \times C_q$. Поэтому D'/W' нециклическая, противоречие. Таким образом, $D' \cong C_q \times C_{q^m}$. □

Лемма 4.1.2. *Пусть $\mathcal{A}$ — S-кольцо над D, для которого выполнено утверждение 2 леммы 1.8.1 в случае $p = 2$ и утверждение 2 теоремы 2 в случае $p = 3$. Тогда найдется $\mathcal{A}$-секция U_1/L_1 такая, что $\mathcal{A}$ — собственное U_1/L_1-сплетение и $\mathrm{Aut}(\mathcal{A}_{U_1})^{U_1/L_1} = \mathrm{Aut}(\mathcal{A}_{U_1/L_1})$.*

Доказательство. Для доказательства леммы покажем, что найдется $\mathcal{A}$-секция U_1/L_1 такая, что $\mathcal{A}$ — собственное U_1/L_1-сплетение и либо $\mathrm{Aut}(\mathcal{A}_{U_1/L_1})$ является 2-изолированной, либо $\mathrm{Aut}(\mathcal{A}_{U_1/L_1}) = \mathrm{Sym}(U_1/L_1) = \mathrm{Aut}(\mathcal{A}_{U_1})^{U_1/L_1}$. В первом случае $\mathrm{Aut}(\mathcal{A}_{U_1})^{U_1/L_1} = \mathrm{Aut}(\mathcal{A}_{U_1/L_1})$, потому что $\mathrm{Aut}(\mathcal{A}_{U_1/L_1}) \approx_2 \mathrm{Aut}(\mathcal{A}_{U_1})^{U_1/L_1}$ и $\mathcal{A}_{U_1/L_1}$ шурово (см. доказательство леммы 1.7.8).

Пусть U/L — $\mathcal{A}$-секция из утверждения 2 леммы 1.8.1 в случае $p = 2$ и утверждения 2 теоремы 2 в случае $p = 3$. 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 1.8.1 в случае $p = 2$ и по теореме 2 в случае $p = 3$ можно считать, что $|U/L| \geq p^2$, $\mathrm{rad}(\mathcal{A}_U) = e$ 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 1.7.7. 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 1.7.7, 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 лемме 1.5.9.

Предположим теперь, что U нециклическая. Тогда $U \cong D_l$ для некоторого $l \leq k$ и для $\mathcal{A}_U$ выполнено одно из утверждений 1,3 леммы 1.8.1, если $p = 2$, и леммы **??**, если $p = 3$. Пусть $\mathcal{A}_U$ регулярно. Если $p = 2$, то $\mathrm{Aut}(\mathcal{A}_{U/L})$ — 2-изолированная по [7, теорема 8.1]. Если $p = 3$ и $\mathcal{A}_U \cong \mathrm{Cyc}(K, D)$, где K — одна из групп $K_0 - K_5$ из таблицы 2, то $\mathrm{Aut}(\mathcal{A}_{U/L})$ — 2-изолированная по лемме 3.3.4. Во всех рассмотренных выше случаях утверждение леммы

выполнено для $U_1 = U$ и $L_1 = L$.

Если $p = 3$ и $\mathcal{A}_U \cong \mathrm{Cyc}(K, D)$, где K — одна из групп $K_6 - K_9$ из таблицы 2, то по лемме 3.5.1 найдется $\mathcal{A}$-секция U_1/L_1 такая, что $\mathcal{A}$ —собственное U_1/L_1-сплетение и $\mathrm{Aut}(\mathcal{A}_{U_1/L_1})$ — 2-изолированная.

Если $\mathcal{A}_U$ нерегулярно, то из леммы 1.8.1 в случае $p = 2$ и из теоремы 2 в случае $p = 3$ 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 $\mathrm{Aut}(\mathcal{A}_{U/L}) = \mathrm{Sym}(U/L) = \mathrm{Aut}(\mathcal{A}_U)^{U/L}$, и утверждение леммы выполнено для $U_1 = U$ и $L_1 = L$. □

§ 4.2. Доказательство теоремы 5

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. Для $\mathcal{A}$ выполнено одно из утверждений 1-3 леммы 1.8.1, если $p = 2$, и одно из утверждений 1-3 теоремы 2, если $p = 3$.

Будем вести доказательство индукцией по k. Пусть $k = 1$. Если $\mathrm{rk}(\mathcal{A}) = 2$, то $\mathcal{A}$, очевидно, отделимо. Если $\mathcal{A}$ является тензорным произведением двух S-колец над циклическими группами порядка p, то $\mathcal{A}$ отделимо по лемме 1.6.3 и лемме 1.7.9. Если $\mathcal{A}$ является U/L-сплетением, то $U = L$ и $|U| = |G/L| = p$, так как $k = 1$. В этом случае $\mathcal{A}$ отделимо по предложению 1.6.9, лемме 4.1.2, и лемме 1.7.9. Если $\mathcal{A} = \mathbb{Z}D$, то, очевидно, $\mathcal{A}$ отделимо. Если $p = 3$ и $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_4, D)$, где K_4 — группа из таблицы 2, то $\mathcal{A}$ удовлетворяет условиям леммы 1.5.11 и, следовательно, отделимо.

Осталось рассмотреть случай, когда $p = 3$ и $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_{10}, D)$, где K_{10} — группа из таблицы 2. В этом случае $|D'| = |D| = 9$ и $\mathrm{rk}(\mathcal{A}') = \mathrm{rk}(\mathcal{A}) = 3$. Из (1.3) следует, что $\mathrm{rad}(\mathcal{A}')$ тривиален, поскольку $\mathrm{rad}(\mathcal{A}) = e$. Если D' циклическая, то по лемме 1.7.7 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 теоремы 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 $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}$. 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 $k \geq 2$. Если $\mathrm{rk}(\mathcal{A}) = 2$, то, очевидно, $\mathcal{A}$ отделимо. Каждое S-кольцо над группой порядка p, где $p \in \{2, 3\}$, отделимо по лемме 1.7.9. Поэтому если $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, где $\mathrm{rk}(\mathcal{A}_H) = 2$ и $|L| = p$, то $\mathcal{A}$ отделимо по лемме 1.6.3.

Предположим, что для $\mathcal{A}$ выполнено утверждение 2 леммы 1.8.1 в случае $p = 2$ и утверждение 2 теоремы 2 в случае $p = 3$. Ввиду леммы 4.1.2 можно считать, что $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$. Тогда по предложению 1.6.9 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 1.7.9. Аналогично, $\mathcal{A}_{D/L}$ отделимо по предположению индукции, если D/L нециклическая, и по по лемме 1.7.9, если D/L циклическая.

Предположим, что для $\mathcal{A}$ выполнено утверждение 3 леммы 1.8.1 в случае $p = 2$ и утверждение 3 теоремы 2 в случае $p = 3$. Тогда $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K, D)$, где $K \leq \mathrm{Aut}(D)$ — одна из групп, представленных в таблице 1 для $p = 2$, и одна из групп $K_0 - K_9$, представленных 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 1.5.11. 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 1.5.11 и лемме 1.6.3.

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 4.2.1. *Верно, что* $D' \cong D$.

Доказательство. Пусть $p = 2$. Проверим, что для D' выполнены условия леммы 4.1.1.

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 1.7.5 вытекает, что F^φ — циклическая подгруппа группы 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 S-кольца $\mathcal{A}$. 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

$$|\pi(X)| = 4,\ \pi(X) = \pi(X)^{-1},\ |\operatorname{rad}(\pi(X))| = 2. \tag{4.1}$$

Пусть

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

— алгебраический изоморфизм, индуцированный φ. Из (1.3) следует, что $\pi(X)^{\varphi_{D/A_1}}$ — порождающее множество группы D'/A_1^φ и (4.1) 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^φ порождается не более, чем двумя элементами, один из которых имеет порядок 2. Заметим, что D'/A_1^φ нециклическая, потому что она содержит как минимум две подгруппы A_2^φ/A_1^φ и E^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 4.1.1.

Пусть $p = 3$. Предположим, что $k = 2$. Компьютерные вычисления с использованием пакета COCO2P [18] показывают, что над группами C_{27} и C_3^3 нет S-колец с такими же тензорами структурных констант, как у одного из S-колец $\operatorname{Cyc}(K_6, D)$, $\operatorname{Cyc}(K_7, D)$, $\operatorname{Cyc}(K_8, D)$, $\operatorname{Cyc}(K_9, D)$. Значит, если $k = 2$, то $D' \cong D \cong C_3 \times C_9$. Далее мы считаем, что $k \geq 3$. Проверим, что для D' выполнятеся лемма 4.1.1.

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 $\mathcal{A}_{A_{k-1}} = \operatorname{Cyc}(M, A_{k-1})$, 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 1.7.5 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 S-кольца $\mathcal{A}$. 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,

$$|\pi(X)| = 3,\ |\operatorname{rad}(\pi(X))| = 3, \tag{4.2}$$

если $K \in \{K_6, K_7\}$, и

$$|\pi(X)| = 6,\ \pi(X) = \pi(X)^{-1},\ |\operatorname{rad}(\pi(X))| = 3, \tag{4.3}$$

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}, (4.2) выполняется для $\pi(X)^{\varphi_{D/A_1}}$, если $K \in \{K_6, K_7\}$, и (4.3) 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 $A_2^{\varphi}/A_1^{\varphi}$ и $E^{\varphi}/A_1^{\varphi}$ порядка 3. Из этого следует, что $D'/A_1^{\varphi} \cong C_3 \times C_{3^{k-1}}$.

В силу леммы 4.1.1 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 4.1.1. Пусть теперь $k = 3$. Положим $E' = \{x \in D' : |x| = 3\}$. Ясно, что $|E'| = 9$. Предположим, что E' — $\mathcal{A}'$-подгруппа. Тогда $E' = E^{\varphi}$ или $E' = A_2^{\varphi}$, так как только E и A_2 являются $\mathcal{A}$-подгруппами порядка 9. Однако, A_2^{φ} циклическая по лемме 1.7.5. Значит, $E' = E^{\varphi}$. Группа D/E циклическая, $\mathcal{A}_{D/E} = \mathbb{Z}(D/E)$ или $\mathcal{A}_{D/E} = \operatorname{Cyc}(M, D/E)$, где $M = \{\varepsilon, \sigma\},\ \sigma : x \to x^{-1}$. В силу леммы 1.7.5 группа D'/E' также циклическая. Заметим, что $|E \cap A_2| = 3$ и, следовательно, $|E' \cap A_2^{\varphi}| = 3$. Таким образом, $D' \cong D \cong C_3 \times C_9$ по лемме 4.1.1.

Предположим, что $D' \cong C_9 \times C_9$. Тогда по доказанному выше E' 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 $E' \subset D_2^{\varphi}$. Пусть $X \subseteq D \setminus D_2$ — старшее базисное множество S-кольца $\mathcal{A}$. 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 $|xE^{'} \cap X^{\varphi}| = 3$, где $x^{'} \in X^{\varphi}$. Если $|X^{\varphi}| = 3$, то $Y^{'} = X^{\varphi}(X^{\varphi})^{-1}$ является $\mathcal{A}^{'}$-множеством, и $Y^{'} \subseteq E^{'}$. Более того, $Y^{'} \not\subseteq A_1^{\varphi}$, так как иначе $\mathrm{rad}(X^{\varphi}) = A_1^{\varphi}$. Следовательно, $E^{'} = \langle A_1^{\varphi}, Y^{'} \rangle$ является $\mathcal{A}^{'}$-подгруппой, противоречие с предположением. Пусть $|X^{\varphi}| = 6$. Если $((x^{'})^2 \cup (x^{'})^{-2})E^{'} \cap D_2^{\varphi} \neq \varnothing$, то $((x^{'})^2 \cup (x^{'})^{-2})E^{'} \subset D_2^{\varphi}$ и, следовательно, $x^{'} \in D_2^{\varphi}$. С другой стороны, $x^{'} \in D^{'} \setminus D_2^{\varphi}$, противоречие. Таким образом, $((x^{'})^2 \cup (x^{'})^{-2})E^{'} \cap D_2^{\varphi} = \varnothing$. Из этого вытекает, что $Y^{'} = X^2 \cap D_2^{\varphi}$ является $\mathcal{A}^{'}$-множеством, и $Y^{'} \subseteq E^{'}$. Заметим, что $Y^{'} \not\subseteq A_1^{\varphi}$, потому что иначе $\mathrm{rad}(X^{\varphi}) = A_1^{\varphi}$. Мы заключаем, что $E^{'} = \langle A_1^{\varphi}, Y^{'} \rangle$ — $\mathcal{A}^{'}$-подгруппа, противоречие. Значит, $|xE^{'} \cap X^{\varphi}| \neq 3$ для любого старшего базисного множества $X \in \mathcal{S}(\mathcal{A})$. Тогда $Y^{'} = (X^{\varphi})^{[3]}$ является $\mathcal{A}^{'}$-множеством по лемме 1.5.5. Так как $D^{'} \cong C_9 \times C_9$, мы получаем, что $Y^{'} \subseteq E^{'}$. Если $Y^{'} \not\subseteq A_1^{\varphi}$, то $E^{'} = \langle A_1^{\varphi}, Y^{'} \rangle$ — $\mathcal{A}^{'}$-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 4.2.2. *Верно, что* $\mathcal{A}^{'} \cong_{\mathrm{Cay}} \mathcal{A}$.

Доказательство. Для $\mathcal{A}^{'}$ выполняется одно из утверждений леммы 1.8.1, если $p = 2$, и одно из утверждений теоремы 2, если $p = 3$. Поскольку $\mathrm{rad}(\mathcal{A})$ тривиален, из (1.3) следует, что $\mathrm{rad}(\mathcal{A}^{'})$ также тривиален. Значит, утверждение 2 леммы 1.8.1 в случае $p = 2$ и утверждение 2 теоремы 2 в случае $p = 3$ для $\mathcal{A}^{'}$ не выполняется. Ясно, что $|\mathcal{S}(\mathcal{A}^{'})| = |\mathcal{S}(\mathcal{A})| > 6$. Следовательно, утверждение 1 леммы 1.8.1 в случае $p = 2$ и утверждение 1 теоремы 2 в случае $p = 3$ для $\mathcal{A}^{'}$ тоже не выполняется. Таким образом, для $\mathcal{A}^{'}$ выполняется утверждение 3 леммы 1.8.1 в случае $p = 2$ и утверждение 3 теоремы 2 в случае $p = 3$, то есть $\mathcal{A}^{'} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K^{'}, D)$, где $K^{'} \leq \mathrm{Aut}(D)$ — одна из групп, представленных в таблице 1 для $p = 2$, и одна из групп $K_0 - K_9$, представленных 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, $\mathcal{A}^{'} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_5, D) \cong_{\mathrm{Cay}} \mathcal{A}$. Если $\mathcal{A}$ несимметрично, то $\mathcal{A}^{'}$ тоже несимметрично и $\mathcal{A}^{'} \cong_{\mathrm{Cay}} \mathrm{Cyc}(K_6, D) \cong_{\mathrm{Cay}} \mathcal{A}$.

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 S-кольца $\mathcal{A}$. 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 4.2.3. *Имеют место равенства* $\mathcal{A} = \langle \underline{Y} \rangle$ *и* $\mathcal{A}' = \langle \underline{Y^\varphi} \rangle$.

Доказательство. Положим $\mathcal{A}_1 = \langle \underline{Y} \rangle$. Из леммы 1.8.1 в случае $p = 2$ и из теоремы 2 в случае $p = 3$ 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 1.8.1 в случае $p = 2$ и утверждение 1 теоремы 2 в случае $p = 3$, 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 $k \geq 2$, 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. Поэтому утверждение 2 леммы 1.8.1 в случае $p = 2$ и утверждение 2 теоремы 2 в случае $p = 3$ не выполняется для $\mathcal{A}_1$. Таким образом, $\mathcal{A}_1$ циклотомическое. Из описания всех циклотомических S-колец над D, которое представлено в лемме 1.8.1 для $p = 2$ и в теореме 2 для $p = 3$, 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 (1.3) 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 E. Они являются $\mathcal{A}$-подгруппами. Группа A_2^φ циклическая $\mathcal{A}'$-подгруппа по лемме 1.7.5, и, следовательно, $A_2^\varphi = A_2$. Значит, $E^\varphi = E$. 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 E. Таким образом, если $Y = X \cup Z$, то $Y^\varphi = X^\varphi \cup Z$ или $Y^\varphi = X^\varphi \cup Z^{-1}$. Поскольку $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}$, рассуждениями, аналогичными проведенным выше, можно показать, что $\mathcal{A}' = \langle \underline{Y^\varphi} \rangle$. □

Лемма 4.2.4. *Алгебраический изоморфизм φ индуцируется изоморфизмом Кэли.*

Доказательство. По лемме 4.2.2 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 1.5.4 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 4.2.3. В этих случаях из леммы 1.5.3 следует, что $\varphi = \varphi_{fg}$.

Пусть теперь $p = 3$ и $K \in \{K_6, K_8\}$. Из леммы 4.2.3 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 1.5.3 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 $X^\varphi = \{y, ba_1^2y, b^2y\}$; если $K = K_8$, то $X^\varphi = \{y, y^{-1}, by, ba_1y^{-1}, b^2a_1^2y, b^2y^{-1}\}$, где y — порождающий элемент A. Положим

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

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 1.5.3 следует, что $\varphi = \varphi_{fgh}$, где φ_{fgh} — алгебраический изоморфизм, индуцированный fgh. □

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 5 завершено.

5. Отделимость S-колец над абелевой группой порядка $4p$

В данной главе изучается вопрос об отделимости S-колец над абелевыми группами порядка $4p$. Основным результатом главы является

Теорема 6. Абелева группа порядка $4p$ отделима относительно класса всех конечных абелевых групп для каждого простого числа p.

Из теоремы 6 и предложения 1.9.2 вытекает

Следствие 3. *Пусть абелева группа G порядка $n = 4p$, где p — простое число, задана своей таблицей Кэли. Тогда для графа Кэли Γ над G и графа Кэли Γ' над произвольной абелевой группой изоморфизм между Γ и Γ' может быть проверен за время* $\mathrm{poly}(n)$.

§ 5.1. Структура S-колец над над абелевой группой порядка $4p$

Пусть p — простое число. Положим $D = \langle a\rangle \times \langle b\rangle$, $C = \langle c\rangle$, и $P = \langle z\rangle$, где $|a| = |b| = 2$, $|c| = 4$, и $|z| = p$. Пусть $E \in \{D, C\}$ и $G = E \times P$. На протяжении данного параграфа $\mathcal{A}$ — S-кольцо над G.

Лемма 5.1.1. *Если $p = 2$ и $E = D$, то выполняется одно из следующих утверждений:*

1) $\mathcal{A} = \mathbb{Z}G$;

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

3) *$\mathcal{A}$ является тензорным произведением двух S-колец над собственными подгруппами группы G;*

4) *$\mathcal{A}$ является сплетением двух S-колец над собственными подгруппами группы G.*

Доказательство. Компьютерные вычисления с использованием пакета COCO2P (см. [18]) показывают, что с точностью до изоморфизма Кэли имеется ровно девять S-колец над G. Для каждого из этих девяти S-колец утверждение леммы проверяется непосредственно. □

С этого момента до конца параграфа мы считаем, что $p \geq 3$.

Лемма 5.1.2. *Если E или P не является $\mathcal{A}$-подгруппой, то выполняется одно из следующих утверждений:*

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

2) $\mathcal{A}$ – *собственное* U/L*-сплетение для некоторой* $\mathcal{A}$*-секции* U/L *такой, что* $|U/L| \leq 2$;

3) $E = D$ *и* $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$, *где* H — $\mathcal{A}$*-подгруппа порядка* 2, L — $\mathcal{A}$*-подгруппа порядка* $2p$, *и* $G = H \times L$.

Доказательство. Пусть $\mathcal{A}$ — S-кольцо над G и H — максимальная $\mathcal{A}$-подгруппа в E. Предположим, что $H \neq E$. Тогда в силу [14, лемма 6.2] выполняется одно из следующих утверждений: (1) $\mathcal{A} = \mathcal{A}_H \wr \mathcal{A}_{G/H}$, где $\mathrm{rk}(\mathcal{A}_{G/H}) = 2$; (2) $\mathcal{A}$ является U/L-сплетением, где $P \leq L < G$ и $U = HL$. В первом случае утверждение 1 леммы выполняется, если H тривиальна, и утверждение 2 леммы выполняется, если H нетривиальна. Во втором случае утверждение 2 леммы выполняется, если $U < G$. Предположим, что $U = G$. Тогда $|H| = 2$ и $G = H \times L$. Из этого следует, что $E = D \cong C_2 \times C_2$. Ясно, что $\mathcal{A}_H = \mathbb{Z}H$. Следовательно, $\mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L$ по утверждению 2 леммы 1.6.1 и утверждение 3 леммы выполняется.

Случай, когда P не является $\mathcal{A}$-подгруппой, двойственен к случаю, когда E не является $\mathcal{A}$-подгруппой, в смысле теории двойственности S-колец над абелевыми группами, см. [10, § 2.2]. Таким образом, если P не является $\mathcal{A}$-подгруппой, то утверждение леммы следует из [10, теорема 2.4, утверждение 2 теоремы 2.5]. □

Далее до конца этого параграфа будем считать, что E и P являются $\mathcal{A}$-подгруппами.

Лемма 5.1.3. *Если* $X, Y \in \mathcal{S}(\mathcal{A})$ *и* $X_E = Y_E$, *то* X *и* Y *рационально сопряжены.*

Доказательство. Утверждение леммы следует из леммы 1.5.4, так как группа $1 \times \mathrm{Aut}(P)$ содержится в центре группы $\mathrm{Aut}(G)$ и $\mathrm{Aut}(P)$ дейтсвует транзитивно на $P^{\#}$. □

Из [10, теорема 5.1] следует, что $\mathcal{A}_P = \mathrm{Cyc}(K, P)$ для некоторой $K \leq \mathrm{Aut}(P)$. Поскольку $|P| = p$, группа $\mathrm{Aut}(P)$ циклическая и, следовательно, K тоже циклическая. Пусть θ — элемент, порождающий группу K. Легко проверяется, что либо $\mathcal{A}_E = \mathbb{Z}E$, либо $\mathcal{A}_E = \mathbb{Z}C_2 \wr \mathbb{Z}C_2$, либо $\mathrm{rk}(\mathcal{A}_E) = 2$. Если $E = C$ и $\mathrm{rk}(\mathcal{A}_E) = 2$, то $\mathcal{A}_E$ не является циклотомическим, потому что в этом случае $E^{\#} \in \mathcal{S}(\mathcal{A}_E)$ и $E^{\#}$ содержит элементы порядков 2 и 4. В остальных случаях прямая проверка показывает, что $\mathcal{A}_E \cong_{\mathrm{Cay}} \mathrm{Cyc}(\langle\sigma\rangle, E)$, где $\sigma \in \mathrm{Aut}(E)$ либо тривиален, либо совпадает с одним из автоморфизмов, представленных в таблице 3.

E	σ	$\lvert\sigma\rvert$	$\mathcal{A}_E$
D	$\sigma_1 : (a, b) \to (b, ab)$	3	$\mathrm{rk}(\mathcal{A}_E) = 2$
D	$\sigma_2 : (a, b) \to (b, a)$	2	$\mathbb{Z}C_2 \wr \mathbb{Z}C_2$
C	$\sigma_3 : c \to c^{-1}$	2	$\mathbb{Z}C_2 \wr \mathbb{Z}C_2$

Таблица 3.

Пусть $U = \langle u \rangle$ и $V = \langle v \rangle$ — циклические группы и $|U|$ делит $|V|$. Тогда V содержит единственную подгруппу W индекса $|U|$. Пусть $\pi : V \to V/W$ — естественный гомоморфизм и $\psi : U \to V/W$ — изоморфизм. Мы можем построить подпрямое произведение $A(U, V, \psi)$ групп U и V следующим образом:

$$A(U, V, \psi) = \{(x, y) \in U \times V | x^{\psi} = y^{\pi}\}.$$

Из определения $A(U, V, \psi)$ следует, что

$$|A(U, V, \psi)| = |V|. \tag{5.1}$$

Назовем подпрямое произведение двух групп *нетривиальным*, если оно не совпадает с их прямым произведением.

Предположим, что $|\sigma|$ делит $|K|$. Обозначим подгруппу индекса $|\sigma|$ группы K через M. Положим

$$\psi : \sigma^i \to M\theta^i, \ i = 0, \ldots, |\sigma| - 1.$$

Ясно, что ψ — изоморфизм из $\langle \sigma \rangle$ в K/M.

Лемма 5.1.4. *Если* $\mathcal{A} \neq \mathcal{A}_E \otimes \mathcal{A}_P$, *то* $\mathcal{A}_E \cong_{\mathrm{Cay}} \mathrm{Cyc}(\langle \sigma \rangle, E)$, $|\sigma|$ *делит* $|K|$, *и* $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(A(\langle \sigma \rangle, K, \psi), G)$, *где* $\sigma \in \mathrm{Aut}(E)$ *один из автоморфизмов, представленных в таблице 3.*

Доказательство. Если $\mathcal{A}_E = \mathbb{Z}E$, то $\mathcal{A} = \mathcal{A}_E \otimes \mathcal{A}_P$ по утверждению 2 леммы 1.6.1, и мы получаем противоречие с предположением леммы. Значит,

$$\mathcal{A}_E = \mathbb{Z}C_2 \wr \mathbb{Z}C_2 \text{ или } \mathrm{rk}(\mathcal{A}_E) = 2.$$

Докажем, что $\mathcal{A} = \mathrm{Cyc}(A', G)$ для некоторой $A' \leq \mathrm{Aut}(G)$. Если $E = D$, то это следует из [14, сс.15-16]. Пусть $E = C$. Заметим, что $\mathcal{A}$ не может быть собственным обобщенным сплетением двух S-колец, потому что E и P являются $\mathcal{A}$-подгруппами. Поскольку $\mathcal{A} \neq \mathcal{A}_E \otimes \mathcal{A}_P$, мы заключаем по [6, теорема 4.1, теорема 4.2], что $\mathcal{A} = \mathrm{Cyc}(A', G)$ для некоторой $A' \leq \mathrm{Aut}(G)$.

Ясно, что $\mathcal{A}_E$ циклотомическое. Мы можем считать, что $\mathcal{A}_E = \mathrm{Cyc}(\langle \sigma \rangle, E)$, где $\sigma \in \{\sigma_1, \sigma_2, \sigma_3\}$. В силу того, что $\mathcal{A}_E = \mathrm{Cyc}((A')^E, E)$, $\mathcal{A}_P = \mathrm{Cyc}((A')^P, P)$, и $\mathcal{A} \neq \mathcal{A}_E \otimes \mathcal{A}_P$, группа A' является нетривиальным подпрямым произведением групп $\langle \sigma \rangle$ и K. Если $|K|$ не делится на $|\sigma|$, то не существует нетривиальных подпрямых произведений групп $\langle \sigma \rangle$ и K, так как $|\sigma| \in \{2, 3\}$. Значит, $|\sigma|$ делит $|K|$. Если $|\sigma| = 2$, то $A(\langle \sigma \rangle, K, \psi)$ — единственное нетривиальное подпрямое произведение групп $\langle \sigma \rangle$ и K. Поэтому $A' = A(\langle \sigma \rangle, K, \psi)$ и утверждение леммы выполняется.

Предположим, что $|\sigma| = 3$. Тогда $\sigma = \sigma_1$, $E = D$, и $\mathrm{rk}(\mathcal{A}_E) = 2$. В этом случае имеется ровно два нетривиальных подпрямых произведения групп $\langle\sigma\rangle$ и K:

$$A(\langle\sigma\rangle, K, \psi) \text{ и } A(\langle\sigma\rangle, K, \xi),$$

где $\xi : \sigma^i \to M\theta^{-i}$, $i = 0, 1, 2$. Следовательно, $A' \in \{A(\langle\sigma\rangle, K, \psi), A(\langle\sigma\rangle, K, \xi)\}$. Прямая проверка показывает, что для каждой инволюции $\tau \in \mathrm{Aut}(E)$, автоморфизм $\tau \times 1 \in \mathrm{Aut}(E) \times \mathrm{Aut}(P)$ является изоморфизмом Кэли из $A(\langle\sigma\rangle, K, \psi)$ в $A(\langle\sigma\rangle, K, \xi)$. Таким образом, $\mathcal{A} \cong_{\mathrm{Cay}} \mathrm{Cyc}(A(\langle\sigma\rangle, K, \psi), G)$ и утверждение леммы выполняется. □

Для заданной группы $K \leq \mathrm{Aut}(P)$ положим $\mathcal{A}_i(K) = \mathrm{Cyc}(A(\langle\sigma_i\rangle, K, \psi), G)$, где $i \in \{1, 2, 3\}$ и σ_i из таблицы 3. Если $K_1, K_2 \leq \mathrm{Aut}(P)$ и $K_1 \neq K_2$, то $\mathrm{Cyc}(K_1, P) \not\cong_{\mathrm{alg}} \mathrm{Cyc}(K_2, P)$ и, значит, $\mathcal{A}_i(K_1) \not\cong_{\mathrm{alg}} \mathcal{A}_j(K_2)$ для всех $i, j \in \{1, 2, 3\}$.

Лемма 5.1.5. *Пусть $K \leq \mathrm{Aut}(P)$. Тогда $\mathcal{A}_i(K) \not\cong_{\mathrm{alg}} \mathcal{A}_j(K)$ при $i \neq j$.*

Доказательство. Заметим, что для каждого $i \in \{1, 2, 3\}$ группа E — единственная $\mathcal{A}_i(K)$-подгруппа порядка 4, $\mathrm{rk}(\mathcal{A}_1(K)_E) = 2$, и $\mathrm{rk}(\mathcal{A}_2(K)_E) = \mathrm{rk}(\mathcal{A}_3(K)_E) = 3$. Поэтому $\mathcal{A}_1(K) \not\cong_{\mathrm{alg}} \mathcal{A}_2(K)$ и $\mathcal{A}_1(K) \not\cong_{\mathrm{alg}} \mathcal{A}_3(K)$.

Пусть теперь $\mathcal{A}$ и $\mathcal{A}'$ — S-кольца над группами $G = D \times P$ и $G' = C \times P$ соответственно, $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_2(K)$, и $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}_3(K)$. Предположим, что $\mathcal{A} \cong_{\mathrm{alg}} \mathcal{A}'$ и $\varphi : \mathcal{A} \to \mathcal{A}'$ — алгебраический изоморфизм. Тогда D^φ и P^φ — $\mathcal{A}'$-подгруппы порядков 4 и p соответственно. Следовательно, $D^\varphi = C$ и $P^\varphi = P$. Пусть $X \in \mathcal{S}(\mathcal{A})$ такое, что $X \not\subseteq D$ и $X_D = \{a, b\}$. Тогда $X = aX_1 \cup bX_2$, где $X_1, X_2 \subseteq P$. Из утверждения 1 леммы 1.6.1 следует, что $X_P = X_1 \cup X_2 \in \mathcal{S}(\mathcal{A}_P)$. В силу леммы 1.5.4, множество $Y = X_P^{(2)}$ является базисным множеством S-кольца $\mathcal{A}_P$. Ясно, что

$$\underline{X}^2 = \underline{X_1}^2 + \underline{X_2}^2 + 2ab\underline{X_1}\ \underline{X_2}.$$

Поэтому

$$c_{X,X}^{Y} \text{ нечетное.} \tag{5.2}$$

Заметим, что $\langle X\rangle = G$. Значит, $\langle X^\varphi\rangle = G'$ по свойствам алгебраического изоморфизма и, следовательно, $X^\varphi = cX_1' \cup c^{-1}X_2'$, где $X_1', X_2' \subseteq P$. Легко видеть, что

$$(\underline{X}^\varphi)^2 = 2\underline{X_1}'\ \underline{X_2}' + c^2((\underline{X_1}')^2 + (\underline{X_2}')^2).$$

Из этого вытекает, что для каждого $Y' \in \mathcal{S}(\mathcal{A}'_P)$, число $c_{X^\varphi,X^\varphi}^{Y'}$ является четным. С другой стороны, $(Y)^\varphi \in \mathcal{S}(\mathcal{A}'_P)$ и (5.2) влечет, что $c_{X^\varphi,X^\varphi}^{Y^\varphi} = c_{X,X}^{Y}$ нечетное, противоречие. Таким образом, $\mathcal{A} \not\cong_{\mathrm{alg}} \mathcal{A}'$ и лемма доказана. □

Пусть $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_i(K)$ для некоторых $K \leq \mathrm{Aut}(P)$ и $i \in \{1,2,3\}$. Из описания автоморфизмов σ_i, приведенного в таблице 3, следует, что группа $\langle \sigma_i \rangle$ имеет единственную регулярную орбиту $O \in \mathcal{S}(\mathcal{A}_E)$. Следуя [14], будем говорить, что $X \in \mathcal{S}(\mathcal{A})$ *старшее* базисное множество, если X лежит вне $E \cup P$ и $X_E = O$. Старшие базисные множества существуют. Действительно, если $X \in \mathcal{S}(\mathcal{A})$ такое, что $gx \in X$, где $g \in O$ и $x \in P^{\#}$, то X лежит вне $E \cup P$ и $X_E = O$ по утверждению 1 леммы 1.6.1. Значит, X старшее.

Лемма 5.1.6. *Предположим, что $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_i(K)$ для некоторых $K \leq \mathrm{Aut}(P)$ и $i \in \{1,2,3\}$. Тогда выполняется одно из следующих утверждений:*

1) *базисное множество X S-кольца $\mathcal{A}$ старшее тогда и только тогда, когда $\langle X \rangle = G$;*

2) *если $X \in \mathcal{S}(\mathcal{A})$ старшее, то $\mathcal{A} = \langle \underline{X} \rangle$.*

Доказательство. Пусть $O \in \mathcal{S}(\mathcal{A}_E)$ — регулярная орбита группы $\langle \sigma_i \rangle$. Прямая проверка показывает, что $\langle Y \rangle = E$ для $Y \in \mathcal{S}(\mathcal{A}_E)$ тогда и только тогда, когда $Y = O$. Значит, $\langle X \rangle = G$ для $X \in \mathcal{S}(\mathcal{A})$ тогда и только тогда, когда X старшее, и утверждение 1 леммы доказано.

Пусть теперь X — старшее базиное множество S-кольца $\mathcal{A}$ и $\mathcal{B} = \langle \underline{X} \rangle$. Докажем, что $\mathcal{A} = \mathcal{B}$. Ясно, что $\mathcal{A} \geq \mathcal{B}$. С одной стороны, X является объединением некоторых базисных множеств S-кольца $\mathcal{B}$, потому что $\underline{X} \in \mathcal{B}$. С другой стороны, X содержится в некотором базисном множестве S-кольца $\mathcal{B}$, так как $\mathcal{A} \geq \mathcal{B}$. Таким образом, $X \in \mathcal{S}(\mathcal{B})$.

Из леммы 5.1.4 следует, что: 1) $|xE \cap X| = 1$; 2) $|xP \cap X| = |K|/3$ при $i = 1$ и $|xP \cap X| = |K|/2$ при $i \in \{2,3\}$. Следовательно, $O = X^{[p]}$ и $X^{[2]}$ — $\mathcal{B}$-множества по лемме 1.5.5. Из этого вытекает, что $E = \langle O \rangle$ и $P = \langle X^{[2]} \rangle$ — $\mathcal{B}$-подгруппы. Утверждение 1 леммы 1.6.1 влечет, что $X_E, X_P \in \mathcal{S}(\mathcal{B})$, а потому

$$\mathcal{B}_E = \mathcal{A}_E \text{ и } \mathcal{B}_P = \mathcal{A}_P. \tag{5.3}$$

Поскольку $X \in \mathcal{S}(\mathcal{B})$ и $X \neq X_E \times X_P$, мы получаем, что $\mathcal{B} \neq \mathcal{B}_E \otimes \mathcal{B}_P$. Значит, лемма 5.1.4 выполняется для $\mathcal{B}$. Множество X также является старшим базисным множеством S-кольца $\mathcal{B}$. Пусть $Y \in \mathcal{S}(\mathcal{B})$ лежит вне $E \cup P$. Если Y старшее, то $Y = X^{(m)}$ для некоторого m, взаимно простого с $|G|$, по лемме 5.1.3. Следовательно, $Y \in \mathcal{S}(\mathcal{A})$ по лемме 1.5.4. Если Y не старшее, то $Y = Y_E \times Y_P$. В силу (5.3), мы заключаем, что $Y \in \mathcal{S}(\mathcal{A})$. Таким образом $\mathcal{B} = \mathcal{A}$ и утверждение 2 леммы доказано. □

§ 5.2. Доказательство теоремы 6

В данном параграфе сохраняются все обозначения, введенные в предыдущем параграфе. Далее на протяжении данного параграфа для краткости будем писать «отделимо» вместо «отделимо относительно $\mathcal{K}_A$». Мы начинаем доказательство с леммы, из которой следует, что каждая собственная секция группы G отделима.

Лемма 5.2.1. *Группы $C_2 \times C_2$, C_p, и C_{2p}, где p — простое число, отделимы.*

Доказательство. Группы $C_2 \times C_2$, C_p, и C_4 отделимы по теореме 5, [11, теорема 1.3], и лемме 1.7.9 соответственно. Предположим, что $p \neq 2$. Пусть $H = H_1 \times H_2$, где $H_1 \cong C_2$ и $H_2 \cong C_p$, и $\mathcal{B}$ — S-кольцо над H. Если $\mathcal{B}$ циклотомическое, то H_1 и H_2 являются $\mathcal{B}$-подгруппами. Ясно, что $\mathcal{B}_{H_1} = \mathbb{Z}H_1$ и, следовательно, $\mathcal{B} = \mathcal{B}_{H_1} \otimes \mathcal{B}_{H_2}$ по утверждению 2 леммы 1.6.1. Теперь применяя [6, теорема 4.1, теорема 4.2] к H и $\mathcal{B}$, мы получаем, что выполняется одно из следующих утверждений: 1) $\mathrm{rk}(\mathcal{B}) = 2$; 2) $\mathcal{B} = \mathbb{Z}H$; 3) $\mathcal{B} = \mathcal{B}_{H_i} \wr \mathcal{B}_{H/H_i}$, $i \in \{1, 2\}$; 4) $\mathcal{B} = \mathcal{B}_{H_1} \otimes \mathcal{B}_{H_2}$. В первом и втором случаях $\mathcal{B}$, очевидно, отделимо. В третьем случае $\mathcal{B}$ отделимо по предложению 1.6.9. В четвертом случае $\mathcal{B}$ отделимо по лемме 1.6.3. Таким образом, $H = C_{2p}$ отделима и лемма доказана. □

Пусть $\mathcal{A}$ — S-кольцо над G. Докажем, что $\mathcal{A}$ отделимо. Если $p = 2$, то либо $G \cong C_8$, либо $G \cong C_4 \times C_2$, либо $G \cong C_2^3$. В первом случае $\mathcal{A}$ отделимо по лемме 1.7.9. Во втором случае $\mathcal{A}$ отделимо по теореме 5. В третьем случае для $\mathcal{A}$ выполнено одно из утверждений леммы 5.1.1. Если для $\mathcal{A}$ выполнено утверждение 1 или утверждение 2 леммы 5.1.1, то, очевидно, $\mathcal{A}$ отделимо. Если для $\mathcal{A}$ выполнено утверждение 3 леммы 5.1.1, то $\mathcal{A}$ отделимо по лемме 5.2.1 и лемме 1.6.3. Если для $\mathcal{A}$ выполнено утверждение 4 леммы 5.1.1, то $\mathcal{A}$ отделимо по лемме 5.2.1 и предложению 1.6.9.

Пусть теперь $p \geq 3$. Из леммы 5.1.2 и леммы 5.1.4 следует, что либо для $\mathcal{A}$ выполняется одно из утверждений леммы 5.1.2, либо $\mathcal{A} = \mathcal{A}_E \otimes \mathcal{A}_P$, либо $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_i(K)$ для некоторых $K \leq \mathrm{Aut}(P)$ и $i \in \{1, 2, 3\}$. Если $\mathrm{rk}(\mathcal{A}) = 2$, то, очевидно, $\mathcal{A}$ отделимо. Предположим, что для $\mathcal{A}$ выполняется утверждение 2 леммы 5.1.2. В этом случае $\mathcal{A}$ является собственным U/L-сплетением для некоторой $\mathcal{A}$-секции U/L такой, что $|U/L| \leq 2$. Проверим, что для $\mathcal{A}$ выполняются все условия предложения 1.6.9. Из леммы 5.2.1 вытекает, что S-кольца $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ отделимы. С одной стороны, $\mathrm{Aut}(\mathcal{A}_U)^{U/L} \leq \mathrm{Aut}(\mathcal{A}_{U/L})$. С другой стороны, поскольку $|U/L| \leq 2$, мы получаем, что

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

Таким образом, $\mathrm{Aut}(\mathcal{A}_U)^{U/L} = \mathrm{Aut}(\mathcal{A}_{U/L})$ и $\mathcal{A}$ отделимо по предложению 1.6.9. Если для $\mathcal{A}$ выполнено утверждение 3 леммы 5.1.2 или $\mathcal{A} = \mathcal{A}_E \otimes \mathcal{A}_P$, то $\mathcal{A}$ отделимо по лемме 5.2.1 и

лемме 1.6.3.

Отстается рассмотреть случай, когда $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_i(K) = \mathrm{Cyc}(A(\langle\sigma_i\rangle, K, \psi), G)$ для некоторых $K \leq \mathrm{Aut}(P)$ и $i \in \{1, 2, 3\}$. В этом случае $\mathcal{A}_P = \mathrm{Cyc}(K, P)$ и $\mathcal{A}_E \neq \mathbb{Z}E$. Каждое базисное множество S-кольца $\mathcal{A}_P$ имеет мощность $|K|$, потому что K действует полурегулярно на $P^{\#}$. Из (5.1) следует, что $|A(\langle\sigma_i\rangle, K, \psi)| = |K|$, а потому каждое базисное множество S-кольца $\mathcal{A}$ имеет мощность не больше, чем $|K|$.

Пусть $\mathcal{A}'$ — S-кольцо над абелевой группой G' и $\varphi : \mathcal{A} \to \mathcal{A}'$ — алгебраический изоморфизм.

Лемма 5.2.2. *Верно, что* $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}$.

Доказательство. Ясно, что $|G'| = 4p$, $E' = E^{\varphi}$ — $\mathcal{A}'$-подгруппа порядка 4, и $P' = P^{\varphi}$ — $\mathcal{A}'$-подгруппа порядка p. Из свойств алгебраического изоморфизма следует, что каждое базисное множество S-кольца $\mathcal{A}'_{P'}$ имеет мощность $|K|$. Поскольку $\mathcal{A}_E \neq \mathbb{Z}E$, то $\mathcal{A}'_{E'} \neq \mathbb{Z}E'$. Предположим, что $\mathcal{A}' = \mathcal{A}'_{E'} \otimes \mathcal{A}'_{P'}$. Тогда существует $Z' \in \mathcal{S}(\mathcal{A}')$ такое, что $|Z'| \geq 2|K|$, так как $\mathcal{A}'_{E'} \neq \mathbb{Z}E'$. Заметим, что $(Z')^{\varphi^{-1}} \in \mathcal{S}(\mathcal{A})$ и $|(Z')^{\varphi^{-1}}| \geq 2|K|$ ввиду свойств алгебраического изоморфизма. Мы приходим к противоречию, потому что каждое базисное множество S-кольца $\mathcal{A}$ имеет мощность не больше, чем $|K|$. Таким образом, $\mathcal{A}' \neq \mathcal{A}_{E'} \otimes \mathcal{A}_{P'}$. Значит, $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}_j(K)$ для некоторого $j \in \{1, 2, 3\}$ по лемме 5.1.4. Если $i \neq j$, то $\mathcal{A}' \ncong_{\mathrm{alg}} \mathcal{A}$ по лемме 5.1.5, что противоречит нашему предположению. Следовательно, $i = j$ и $\mathcal{A}' \cong_{\mathrm{Cay}} \mathcal{A}$. □

Лемма 5.2.3. *Алгебраический изоморфизм φ индуцируется изоморфизмом Кэли.*

Доказательство. В силу леммы 5.2.2, существует изоморфизм Кэли f из $\mathcal{A}$ в $\mathcal{A}'$. Пусть $X \in \mathcal{S}(\mathcal{A})$ — старшее базисное множество. Тогда $\langle X\rangle = G$ по утверждению 1 леммы 5.1.6. Значит, $\langle X^{\varphi}\rangle = G'$ и $\langle X^{f}\rangle = G'$ по свойствам алгебраического изоморфизма. Ввиду утверждения 1 леммы 5.1.6, множества X^{φ} и X^{f} являются старшими базисными множествами S-кольца $\mathcal{A}'$. Из леммы 5.1.3 вытекает, что X^{φ} и X^{f} рационально сопряжены. Следовательно, существует изоморфизм Кэли f_1 из $\mathcal{A}'$ на себя такой, что $X^{ff_1} = X^{\varphi}$. Изоморфизм Кэли ff_1 из $\mathcal{A}$ в $\mathcal{A}'$ индуцирует алгебраический изоморфизм φ_{ff_1}, и $X^{\varphi_{ff_1}} = X^{ff_1} = X^{\varphi}$. Заметим, что $\mathcal{A} = \langle\underline{X}\rangle$ и $\mathcal{A}' = \langle\underline{X}^{\varphi}\rangle$ по утверждению 2 леммы 5.1.6. Таким образом, $\varphi = \varphi_{ff_1}$ по лемме 1.5.3. □

Мы доказали, что если $\mathcal{A} \cong_{\mathrm{Cay}} \mathcal{A}_i(K)$ для некоторых $K \leq \mathrm{Aut}(P)$ и $i \in \{1, 2, 3\}$, то каждый алгебраический изоморфизм S-кольца $\mathcal{A}$ индуцируется изоморфизмом Кэли. Значит, в этом случае $\mathcal{A}$ отделимо и доказательство теоремы 6 завершено.

Заключение

В диссертации изучались вопросы о шуровости и отделимости S-колец над конечными группами, тесно связанные с проблемой изоморфизма графов Кэли. Вопрос об отделимости S-колец является частным случаем общего вопроса о том, когда комбинаторная структура определяется с точностью до изоморфизма своими параметрами. Были получены следующие результаты.

1. Доказано, что группы $M_{3^k} = \langle a, b : a^{3^{k-1}} = b^3 = e, a^b = a^{3^{k-2}+1} \rangle$, $k \geq 3$, нешуровы.

2. Получено описание всех S-колец над группами $C_3 \times C_{3^k}$, $k \geq 1$; доказана шуровость этих групп.

3. Доказано, что все S-кольца над группами $C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$, и $E_4 \times C_p$, где p — простое число, отделимы относительно класса всех конечных абелевых групп.

Эти результаты завершают классификацию шуровых p-групп нечетного порядка, а также дают первые примеры бесконечных серий нециклических групп, все S-кольца над которыми отделимы. Кроме того, из полученных результатов следует, что изоморфизм двух графов Кэли над каждой из групп $C_p \times C_{p^k}$, где $p \in \{2, 3\}$ и $k \geq 1$, и $E_4 \times C_p$, где p — простое число, может быть проверен за полиномиальное время от порядка группы. Разработанные методы могут быть использованы для дальнейших исследований по теории S-колец, в частности для проверки шуровости и отделимости S-колец над различными группами.

Список литературы

[1] Б. Вейсфейлер, А. Леман, Приведение графа к каноническому виду и возникающая при этом алгебра // Научно-техн. информ. Сб. ВИНИТИ. — 1968. — Т. 2, № 9. — С. 12–16.

[2] С. Евдокимов, Шуровость и отделимость ассоциативных схем // Дис. на соиск. учен. ст. докт. физ.-мат. наук. — СПбГУ, СПб.— 2004.

[3] С. Евдокимов, И. Пономаренко, Об одном семействе колец Шура над конечной циклической группой // Алгебра и анализ. — 2001. — Т. 13, № 3. — С. 139–154.

[4] С. Евдокимов, И. Пономаренко, Характеризация циклотомических схем и нормальные кольца Шура над циклической группой // Алгебра и анализ. — 2002. — Т. 14, № 2. — С. 11–55.

[5] С. Евдокимов, И. Пономаренко, Распознавание и проверка изоморфизма циркулянтных графов за полиномиальное время // Алгебра и анализ. — 2003. — Т. 15, № 6. — С. 1–34.

[6] С. Евдокимов, И. Пономаренко, Шуровость S-колец над циклической группой и обобщенное сплетение групп перестановок // Алгебра и анализ. — 2012. — Т. 24, № 3. — С. 84–127.

[7] М. Музычук, И. Пономаренко, О 2-группах Шура // Зап. научн. сем. ПОМИ. — 2015. — Т. 435. — С. 113–162.

[8] G. Chen, I. Ponomarenko, Lectures on Coherent Configurations // http://www.pdmi.ras.ru/~inp/ccNOTES.pdf. — 2019.

[9] S. Evdokimov, I. Ponomarenko, Permutation group approach to association schemes // European J. Combin. — 2009. — Vol. 30, no. 6. — P. 1456–1476.

[10] S. Evdokimov, I. Ponomarenko, Schur rings over a product of Galois rings // Beitr. Algebra Geom. — 2014. — Vol. 55, no. 1. — P. 105–138.

[11] S. Evdokimov, I. Ponomarenko, On separability problem for circulant S-rings // Алгебра и анализ. — 2016. — Т. 28, № 1. — С. 32–51.

[12] S. Evdokimov, I. Ponomarenko, Coset closure of a circulant S-ring and schurity problem // J. Algebra Appl. — 2016. — Vol. 15, no. 4. — Article ID 1650068, 49 pp.

[13] S. Evdokimov, I. Kovács, I. Ponomarenko, Characterization of cyclic Schur groups // Алгебра и анализ. — 2013. — Т. 25, № 1. — С. 61–85.

[14] S. Evdokimov, I. Kovács, I. Ponomarenko, On schurity of finite abelian groups // Commun. Algebra. — 2016. — Vol. 44, no. 1. — P. 101–117.

[15] Ja. Golfand, N. Najmark, R. Pöschel, The structure of S-rings over $\mathbb{Z}_{2^m}$ // Preprint P-01/85 Akad. der Wiss. der DDR, ZIMM, Berlin. — 1985.

[16] M. Klin, R. Pöschel, The isomorphism problem for circulant digraphs with p^n vertices // Preprint P-34/80 Akad. der Wiss. der DDR, ZIMM, Berlin. — 1980.

[17] M. Klin, R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings // Colloq. Math. Soc. Janos Bolyai. — 1981. — Vol. 25. — P. 405–434.

[18] M. Klin, C. Pech, S. Reichard, COCO2P — a GAP package, 0.14 // http://www.math.tu-dresden.de/ pech/COCO2P. — 2015.

[19] M. Muzychuk, A solution of the isomorphism problem for circulant graphs // Proc. Lond. Math. Soc. — 2004. — Vol. 88, no. 1. — P. 1–41.

[20] M. Muzychuk, I. Ponomarenko, Schur rings // European J. Combin. — 2009. — Vol. 30, no. 6. — P. 1526–1539.

[21] M. Muzychuk, I. Ponomarenko, On quasi-thin association schemes // J. Algebra. — 2012. — Vol. 351, no. 1. — P. 467–489.

[22] R. Nedela, I. Ponomarenko, Recognizing and testing isomorphism of Cayley graphs over an abelian group of order $4p$ in polynomial time // to appear in: J. Širaň et al (eds). Isomorphisms, Symmetry and Computations in Algebraic Graph Theory, Springer. — 2019.

[23] I. Ponomarenko, A. Vasil'ev, On non-abelian Schur groups // J. Algebra Appl. — 2014. — Vol. 13, no. 8. — Article ID 1450055, 22 pp.

[24] R. Pöschel, Untersuchungen von S-Ringen insbesondere im Gruppenring von p-Gruppen // Math. Nachr. — 1974. — Vol. 60. — P. 1–27.

[25] I. Schur, Zur theorie der einfach transitiven Permutationgruppen // S.-B. Preus Akad. Wiss. Phys.-Math. Kl. — 1933. — Vol. 18, no. 20. — P. 598–623.

[26] B. Yu. Weisfeiler, On the construction and identification of graphs // Lecture Notes in Math. — 1976. — Vol. 558.

[27] H. Wielandt, Finite permutation groups // Academic Press, New York - London. — 1964.

[28] H. Wielandt, Permutation groups through invariant relations and invariant functions // Lecture Notes Dept. Math., Ohio State Univ., Colombus, Ohio. — 1969.

[29] M. Ziv-Av, Enumeration of Schur rings over small groups // CASC Workshop 2014, LNCS 8660. — 2014.

Работы автора по теме диссертации

[30] G. Ryabov, On Schur 3-groups // Сиб. электрон. матем. изв. — 2015. — Т. 12. — С. 223–231.

[31] G. Ryabov, On Schur p-groups of odd order // J. Algebra Appl. — 2017. — Vol. 16, no. 3. — Article ID 1750045, 29 pp.

[32] Г. Рябов, Об отделимости колец Шура над абелевыми p-группами // Алгебра и логика. — 2018. — Т. 57, № 1. — С. 73–101.

[33] Г. Рябов, Отделимость колец Шура над абелевой группой порядка $4p$ // Зап. научн. сем. ПОМИ. — 2018. — Т. 470. — С. 179–193.

[34] Г. Рябов, Об абелевых 3-группах Шура // Материалы международной конференции «Мальцевские чтения». — 2015. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 118.

[35] G. Ryabov, On abelian Schur 3-groups // Abstracts of the 8th Slovenian Conference on Graph Theory. — 2015. — Ljubljana, Slovenia: Institute of Mathematics, Physics and Mechanics. — P. 46.

[36] G. Ryabov, On Schur 3-groups // Материалы международной конференции «Дискретная математика, алгебра и их приложения». — 2015. — Минск: ИМ НАН Беларуси, Белорус. гос. ун-т. — С. 75.

[37] G. Ryabov, On the isomorphism problem for Cayley graphs over abelian p-groups // Материалы международной конференции «Graphs and Groups, Spectra and Symmetries». — 2016. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 98.

[38] G. Ryabov, On separability problem for S-rings over abelian p-groups // Материалы международной конференции «Мальцевские чтения». — 2016. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 130.

[39] G. Ryabov, Separability of Cayley schemes over abelian p-groups // Материалы международной конференции «Workshop on Group Theory and Algebraic Combinatorics». — 2017. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 31.

[40] G. Ryabov, On abelian Schur groups of odd order // Материалы международной конференции «Groups and Graphs, Metrics and Manifolds». — 2017. — Екатеринбург: ИММ УРО РАН, Урал. фед. ун-т. — С. 89.

[41] G. Ryabov, Separability and schurity of p-Schur rings over an elementary abelian group // Материалы международной конференции «Теория групп и ее приложения». — 2018. — Краснодар: Куб. гос. ун-т., ИММ УРО РАН. — С. 177.

[42] G. Ryabov, Separability and schurity of Cayley schemes over abelian groups // Abstracts of International Conference «Symmetry vs. Regularity». — 2018. — Plzen, Czech Republic: University of West Bohemia. — P. 36.

[43] G. Ryabov, CI-property for decomposable Schur rings over an elementary abelian group // Материалы международной конференции «Graphs and Groups, Representations and Relations». — 2018. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 79.

[44] G. Ryabov, Infinite family of non-schurian separable association schemes // Материалы международной конференции «Мальцевские чтения». — 2018. — Новосибирск: ИМ СО РАН, Новосиб. гос. ун-т. — С. 136.