Math-Net.Ru
All Russian mathematical portal

S. A. Evdokimov, I. N. Ponomarenko, On a family of Shur rings over a finite cyclic group,
Algebra i Analiz, 2001, Volume 13, Issue 3, 139–154

https://www.mathnet.ru/eng/aa940

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.82
May 20, 2025, 19:31:22

Алгебра и анализ
Том 13 (2001), вып. 3

К 125-летию И. Шура

ОБ ОДНОМ СЕМЕЙСТВЕ КОЛЕЦ ШУРА НАД КОНЕЧНОЙ ЦИКЛИЧЕСКОЙ ГРУППОЙ

© С. А. Евдокимов, И. Н. Пономаренко

Мы опровергаем длительное время существующую гипотезу о том, что каждое кольцо Шура над конечной циклической группой определяется подходящей группой перестановок, содержащей эту циклическую группу в качестве регулярной подгруппы. Кроме того, мы даем отрицательный ответ на вопрос — индуцируется ли всякий слабый изоморфизм колец Шура над конечной циклической группой сильным изоморфизмом.

§1. Введение

В 1933 г. И. Шур показал, что каждая примитивная группа перестановок, содержащая регулярную циклическую подгруппу составного порядка, является дважды транзитивной. В отличие от В. Бернсайда, использовавшего теорию характеров, чтобы доказать аналогичное утверждение для циклических p-групп, идея Шура состояла в сведении проблемы к изучению специальных подколец группового кольца. А именно, он показал, что для любой группы перестановок, содержащей регулярную подгруппу G, подмодуль группового кольца группы G, натянутый на орбиты стабилизатора точки исходной группы (рассматриваемые после выбора точки естественным образом как подмножества G), 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. С тех пор любое подкольцо группового кольца группы G, удовлетворяющее этим свойствам, называется кольцом Шура (для

Поддержано грантом РФФИ, 96-15-96060 и грантами РФФИ, 96-15-96060, 99-01-00098.

краткости S-кольцом) над G. Г. Виландт писал в [13, с. 54], что „Шур длительное врмя считал, что каждое S-кольцо определяется подходящей группой перестановок“. Это предположение оказалось, однако, неверным и первые контрпримеры были найдены Виландтом в [12, теорема 25.7]. В честь этого заблуждения Шура S-кольца, возникающие из групп перестановок, стали называться шуровыми. Следует отметить, что все контрпримеры, найденные Виландтом, являются S-кольцами над нециклическими группами. Принимая во внимание то, что сам Шур работал в основном с S-кольцами над циклической группой, и тот факт, что такие S-кольца являются шуровыми, когда порядок группы равен степени простого числа [10, 1] или произведению двух различных простых чисел [5], можно предположить (и это в действительности до настоящего времени являлось гипотезой[1]), что любое S-кольцо над конечной циклической группой шурово. Некоторые специалисты полагали, что эта гипотеза уж во всяком случае справедлива, если порядок группы свободен от квадратов. В настоящей работе мы показываем, что она неверна даже при этом предположении (см. утверждение (1) теоремы 1.1).

В 80-е годы теория колец Шура была применена для исследования проблемы изоморфизма графов Кэли. Любой такой граф Γ, определенный над группой G, задается некоторым подмножеством X_Γ этой группы (окрестность единицы) и определяет S-кольцо $\mathcal{A}_\Gamma$, являющееся наименьшим S-кольцом над G, содержащим элемент $\xi_\Gamma = \sum_{x \in X_\Gamma} x$ группового кольца. Более того, любой изоморфизм из Γ в другой граф Кэли Γ' индуцирует слабый изоморфизм $\varphi : \mathcal{A}_\Gamma \to \mathcal{A}_{\Gamma'}$, для которого $\varphi(\xi_\Gamma) = \xi_{\Gamma'}$. (Под слабым изоморфизмом S-колец мы понимаем изоморфизм $\mathbb{Z}$-модулей, сохраняющий групповое и покомпонентное умножения). С другой стороны, для данных графов Кэли Γ и Γ' легко проверить, существует или нет слабый изоморфизм из $\mathcal{A}_\Gamma$ в $\mathcal{A}_{\Gamma'}$, удовлетворяющий последнему свойству. Таким образом, для графов Кэли проблема изоморфизма сводится к следующей проблеме: индуцирован или нет данный слабый изоморфизм S-колец каким-либо сильным изоморфизмом последних. (По поводу определения сильного изоморфизма см. п. 2.2; любой такой изоморфизм, индуцирующий описанный выше слабый изоморфизм $\varphi : \mathcal{A}_\Gamma \to \mathcal{A}_{\Gamma'}$, есть не что иное, как изоморфизм из Γ в Γ'). Мы называем S-кольцо отделимым, если любой слабый изоморфизм из него в другое S-кольцо над той же группой индуцируется сильным изоморфизмом. Если бы любое S-кольцо было отделимым, то проблема изоморфизма для графов Кэли стала бы тривиальной. В настоящей работе мы показываем, что существуют S-кольца (даже над циклической группой порядка свободного от квадратов), которые не являются отделимыми (см. утверждение (2) теоремы

[1]Эта гипотеза была сообщена авторам М. Клином.

1.1). Это до определенной степени объясняет, почему проблема изоморфизма циркулянтных графов все еще остается открытой [9].

Следующее утверждение представляет основной результат работы.

Теорема 1.1. *Пусть* $n = p_1p_2p_3p_4n'$, *где* p_1, p_2, p_3, p_4 *— простые числа с условием* $\{p_1, p_2\} \cap \{p_3, p_4\} = \varnothing$ *и* n' *— положительное целое число, и* $D =$ *НОД*$(p_1 - 1, p_2 - 1, p_3 - 1, p_4 - 1)$. *Тогда*

(1) *если* $D > 2$, *то над циклической группой порядка* n *существуют нешуровы* S*-кольца;*

(2) *если* D *не свободно от квадратов, то над циклической группой порядка* n *существуют неотделимые* S*-кольца.*

Наименьшие примеры нешуровых равно, как и неотделимых S-колец, гарантируемые теоремой 1.1, возникают при $n = 5^2 \cdot 13^2$ в общем случае и при $n = 5 \cdot 13 \cdot 17 \cdot 29$ в предположении, что n свободно от квадратов. Явные конструкции приводятся в §4. На самом деле доказательство теоремы показывает, что если $D > 2$ (соответственно D не свободно от квадратов), то каждое S-кольцо над циклической группой порядка n' приводит по крайней мере к одному нешурову (соответственно неотделимому) S-кольцу над циклической группой порядка n.

Следует отметить, что проблемы, рассматриваемые в настоящей работе аналогичны проблемам, возникающим в теории отделимости и шуровости когерентных конфигураций, развитой авторами в серии статей (см. [4] и ссылки в ней). В частности, в [4] были введены числа шуровости и отделимости когерентной конфигурации, показывающие насколько последняя может быть нешуровой или неотделимой. Более того, там же было доказано, что эти числа могут быть произвольно большими. Было бы интересно определить и изучить подобные числа для S-колец.

Доказательство теоремы 1.1 основано на конструкции обобщенного сплетения двух S-колец, определяемого и изучаемого в §3 (см. также [6], где аналогичная операция была введена под именем „wedge product“). Результатом такой операции является S-кольцо, получающееся, грубо говоря, отождествлением фактор-S-кольца первого операнда с под-S-кольцом второго. На самом деле значение этой конструкции выходит за рамки настоящей работы, поскольку, как показано в [6], каждое S-кольцо над конечной циклической группой может быть получено с помощью тензорных произведений и обобщенных сплетений из S-колец $\mathbb{Z}$-размерности 2 и орбитных S-колец, определяемых в конце п. 2.1.

В §2 приводятся определения и обозначения, относящиеся к S-кольцам над конечными группами (включая определения шуровости и отделимости). К сожалению, в теории S-колец не существует общепринятой терминологии

[12, 10, 5, 8, 9]. Терминология настоящей работы согласована с терминологией из [11, 2, 4] и отражает тот факт, что каждое S-кольцо может быть естественным образом рассмотрено как клеточное кольцо [3]. Например, алгебраические и комбинаторные изоморфизмы из [9] суть не что иное, как изоморфизмы из [8] и S-изоморфизмы из [5], и называются здесь слабыми и сильными изоморфизмами соответственно.

Обозначения. Как обычно, мы обозначаем через $\mathbb{Z}$, $\mathbb{Z}_n$ и $\mathbb{Z}_n^*$ (n — положительное целое число) кольцо целых чисел, кольцо целых чисел по модулю n и группу обратимых элементов из $\mathbb{Z}_n$. Мы сохраняем обозначение $\mathbb{Z}_n$ также для аддитивной группы кольца $\mathbb{Z}_n$.

Свободный $\mathbb{Z}$-модуль, натянутый на элементы множества A, обозначается через $\mathbb{Z}[A]$. Для $X \subset A$ мы полагаем $\xi(X) = \sum_{x \in X} x$. Гомоморфизм из $\mathbb{Z}[A]$ в $\mathbb{Z}[B]$, индуцированный отображением $f : A \to B$, обозначается также буквой f.

Мощность конечного множества X обозначается через $|X|$.

§2. Кольца Шура

2.1. Пусть G — конечная группа. На $\mathbb{Z}$-модуле $\mathbb{Z}[G]$ определим инволюцию, групповое умножение и адамарово умножение, полагая

$$\xi^* = \sum_{g \in G} a_g g^{-1}, \quad \xi \cdot \eta = \sum_{g,h \in G} a_g b_h gh, \quad \xi \circ \eta = \sum_{g \in G} a_g b_g g,$$

где $\xi = \sum_{g \in G} a_g g$ и $\eta = \sum_{g \in G} b_g g$. Очевидно, $\xi(X^{-1}) = \xi(X)^*$ и $\xi(X \cap Y) = \xi(X) \circ \xi(Y)$ для любых $X, Y \subset G$.

Согласно [12], подмодуль $\mathcal{A}$ модуля $\mathbb{Z}[G]$ называется *кольцом* Шура (кратко *S-кольцом*) над G, если он замкнут относительно инволюции, группового и адамарова умножений, а также содержит единицы 1 и $\xi(G)$ относительно этих умножений. Легко видеть, что каждое S-кольцо $\mathcal{A}$ имеет единственным образом определенный $\mathbb{Z}$-базис, состоящий из элементов $\xi(X)$, где X пробегает семейство $\mathcal{S} = \mathcal{S}(\mathcal{A})$ (также единственным образом определяемое по $\mathcal{A}$) попарно-непересекающихся непустых подмножеств множества G таких, что

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X \in \mathcal{S}} X = G \quad \text{и} \quad X \in \mathcal{S} \Rightarrow X^{-1} \in \mathcal{S}.$$

Элементы семейства $\mathcal{S}(\mathcal{A})$ называются *базисными множествами* кольца $\mathcal{A}$; множество их всевозможных объединений обозначим через $\mathcal{S}^*(\mathcal{A})$. Базисное множество кольца $\mathcal{A}$, содержащее $x \in G$, обозначается через $[x]$.

Множество всех S-колец над группой G упорядочено по включению. Наибольшим и наименьшим элементами этого множества являются соответственно кольца $\mathbb{Z}[G]$ и $\mathbb{Z}1+\mathbb{Z}\xi$, где $\xi=\xi(G\setminus\{1\})$. Пусть далее K — подгруппа группы $\mathrm{Aut}(G)$. Тогда множество $\mathcal{A}$ всех K-инвариантных элементов из $\mathbb{Z}[G]$ является очевидным образом S-кольцом над G. Легко видеть, что $\mathcal{S}(\mathcal{A})$ совпадает с множеством всех орбит группы K на G. Мы называем такое S-кольцо орбитным и обозначаем его через $\mathcal{O}(K,G)$.

2.2. Имеется два естественных типа изоморфизмов S-колец. А именно, мы говорим, что S-кольца $\mathcal{A}$ над G и $\mathcal{A}'$ над G' являются *изоморфными по Кэли*, если существует изоморфизм групп $f:G\to G'$ такой, что $f(\mathcal{A})=\mathcal{A}'$ (см. обозначения). Любой такой изоморфизм называется *изоморфизмом Кэли* из $\mathcal{A}$ в $\mathcal{A}'$. С другой стороны, $\mathcal{A}$ и $\mathcal{A}'$ называются *слабо изоморфными*, если существует $\mathbb{Z}$-модульный изоморфизм $\varphi:\mathcal{A}\to\mathcal{A}'$ (называемый *слабым изоморфизмом* из $\mathcal{A}$ в $\mathcal{A}'$) такой, что

$$\varphi(\xi\cdot\eta)=\varphi(\xi)\cdot\varphi(\eta),\quad \xi,\eta\in\mathcal{A}, \tag{1}$$

$$\varphi(\xi\circ\eta)=\varphi(\xi)\circ\varphi(\eta),\quad \xi,\eta\in\mathcal{A}. \tag{2}$$

Из (2) следует, что φ индуцирует биекцию $X\mapsto X^{\varphi}$ из $\mathcal{S}^*(\mathcal{A})$ на $\mathcal{S}^*(\mathcal{A}')$ (переводящую $\mathcal{S}(\mathcal{A})$ в $\mathcal{S}(\mathcal{A}')$) такую, что $\varphi(\xi(X))=\xi(X^{\varphi})$. Легко видеть, что $\{1\}^{\varphi}=\{1'\}$ и $G^{\varphi}=G'$. Можно доказать также, что $(X^{-1})^{\varphi}=(X^{\varphi})^{-1}$ и $|X^{\varphi}|=|X|$ для всех $X\in\mathcal{S}^*(\mathcal{A})$.

Еще один тип изоморфизмов S-колец происходит из изоморфизмов когерентных конфигураций [5]. А именно, биекция $f:G\to G'$ называется *сильным изоморфизмом* из $\mathcal{A}$ в $\mathcal{A}'$, если

$$f([x]y)=[f(x)]f(y),\quad x,y\in G. \tag{3}$$

Из определения немедленно следует, что $f(1)=1'$ и отображение $X\mapsto f(X)$ является биекцией из $\mathcal{S}(\mathcal{A})$ на $\mathcal{S}(\mathcal{A}')$. Поэтому f индуцирует $\mathbb{Z}$-модульный изоморфизм из $\mathcal{A}$ в $\mathcal{A}'$, удовлетворяющий условию (2). Нетрудно проверить, что он удовлетворяет также условию (1),[2] и потому является слабым изоморфизмом из $\mathcal{A}$ в $\mathcal{A}'$. Конечно, каждый изоморфизм Кэли является сильным изоморфизмом.

Для слабого изоморфизма $\varphi:\mathcal{A}\to\mathcal{A}'$ обозначим через $\mathrm{Iso}(\mathcal{A},\mathcal{A}',\varphi)$ множество всех сильных изоморфизмов из $\mathcal{A}$ в $\mathcal{A}'$, индуцирующих φ. Мы говорим,

[2]Это тривиально для клеточных колец [2] и потому выполнено также и для S-колец, поскольку при естественном соответствии между ними слабые (соответственно сильные) изоморфизмы S-колец переходят в слабые (соответственно сильные) изоморфизмы клеточных колец; см. также [9, предложение 1.7].

что S-кольцо $\mathcal{A}$ над G является *отделимым*, если $\mathrm{Iso}(\mathcal{A},\mathcal{A}',\varphi)\ne\varnothing$ для всех слабых изоморфизмов $\varphi:\mathcal{A}\to\mathcal{A}'$, где $\mathcal{A}'$ — S-кольцо над G. Далее, множество $\mathrm{Iso}(\mathcal{A},\mathcal{A},\mathrm{id}_{\mathcal{A}})$ является, очевидно, группой перестановок на G. Мы обозначаем ее через $\mathrm{Aut}(\mathcal{A})$ и называем *группой автоморфизмов* S-кольца $\mathcal{A}$. Последнее называется *шуровым*, если множество $\mathcal{S}(\mathcal{A})$ совпадает с множеством всех орбит группы $\mathrm{Aut}(\mathcal{A})$ на G. Отметим, что свойства S-кольца — быть отделимым или шуровым, очевидно, сохраняются при сильных изоморфизмах.

2.3. Пусть $\mathcal{A}$ — S-кольцо над G, H — подгруппа группы G, принадлежащая множеству $\mathcal{S}^*(\mathcal{A})$ и $i:H\to G$ — естественная инъекция. Тогда легко видеть, что $\mathbb{Z}$-модуль $\mathcal{A}_H=i^{-1}(\mathcal{A})$ является S-кольцом над H, причем

$$\mathcal{S}(\mathcal{A}_H)=\{i^{-1}(X):X\in\mathcal{S}(\mathcal{A}),X\subset\mathrm{im}(i)\}.$$

Если дополнительно H нормальна в G, то аналогично $\mathbb{Z}$-модуль $\mathcal{A}_{G/H}=\pi(\mathcal{A})$, где $\pi:G\to G/H$ — естественная сюръекция, является S-кольцом над группой G/H,

$$\mathcal{S}(\mathcal{A}_{G/H})=\{\pi(X):X\in\mathcal{S}(\mathcal{A})\}$$

и, более того, $\pi(\xi(X))$ есть положительное целое кратное $\xi(\pi(X))$ для всех $X\in\mathcal{S}(\mathcal{A})$ (см., например, [8, Предложение 1.6]). Последнее означает, что для любого $X\in\mathcal{S}(\mathcal{A})$ число $|Hx\cap X|$ не зависит от выбора $x\in X$. Нетрудно проверить, что $\pi^{-1}(\xi)\in\mathcal{A}$ для всех $\xi\in\mathcal{A}_{G/H}$. Из определений следует, что если $\mathcal{A}$ — шурово S-кольцо, то кольца $\mathcal{A}_H$ и $\mathcal{A}_{G/H}$ также шуровы.

Все сказанное в предыдущем абзаце без труда переносится на случай, когда $i:G_1\to G$ и $\pi:G\to G_2$ — мономорфизм и эпиморфизм, для которых $\mathrm{im}(i)$ и $\ker(\pi)$ принадлежат $\mathcal{S}^*(\mathcal{A})$, где G_1 и G_2 — произвольные конечные группы. В частности, $\mathbb{Z}$-модули $i^{-1}(\mathcal{A})$ и $\pi(\mathcal{A})$ являются S-кольцами над группами G_1 и G_2 соответственно.

Пусть $\mathcal{A}$ и $\mathcal{A}'$ — S-кольца над G и G' и $\varphi:\mathcal{A}\to\mathcal{A}'$ — слабый изоморфизм. Если H — подгруппа группы G, принадлежащая множеству $\mathcal{S}^*(\mathcal{A})$, то $H'=H^{\varphi}$ — подгруппа группы G', принадлежащая множеству $\mathcal{S}^*(\mathcal{A}')$, причем $|H|=|H'|$. Ясно, что $\varphi(\mathcal{A}_H)=\mathcal{A}'_{H'}$. Поэтому φ индуцирует слабый изоморфизм

$$\varphi_H:\mathcal{A}_H\to\mathcal{A}'_{H'}.$$

Аналогично если H нормальна в G, то H' нормальна в G' и φ индуцирует слабый изоморфизм

$$\varphi_{G/H}:\mathcal{A}_{G/H}\to\mathcal{A}'_{G'/H'}$$

такой, что $\varphi_{G/H}(\pi(\xi))=\pi'(\varphi(\xi))$, $\xi\in\mathcal{A}$, где $\pi:G\to G/H$ и $\pi':G'\to G'/H'$ — естественные сюръекции [8, лемма 1.7].

Пусть теперь $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$. Тогда $f(H) = H'$. Поэтому ограничение изоморфизма f на H принадлежит $\mathrm{Iso}(\mathcal{A}_H, \mathcal{A}'_{H'}, \varphi_H)$. Обозначим его через f_H. Далее, если H нормальна в G, то из условия (3) и последнего равенства вытекает, что $f(Hx) = H'f(x)$ для всех $x \in G$. Таким образом, f индуцирует биекцию $f_{G/H} : G/H \to G'/H'$, очевидно принадлежащую множеству $\mathrm{Iso}(\mathcal{A}_{G/H}, \mathcal{A}'_{G'/H'}, \varphi_{G/H})$.

§3. Обобщенные сплетения

Пусть $\mathcal{A}_k$ — S-кольцо над группой G_k $(k = 1, 2)$, M — группа и $\pi_0 : G_1 \to M$ и $i_0 : M \to G_2$ — эпиморфизм и мономорфизм соответственно такие, что

$$\ker(\pi_0) \in \mathcal{S}^*(\mathcal{A}_1), \quad \mathrm{im}(i_0) \in \mathcal{S}^*(\mathcal{A}_2), \quad \pi_0(\mathcal{A}_1) = (i_0)^{-1}(\mathcal{A}_2). \tag{4}$$

Пусть, кроме того, G — некоторая группа и $i : G_1 \to G$ и $\pi : G \to G_2$ — мономорфизм и эпиморфизм такие, что

$$\mathrm{im}(i) \geqslant \ker(\pi), \quad \pi_0 \circ i_0 = i \circ \pi. \tag{5}$$

Легко видеть, что $\ker(\pi) = i(\ker(\pi_0))$ и $\mathrm{im}(i) = \pi^{-1}(\mathrm{im}(i_0))$.

Теорема 3.1. *Пусть $\mathcal{A}$ — наименьшее S-кольцо над группой G, содержащее множество $i(\mathcal{A}_1) \cup \pi^{-1}(\mathcal{A}_2)$. Тогда*

$$\mathcal{S}(\mathcal{A}) = \mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A}), \quad \mathcal{S}_1(\mathcal{A}) \cap \mathcal{S}_2(\mathcal{A}) = \varnothing,$$

где $\mathcal{S}_1(\mathcal{A}) = \{i(X) : X \in \mathcal{S}(\mathcal{A}_1)\}$ и $\mathcal{S}_2(\mathcal{A}) = \{\pi^{-1}(X) : X \in \mathcal{S}(\mathcal{A}_2),\ X \not\subset \mathrm{im}(i \circ \pi)\}$.

Доказательство. Обозначим через $\mathcal{A}'$ подмодуль модуля $\mathbb{Z}[G]$, порожденный множеством $\Xi = \{\xi(X') : X' \in \mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A})\}$. Из формул (4) и (5) следует, что $\mathcal{S}_1(\mathcal{A}) \cap \mathcal{S}_2(\mathcal{A}) = \varnothing$ и элементы множества $\mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A})$ образуют разбиение группы G. Таким образом, множество Ξ является $\mathbb{Z}$-базисом модуля $\mathcal{A}'$. Ясно, что $\mathcal{A}' \subset \mathcal{A}$. Поэтому для завершения доказательства достаточно проверить, что $\mathcal{A} \subset \mathcal{A}'$. С этой целью мы докажем сначала, что множество $i(\mathcal{A}_1) \cup \pi^{-1}(\mathcal{A}_2)$ содержится в $\mathcal{A}'$, а затем установим, что модуль $\mathcal{A}'$ замкнут относительно группового умножения в $\mathbb{Z}[G]$ (замкнутость $\mathcal{A}'$ относительно инволюции очевидна).

Нетривиальная часть первого утверждения состоит в проверке того, что

$$\xi(\pi^{-1}(X)) \in i(\mathcal{A}_1) \quad \text{для всех } X \in \mathcal{S}(\mathcal{A}_2),\ X \subset \mathrm{im}(i \circ \pi). \tag{6}$$

Пусть $X = (i\circ\pi)(Y)$ для некоторого $Y \subset G_1$. Тогда в силу равенства $i\circ\pi = \pi_0\circ i_0$ мы имеем $X = (\pi_0 \circ i_0)(Y) = i_0(\pi_0(Y))$. Если теперь $X \in \mathcal{S}(\mathcal{A}_2)$, то формула (4) влечет, что множество $\pi_0(Y)$ принадлежит множеству $\mathcal{S}((i_0)^{-1}(\mathcal{A}_2))$ и $\mathcal{S}((i_0)^{-1}(\mathcal{A}_2)) = \mathcal{S}(\pi_0(\mathcal{A}_1))$. Поэтому $\pi_0(Y) \in \mathcal{S}(\pi_0(\mathcal{A}_1))$. Предполагая, не умаляя общности, что Y есть объединение классов смежности по группе $\ker(\pi_0)$, мы заключаем, что $Y \in \mathcal{S}^*(\mathcal{A}_1)$ (см. п. 2.3). Таким образом,

$$\xi(\pi^{-1}(X)) = \xi(\pi^{-1}((i \circ \pi)(Y))) = \xi(i(Y))$$

и, следовательно, $\xi(\pi^{-1}(X)) \in i(\mathcal{A}_1)$.

Пусть теперь X', $Y' \in \mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A})$. Докажем, что $\xi(X')\xi(Y') \in \mathcal{A}'$. Если X', $Y' \in \mathcal{S}_1(\mathcal{A})$, то это есть следствие замкнутости кольца $\mathcal{A}_1$ относительно группового умножения в $\mathbb{Z}[G_1]$. Если X', $Y' \in \mathcal{S}_2(\mathcal{A})$, то это следует из непосредственно проверяемого равенства

$$\pi^{-1}(\xi_1)\pi^{-1}(\xi_2) = a\pi^{-1}(\xi_1\xi_2), \quad \xi_1, \xi_2 \in \mathbb{Z}[G_2], \tag{7}$$

где $a = |\ker(\pi)|$, замкнутости кольца $\mathcal{A}_2$ относительно умножения в $\mathbb{Z}[G_2]$ и формулы (6). Пусть, наконец, $X' \in \mathcal{S}_1(\mathcal{A})$ и $Y' \in \mathcal{S}_2(\mathcal{A})$. Тогда $X' = i(X)$ для $X \in \mathcal{S}(\mathcal{A}_1)$, $Y' = \pi^{-1}(Y)$ для $Y \in \mathcal{S}(\mathcal{A}_2)$, $Y \subset G_2 \setminus \mathrm{im}(i \circ \pi)$, и из равенства (4) мы находим, что $\pi_0(X) = (i_0)^{-1}(Z)$ для некоторого $Z \in \mathcal{S}(\mathcal{A}_2)$. Достаточно доказать, что

$$\xi(X')\xi(Y') = b\pi^{-1}(\xi(Z)\xi(Y)) \tag{8}$$

для некоторого целого b. С этой целью заметим, что $X' \subset \pi^{-1}(Z)$ и положительное целое число $|X' \cap Lg|$ не зависит от выбора $Lg \subset \pi^{-1}(Z)$, где $L = \ker(\pi)$ (см. п. 2.3). Обозначим это число через b. Тогда, очевидно, $\xi(X' \cap Lg)\xi(Lh) = b\xi(Lgh)$ для всех $h \in G$. С другой стороны, $\xi(Lg)\xi(Lh) = a\xi(Lgh)$. Таким образом,

$$\xi(X')\xi(Lh) = b \sum_{Lg, Lg\cap X' \neq \varnothing} \xi(Lgh) = b \sum_{Lg, Lg \subset \pi^{-1}(Z)} \xi(Lgh) = (b/a)\xi(\pi^{-1}(Z))\xi(Lh).$$

Замечая теперь, что $\xi(Lh) = \xi(\pi^{-1}(\pi(Lh))$, суммируя по всем $Lh \subset Y'$ (при этом $\{Lh\}$ пробегает Y) и применяя (7) для $\xi_1 = \xi(Z)$ и $\xi_2 = \xi(Y)$, мы получаем (8). •

Мы говорим, что $\mathcal{S}$-кольцо $\mathcal{A}$, определенное в теореме 3.1, является *обобщенным сплетением* $\mathcal{S}$-колец $\mathcal{A}_1$ и $\mathcal{A}_2$ относительно $\mathcal{M} = (M, i_0, \pi_0)$ и $\mathcal{G} = (G, i, \pi)$, и обозначаем его через $\mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G})} \mathcal{A}_2$. Если G_1 — подгруппа группы G, $G_2 = G/\ker(\pi)$, $M = G_1/\ker(\pi)$ и i, i_0 и π, π_0 — естественные инъекции и сюръекции, то обобщенное сплетение называется *стандартным*. Легко видеть, что любое обобщенное сплетение отличается от стандартного лишь на изоморфизм Кэли.

Например, для положительных целых чисел p, q, r пусть $G_1 = \mathbb{Z}_{pq}$, $G_2 = \mathbb{Z}_{qr}$, $\mathcal{A}_1 = \mathbb{Z}[G_1]$, $\mathcal{A}_2 = \mathbb{Z}[G_2]$, $M = \mathbb{Z}_q$, $G = \mathbb{Z}_{pqr}$ и i_0, π_0, i, π — гомоморфизмы, переводящие 1 в 1 для π_0 и π, и 1 в r для i_0 и i. Тогда S-кольцо $\mathcal{A}$ имеет pq одноэлементных базисных множеств $\{rx\}$, $x = 0, 1, \ldots, pq-1$, и $q(r-1)$ p-элементных базисных множеств $\{x+qry : y = 0, 1, \ldots, p-1\}$, $x = 0, 1, \ldots, qr-1$, $x \neq 0 \pmod r$.

Важный частный случай нашей конструкции, объясняющий ее название, возникает при $|M| = 1$. Если обобщенное сплетение является стандартным, то в этом случае каждый элемент из $\mathcal{S}(\mathcal{A})$ либо совпадает с некоторым элементом из $\mathcal{S}(\mathcal{A}_1)$, либо равен объединению классов смежности по G_1, принадлежащих некоторому множеству $X \in \mathcal{S}(\mathcal{A}_2)$, $X \neq \{1_{G_2}\}$; читатель, знакомый с соответствием между S-кольцами и клеточными кольцами [3], легко заметит, что клеточное кольцо, отвечающее $\mathcal{A}$, является сплетением в смысле [11] клеточных колец, отвечающих $\mathcal{A}_1$ и $\mathcal{A}_2$. Далее, группа G, над которой определено $\mathcal{A}$, является расширением G_1 при помощи G_2. Хорошо известно [7], что в абелевом случае классы таких расширений по модулю изоморфизмов, тождественных на G_1 и G_2, образуют относительно операции сложения расширений конечную абелеву группу $\mathrm{Ext}_{\mathbb{Z}}(G_2, G_1)$. Например, если группы G_1 и G_2 циклические, то $\mathrm{Ext}_{\mathbb{Z}}(G_2, G_1)$ также циклическая группа порядка НОД $(|G_1|, |G_2|)$. Более того, образующим этой группы соответствуют циклические группы G.

Для произвольной тройки $\mathcal{M}$ легко найти по G_1 и G_2 группу G, удовлетворяющую соотношениям (5). Более того, если группы G_1 и G_2 циклические, то G также можно выбрать циклической. Конечно, в общем случае группа G не определяется единственным образом с точностью до изоморфизма. Однако если такие группы и изоморфны, отвечающим им обобщенные сплетения не обязательно изоморфны по Кэли даже при $|M| = 1$. Тем не менее имеет место следующее утверждение.

Теорема 3.2. *Для фиксированных $\mathcal{A}_1$, $\mathcal{A}_2$ и $\mathcal{M}$ все S-кольца $\mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G})} \mathcal{A}_2$ попарно сильно изоморфны.*

Доказательство. Пусть $\mathcal{A} = \mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G})} \mathcal{A}_2$ и $\mathcal{A}' = \mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G}')} \mathcal{A}_2$. Не умаляя общности, предположим, что эти обобщенные сплетения стандартные. Тогда $G = G'$ (как множества), группа G_1 является подгруппой как G, так и G', и $G/L = G'/L = G_2$ (как группы), где $L = \ker(\pi) = \ker(\pi')$. В частности, совпадают и множества левых классов смежности групп G и G' по подгруппе G_1. Обозначим это множество через H. Определим биекцию $f : G \to G'$

следующим образом. Если $x \in G_1$, то положим $f(x) = x$. Далее, для каждого $T \in H \setminus \{G_1\}$ выберем произвольно g_T, $g'_T \in T$ так, чтобы $Lg_T = Lg'_T$, и положим по определению

$$f(xg_T) = xg'_T, \quad x \in G_1$$

(здесь и ниже умножения в левой и правой частях формул являются умножениями в G и G' соответственно). Таким образом, f — корректно определенная биекция множества G на себя, сохраняющая каждый класс смежности по L. Покажем, что f является сильным изоморфизмом из $\mathcal{A}$ в $\mathcal{A}'$. Для этого заметим, что по определению f мы имеем $f([x]) = [f(x)]$ для всех $x \in G$. Так что равенство (3) эквивалентно включению $f([x]y) \subset [f(x)]f(y)$, x, $y \in G$, которое, как легко видеть, эквивалентно соотношению

$$f(xy) \in [f(x)]f(y), \quad x, y \in G. \tag{9}$$

Докажем последнее. В самом деле, утверждение тривиально для x, $y \in G_1$. Если $x \in G \setminus G_1$, $y \in G$, то оно следует из того факта, что $[f(x)] \supset Lx$ (см. теорему 3.1) и очевидного равенства $Lxy = LxLy$. Пусть, наконец, $x \in G_1$ и $y \in G \setminus G_1$. Тогда $y \in T$ для некоторого $T \in H \setminus \{G_1\}$, и по определению f мы имеем

$$f(xy) = f(xzg_T) = xzg'_T = xf(y) = f(x)f(y),$$

где $y = zg_T$ для $z \in G_1$. Это доказывает (9). •

В завершение параграфа изучим слабые изоморфизмы обобщенных сплетений, которые без умаления общности будем считать стандартными.

Теорема 3.3. *Пусть $\mathcal{A} = \mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G})} \mathcal{A}_2$ и $\mathcal{A}' = \mathcal{A}'_1 \wr_{(\mathcal{M}',\mathcal{G}')} \mathcal{A}'_2$ — стандартные обобщенные сплетения. Тогда отображение*

$$\varphi \mapsto (\varphi_{G_1}, \varphi_{G_2}) \tag{10}$$

определяет биекцию между множеством всех слабых изоморфизмов $\varphi : \mathcal{A} \to \mathcal{A}'$ таких, что $\varphi(i(\mathcal{A}_1)) = i'(\mathcal{A}'_1)$ и $\varphi(\pi^{-1}(\mathcal{A}_2)) = (\pi')^{-1}(\mathcal{A}'_2)$, и множеством всех пар (φ_1, φ_2) слабых изоморфизмов $\varphi_1 : \mathcal{A}_1 \to \mathcal{A}'_1$, $\varphi_2 : \mathcal{A}_2 \to \mathcal{A}'_2$, для которых $(\varphi_1)_M = (\varphi_2)_M$.

Доказательство. Корректность определения отображения (10) вытекает из очевидных равенств $(\varphi_{G_1})_M = (\varphi_{G_2})_M = \varphi_M$. Его инъективность следует из теоремы 3.1, поскольку $(i(X))^\varphi = i'(X^{\varphi_{G_1}})$ для любых $X \in \mathcal{S}(\mathcal{A}_1)$ и $(\pi^{-1}(X))^\varphi = (\pi')^{-1}(X^{\varphi_{G_2}})$ для любых $X \in \mathcal{S}(\mathcal{A}_2)$. Для доказательства сюръективности рассмотрим слабые изоморфизмы $\varphi_1 : \mathcal{A}_1 \to \mathcal{A}'_1$ и $\varphi_2 : \mathcal{A}_2 \to \mathcal{A}'_2$, для которых

$(\varphi_1)_M = (\varphi_2)_M$. Определим биекцию из множества $\mathcal{S}(\mathcal{A}) = \mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A})$ на множество $\mathcal{S}(\mathcal{A}') = \mathcal{S}_1(\mathcal{A}') \cup \mathcal{S}_2(\mathcal{A}')$ (см. теорему 3.1) следующим образом:

$$Y^\varphi = \begin{cases} i'(X^{\varphi_1}), & \text{если } Y = i(X),\ X \in \mathcal{S}(\mathcal{A}_1), \\ (\pi')^{-1}(X^{\varphi_2}), & \text{если } Y = \pi^{-1}(X),\ X \in \mathcal{S}(\mathcal{A}_2),\ X \subset G_2 \setminus M. \end{cases} \tag{11}$$

Эта биекция задает естественный $\mathbb{Z}$-модульный изоморфизм из $\mathcal{A}$ в $\mathcal{A}'$, обозначаемый также через φ. Легко видеть, что φ удовлетворяет условию (2). Докажем, что он удовлетворяет также условию (1). Если ξ_1, $\xi_2 \in i(\mathcal{A}_1)$, то это следует из того факта, что φ_1 удовлетворяет этому условию. Далее, соотношение $(\varphi_1)_M = (\varphi_2)_M$ влечет, что равенство $(\pi^{-1}(X))^\varphi = (\pi')^{-1}(X^{\varphi_2})$ выполняется для всех $X \in \mathcal{S}(\mathcal{A}_2)$ (ср. (11)). Отсюда с учетом равенства (7) и того факта, что φ_2 удовлетворяет условию (1), мы заключаем, что φ удовлетворяет этому условию для всех ξ_1, $\xi_2 \in \pi^{-1}(\mathcal{A}_2)$. Если, наконец, $\xi_1 \in i(\mathcal{A}_1)$ и $\xi_2 \in \pi^{-1}(\mathcal{A}_2)$, то требуемое утверждение следует из равенства (8) и сказанного выше. Таким образом, отображение φ является слабым изоморфизмом. Это завершает доказательство теоремы, поскольку очевидно, что $\varphi_{G_1} = \varphi_1$ и $\varphi_{G_2} = \varphi_2$. •

§4. Явные конструкции

Ниже мы будем иметь дело с S-кольцами над циклическими группами $\mathbb{Z}_n$ для различных n. Для положительного целого числа n и его делителя m обозначим через $i_{m,n} : \mathbb{Z}_m \to \mathbb{Z}_n$ и $\pi_{n,m} : \mathbb{Z}_n \to \mathbb{Z}_m$ групповые гомоморфизмы, переводящие 1 в n/m и в 1 соответственно. Используя их, мы отождествляем с $\mathbb{Z}_m$ как подгруппу $i_{m,n}(\mathbb{Z}_m)$, так и фактор-группу $\mathbb{Z}_n/\ker(\pi_{n,m})$ группы $\mathbb{Z}_n$. Если $\mathcal{A}$ — S-кольцо над $\mathbb{Z}_n$ и $\mathbb{Z}_m$ принадлежит множеству $\mathcal{S}^*(\mathcal{A})$, то обозначим $\mathcal{A}_{\mathbb{Z}_m}$ через $\mathcal{A}_m$ и $\mathcal{A}_{\mathbb{Z}_n/\mathbb{Z}_m}$ через $\mathcal{A}^{n/m}$. Аналогично если φ и f — слабый и сильный изоморфизмы из $\mathcal{A}$ в другое S-кольцо, то мы пишем φ_m и f_m вместо $\varphi_{\mathbb{Z}_m}$ и $f_{\mathbb{Z}_m}$, а также $\varphi^{n/m}$ и $f^{n/m}$ вместо $\varphi_{\mathbb{Z}_n/\mathbb{Z}_m}$ и $f_{\mathbb{Z}_n/\mathbb{Z}_m}$. Пусть, наконец, $\mathcal{A}_l$ — S-кольцо над $\mathbb{Z}_{n_l}$ $(l = 1, 2)$, причем $(\mathcal{A}_1)^m = (\mathcal{A}_2)_m$ для некоторого m, делящего оба числа n_1 и n_2. Тогда для $\mathcal{M} = (\mathbb{Z}_m, i_{m,n_2}, \pi_{n_1,m})$ и $\mathcal{G} = (\mathbb{Z}_n, i_{n_1,n}, \pi_{n,n_2})$, где $n = n_1 n_2/m$, выполнены условия (4) и (5). В этом случае обобщенное сплетение $\mathcal{A}_1 \wr_{(\mathcal{M},\mathcal{G})} \mathcal{A}_2$ будет обозначаться через $\mathcal{A}_1 \wr_m \mathcal{A}_2$. Мы опускаем m, если $m = 1$.

Пусть p_1, p_2, p_3, p_4 — простые числа, причем $\{p_1, p_2\} \cap \{p_3, p_4\} = \varnothing$, и d — положительное целое число, делящее $p_i - 1$ для всех $i = 1, \ldots, 4$. Обозначим через K_i подгруппу группы $\mathbb{Z}_{p_i}^*$ порядка d и через $\mathcal{A}_i$ — орбитное S-кольцо $\mathcal{O}(K_i, \mathbb{Z}_{p_i})$ (см. п. 2.1; здесь и ниже мы отождествляем группы $\mathrm{Aut}(\mathbb{Z}_n)$ и $\mathbb{Z}_n^*$ для всех n). Для $i \in \{1, 2\}$, $j \in \{3, 4\}$ зафиксируем изоморфизм $f_{i,j} : K_i \to K_j$ и положим

$$K_{i,j} = \{(x, y) \in K_i \times K_j : f_{i,j}(x) = y\}. \tag{12}$$

Отметим, что поскольку $p_i \neq p_j$, то $\mathbb{Z}^*_{p_ip_j} = \mathbb{Z}^*_{p_i} \times \mathbb{Z}^*_{p_j}$. Поэтому $K_{i,j}$ является подгруппой порядка d группы $\mathbb{Z}^*_{p_ip_j}$. Положим $\mathcal{A}_{i,j} = \mathcal{O}(K_{i,j}, \mathbb{Z}_{p_ip_j})$. Легко видеть, что подгруппы $\mathbb{Z}_{p_i}$ и $\mathbb{Z}_{p_j}$ группы $\mathbb{Z}_{p_ip_j}$ являются объединениями базисных множеств S-кольца $\mathcal{A}_{i,j}$, причем $[1] = K_{i,j}$. Прямое вычисление показывает, что

$$(\mathcal{A}_{1,3})^{p_3} = \mathcal{A}_3 = (\mathcal{A}_{2,3})_{p_3}, \quad (\mathcal{A}_{1,4})^{p_4} = \mathcal{A}_4 = (\mathcal{A}_{2,4})_{p_4}.$$

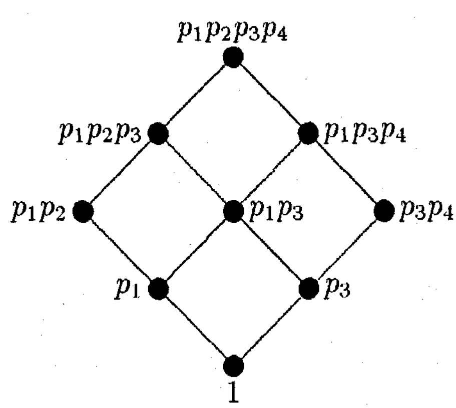
Поэтому мы можем образовать S-кольца $\mathcal{A}_{1,2,3} = \mathcal{A}_{1,3} \wr_{p_3} \mathcal{A}_{2,3}$ над $\mathbb{Z}_{p_1p_2p_3}$ и $\mathcal{A}_{1,2,4} = \mathcal{A}_{1,4} \wr_{p_4} \mathcal{A}_{2,4}$ над $\mathbb{Z}_{p_1p_2p_4}$. По определению $\mathcal{A}_{1,2,3}$ мы заключаем, что $\mathbb{Z}_{p_1p_3}, \mathbb{Z}_{p_1} \in \mathcal{S}^*\ (\mathcal{A}_{1,2,3})$ и $(\mathcal{A}_{1,2,3})_{p_1p_3} = \mathcal{A}_{1,3}$, $(\mathcal{A}_{1,2,3})^{p_2p_3} = \mathcal{A}_{2,3}$. Таким образом, $\mathbb{Z}_{p_3}, \mathbb{Z}_{p_1p_2} \in \mathcal{S}^*(\mathcal{A}_{1,2,3})$. Прямая проверка с использованием теоремы 3.1 показывает, что $(\mathcal{A}_{1,2,3})^{p_1p_2} = (\mathcal{A}_{1,2,3})_{p_1p_2} = \mathcal{A}_1 \wr \mathcal{A}_2$. Аналогично проверяется, что $\mathbb{Z}_{p_4}, \mathbb{Z}_{p_1p_2} \in \mathcal{S}^*\ (\mathcal{A}_{1,2,4})$ и $(\mathcal{A}_{1,2,4})^{p_1p_2} = (\mathcal{A}_{1,2,4})_{p_1p_2} = \mathcal{A}_1 \wr \mathcal{A}_2$. В частности,

$$(\mathcal{A}_{1,2,3})^{p_1p_2} = \mathcal{A}_1 \wr \mathcal{A}_2 = (\mathcal{A}_{1,2,4})_{p_1p_2}.$$

Таким образом, можно определить S-кольцо $\mathcal{A} = \mathcal{A}(\{p_i\}, d, \{f_{i,j}\})$ над $\mathbb{Z}_{p_1p_2p_3p_4}$, полагая

$$\mathcal{A} = \mathcal{A}_{1,2,3} \wr_{p_1p_2} \mathcal{A}_{1,2,4}.$$

Структура этого S-кольца становится яснее из вида решетки подгрупп, принадлежащих $\mathcal{S}^*(\mathcal{A})$, приведенной на рисунке. Отметим, что если $p_1 = p_2$ и $p_3 = p_4$, то эта решетка содержит все подгруппы группы $\mathbb{Z}_{p_1p_2p_3p_4}$. Легко видеть также, что $\mathcal{A}_{p_1p_2} = \mathcal{A}_1 \wr \mathcal{A}_2$ и $\mathcal{A}_{p_3p_4} = \mathcal{A}_3 \wr \mathcal{A}_4$.



Решетка подгрупп S-кольца $\mathcal{A}$.

Ниже мы изучим свойства S-кольца $\mathcal{A}$ в зависимости от выбора параметров p_i, d и $f_{i,j}$. Если эти параметры зафиксированы, то для каждого делителя d' числа d обозначим через $\mathcal{A}(d')$ S-кольцо, полученное тем же способом, что и $\mathcal{A}$ с заменой d на d' и изоморфизма $f_{i,j}$ на его ограничение на подгруппу группы K_i порядка d'. Таким образом, $\mathcal{A} = \mathcal{A}(d)$ и $\mathcal{A}(d') \supset \mathcal{A}$ для всех d'.

Лемма 4.1. *Во введенных выше обозначениях положим* $f = f_{1,3} \circ f_{2,3}^{-1} \circ f_{2,4} \circ f_{1,4}^{-1}$. *Тогда* $f \in \mathrm{Aut}(K_1)$ *и имеют место следующие утверждения*:

(1) *если* $f \neq id_{K_1}$, *то S-кольцо $\mathcal{A}$ является нешуровым*;

(2) *если дополнительно для некоторого d', делящего d, f тождествен на подгруппе порядка d' и фактор-группе по ней, то S-кольцо $\mathcal{A}(d')$ является неотделимым.*

Доказательство. Рассмотрим произвольный автоморфизм $g \in \mathrm{Aut}(\mathcal{A})$. Положим

$$\begin{aligned}
g_{1,3} &= (g_{p_1p_2p_3})_{p_1p_3}, & g_{1,4} &= (g^{p_1p_2p_4})_{p_1p_4},\\
g_{2,3} &= (g_{p_1p_2p_3})^{p_2p_3}, & g_{2,4} &= (g^{p_1p_2p_4})^{p_2p_4},\\
g_1 &= (g_{1,3})_{p_1} = (g_{1,4})_{p_1}, & g_2 &= (g_{2,3})_{p_2} = (g_{2,4})_{p_2},\\
g_3 &= (g_{1,3})_{p_3} = (g_{2,3})_{p_3}, & g_4 &= (g_{1,4})_{p_4} = (g_{2,4})_{p_4}.
\end{aligned}$$

Тогда $g_{i,j} \in \mathrm{Aut}(\mathcal{A}_{i,j})$, $i = 1, 2$, $j = 3, 4$, и $g_k \in \mathrm{Aut}(\mathcal{A}_k)$, $k = 1, \ldots, 4$ (см. п. 2.3). Ниже мы пишем $x^{g_{i,j}}$ вместо $g_{i,j}(x)$ и x^{g_k} вместо $g_k(x)$.

Согласно [5, теорема 3.4, (1), (b_2)], каждый автоморфизм S-кольца $\mathcal{A}_{i,j}$ над $\mathbb{Z}_{p_ip_j}$ задается умножением на некоторый элемент группы $\mathbb{Z}_{p_ip_j}^*$ (напомним, что $p_i \neq p_j$). Поэтому найдется элемент $m_{i,j} \in \mathbb{Z}_{p_ip_j}^*$ такой, что $x^{g_{i,j}} = m_{i,j}x$ для всех $x \in \mathbb{Z}_{p_ip_j}$. Более того, автоморфизм g_k, индуцированный при $k = 1, 2$ как $g_{k,3}$, так и $g_{k,4}$, а при $k = 3, 4$ как $g_{1,k}$, так и $g_{2,k}$, определяет элемент $m_k \in \mathbb{Z}_{p_k}^*$ такой, что $x^{g_k} = m_k x$, $x \in \mathbb{Z}_{p_k}$, причем $m_{i,j} = (m_i, m_j)$ для всех i, j. Покажем, что

$$f_{i,j}(m_i) = m_j, \quad i = 1, 2, \; j = 3, 4. \tag{13}$$

Действительно, из определения $m_{i,j}$ следует, что $1^{g_{i,j}} = m_{i,j}$, и потому $m_{i,j} \in K_{i,j}$. Таким образом, $(m_i, m_j) = m_{i,j} = (m_i, f_{i,j}(m_i))$ (см. (12)). Это доказывает равенство (13). Вспоминая определение чисел m_i, получаем

$$f_{i,j}(y^{g_i}) = f_{i,j}(m_i y) = f_{i,j}(m_i) f_{i,j}(y) = m_j f_{i,j}(y) = f_{i,j}(y)^{g_j} \tag{14}$$

для всех $y \in K_i$, $i = 1, 2$, $j = 3, 4$.

Докажем утверждение (1). Из (14) следует, что $f(y^{g_1}) = f(y)^{g_1}$ для всех $g \in \mathrm{Aut}(\mathcal{A})$ и $y \in K_1$. Поэтому $f(1^{g_1}) = f(1)^{g_1} = 1^{g_1}$. Таким образом,

$$1^{g_1} \notin X \quad \text{для всех } g \in \mathrm{Aut}(\mathcal{A}), \tag{15}$$

где $X = \{x \in K_1 : f(x) \neq x\}$. По условию утверждения (1) множество X непусто. Пусть $x^* \in X$. Тогда из (15) следует, что x^* и 1 как элементы подгруппы $\mathbb{Z}_{p_1}$ принадлежат различным орбитам группы $\mathrm{Aut}(\mathcal{A})$. Поскольку эти элементы принадлежат в то же самое время одному и тому же базисному множеству S-кольца $\mathcal{A}$, мы заключаем, что $\mathcal{A}$ нешурово.

Докажем утверждение (2). Положим

$$x_3 = f_{1,3}(x^*), \quad x_2 = f_{2,3}^{-1}(x_3), \quad x_4 = f_{2,4}(x_2), \quad x_1 = f_{1,4}^{-1}(x_4), \tag{16}$$

где x^* имеет тот же смысл, что и выше. Тогда $(x_i, x_j) \in K_{i,j}$ для всех $i = 1,2$ и $j = 3,4$. Обозначим через $\varphi_{i,j}$ слабый изоморфизм S-кольца $\mathcal{A}'_{i,j} = (\mathcal{A}(d'))_{i,j}$, задаваемый умножением на $m'_{i,j} = (x_i, x_j)$. Из очевидных равенств $(\varphi_{1,3})^{p_3} = (\varphi_{2,3})_{p_3}$ и $(\varphi_{1,4})^{p_4} = (\varphi_{2,4})_{p_4}$ по теореме 3.3 заключаем, что существуют единственным образом определенные слабые изоморфизмы $\varphi_{1,2,3}$ и $\varphi_{1,2,4}$ S-колец $\mathcal{A}'_{1,2,3} = \mathcal{A}'_{1,3} \wr_{p_3} \mathcal{A}'_{2,3}$ и $\mathcal{A}'_{1,2,4} = \mathcal{A}'_{1,4} \wr_{p_4} \mathcal{A}'_{2,4}$ такие, что $(\varphi_{1,2,3})_{p_1p_3} = \varphi_{1,3}$, $(\varphi_{1,2,3})^{p_2p_3} = \varphi_{2,3}$ и $(\varphi_{1,2,4})_{p_1p_4} = \varphi_{1,4}$, $(\varphi_{1,2,4})^{p_2p_4} = \varphi_{2,4}$ соответственно. Проверим, что

$$(\varphi_{1,2,3})^{p_1p_2} = (\varphi_{1,2,4})_{p_1p_2}. \tag{17}$$

Поскольку $(\mathcal{A}'_{1,2,3})^{p_1p_2} = (\mathcal{A}'_{1,2,4})_{p_1p_2} = \mathcal{A}'_1 \wr \mathcal{A}'_2$, где $\mathcal{A}'_i = (\mathcal{A}(d'))_i$, $i = 1,2$, достаточно доказать, что $(\varphi_{1,3})_{p_1} = (\varphi_{1,4})_{p_1}$ и $(\varphi_{2,3})_{p_2} = (\varphi_{2,4})_{p_2}$. Последнее равенство прямо следует из определения изоморфизмов $\varphi_{i,j}$. Поскольку слабые изоморфизмы $(\varphi_{1,3})_{p_1}$ и $(\varphi_{1,4})_{p_1}$ отвечают умножениям на x^* и x_1 соответственно, то для доказательства первого равенства необходимо проверить лишь, что $(x^*)^{-1}x_1 \in K'_1$, где K'_1 — подгруппа группы K_1 порядка d'. Однако из условия утверждения (2) следует, что $f(K'_1 x) = K'_1 x$ для всех $x \in K_1$. Поэтому с учетом равенства $x_1 = f(x^*)$, вытекающего из (16), имеем $(x^*)^{-1}x_1 = (x^*)^{-1}f(x^*) \in K'_1$.

Из теоремы 3.3 и равенства (17) следует, что $\varphi_{1,2,3} = \varphi_{p_1p_2p_3}$ и $\varphi_{1,2,4} = \varphi_{p_1p_2p_4}$ для единственным образом определенного слабого изоморфизма $\varphi : \mathcal{A}' \to \mathcal{A}'$. По определению изоморфизм φ тождествен на $\mathcal{A}$ и φ_{p_1} переводит базисное множество кольца $\mathcal{A}'_1$, содержащее 1, в базисное множество кольца $\mathcal{A}'_1$, содержащее x^*. Предположим, что φ индуцируется сильным изоморфизмом g кольца $\mathcal{A}'$. Тогда g является автоморфизмом S-кольца $\mathcal{A}$

и $1^{g_1} \in K'_1 x^*$. С другой стороны, из условия утверждения (2) следует, что $f(h) = h$ для всех $h \in K'_1$. Поскольку $f(x^*) \neq x^*$, то это влечет, что $K'_1 x^* \subset X$, где X — то же множество, что и в (15). Таким образом, $1^{g_1} \notin K'_1 x^*$ в силу (15). Полученное противоречие показывает, что φ не индуцируется никаким сильным изоморфизмом S-кольца $\mathcal{A}'$, и потому $\mathcal{A}'$ неотделимо. •

Доказательство теоремы 1.1. Пусть $n = p_1 p_2 p_3 p_4 n'$ и D, как в условии теоремы. Пусть, кроме того, $\mathcal{A} = \mathcal{A}(\{p_i\}, d, \{f_{i,j}\})$ есть S-кольцо над $\mathbb{Z}_{p_1 p_2 p_3 p_4}$, построенное в начале этого параграфа. Для доказательства утверждения (1) обозначим через d любой делитель числа D, больший 2 (например, D). Тогда порядок группы $\mathrm{Aut}(K_1)$ не меньше 2. Поэтому изоморфизмы $f_{i,j}$ могут быть выбраны таким образом, чтобы выполнялось условие утверждения (1) леммы 4.1 (например, $f_{1,3}$, $f_{2,3}$, $f_{2,4}$ произвольны, а $f_{1,4} \neq f_{1,3} \circ f_{2,3}^{-1} \circ f_{2,4}$). Используя эту лемму, заключаем, что S-кольцо $\mathcal{A}$ нешурово. Если теперь $\mathcal{B}$ — произвольное S-кольцо над $\mathbb{Z}_{n'}$, то в силу равенства $\mathcal{A} = (\mathcal{A} \wr \mathcal{B})_{p_1 p_2 p_3 p_4}$ S-кольцо $\mathcal{A} \wr \mathcal{B}$ также нешурово, что доказывает утверждение (1).

Для доказательства утверждения (2) обозначим через d любой несвободный от квадратов делитель числа D (например, D). Пусть $d' > 1$ — любое положительное целое число такое, что $(d')^2$ делит d (например, простое l, для которого l^2 делит d). Обозначим через f любой автоморфизм группы K_1, переводящий ее образующую в другую образующую, принадлежащую тому же самому классу смежности по подгруппе K'_1 порядка d'. Тогда $f \neq \mathrm{id}_{K_1}$ и f действует тождественно на K'_1 и K/K'_1. Выберем изоморфизмы $f_{i,j}$ так, чтобы $f_{1,3} \circ f_{2,3}^{-1} \circ f_{2,4} \circ f_{1,4}^{-1} = f$. Тогда в силу утверждения (2) леммы 4.1 S-кольцо $\mathcal{A}' = \mathcal{A}(d')$ неотделимо. Следовательно, найдется слабый изоморфизм φ из $\mathcal{A}'$ в некоторое S-кольцо $\mathcal{A}''$ над той же группой, для которого $\mathrm{Iso}(\mathcal{A}', \mathcal{A}'', \varphi) = \varnothing$. Если теперь $\mathcal{B}$ — произвольное S-кольцо над $\mathbb{Z}_{n'}$, то слабый изоморфизм из S-кольца $\mathcal{A}' \wr \mathcal{B}$ в S-кольцо $\mathcal{A}'' \wr \mathcal{B}$, отвечающий по теореме 3.3 паре $(\varphi, \mathrm{id}_{\mathcal{B}})$, не индуцируется, очевидно, никаким сильным изоморфизмом. Поэтому S-кольцо $\mathcal{A}' \wr \mathcal{B}$ не является отделимым и утверждение (2), а вместе с ним и вся теорема, доказаны. •

Список литературы

[1] Гольфанд Я. Ю., Клин М. Х., Наймарк Н. Л., *Строение S-колец над $\mathbb{Z}_{2^m}$*, XVI Всесоюзная алгебраическая конференция (Ленинград, 1981). Тезисы. Ч. 2, ЛОМИ и др., Л., 1981, сс. 195–196.

[2] Евдокимов С., Пономаренко И., *О примитивных клеточных алгебрах*, Зап. науч. семин. ПОМИ **256** (1999), 38–68.

[3] Клин М. Х., *Об аксиоматике клеточных колец*, Исследования по алгебраической теории комбинаторных объектов, Тр. семин., ВНИИСИ, М., 1985, сс. 6–32.

[4] Evdokimov S., Ponomarenko I., *Separability number and schurity number of coherent configurations*, Electron. J. Combin. 7 (2000, #R31).

[5] Klin M. H., Pöschel R., *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Algebraic Methods in Graph Theory (Szeged, 1978). Vol. 1, 2, Colloq. Math. Soc. János Bolyai, vol. 25, North-Holland, Amsterdam-New York, 1981, pp. 405–434.

[6] Leung K. H., Man S. H., *On Schur rings over cyclic groups.* II, J. Algebra **183** (1996), 273–285.

[7] Mac Lane S., *Homology*, Grundlehren Math. Wiss., vol. 114, Springer-Verlag, Berlin etc., 1963.

[8] Muzychuk M. E., *On the structure of basis sets of Schur rings over cyclic groups*, J. Algebra **169** (1994), 655–678.

[9] Muzychuk M., Pöschel R., *Isomorphism criteria for circulant graphs*, Preprint no. MATH-AL-9-1999, Techn. Univ. Dresden, 1999.

[10] Pöschel R., *Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen*, Math. Nachr. **60** (1974), 1–27.

[11] Weisfeiler B. Yu. (ed.), *On the construction and identification of graphs*, Lecture Notes in Math., vol. 558, Springer-Verlag, Berlin etc., 1976.

[12] Wielandt H., *Finite permutation groups*, Academie Press, New York-London, 1964.

[13] Wielandt H., *Permutation groups through invariant relations and invariant functions*, Lecture Notes Dept. Math., Ohio State Univ., Columbus, Ohio, 1969.

С.-Петербургский институт
информатики и автоматизации РАН
199178 Санкт-Петербург
14-я линия В. О., 39
Россия
E-mail: evdokim@pdmi.ras.ru

Поступило 13 сентября 2000 г.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
191011, Санкт-Петербург
наб. р. Фонтанки, 27
Россия
E-mail: inp@pdmi.ras.ru