С. А. Евдокимов, И. Н. Пономаренко, Характеризация циклотомических схем и нормальные кольца Шура над циклической группой,
Алгебра и анализ, 2002, том 14, выпуск 2, 11–55

Алгебра и анализ
Том 14 (2002), вып. 2

ХАРАКТЕРИЗАЦИЯ ЦИКЛОТОМИЧЕСКИХ СХЕМ И НОРМАЛЬНЫЕ КОЛЬЦА ШУРА НАД ЦИКЛИЧЕСКОЙ ГРУППОЙ

© С. А. Евдокимов, И. Н. Пономаренко

Хорошо известно, что циклотомическая схема $\mathcal{C}$ на конечном поле $\mathbb{F}$ в общем случае не может быть охарактеризована с точностью до изоморфизма своими числами пересечений. Мы показываем, что числа пересечений некоторой схемы $\widehat{\mathcal{C}}^{(b)}$ на b-й декартовой степени множества $\mathbb{F}$, где b — базовое число группы $\mathrm{Aut}(\mathcal{C})$, образуют полное множество инвариантов для $\mathcal{C}$. Здесь важно отметить, что $b \leqslant 3$ для несобственной $\mathcal{C}$ и что схема $\widehat{\mathcal{C}}^{(b)}$ определяется для произвольной (не обязательно циклотомической) схемы $\mathcal{C}$ чисто комбинаторным путем. Доказательство основного результата базируется на полном описании вводимых в данной статье нормальных колец Кэли и нормальных колец Шура над конечной циклической группой. Развитая техника позволяет установить, что произвольное кольцо Шура над циклической группой, отличное от группового, обладает нетривиальным автоморфизмом.

§1. Введение

В конце 60-х годов Д. Хигман [10], изучая перестановочные представления классических групп, пришел к понятию когерентной конфигурации, играющему ключевую роль в настоящей работе. Пусть V — конечное множество и $\mathcal{R}$ — некоторое множество бинарных отношений на V. Пара $\mathcal{C} = (V, \mathcal{R})$ называется *когерентной конфигурацией* или *схемой* на V, если выполнены следующие условия:

(C1) $\mathcal{R}$ образует разбиение множества V^2,
(C2) диагональ множества V^2 является объединением элементов из $\mathcal{R}$,
(C3) $\mathcal{R}$ замкнуто относительно перестановки координат,
(C4) если $R, S, T \in \mathcal{R}$, то число $|\{v \in V : (u, v) \in R,\ (v, w) \in S\}|$ не зависит от выбора пары $(u, w) \in T$.

Оба автора поддержаны грантами РФФИ, 99-01-00098, 01-01-00219.

Элементы множества V, отношения из $\mathcal{R}$ и числа из условия (C4) называются соответственно *точками, базисными отношениями* и *числами пересечений* схемы $\mathcal{C}$. Последние, очевидно, являются ее инвариантами относительно изоморфизмов схем, т.е. биекций между точками, сохраняющих базисные отношения.

Одним из главных источников схем являются конечные группы. А именно каждая группа перестановок $\Gamma \leqslant \mathrm{Sym}(V)$ определяет схему $\mathrm{Con}(\Gamma) = (V, \mathcal{R})$, где $\mathcal{R}$ — множество всех орбит группы Γ на V^2. Это позволяет рассматривать Γ как группу автоморфизмов схемы $\mathcal{C} = \mathrm{Con}(\Gamma)$, т.е. как подгруппу группы

$$\mathrm{Aut}(\mathcal{C}) = \{g \in \mathrm{Sym}(V) : R^g = R,\ R \in \mathcal{R}\},$$

называемой *группой автоморфизмов* схемы $\mathcal{C}$. Распространяя это определение на произвольную схему $\mathcal{C}$, мы приходим к отображениям $\Gamma \mapsto \mathrm{Con}(\Gamma)$ и $\mathcal{C} \mapsto \mathrm{Aut}(\mathcal{C})$ между схемами и группами перестановок на V. Эти отображения, не являясь взаимно-обратными, определяют соответствие Галуа относительно естественных частичных порядков на этих множествах. Схема $\mathcal{C}$ называется *шуровой*, если она является замкнутым объектом при этом соответствии (употребление термина „шуровость“ объясняется тем обстоятельством, что именно И. Шур был, по-видимому, первым, кто использовал для изучения группы перестановок централизаторное кольцо этой группы, т.е. кольцо смежности ее схемы). Следует отметить, что шуровы схемы сравнительно редки. Например, однородная схема, отвечающая конечной проективной плоскости, шурова тогда и только тогда, когда эта плоскость дезаргова [7].

В настоящей статье мы изучаем циклотомические схемы, введенные Ф. Дельсартом и определяемые следующим образом. Пусть $\mathbb{F}$ — конечное поле из q элементов и H — подгруппа индекса m его мультипликативной группы $\mathbb{F}^\times$. Для $a \in \mathbb{F}$ положим

$$R_a = \{(x, y) \in \mathbb{F}^2 : x - y \in aH\}.$$

Тогда пара $(\mathbb{F}, \{R_a : a \in \mathbb{F}\})$ удовлетворяет условиям (C1)–(C4) и называется *циклотомической* схемой на $\mathbb{F}$ [1]. Легко видеть, что число пересечения этой схемы, отвечающее отношениям R_a, R_b, R_c с $a, b, c \neq 0$, равно количеству решений $\xi, \eta \in \{0, 1, \ldots, (q-1)/m - 1\}$ уравнения $ag^{m\xi} + b = cg^{m\eta}$, где g — примитивный элемент поля $\mathbb{F}$. Явное вычисление этих целых чисел, называемых циклотомическими, является трудной теоретико-числовой проблемой [13, с. 305]. Более того, в отличие от многих классических схем числа пересечений циклотомической схемы не определяют ее с точностью до изоморфизма. Например, имеется большое число попарно неизоморфных схем, возникающих из конференс-матриц и матриц Адамара и имеющих те же числа пересечений, что и схемы Пэли, т.е. циклотомические схемы с $m = 2$. В настоящей статье мы находим полное множество инвариантов произвольной

циклотомической схемы путем расширения множества ее чисел пересечений. Для этой цели используется подход, развитый авторами в серии статей [4–7] (по поводу точных определений см. §2 и 3).

Естественная биекция между бинарными отношениями на множестве V и $\{0,1\}$-матрицами кольца $\mathrm{Mat}_V = \mathrm{Mat}_V(\mathbb{Z})$ индуцирует биекцию между схемами на V и клеточными кольцами на V, т.е. подкольцами кольца Mat_V, замкнутыми относительно адамарова (покомпонентного) умножения и транспонирования и содержащими единичную матрицу и матрицу из всех единиц.[1] При таком соответствии схема $\mathrm{Con}(\Gamma)$, отвечающая группе перестановок Γ, переходит в централизаторное кольцо $\mathcal{Z}(\Gamma)$ этой группы. Пусть $\mathcal{C}$ — произвольная схема на V и W — соответствующее ей клеточное кольцо (кольцо смежности схемы $\mathcal{C}$). Для натурального числа m определим $\widehat{\mathcal{C}}^{(m)}$ как схему, соответствующую наименьшему клеточному кольцу $\widehat{W}^{(m)}$ на множестве V^m, содержащему m-ю тензорную степень кольца W и матрицу смежности рефлексивного отношения, отвечающего диагонали множества V^m. Нас интересует минимальное m, для которого множество чисел пересечений схемы $\widehat{\mathcal{C}}^{(m)}$ определяет $\mathcal{C}$ с точностью до изоморфизма. Мы называем такое число *числом отделимости* схемы $\mathcal{C}$, обозначаем его через $s(\mathcal{C})$ и полагаем $s(W) = s(\mathcal{C})$. Таким образом, $s(\mathcal{C}) \leqslant m$ тогда и только тогда, когда $\mathcal{C}$ характеризуется числами пересечений схемы $\widehat{\mathcal{C}}^{(m)}$ или, другими словами, когда множество этих чисел является полным множеством инвариантов схемы $\mathcal{C}$. Число отделимости было введено и изучено в статье [7]; там же оно было вычислено для нескольких классических семейств схем.

Как было отмечено выше, существуют циклотомические схемы $\mathcal{C}$, для которых $s(\mathcal{C}) \geqslant 2$. С другой стороны, из [7, теорема 5.1] следует, что $s(\mathcal{C}) \leqslant 2$ для любой импримитивной циклотомической схемы. Наконец, если $\mathcal{C}$ — примитивная циклотомическая схема на простом числе точек, то $s(\mathcal{C}) \leqslant 4$ [7, теорема 5.4]. В настоящей статье мы оцениваем число отделимости произвольной циклотомической схемы через *базовое число* ее группы автоморфизмов. Здесь базовое число $b(\Gamma)$ группы перестановок Γ определяется как минимальное число точек таких, что подгруппа группы Γ, оставляющая на месте каждую из них, тривиальна. В [14] показано, что если $\mathcal{C}$ — собственная циклотомическая схема (т.е. $H \neq \mathbb{F}^\times$), то

$$\mathrm{Aut}(\mathcal{C}) \leqslant \{x \mapsto ax^\sigma + b,\ x \in \mathbb{F} : a \in H,\ \sigma \in \mathrm{Aut}(\mathbb{F}),\ b \in \mathbb{F}\}. \qquad (1)$$

В частности, базовое число группы $\mathrm{Aut}(\mathcal{C})$ не превосходит 3. Следующая теорема представляет основной результат статьи.

Теорема 1.1. *Пусть $\mathcal{C}$ — циклотомическая схема на конечном поле. Тогда $s(\mathcal{C}) \leqslant b(\mathrm{Aut}(\mathcal{C}))$.*

[1] В работах [18, 19] и [3–8] была развита теория клеточных алгебр над $\mathbb{C}$. Эта теория, за исключением ее представленческих аспектов, полностью переносится на клеточные кольца.

Если схема $\mathcal{C}$ не является собственной, то, очевидно, $s(\mathcal{C}) = 1$ и неравенство тривиально. Доказательство теоремы 1.1 в общем случае приводится в конце Введения. Здесь отметим лишь, что по этой теореме $s(\mathcal{C}) \leqslant 3$ для любой циклотомической схемы $\mathcal{C}$. Мы не знаем, является ли эта оценка точной.

Пусть W — кольцо смежности собственной циклотомической схемы. Наш подход к оценке числа $s(W)$ состоит в изучении структуры кольца $W_{v_1,\dots,v_l}$, где $v_1, \dots, v_l \in \mathbb{F}$, которое по определению является наименьшим клеточным кольцом на $\mathbb{F}$, содержащим W и матричные единицы, соответствующие точкам $v_1, \dots, v_l$. (Для наших целей достаточно считать, что $l \leqslant 2$). Оказывается, что с кольцом W_u, где $u = 0_{\mathbb{F}}$, естественным образом можно связать некоторое клеточное кольцо W^* на циклической группе $G = \mathbb{F}^\times$ (см. (22)) так, что

$$G \leqslant \mathrm{Aut}(W^*) \leqslant G \cdot \mathrm{Aut}(G).$$

В нашей терминологии это означает, что W^* является *нормальным кольцом Кэли* над группой G (см. п. 4.2 и 4.3). Полная характеризация нормальных колец Кэли над циклической группой приводится в теореме 6.1. Она основана на описании колец Шура над циклической группой, полученном в статьях [11, 12], и на взаимно-однозначном соответствии между кольцами Шура и кольцами Кэли (см. теорему 4.2). Эта характеризация, влечет, в частности, что кольца W^* и $(W^*)_v$, где $v = 1_{\mathbb{F}}$, являются шуровыми, что позволяет доказать шуровость клеточных колец W_u и $W_{u,v}$ и, учитывая (1), в конечном счете оценить число $s(W)$. Ряд утверждений о кольцах Шура над циклической группой, не связанных напрямую с основным результатом статьи, представляет самостоятельный интерес. В частности, мы полностью описываем группы автоморфизмов нормальных колец Шура (импликация (1) $\Longrightarrow$ (3) теоремы 6.1). Для каждого такого кольца мы находим группы его слабых и сильных изоморфизмов (см. теорему 6.6). Упомянем также теорему 5.8, утверждающую, что единственным кольцом Шура над циклической группой, обладающим тривиальной группой автоморфизмов, является ее групповое кольцо.

Структура упомянутых выше колец $W_{v_1,\dots,v_l}$ проясняется в формулируемой ниже теореме 1.2. Это позволяет, в частности, найти базовое число $b(W)$ клеточного кольца W, которое по определению является минимальным l таким, что кольцо $W_{v_1,\dots,v_l}$ совпадает с полным матричным кольцом. Кроме того, развитая техника дает возможность также явно описать и клеточные кольца $\widehat{W}^{(l)}$ для всех l. Полученные результаты показывают, что знание группы $\Gamma = \mathrm{Aut}(W)$ не является необходимым для эффективного вычисления колец $\mathcal{Z}(\Gamma_{v_1,\dots,v_l})$ и $\mathcal{Z}_l(\Gamma)$; здесь $\Gamma_{v_1,\dots,v_l}$ — поточечный стабилизатор множества $\{v_1, \dots, v_l\}$ в Γ и $\mathcal{Z}_l(\Gamma) = \mathcal{Z}(\widehat{\Gamma}^{(l)})$, где $\widehat{\Gamma}^{(l)}$ — группа перестановок, индуцированная действием группы Γ на упорядоченных l-множествах точек. Это представляется интересным, поскольку в общем случае ситуация не столь хороша, как в циклотомическом (см. п. 2.6 и 3.1). По той же причине теорема 1.2

формулируется в более общем виде, чем это необходимо для доказательства основного результата.

Теорема 1.2. *Пусть W — кольцо смежности циклотомической схемы на конечном поле $\mathbb{F}$. Тогда*

(1) $b(W) = b(\mathrm{Aut}(W))$,
(2) $W_{v_1,\dots,v_{m-1}} = \mathcal{Z}(\mathrm{Aut}(W)_{v_1,\dots,v_{m-1}})$ *для всех* $m \geqslant 1$ *и* $v_1, \dots, v_{m-1} \in \mathbb{F}$,
(3) $\widehat{W}^{(m)} = \mathcal{Z}_m(\mathrm{Aut}(W))$ *для всех* $m \geqslant 1$.

Доказательство. Утверждение (1) немедленно следует из утверждения (2). Если схема не является собственной, то утверждение (2) очевидно, а утверждение (3) следует из равенства $\mathcal{Z}(\widehat{\mathrm{Sym}(V)})^{(m)} = \mathcal{Z}_m(\mathrm{Sym}(V))$ [6, формула (2)]. Не умаляя общности, предположим далее, что схема является собственной и $m \geqslant 2$. Кольца W^* и $\widehat{W}^*$, определенные в (22), являются шуровыми по теореме 8.1. Поэтому кольца W_u, где $u = 0_{\mathbb{F}}$, и $\widehat{W}^{(2)}$, также шуровы (см. утверждение (3) теоремы 4.8). Отсюда при $m = 2$ следует утверждение (3) и в силу транзитивности группы $\mathrm{Aut}(W)$ также утверждение (2). Пусть теперь $m \geqslant 3$. Тогда следствие 6.2 влечет, что кольцо $(W^*)_{v_2,\dots,v_{m-1}}$ является 1-регулярным для всех точек $v_2, \dots, v_{m-1}$ кольца W, отличных от u (по поводу 1-регулярности см. §9). По лемме 9.2 таковым же является и кольцо $(W')_{v_2,\dots,v_{m-1}}$, где W' — кольцо, определенное в (21). Поэтому кольцо $W_{v_1,v_2,\dots,v_{m-1}}$ является 1-регулярным при $v_1 = u$ и тех же $v_2, \dots, v_{m-1}$. Это доказывает как утверждение (2) (по теореме 9.3 и транзитивности группы $\mathrm{Aut}(W)$), так и утверждение (3) (по теореме 9.6). •

Случай $m = 2$ утверждения (3) оказался достаточно трудоемким (трудности возникают, когда $\mathrm{Aut}(W) \cap \mathrm{Aut}(\mathbb{F}) \neq \{1\}$, т.е. $b(\mathrm{Aut}(W)) = 3$). Его доказательство занимает бóльшую часть §8 и использует кольца Шура над неабелевыми группами. А именно с клеточным кольцом $\widehat{W}^{(2)}$ мы связываем кольцо Кэли $\widehat{W}^*$ над группой Γ, равной полупрямому произведению аддитивной группы поля $\mathbb{F}$ на его мультипликативную группу. Из теоремы 4.8 вытекает, что кольцо $\widehat{W}^*$ нормально и $\mathrm{Aut}(\widehat{W}^*) \leqslant \Gamma \cdot \mathrm{Aut}(\mathbb{F})$. Более того, соответствующее ему кольцо Шура $\widehat{A}^*$ содержит p попарно изоморфных подколец, одно из которых отвечает нормальному кольцу Кэли W^* (см. выше), где p — характеристика поля $\mathbb{F}$. Используя эти факты, теорему 6.1, а также свойства конечных полей, мы показываем, что $\widehat{A}^*$ является орбитным кольцом (см. теорему 8.2) и, следовательно, клеточные кольца $\widehat{W}^*$ и $\widehat{W}^{(2)}$ шуровы.

Доказательство теоремы 1.1. Пусть W — кольцо смежности схемы $\mathcal{C}$ и $b = b(\mathrm{Aut}(\mathcal{C}))$. Тогда из утверждения (2) теоремы 1.2 и импликации (1) $\Longrightarrow$ (2) леммы 9.1 следует, что существуют точки $v_1, \dots, v_{b-1}$ схемы $\mathcal{C}$ такие, что кольцо $W_{v_1,\dots,v_{b-1}}$ является 1-регулярным. Поэтому $s(W_{v_1,\dots,v_{b-1}}) = 1$ по теореме 9.3 и, следовательно, $s(W) \leqslant b$ в силу утверждения (1) теоремы 3.2. •

Еще одно доказательство теоремы 1.1 основано на утверждении (3) теоремы 1.2. В этом случае используется импликация (1) $\Longrightarrow$ (3) леммы 9.1 (вместо импликации (1) $\Longrightarrow$ (2)) и утверждение (2) теоремы 3.2 (вместо утверждения (1)).

Статья состоит из девяти параграфов. §2 содержит основные определения и обозначения, относящиеся к клеточным кольцам. В §3 мы определяем число отделимости клеточного кольца и кратко излагаем теорию m-расширенных колец и m-изоморфизмов. В §4 содержатся определения и обозначения, относящиеся к кольцам Шура над конечными группами. Далее, мы вводим кольца Кэли и прослеживаем их связь с кольцами Шура. Затем мы определяем нормальные кольца Кэли и нормальные кольца Шура, описываем их элементарные свойства и приводим примеры нормальных колец Кэли, связанных с циклотомическими схемами. В §5 рассматриваются кольца Шура над циклической группой. В §6 формулируется сильный критерий нормальности колец Кэли и колец Шура над циклической группой и выводятся его многочисленные следствия. Доказательство теоремы 6.1 содержится в §7. Шуровость клеточных колец W^* и $\widehat{W}^*$, используемых при доказательстве теоремы 1.2, устанавливается в §8. Наконец, в §9 мы определяем и изучаем 1-регулярные клеточные кольца, необходимые для доказательства основных результатов.

Все используемые в этой статье понятия и результаты, касающиеся групп перестановок и конечных полей, могут быть найдены соответственно в [20, 21, 2] и [13].

Обозначения. Как обычно, мы обозначаем через $\mathbb{C}$ и $\mathbb{Z}$ поле комплексных чисел и кольцо целых чисел.

На протяжении всей статьи через V обозначается конечное множество из $n = |V|$ элементов. Подмножество множества $V \times V$ называется отношением на V. Для отношения R на V мы определяем его носитель V_R как минимальное по включению множество $U \subset V$, для которого $R \subset U \times U$. Если $u \in V$, то множество $R(u) = \{v \in V : (u, v) \in R\}$ называется окрестностью точки u в отношении R.

Под эквивалентностью E на V всегда понимается обычное отношение эквивалентности на некотором подмножестве множества V (совпадающем с V_E); множество ее классов обозначается через V/E.

Кольцо всех целочисленных матриц, строки и столбцы которых индексированы элементами из V, обозначается через Mat_V, его единичная матрица — через I_V, а матрица из всех единиц — через J_V.

Для $U \subset V$ кольцо Mat_U естественным образом рассматривается как подкольцо кольца Mat_V. Если $A \in \mathrm{Mat}_V$, то через A_U обозначается подматрица матрицы A, отвечающая U.

Матрица смежности отношения R обозначается через $A(R)$; по определению это $\{0,1\}$-матрица из Mat_V, (u, v)-элемент которой равен 1 тогда и

только тогда, когда $(u, v) \in R$.

Матрица, транспонированная к матрице A, обозначается через A^T. Если R — отношение на V, то через R^T обозначается отношение, матрица смежности которого равна $A(R)^T$.

Каждая биекция $g : V \to V'$ $(v \mapsto v^g)$ определяет естественный кольцевой изоморфизм из Mat_V на $\mathrm{Mat}_{V'}$. Образ матрицы A при этом изоморфизме обозначается через A^g. Если R — отношение на V, то через R^g мы обозначаем отношение на V' с матрицей смежности $A(R)^g$.

Группа всех перестановок множества V обозначается через $\mathrm{Sym}(V)$. Если $\Gamma \leqslant \mathrm{Sym}(V)$ — ее подгруппа, то через $\mathrm{Orb}(\Gamma) = \mathrm{Orb}(\Gamma, V)$ обозначается множество всех орбит группы Γ на V.

Пусть G — группа. Группа перестановок на G, определенная правыми (соответственно левыми) умножениями, обозначается через G_{right} (соответственно G_{left}). Если группа K точно действует на G как группа ее автоморфизмов, то мы отождествляем полупрямое произведение $G \cdot K$ с группой перестановок на множестве G, порожденной группой G_{right} и подгруппой в $\mathrm{Sym}(G)$, индуцированной действием K.

§2. Клеточные кольца

2.1. Пусть V — конечное множество. *Клеточным* кольцом на V называется подкольцо W кольца Mat_V, удовлетворяющее следующим условиям:

(A1) $I_V, J_V \in W$,
(A2) $\forall A \in W : \quad A^T \in W$,
(A3) $\forall A, B \in W : \quad A \circ B \in W$,

где через $A \circ B$ обозначается адамарово (поэлементное) произведение матриц A и B. Элементы множества V называются *точками*, а само это множество — *множеством точек* клеточного кольца W. Число $\mathrm{rk}(W) = \dim_{\mathbb{Z}}(W)$ называется *рангом* кольца W.

Каждое клеточное кольцо W на V имеет однозначно-определённый $\mathbb{Z}$-базис $\mathcal{M} = \mathcal{M}(W)$, состоящий из $\{0,1\}$-матриц, для которых

$$\sum_{A \in \mathcal{M}} A = J_V \quad \text{и} \quad A \in \mathcal{M} \Longrightarrow A^T \in \mathcal{M}. \tag{2}$$

Этот базис называется *стандартным базисом* кольца W, его элементы — *базисными матрицами*, а отвечающие ему структурные константы — *структурными константами* кольца W. Обозначим через $\mathcal{M}^* = \mathcal{M}^*(W)$ множество всех сумм различных элементов из $\mathcal{M}$, т.е. множество всевозможных $\{0,1\}$-матриц, принадлежащих кольцу W.

Клеточные кольца W на V и W' на V' называются *сильно-изоморфными*, если $W^g = W'$ для некоторой биекции $g : V \to V'$, называемой *сильным изоморфизмом* из W в W'. Множество всех таких изоморфизмов обозначается

через $\mathrm{Iso}(W, W')$. Группа $\mathrm{Iso}(W) = \mathrm{Iso}(W, W)$ содержит нормальную подгруппу

$$\mathrm{Aut}(W) = \{g \in \mathrm{Sym}(V) : A^g = A,\ A \in W\},$$

называемую *группой автоморфизмов* кольца W. Обратно, для каждой группы перестановок $\Gamma \leqslant \mathrm{Sym}(V)$ ее *централизаторное кольцо*

$$\mathcal{Z}(\Gamma) = \{A \in \mathrm{Mat}_V : A^g = A,\ g \in \Gamma\}$$

является клеточным кольцом на V. Если группа Γ' действует на множестве V, то мы полагаем $\mathcal{Z}(\Gamma', V) = \mathcal{Z}(\Gamma)$, где Γ — группа перестановок на V, индуцированная этим действием. Клеточное кольцо W называется *шуровым*, если $W = \mathcal{Z}(\mathrm{Aut}(W))$, или, другими словами, если его стандартный базис состоит из матриц смежности 2-орбит группы $\mathrm{Aut}(W)$.

Множество всех клеточных колец на V частично упорядочено по включению. Наибольшим и наименьшим элементом этого множества являются соответственно полное матричное кольцо Mat_V и кольцо $\mathcal{Z}(\mathrm{Sym}(V))$ с $\mathbb{Z}$-базисом $\{I_V, J_V\}$. Мы пишем $W \leqslant W'$, если $W \subset W'$. Легко видеть, что для клеточных колец $W_1, W_2 \leqslant \mathrm{Mat}_V$ множество $W_1 \cap W_2$ также является клеточным кольцом на V. Отсюда следует, что существует наименьшее клеточное кольцо W на V, для которого $W_1 \leqslant W$ и $W_2 \leqslant W$. Таким образом, множество всех клеточных колец на V образует решетку.

2.2. Пусть $W \leqslant \mathrm{Mat}_V$ — клеточное кольцо, $\mathcal{M} = \mathcal{M}(W)$ и $\mathcal{M}^* = \mathcal{M}^*(W)$. Положим

$$\mathrm{Cel}(W) = \{U \subset V : I_U \in \mathcal{M}\},\quad \mathrm{Cel}^*(W) = \{U \subset V : I_U \in \mathcal{M}^*\}.$$

Каждый элемент из $\mathrm{Cel}(W)$ (соответственно из $\mathrm{Cel}^*(W)$) называется *клеткой* (соответственно *клеточным множеством*) кольца W. Очевидно, что множество V является дизъюнктным объединением клеток. Кольцо W называется *однородным*, если $|\mathrm{Cel}(W)| = 1$.

Для $U_1, U_2 \in \mathrm{Cel}^*(W)$ положим $\mathcal{M}_{U_1,U_2} = \{A \in \mathcal{M} : I_{U_1} A I_{U_2} = A\}$. Тогда

$$\mathcal{M} = \bigcup_{U_1,U_2 \in \mathrm{Cel}(W)} \mathcal{M}_{U_1,U_2} \quad \text{(дизъюнктное объединение)}.$$

Для $A \in \mathcal{M}_{U_1,U_2}$, где $U_1, U_2 \in \mathrm{Cel}(W)$, обозначим через $d_{\mathrm{out}}(A)$ (соответственно $d_{\mathrm{in}}(A)$) коэффициент при I_{U_1} (соответственно при I_{U_2}) в разложении матрицы AA^T (соответственно A^TA) относительно стандартного базиса кольца W.[2] Если кольцо W однородно, то $d_{\mathrm{out}}(A) = d_{\mathrm{in}}(A)$ для всех $A \in \mathcal{M}$; это число

[2]Легко видеть, что это натуральное число равно числу единиц в каждой строке (соответственно столбце) матрицы A с индексом из U_1 (соответственно U_2).

обозначается через $d(A)$ и называется *степенью* матрицы A.[3] Клеточное кольцо W называется *полурегулярным*, если $d_{\text{in}}(A) = d_{\text{out}}(A) = 1$ для всех $A \in \mathcal{M}$. Однородное полурегулярное кольцо называется *регулярным*. Согласно [7, теорема 4.4], каждое полурегулярное (регулярное) кольцо является шуровым и потому совпадает с централизаторным кольцом полурегулярной (регулярной) группы перестановок.

Иногда вместо $\{0,1\}$-матриц удобнее иметь дело с бинарными отношениями R на V, для которых $A(R) \in W$. Мы определяем $\mathcal{R}$ (соответственно $\mathcal{R}^*$, $\mathcal{R}_{U_1,U_2}$) как множество всех таких R, что $A(R)$ принадлежит $\mathcal{M}$ (соответственно $\mathcal{M}^*$, $\mathcal{M}_{U_1,U_2}$). Отношения из $\mathcal{R}$ называются *базисными отношениями* кольца W. Мы используем все понятия и обозначения, введенные для базисных матриц клеточных колец (степень, $d(A)$, ...), также и для базисных отношений. В действительности, пара $\mathcal{C} = (V, \mathcal{R})$ является когерентной конфигурацией, отвечающей кольцу W (см. §1). Легко видеть, что числа пересечений схемы $\mathcal{C}$ совпадают со структурными константами кольца W.

2.3. Пусть $W \leqslant \mathrm{Mat}_V$ — клеточное кольцо и E — эквивалентность на V. Мы говорим, что E является *эквивалентностью* кольца W, если $E \in \mathcal{R}^*$. В этом случае носитель V_E отношения E, очевидно, является клеточным множеством этого кольца. Множество всех эквивалентностей кольца W обозначается через $\mathcal{E}(W)$. Положим $\mathcal{B}(W) = \bigcup_{E \in \mathcal{E}(W)} V/E$. Каждый элемент этого множества называется *блоком* кольца W. Из определения немедленно следует, что $\mathrm{Cel}^*(W) \subset \mathcal{B}(W)$.

Для каждого блока $U \in \mathcal{B}(W)$ множество $W_U = \{A_U : A \in W\}$ является подкольцом кольца Mat_U. Оно, очевидно, замкнуто относительно транспонирования и адамарова умножения и содержит матрицы I_U и J_U. Таким образом, W_U является клеточным кольцом на U; оно называется *ограничением* W на U. Более того,

$$\mathcal{M}(W_U) = \{A_U : A \in \mathcal{M},\ I_U A I_U \neq 0\}. \tag{3}$$

Из первой части формулы (2) следует, что каждая базисная матрица кольца W_U представляется единственным образом в виде A_U для $A \in \mathcal{M}(W)$. Если $U \in \mathrm{Cel}^*(W)$, то в силу (3) базисные матрицы из W_U находятся во взаимнооднозначном соответствии с матрицами из $\mathcal{M}_{U,U}$.

2.4. Для клеточных колец наряду с понятием сильного изоморфизма мы рассматриваем также понятие слабого изоморфизма [7]. Клеточные кольца $W \leqslant \mathrm{Mat}_V$ и $W' \leqslant \mathrm{Mat}_{V'}$ называются *слабо-изоморфными*, если существует $\mathbb{Z}$-модульный изоморфизм $\varphi : W \to W'$ такой, что

$$\varphi(A \cdot B) = \varphi(A) \cdot \varphi(B),\ \ \varphi(A \circ B) = \varphi(A) \circ \varphi(B) \quad \text{для всех } A, B \in W. \tag{4}$$

[3] Отображение $A \mapsto d(A)$ индуцирует по линейности кольцевой гомоморфизм из W в $\mathbb{Z}$.

Любой такой изоморфизм называется *слабым изоморфизмом* из W в W'. Из определения немедленно следует, что φ переводит $\{0,1\}$-матрицы в $\{0,1\}$-матрицы, причем $\varphi(I_V) = I_{V'}$ и $\varphi(J_V) = J_{V'}$. Можно показать [6, лемма 4.1], что $\varphi(A^T) = \varphi(A)^T$ для всех $A \in \mathcal{M}(W)$. Кроме того, φ индуцирует естественную биекцию $U \mapsto U^\varphi$ из $\mathrm{Cel}^*(W)$ на $\mathrm{Cel}^*(W')$, сохраняющую клетки, такую, что $\varphi(I_U) = I_{U^\varphi}$; при этом $|U| = |U^\varphi|$ и, в частности, $|V| = |V'|$. Отметим также, что $\varphi(\mathcal{M}) = \mathcal{M}'$ и, более того,

$$\varphi(\mathcal{M}_{U_1,U_2}) = \mathcal{M}'_{U_1^\varphi,U_2^\varphi} \quad \text{для всех } U_1, U_2 \in \mathrm{Cel}^*(W), \tag{5}$$

где $\mathcal{M} = \mathcal{M}(W)$ и $\mathcal{M}' = \mathcal{M}(W')$; при этом структурные константы кольца W равны соответствующим структурным константам кольца W'.

Очевидно, что композиция слабых изоморфизмов и обратный к слабому изоморфизму являются также слабыми изоморфизмами. Множество всех слабых изоморфизмов из W в W' обозначается через $\mathrm{Isow}(W, W')$. Легко видеть, что каждый сильный изоморфизм из W в W' индуцирует слабый изоморфизм между этими кольцами. Для $\varphi \in \mathrm{Isow}(W, W')$ положим

$$\mathrm{Iso}(W, W', \varphi) = \{f \in \mathrm{Iso}(W, W') : \varphi_f = \varphi\},$$

где φ_f — слабый изоморфизм, индуцированный сильным изоморфизмом f. Если $W = W'$, мы пишем $\mathrm{Isow}(W)$ вместо $\mathrm{Isow}(W, W)$ и $\mathrm{Iso}(W, \varphi)$ вместо $\mathrm{Iso}(W, W, \varphi)$.

Следующее утверждение [7, лемма 2.2] описывает свойства слабых изоморфизмов клеточных колец на языке отношений.

Лемма 2.1. *Пусть $W \leq \mathrm{Mat}_V$ и $W' \leq \mathrm{Mat}_{V'}$ — клеточные кольца и $\varphi \in \mathrm{Isow}(W, W')$. Тогда φ индуцирует биекцию $R \mapsto R^\varphi$ из множества $\mathcal{R}^*(W)$ на множество $\mathcal{R}^*(W')$ такую, что $\varphi(A(R)) = A(R^\varphi)$. Более того, эта биекция отображает $\mathcal{R}(W)$ на $\mathcal{R}(W')$, причем*

(1) $(R^\varphi)^T = (R^T)^\varphi$, $d_{\mathrm{in}}(R) = d_{\mathrm{in}}(R^\varphi)$, $d_{\mathrm{out}}(R) = d_{\mathrm{out}}(R^\varphi)$ *и* $|R| = |R^\varphi|$,

(2) $E \in \mathcal{E}(W)$ *тогда и только тогда, когда* $E^\varphi \in \mathcal{E}(W')$, *причем* $|V_E| = |V'_{E^\varphi}|$ *и* $|V/E| = |V'/E^\varphi|$

для любых $R \in \mathcal{R}(W)$ и $E \in R^*(W)$. •

2.5. Пусть $W \leq \mathrm{Mat}_V$ — клеточное кольцо и Φ — подгруппа группы $\mathrm{Isow}(W)$. Тогда, согласно [4, лемма 3.1], множество $W^\Phi = \{A \in W : \varphi(A) = A,\ \varphi \in \Phi\}$ является клеточным кольцом на V. Если G — подгруппа группы $\mathrm{Iso}(W)$, то мы полагаем $W^G = W^\Phi$, где $\Phi = \{\varphi_f : f \in G\}$. Очевидно, $G \leqslant \mathrm{Aut}(W^G)$. Следующее утверждение будет использовано при доказательстве теоремы 4.8.

Теорема 2.2. *Пусть W — клеточное кольцо, $G \leqslant \mathrm{Iso}(W)$ и $\rho : G \to \mathrm{Sym}(\mathrm{Cel}(W))$ — гомоморфизм, индуцированный действием группы G на множестве $\mathrm{Cel}(W)$. Предположим, что выполнены следующие условия*:

(1) $\mathrm{im}(\rho)$ — *регулярная подгруппа группы* $\mathrm{Sym}(\mathrm{Cel}(W))$,

(2) $\ker(\rho) \leqslant \mathrm{Aut}(W)$.

Тогда $\mathrm{Aut}(W^G) = G\,\mathrm{Aut}(W)$. *Кроме того, кольца* W *и* W^G *шуровы или нет одновременно.*

Доказательство. Первое утверждение теоремы вытекает из следующей ниже леммы 2.3: условие (1) этой леммы выполнено, поскольку любая регулярная группа 2-замкнута [21, следствие 5.4], в то время как условие (2) является следствием того, что в нашем случае подгруппа группы G, фиксирующая какую-либо клетку кольца W, равна $\ker(\rho)$.

Лемма 2.3. *В обозначениях теоремы равенство* $\mathrm{Aut}(W^G) = G\,\mathrm{Aut}(W)$ *имеет место, если выполнены следующие условия:*

(1) *группа* $\mathrm{im}(\rho)$ *является 2-замкнутой,*

(2) *для любых* $U_1, U_2 \in \mathrm{Cel}(W)$ *действие группы* $\{g \in G : U_1^g = U_1,\ U_2^g = U_2\}$ *на множестве* $\mathcal{R}_{U_1,U_2}$ *тривиально.*

Доказательство. Поскольку $G \leqslant \mathrm{Aut}(W^G)$, имеем $\mathrm{Aut}(W^G) \geqslant G\,\mathrm{Aut}(W)$. Для доказательства обратного включения пусть $R \in \mathcal{R}(W^G)$. Тогда из определения кольца W^G следует, что $R = \bigcup_{g\in G} S^g$ для некоторого $S \in \mathcal{R}(W)$. Поэтому

$$R = \bigcup_{(U_1,U_2)\in O} R_{U_1,U_2}, \quad R_{U_1,U_2} = R \cap (U_1 \times U_2), \tag{6}$$

для некоторой 2-орбиты O группы $\mathrm{im}(\rho)$. По условию (2)

$$R_{U_1,U_2} \in \mathcal{R}(W) \quad \text{для всех } (U_1, U_2) \in O. \tag{7}$$

По определению кольца W^G эквивалентность с множеством классов $\mathrm{Cel}(W)$ принадлежит множеству $\mathcal{E}(W^G)$. Обозначим через $\rho' : \mathrm{Aut}(W^G) \to \mathrm{Sym}(\mathrm{Cel}(W))$ гомоморфизм, индуцированный действием группы $\mathrm{Aut}(W^G)$ на множестве $\mathrm{Cel}(W)$. Ясно, что $\rho'|_G = \rho$. Более того, согласно формуле (6), группы $\rho(G)$ и $\rho'(\mathrm{Aut}(W^G))$ имеют одни и те же 2-орбиты. Поэтому условие (1) влечет, что $\rho(G) = \rho'(\mathrm{Aut}(W^G))$. С другой стороны, формула (7) показывает, что $\ker(\rho') \leqslant \mathrm{Aut}(W)$. Таким образом, $\mathrm{Aut}(W^G) \leqslant G\,\mathrm{Aut}(W)$, что завершает доказательство леммы. •

Легко видеть, что кольцо W^G шурово всякий раз, когда шурово кольцо W. Обратно, предположим, что кольцо W^G шурово. Пусть $S \in \mathcal{R}(W)$. Тогда $S = R_{U_1,U_2}$ для некоторых $R \in \mathcal{R}(W^G)$ и $U_1, U_2 \in \mathrm{Cel}(W)$ (см. (6), (7)). Поскольку группа $\mathrm{Aut}(W^G)$ транзитивно действует на множестве R, подгруппа этой группы, фиксирующая U_1 и U_2 как множества, транзитивно действует на S. Однако последняя группа равна $\ker(\rho)$ по условию (1) и потому содержится в $\mathrm{Aut}(W)$ по условию (2). Таким образом, кольцо W шурово. •

2.6. Для подмножеств $X_1, \dots, X_s$ кольца Mat_V обозначим через $[X_1, \dots, X_s]$ их *клеточное замыкание*, т.е. наименьшее клеточное кольцо на V, содержащее каждое из них. Мы опускаем фигурные скобки, когда $X_i = \{A_i\}$. Для клеточного кольца $W \leqslant \mathrm{Mat}_V$ и точек $v_1, \dots, v_s \in V$ мы полагаем $W_{v_1,\dots,v_s} = [W, I_{v_1}, \dots, I_{v_s}]$, где $I_{v_i} = I_{\{v_i\}}$, и называем это кольцо *расширением* кольца W относительно точек $v_1, \dots, v_s$ или $(v_1, \dots, v_s)$-расширением W. Легко видеть, что

$$W_{v_1,\dots,v_s} \leqslant \mathcal{Z}(\mathrm{Aut}(W)_{v_1,\dots,v_s}), \quad \mathrm{Aut}(W_{v_1,\dots,v_s}) = \mathrm{Aut}(W)_{v_1,\dots,v_s}. \tag{8}$$

Отметим, что существуют клеточные кольца, для которых первое включение является строгим. В неоднородном случае простейший пример получается „добавлением“ новой точки к произвольному нешуровому кольцу. Наименьшим известным авторам однородным кольцом с нешуровым одноточечным расширением является клеточное кольцо ранга 4 на 182 точках, получающееся из проективной плоскости Холла порядка 9. Из формул (8) следует, что если кольцо W шурово, то клетки его одноточечного расширения W_v совпадают с орбитами группы $\mathrm{Aut}(W)_v$, т.е. с окрестностями точки v в базисных отношениях кольца W. В общем случае можно утверждать лишь, что эти окрестности являются клеточными множествами кольца W_v.

§3. Число отделимости клеточного кольца

В этом параграфе мы приводим краткий обзор теории m-расширенных клеточных колец и m-изоморфизмов, развитой в статьях [4–7], в той ее части, которая необходима для определения числа отделимости.

3.1. Пусть $\Gamma \leqslant \mathrm{Sym}(V)$ — группа перестановок. Для натурального числа m обозначим через $\widehat{\Gamma}^{(m)}$ группу перестановок, определяемую покоординатным действием группы Γ на множестве V^m. Легко видеть, что эта группа совпадает со стабилизатором множества

$$\Delta = \Delta^{(m)}(V) = \{(v, \dots, v) \in V^m : v \in V\}$$

в m-й декартовой степени группы Γ, действующей покоординатно на V^m. Отсюда следует, что кольцо $\mathcal{Z}_m(\Gamma) = \mathcal{Z}(\widehat{\Gamma}^{(m)})$ содержит как m-ю тензорную степень кольца $\mathcal{Z}(\Gamma)$, так и матрицу I_Δ. Это наводит на мысль ввести следующее определение. Для клеточного кольца $W \leqslant \mathrm{Mat}_V$ положим

$$\widehat{W}^{(m)} = [W^m, I_\Delta], \tag{9}$$

где W^m — m-я тензорная степень кольца W. Клеточное кольцо $\widehat{W}^{(m)} \leqslant \mathrm{Mat}_{V^m}$ называется *m-расширенным кольцом* кольца W. Ясно, что $\widehat{W}^{(1)} = W$. Более того, можно доказать [6, теорема 3.2], что

$$\widehat{W}^{(m)} = [W^m, \ \mathcal{Z}_m(\mathrm{Sym}(V))].^4 \tag{10}$$

Так что множество $\mathcal{R}^*(\widehat{W}^{(m)})$ содержит все бинарные отношения на V^m, инвариантные относительно $\mathrm{Sym}(V)$, и, в частности, отношения, определяемые равенствами координат.

Из формулы (9) следует, что $\mathrm{Aut}(\widehat{W}^{(m)}) = \widehat{\mathrm{Aut}(W)}^{(m)}$. Поэтому $\widehat{W}^{(m)} \leqslant \mathcal{Z}_m(\mathrm{Aut}(W))$. Отметим, что равенство имеет место не всегда (даже при $W = \mathcal{Z}(\Gamma)$); наименьшим известным авторам примером служит однородное клеточное кольцо ранга 4 на 62 точках, отвечающее проективной плоскости порядка 5. Тем не менее равенство имеет место для всех $m \geqslant n$, где $n = |V|$. Это вытекает из следствия 9.7 настоящей статьи, поскольку $b(W) \leqslant n - 1$.

Следующее утверждение, устанавливающее связь между $(m-1)$-точечными расширениями кольца W и некоторыми частями кольца $\widehat{W}^{(m)}$, будет использовано в последующих параграфах.

Лемма 3.1. *Пусть $W \leqslant \mathrm{Mat}_V$ — клеточное кольцо, m — натуральное число и $\widehat{W} = \widehat{W}^{(m)}$. Для $v_1, \ldots, v_{m-1} \in V$ положим $U = \{\overline{u} \in V^m : u_i = v_i,\ i = 1, \ldots, m-1\}$. Тогда $U \in \mathcal{B}(\widehat{W})$ и*

$$\widehat{W}_U \geqslant (W_{v_1,\ldots,v_{m-1}})^{\zeta},$$

где $\zeta : V \to U$ — биекция, переводящая v в $(v_1, \ldots, v_{m-1}, v)$.

Доказательство следует из [5, лемма 3.1] с учетом того, что множество U является классом эквивалентности $\{(\overline{u}, \overline{v}) \in V^m \times V^m : u_i = v_i,\ i = 1, \ldots, m-1\}$, принадлежащей множеству $\mathcal{E}(\widehat{W})$. •

3.2. Пусть $\varphi : W \to W'$ — слабый изоморфизм из клеточного кольца $W \leq \mathrm{Mat}_V$ в клеточное кольцо $W' \leq \mathrm{Mat}_{V'}$. Слабый изоморфизм $\psi : \widehat{W}^{(m)} \to \widehat{W'}^{(m)}$ называется *m-расширением* изоморфизма φ, если

$$\psi(I_\Delta) = I_{\Delta'} \quad \text{и} \quad \psi(A) = \varphi^m(A) \text{ для всех } A \in W^m,$$

где $\Delta = \Delta^{(m)}(V)$, $\Delta' = \Delta^{(m)}(V')$ и φ^m — слабый изоморфизм из W^m в $(W')^m$, индуцированный φ. Легко видеть, что любой слабый изоморфизм имеет 1-расширение, совпадающее с ним самим. Однако если $m \geqslant 2$, то m-расширение существует не всегда. Например, прямое вычисление показывает, что индуцированный транспонированием слабый изоморфизм кольца смежности единственной схемы на 15 точках с параметрами Пэли не имеет 2-расширения. Очевидно, что если m-расширение существует, то оно определено однозначно.

Слабый изоморфизм называется *m-изоморфизмом*, если он имеет m-расширение. Множество всех m-изоморфизмов из W в W' обозначается через $\mathrm{Isow}_m(W, W')$. Можно доказать [6, теорема 4.5 и формула (7)], что

$$\mathrm{Isow}(W, W') = \mathrm{Isow}_1(W, W') \supset \ldots \supset \mathrm{Isow}_n(W, W') = \ldots = \mathrm{Isow}_\infty(W, W'), \quad (11)$$

[4] В статьях [4–7] кольцо $\widehat{W}^{(m)}$ определялось формулой (10).

где через $\mathrm{Isow}_\infty(W, W')$ обозначается множество всех слабых изоморфизмов из W в W', индуцированных сильными изоморфизмами. Клеточное кольцо W называется *m-отделимым*, если $\mathrm{Isow}_m(W, W') = \mathrm{Isow}_\infty(W, W')$ для любого клеточного кольца W'. Схема называется m-отделимой, если m-отделимо ее кольцо смежности. Из формулы (11) следует, что m-отделимое кольцо является l-отделимым для всех $l \geqslant m$. Положим

$$s(W) = \min\{m : W \text{ является } m - \text{отделимым}\}$$

и назовем это натуральное число *числом отделимости* кольца W. Число отделимости $s(\mathcal{C})$ схемы $\mathcal{C}$ определяется как число отделимости ее кольца смежности.

В некоторых случаях число отделимости может быть легко вычислено. Например, $s(W) = 1$, если кольцо W имеет ранг 2 или полурегулярно. В частности, $s(\mathrm{Mat}_V) = 1$. Менее тривиальный факт состоит в том, что все схемы Джонсона, Хэмминга и Грассмана являются 2-отделимыми [7]. Более того, для схем, принадлежащих первым двум семействам, можно найти точное значение числа отделимости. В общем случае ситуация значительно более сложная. А именно, как доказано в статье [6], существуют клеточные кольца с произвольно большим числом отделимости. Точнее,

$$\liminf_{n(W)\to\infty} \frac{s(W)}{n(W)} > 0,$$

где W пробегает все клеточные кольца и $n(W)$ — число точек кольца W. С другой стороны, можно доказать, что $s(W) \leqslant \lceil n/3 \rceil$ для всех клеточных колец на n точках.

Следующая теорема дает верхние оценки числа отделимости клеточного кольца через числа отделимости его расширений.

Теорема 3.2 [7, теорема 4.6]. *Пусть $W \leqslant \mathrm{Mat}_V$ — клеточное кольцо. Тогда*

(1) $s(W) \leqslant s(W_v) + 1$ *для всех* $v \in V$,

(2) $s(W) \leqslant m\, s(\widehat{W^{(m)}})$ *для всех* $m \geqslant 1$.

Сделаем несколько замечаний о взаимосвязи между понятием отделимости и характеризацией схем. Пусть $\mathcal{C}$ — схема. Говоря, что числа пересечений схем $\mathcal{C}$ и $\mathcal{C}'$ одинаковы, мы имеем в виду, что задан некоторый слабый изоморфизм $\varphi : W \to W'$, где W и W' — кольца смежности соответственно $\mathcal{C}$ и $\mathcal{C}'$. Таким образом, схема $\mathcal{C}$ характеризуется своими числами пересечений тогда и только тогда, когда $s(\mathcal{C}) = 1$. Такое понимание характеризации схем полностью соответствует точке зрения, принятой в книге [1]. Далее, числа пересечений схемы $\widehat{\mathcal{C}^{(m)}}$ (структурные константы кольца $\widehat{W^{(m)}}$) можно было бы назвать m-мерными числами пересечений схемы $\mathcal{C}$. В этом случае естественно считать m-мерные числа пересечений схем $\mathcal{C}$ и $\mathcal{C}'$ одинаковыми, если

числа пересечений схем $\mathcal{C}$ и $\mathcal{C}'$ одинаковы и соответствующий слабый изоморфизм φ имеет m-расширение. Таким образом, схема $\mathcal{C}$ характеризуется числами пересечений схемы $\widehat{\mathcal{C}}^{(m)}$ (m-мерными числами пересечений схемы $\mathcal{C}$) тогда и только тогда, когда $s(\mathcal{C}) \leqslant m$.

§4. Кольца Шура и кольца Кэли. Нормальность

4.1. 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 $X, Y \subset G$, где $\xi(X) = \sum_{x\in X} x$.

Согласно [20] (см. также [9]), 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. Число $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ называется *рангом* кольца $\mathcal{A}$. 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 $\mathcal{A}'$ равно образу кольца $\mathcal{A}$ относительно изоморфизма из $\mathbb{Z}[G]$ в $\mathbb{Z}[G']$, индуцированного f.

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

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

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 подгрупп группы G, принадлежащих множеству $\mathcal{S}^*(\mathcal{A})$, обозначается через $\mathcal{H}(\mathcal{A})$. Нетрудно проверить, что $\mathcal{H}(\mathcal{A})$ содержит любую подгруппу $\langle X\rangle$, порожденную множеством $X \in \mathcal{S}^*(\mathcal{A})$.

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. Мы называем такое S-кольцо *орбитным* и обозначаем его через $\mathcal{O}(K, G)$.

Пусть $\mathcal{A}_1$ и $\mathcal{A}_2$ — S-кольца над группами G_1 и G_2 соответственно. Тогда их тензорное произведение $\mathcal{A}_1 \otimes \mathcal{A}_2$ является очевидно S-кольцом над группой $G_1 \times G_2$, причем $\mathcal{S}(\mathcal{A}_1 \otimes \mathcal{A}_2) = \{X_1 \times X_2 : X_1 \in \mathcal{S}(\mathcal{A}_1), X_2 \in \mathcal{S}(\mathcal{A}_2)\}$. В случае орбитных S-колец справедливо также следующее равенство:

$$\mathcal{O}(K_1 \times K_2, G_1 \times G_2) = \mathcal{O}(K_1, G_1) \otimes \mathcal{O}(K_2, G_2), \tag{12}$$

где $K_i \leqslant \mathrm{Aut}(G_i)$, $i = 1, 2$.

Пусть $\mathcal{A}$ — S-кольцо над группой G, $H \in \mathcal{H}(\mathcal{A})$ 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 подгруппа 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, причем

$$\mathcal{S}(\mathcal{A}_{G/H}) = \{\pi(X) : X \in \mathcal{S}(\mathcal{A})\}. \tag{13}$$

(Мы сохраняем обозначения i и π также для индуцированных гомоморфизмов соответствующих $\mathbb{Z}$-модулей.) Для $X \subset G$ множество

$$\mathrm{rad}(X) = \{g \in G : gX = Xg = X\} \tag{14}$$

является очевидным образом подгруппой группы G; она называется *радикалом* множества X. Эквивалентно, $\mathrm{rad}(X)$ определяется как наибольшая подгруппа группы G, для которой множество X является объединением как левых, так и правых классов смежности по ней. Из определения следует, что $\mathrm{rad}(\pi(X)) = \pi(\mathrm{rad}(X))$ для любого эпиморфизма π группы G такого, что $\ker(\pi) \leqslant \mathrm{rad}(X)$. В частности, если $\ker(\pi) = \mathrm{rad}(X)$, то $\mathrm{rad}(\pi(X)) = \{1\}$. Если $X \in \mathcal{S}^*(\mathcal{A})$, то, как легко видеть, $\mathrm{rad}(X) \in \mathcal{H}(\mathcal{A})$.

4.2. S-кольца естественным образом приводят к клеточным кольцам специального вида, определяемым ниже.

Определение 4.1. Пусть G — группа. Клеточное кольцо $W \leqslant \mathrm{Mat}_G$ называется кольцом Кэли над G, если группа G_{right} содержится в группе $\mathrm{Aut}(W)$.

Из определения следует, что каждое кольцо Кэли однородно. Наименьшим и наибольшим кольцами Кэли над G являются соответственно кольца $Z(\mathrm{Sym}(G))$ и $Z(G_{\mathrm{right}})$. Отметим, что каждое базисное отношение кольца Кэли над G может рассматриваться как множество ребер некоторого графа Кэли на G, а схема, соответствующая этому кольцу, — как раскрашенный граф Кэли на G.

Для группы G отображение

$$\rho_G : \mathbb{Z}[G] \to \mathrm{Mat}_G(\mathbb{Z}), \quad g \mapsto P_g, \tag{15}$$

где P_g — перестановочная матрица, отвечающая левому умножению на g, является, очевидно, кольцевым мономорфизмом, образ которого совпадает с обертывающим кольцом группы G_{left}, т.е. с $\mathcal{Z}(G_{\mathrm{right}})$. Более того, это отображение переводит адамарово умножение и инволюцию кольца $\mathbb{Z}[G]$ в адамарово умножение и инволюцию кольца Mat_G. Легко видеть, что мономорфизм (15) индуцирует биекцию $X \mapsto X^{\rho_G}$ между подмножествами группы G и бинарными отношениями на G, инвариантными относительно группы G_{right}, такую, что $A(X^{\rho_G}) = \rho_G(\xi(X))$. Следующее утверждение следует непосредственно из определений.

Теорема 4.2. *Отображение* (15) *определяет биекцию* $\mathcal{A} \mapsto W$ *между S-кольцами над* G *и кольцами Кэли над* G. *Более того,* $\mathcal{S}(\mathcal{A})^{\rho_G} = \mathcal{R}(W)$, $\mathcal{S}^*(\mathcal{A})^{\rho_G} = \mathcal{R}^*(W)$, $\mathcal{H}(\mathcal{A})^{\rho_G} = \mathcal{E}(W)$ *и для* $H \in \mathcal{H}(\mathcal{A})$ *имеют место равенства* $G/E = \{Hg : g \in G\}$, *где* $E = H^{\rho_G}$, *и* $\rho_H(\mathcal{A}_H) = W_H$. •

Теорема 4.2 дает возможность перенести понятия слабого и сильного изоморфизмов с клеточных колец на S-кольца. А именно S-кольца $\mathcal{A}$ над G и $\mathcal{A}'$ над G' называются *слабо-изоморфными* (см. (4)), если существует $\mathbb{Z}$-модульный изоморфизм $\varphi : \mathcal{A} \to \mathcal{A}'$ (называемый *слабым изоморфизмом* из $\mathcal{A}$ в $\mathcal{A}'$) такой, что

$$\varphi(\xi \cdot \eta) = \varphi(\xi) \cdot \varphi(\eta), \quad \varphi(\xi \circ \eta) = \varphi(\xi) \circ \varphi(\eta) \quad \text{для всех } \xi, \eta \in \mathcal{A}. \tag{16}$$

Из леммы 2.1 следует, что φ индуцирует биекцию $X \mapsto X^\varphi$ из $\mathcal{S}^*(\mathcal{A})$ на $\mathcal{S}^*(\mathcal{A}')$ такую, что $\varphi(\xi(X)) = \xi(X^\varphi)$ (эта биекция переводит $\mathcal{S}(\mathcal{A})$ в $\mathcal{S}(\mathcal{A}')$ и $\mathcal{H}(\mathcal{A})$ в $\mathcal{H}(\mathcal{A}')$). Можно доказать также, что $(X^{-1})^\varphi = (X^\varphi)^{-1}$ и $|X^\varphi| = |X|$ для всех $X \in \mathcal{S}^*(\mathcal{A})$.

Аналогично под сильным изоморфизмом из $\mathcal{A}$ в $\mathcal{A}'$ мы понимаем сильный изоморфизм соответствующих колец Кэли, переводящий 1_G в $1_{G'}$ (заметим, что если кольца Кэли сильно-изоморфны, то, очевидно, существует сильный изоморфизм такого вида). Отсюда следует, что каждый сильный изоморфизм S-колец индуцирует слабый изоморфизм этих колец, отвечающий слабому изоморфизму соответствующих колец Кэли.

Лемма 4.3. *Биекция* $f : G \to G'$ *является сильным изоморфизмом из* $\mathcal{A}$ *в* $\mathcal{A}'$ *тогда и только тогда, когда*

$$f([x]y) = [f(x)]f(y), \quad x, y \in G. \tag{17}$$

В частности, любой изоморфизм Кэли S-колец является сильным изоморфизмом.

Доказательство. Пусть f — сильный изоморфизм из $\mathcal{A}$ в $\mathcal{A}'$. Тогда $f \in \mathrm{Iso}(W, W')$, где $W = \rho_G(\mathcal{A})$ и $W' = \rho_{G'}(\mathcal{A}')$, причем $f(1) = 1$. Для $X \in \mathcal{S}(\mathcal{A})$

положим $R = X^{\rho_G}$, $R' = R^f$, $X' = (R')^{\rho_{G'}^{-1}}$. Из определений следует, что для $x, y \in G$ мы имеем

$$x \in X \iff (y, xy) \in R \iff (f(y), f(xy)) \in R' \iff f(xy)f(y)^{-1} \in X'.$$

Поскольку изоморфизм f является биекцией, это влечет, что $f(Xy)f(y)^{-1} = X'$. Последнее равенство показывает, что $X' = f(X)f(1)^{-1} = f(X)$, и потому может быть переписано в виде $f([x]y)f(y)^{-1} = [f(x)]$, где $x \in X$, что завершает доказательство. •

По аналогии с клеточными кольцами мы используем обозначения $\mathrm{Isow}(\mathcal{A}, \mathcal{A}')$, $\mathrm{Isow}(\mathcal{A})$, $\mathrm{Iso}(\mathcal{A}, \mathcal{A}')$, $\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$, $\mathrm{Iso}(\mathcal{A})$, $\mathrm{Iso}(\mathcal{A}, \varphi)$ и $\mathrm{Aut}(\mathcal{A})$. Последняя группа называется *группой автоморфизмов* S-кольца $\mathcal{A}$. Из ее определения следует, что

$$\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(W)_v, \quad \mathrm{Aut}(W) = G_{\mathrm{right}}\,\mathrm{Aut}(\mathcal{A}), \tag{18}$$

где W — кольцо Кэли, соответствующее S-кольцу $\mathcal{A}$, и $v = 1_G$. Легко видеть, что группа $\mathrm{Aut}(\mathcal{A})$ тривиальна, если $\mathcal{A} = \mathbb{Z}[G]$, и равна $\mathrm{Sym}(G)_v$, если $\mathrm{rk}(\mathcal{A}) = 2$. Без труда проверяется также, что $\mathrm{Aut}(\mathcal{A}_1 \otimes \mathcal{A}_2) = \mathrm{Aut}(\mathcal{A}_1) \times \mathrm{Aut}(\mathcal{A}_2)$. S-кольцо $\mathcal{A}$ называется *шуровым*, если кольцо W шурово, т.е. если $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A}))$. Отметим, что каждое орбитное S-кольцо, очевидно, шурово.

Пусть $\varphi \in \mathrm{Isow}(\mathcal{A}, \mathcal{A}')$. Если $H \in \mathcal{H}(\mathcal{A})$, то, следуя [9], обозначим через φ_H слабый изоморфизм из $\mathcal{A}_H$ в $\mathcal{A}_{H'}$, индуцированный слабым изоморфизмом φ. Если дополнительно H нормальна в G, то обозначим через $\varphi_{G/H}$ слабый изоморфизм из $\mathcal{A}_{G/H}$ в $\mathcal{A}'_{G'/H'}$, индуцированный слабым изоморфизмом φ. Для $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ мы используем аналогичные обозначения f_H и $f_{G/H}$. Если $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$, то, очевидно, $f_H \in \mathrm{Iso}(\mathcal{A}_H, \mathcal{A}'_{H'}, \varphi_H)$ и $f_{G/H} \in \mathrm{Iso}(\mathcal{A}_{G/H}, \mathcal{A}'_{G/H'}, \varphi_{G/H})$.

4.3. Кольцо Кэли W над группой G называется *нормальным*, если G_{right} является нормальной подгруппой группы $\mathrm{Aut}(W)$. Поскольку каждая регулярная группа 2-замкнута, каждое регулярное кольцо Кэли нормально. Более общо, кольцо $\mathcal{Z}(\Gamma)$ является нормальным кольцом Кэли, если Γ является 2-замкнутой подгруппой группы $\mathrm{Sym}(G)$ такой, что $G \leqslant \Gamma \leqslant G \cdot \mathrm{Aut}(G)$. В действительности каждое шурово нормальное кольцо Кэли может быть получено таким путем (см. следствие 4.6). Однако существуют и нешуровы нормальные кольца. Простой пример получается из нешурова S-кольца над элементарной абелевой группой порядка p^2 при $p \geqslant 5$ [16, 20].

В настоящей статье мы полностью описываем нормальные кольца Кэли над циклической группой. В общем случае мы ограничимся перечислением лишь некоторых простейших свойств.

Лемма 4.4. *Имеют место следующие утверждения*:

(1) *каждое кольцо Кэли, содержащее нормальное кольцо Кэли над той же группой, является нормальным*;
(2) *тензорное произведение колец Кэли нормально тогда и только тогда, когда нормален каждый сомножитель.* •

Приведем простую характеризацию нормальных колец Кэли.

Теорема 4.5. *Пусть W — кольцо Кэли над группой G. Тогда W нормально в том и только в том случае, если* $\mathrm{Aut}(W) \leqslant G \cdot \mathrm{Aut}(G)$.

Доказательство. Достаточность очевидна. Обратно, пусть кольцо W нормально. Достаточно проверить, что $\mathrm{Aut}(W)_v \leqslant \mathrm{Aut}(G)$, где $v = 1_G$. Поскольку группа $\mathrm{Aut}(W)_v$ нормализует группу G_{right}, для каждого $f \in \mathrm{Aut}(W)_v$ существует $\sigma_f \in \mathrm{Aut}(G)$ такой, что

$$f^{-1} g_{\mathrm{right}} f = (g^{\sigma_f})_{\mathrm{right}}, \quad g \in G, \tag{19}$$

где g_{right} — перестановка множества G, индуцированная правым умножением на g. Образы точки v под действием перестановок из левой и правой частей формулы (19) равны соответственно $(v^{f^{-1}} g)^f = g^f$ и $v g^{\sigma_f} = g^{\sigma_f}$. Таким образом, из (19) следует, что $g^f = g^{\sigma_f}$ для всех $g \in G$. Это означает, что $f = \sigma_f$, откуда вытекает требуемое утверждение. •

В качестве следствия мы получаем следующее утверждение, которое ниже будет в значительной степени уточнено для циклических групп (см. следствие 6.3).

Следствие 4.6. *Группы автоморфизмов нормальных колец Кэли над группой G суть в точности 2-замкнутые подгруппы ее голоморфа $G \cdot \mathrm{Aut}(G)$, содержащие G.* •

Будем говорить, что S-кольцо является нормальным, если нормально соответствующее ему кольцо Кэли. Легко видеть, что для нормальных S-колец справедлив аналог леммы 4.4. Более того, в качестве следствия теоремы 4.5 и равенств (18) мы получаем следующее утверждение.

Теорема 4.7. *Пусть $\mathcal{A}$ — S-кольцо над группой G. Тогда $\mathcal{A}$ нормально в том и только в том случае, если* $\mathrm{Aut}(\mathcal{A}) \leqslant \mathrm{Aut}(G)$. •

4.4. Важным примером нормального кольца Кэли является собственное циклотомическое кольцо W на конечном поле $\mathbb{F}$, т.е. кольцо смежности собственной циклотомической схемы $\mathcal{C}$ на $\mathbb{F}$ (см. §1). Действительно, поскольку $\mathrm{Aut}(W) = \mathrm{Aut}(\mathcal{C})$, равенство (1) показывает, что W — нормальное кольцо

Кэли над аддитивной группой поля $\mathbb{F}$. Опишем две другие естественные конструкции нормальных колец Кэли, получающиеся из циклотомических схем. Они будут использованы при доказательстве основных результатов статьи.

Обозначим через A и G аддитивную и мультипликативную группы поля $\mathbb{F}$ и через $\Gamma = A \cdot G$ их полупрямое произведение, в котором G действует на A умножениями, так что $(a_1 \cdot g_1)(a_2 \cdot g_2) = (a_1 g_2 + a_2) \cdot (g_1 g_2)$. Отметим, что группа $\mathrm{Aut}(\mathbb{F})$ точно действует на группах A, G и Γ как группа их автоморфизмов. Ниже мы будем отождествлять $\mathrm{Aut}(\mathbb{F})$ с соответствующими подгруппами групп $\mathrm{Aut}(A)$, $\mathrm{Aut}(G)$ и $\mathrm{Aut}(\Gamma)$. Действие полупрямого произведения $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ на поле $\mathbb{F}$ задается формулой

$$x^{\gamma \cdot \sigma} = a + x^{\sigma} g, \quad \gamma = a \cdot g \in \Gamma, \quad \sigma \in \mathrm{Aut}(\mathbb{F}), \quad x \in \mathbb{F}. \tag{20}$$

Легко видеть, что отображение

$$\widehat{f} : \mathbb{F}^2 \setminus \Delta \to \Gamma, \quad (x, y) \mapsto x \cdot (y - x),$$

где $\Delta = \Delta^{(2)}(\mathbb{F})$, является биекцией. Более того, оно переводит покоординатное действие группы $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ на $\mathbb{F}^2 \setminus \Delta$ в естественное действие группы $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ на Γ (Γ действует на себе правыми умножениями).

Пусть W — циклотомическое кольцо на $\mathbb{F}$. Положим

$$W' = ((W_u)_{\mathbb{F}^\times})^f, \quad \widehat{W}' = (\widehat{W}_{\widehat{\mathbb{F}}^\times})^{\widehat{f}}, \tag{21}$$

где $u = 0_{\mathbb{F}}$, $\mathbb{F}^\times = \mathbb{F} \setminus \{u\}$, $f : \mathbb{F}^\times \to G$ — тождественное отображение, $\widehat{\mathbb{F}}^\times = \mathbb{F}^2 \setminus \Delta$ и $\widehat{W} = \widehat{W}^{(2)}$. Из очевидного включения $\mathrm{AGL}(1, \mathbb{F}) \leqslant \mathrm{Iso}(W)$ следует, что $G_{\mathrm{right}} \leqslant \mathrm{Iso}(W')$ и $\Gamma_{\mathrm{right}} \leqslant \mathrm{Iso}(\widehat{W}')$. Поэтому, используя конструкцию, описанную в конце п. 2.5, можно ввести в рассмотрение клеточные кольца

$$W^* = (W')^{G_{\mathrm{right}}}, \quad \widehat{W}^* = (\widehat{W}')^{\Gamma_{\mathrm{right}}}. \tag{22}$$

Таким образом, W^* — кольцо Кэли над G и $\widehat{W}^*$ — кольцо Кэли над Γ. Опишем свойства кольца $\widehat{W}^*$, которые будут использованы в следующей теореме и теореме 8.1.

Прямое вычисление показывает, что эквивалентность на множестве $\widehat{\mathbb{F}}^\times$, определяемая равенством первых координат, и отношение степени 1 на том же множестве, определяемое перестановкой координат (очевидно, принадлежащие множеству $\mathcal{R}^*(\widehat{W}_{\widehat{\mathbb{F}}^\times})$ и инвариантные относительно группы Γ) переводятся отображением $\widehat{f}$ соответственно в $E_G = G^{\rho_\Gamma}$ и $R_s = \{s\}^{\rho_\Gamma}$, где s — элемент группы Γ с A-компонентой $1_{\mathbb{F}}$ и G-компонентой $-1_{\mathbb{F}}$. Поэтому

$$E_G \in \mathcal{E}(\widehat{W}^*), \quad R_s \in \mathcal{R}(\widehat{W}^*). \tag{23}$$

Отметим также, что $s^2 = 1_\Gamma$ и что эквивалентность $E_{G_1} = (G_1)^{\rho_\Gamma}$, где $G_1 = sGs$, является образом эквивалентности на множестве $\widehat{\mathbb{F}}^\times$, определяемой равенством вторых координат. Таким образом, $E_{G_1} \in \mathcal{E}(\widehat{W}^*)$.

Теорема 4.8. *Пусть W — собственное циклотомическое кольцо на конечном поле $\mathbb{F}$. Тогда во введенных выше обозначениях имеют место следующие утверждения:*

(1) $\mathrm{Aut}(W^*) \leqslant G \cdot \mathrm{Aut}(\mathbb{F})$ *и* $\mathrm{Aut}(\widehat{W}^*) \leqslant \Gamma \cdot \mathrm{Aut}(\mathbb{F})$; *в частности, кольца Кэли W^* и $\widehat{W}^*$ нормальны;*

(2) $G \in \mathcal{B}(\widehat{W}^*)$ *и* $(\widehat{W}^*)_G \geqslant W^*$;

(3) *клеточные кольца W_u и W^* (соответственно $\widehat{W}$ и $\widehat{W}^*$) шуровы или нет одновременно.*

Доказательство. Докажем утверждения (1) и (3). Заметим прежде всего, что условия леммы 9.4 из §9 выполнены для кольца W при $X = \mathbb{F}^\times$ и для кольца $\widehat{W}$ при $X = \widehat{\mathbb{F}}^\times$ (в последнем случае $\Delta \in \mathrm{Cel}(\widehat{W})$, и мы полагаем $R_\Delta = (\widehat{\mathbb{F}}^\times \times \Delta) \cap E$, где E — эквивалентность кольца $\widehat{W}$, определяемая равенством первых координат). Таким образом, по утверждению (1) этой леммы мы имеем

$$\mathrm{Aut}((W_u)_{\mathbb{F}^\times}) = \mathrm{Aut}(W)_{\mathbb{F}^\times}, \quad \mathrm{Aut}((\widehat{W}_{\widehat{\mathbb{F}}^\times}) = \mathrm{Aut}(\widehat{W})_{\widehat{\mathbb{F}}^\times},$$

причем клеточные кольца W_u, $(W_u)_{\mathbb{F}^\times}$ и W' (соответственно $\widehat{W}$, $\widehat{W}_{\widehat{\mathbb{F}}^\times}$ и $\widehat{W}'$) шуровы или нет одновременно. В силу включения (1) группа $\mathrm{Aut}(W)_{\mathbb{F}^\times}$ (соответственно $\mathrm{Aut}(\widehat{W})_{\widehat{\mathbb{F}}^\times}$) содержится в группе перестановок, определяемой, согласно (20), естественным действием группы $G \cdot \mathrm{Aut}(\mathbb{F})$ (соответственно $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$) на множестве $\mathbb{F}^\times$ (соответственно $\widehat{\mathbb{F}}^\times$). Таким образом,

$$\mathrm{Aut}(W') \leqslant G \cdot \mathrm{Aut}(\mathbb{F}), \quad \mathrm{Aut}(\widehat{W}') \leqslant \Gamma \cdot \mathrm{Aut}(\mathbb{F}),$$

и для завершения доказательства утверждений (1) и (3) достаточно проверить, что условия леммы 2.2 выполняются как для кольца W' и группы G_{right}, так и для кольца $\widehat{W}'$ и группы Γ_{right}. Для проверки этого заметим, что окрестность точки u в базисном отношении клеточного кольца W является клеточным множеством кольца W_u, в то время как само базисное отношение является клеточным множеством кольца $\widehat{W}$ (первое очевидно, а второе следует из [5, предложение 3.6(1)]). Поскольку W — шурово кольцо, оба клеточных множества в действительности являются клетками. Поэтому любая клетка кольца $(W_u)_{\mathbb{F}^\times}$ имеет вид Hg, а любая клетка кольца $\widehat{W}_{\widehat{\mathbb{F}}^\times}$ имеет вид $\{(x, y) \in \widehat{\mathbb{F}}^\times : x - y \in Hg\}$, где H — группа из определения циклотомической схемы. Таким образом,

$$\mathrm{Cel}(W') = \{Hg : g \in G\}, \quad \mathrm{Cel}(\widehat{W}') = \{AH\gamma : \gamma \in \Gamma\}.$$

Далее, группа G_{right} регулярно действует на множестве $\mathrm{Cel}(W')$, а группа Γ_{right} регулярно действует на множестве $\mathrm{Cel}(\widehat{W}')$. Поскольку ядра этих действий равны соответственно $H \leqslant \mathrm{Aut}(W')$ и $AH \leqslant \mathrm{Aut}(\widehat{W}')$, условия леммы 2.2 действительно выполнены.

Докажем утверждение (2). Заметим сначала, что $G \in \mathcal{B}(\widehat{W}^*)$, поскольку эквивалентность $E_G = G^{\rho_\Gamma}$ принадлежит множеству $\mathcal{E}(\widehat{W}^*)$ (см. формулу (23) и теорему 4.2). Далее, поскольку группа Γ_{right} регулярно действует на множестве $\Gamma/E_G = \{G\gamma : \gamma \in \Gamma\}$ и стабилизатор множества G в этой группе равен G_{right}, мы имеем

$$(\widehat{W}^*)_G = ((\widehat{W}')^{\Gamma_{\mathrm{right}}})_G = (\widehat{W}'_G)^{G_{\mathrm{right}}}. \tag{24}$$

С другой стороны, обозначим через $\widehat{f}_1 : U\setminus\{(u,u)\} \to G$ и $\zeta_1 : \mathbb{F}^\times \to U\setminus\{(u,u)\}$ биекции, индуцированные отображениями $\widehat{f}$ и ζ, где $U = \{u\} \times \mathbb{F}$. Тогда, очевидно, $\zeta_1 \circ \widehat{f}_1 = f$. Применяя лемму 3.1 при $m = 2$ и $v_1 = u$, мы находим, что

$$\widehat{W}'_G = ((\widehat{W}_{\mathbb{F}^\times})^{\widehat{f}})_G = ((\widehat{W}_U)_{U\setminus\{(u,u)\}})^{\widehat{f}_1} \geqslant (((W_u)_{\mathbb{F}^\times})^{\zeta_1})^{\widehat{f}_1} = ((W_u)_{\mathbb{F}^\times})^f = W'. \tag{25}$$

Таким образом, утверждение (2) следует из (24), (25) и определения кольца W^*. •

§5. Кольца Шура над циклической группой

5.1. Напомним основные факты о конечных циклических группах (см., например, [17]). Пусть G — конечная циклическая группа порядка n и $\mathcal{P}(G)$ — множество всех простых делителей числа n. Для $p \in \mathcal{P}(G)$ обозначим через G_p силовскую p-подгруппу группы G. Тогда имеют место канонические разложения

$$G = \prod_{p\in\mathcal{P}(G)} G_p, \quad \mathrm{Aut}(G) = \prod_{p\in\mathcal{P}(G)} \mathrm{Aut}(G_p). \tag{26}$$

Каждый автоморфизм группы G имеет вид $x \mapsto x^m$ для некоторого целого числа m, взаимно-простого с n; мы обозначаем его через $\sigma_m = \sigma_{m,G}$.

Пусть $p \in \mathcal{P}(G)$. Тогда $|G_p| = p^k$, где $k \geqslant 1$. Если p нечетно, то $\mathrm{Aut}(G_p)$ является циклической группой порядка $(p-1)p^{k-1}$. Если $p = 2$, то группа $\mathrm{Aut}(G_p)$ тривиальна при $k = 1$ и изоморфна прямому произведению циклической группы порядка 2 и циклической группы порядка 2^{k-2} при $k \geqslant 2$. Точнее,

$$\mathrm{Aut}(G_p) = A_{1,p} \times A_{2,p}, \tag{27}$$

где группы $A_{1,p}$ и $A_{2,p}$ определяются следующим образом. Если p нечетно, то $A_{1,p}$ — единственная подгруппа группы $\mathrm{Aut}(G_p)$ порядка $p-1$, в то время как $A_{2,p} = \{\sigma_m : m = 1 \pmod p\}$. Если $p = 2$, то $A_{1,p} = \{\sigma_1, \sigma_{-1}\}$ и $A_{2,p} = \{\sigma_m : m = 1 \pmod 4\}$.

Пусть $K \leqslant \mathrm{Aut}(G)$. Если g — образующая группы G, то, очевидно, радикал множества $\{g^\sigma : \sigma \in K\}$ не зависит от выбора g. Мы называем эту подгруппу группы G *радикалом* группы K и обозначаем ее через $\mathrm{rad}(K)$. Следующее утверждение в случае, когда G является p-группой, фактически характеризует те K, для которых $|\mathrm{rad}(K)| \leqslant 2$.

N	$K=\{\sigma_m : m\in M\}$	k	$\lvert\mathrm{rad}(K)\rvert$	$\lvert K\rvert$
1	$M=\{1\}$	$k\geqslant 0$	1	1
2	$M=\{1,n/2\}$	$k\geqslant 2$	2	2
3	$M=\{1,-1\}$	$k\geqslant 3$	1	2
4	$M=\{1,1+n/2,-1,-1+n/2\}$	$k\geqslant 4$	2	4
5	$M=\{1,-1+n/2\}$	$k\geqslant 3$	1	2
6	$M=\{1,1+n/2,-1+n/4,-1+3n/4\}$	$k\geqslant 4$	2	4

Лемма 5.1. *Пусть G — циклическая группа порядка $n=p^k$ и $K\leqslant \mathrm{Aut}(G)$. Тогда*

(1) *если p нечетно, то $|\mathrm{rad}(K)|=1$ тогда и только тогда, когда $K\leqslant A_{1,p}$;*
(2) *если $p=2$, то $|\mathrm{rad}(K)|\leqslant 2$ тогда и только тогда, когда группа K принадлежит одному из шести семейств, перечисленных в таблице.*

Доказательство. Пусть p нечетно. Тогда, очевидно, $K\cap A_{2,p}=\{\sigma_m : m=1\,(\mathrm{mod}\,p^r)\}$ для единственным образом определенного натурального числа $r\leqslant k$. Поэтому $\mathrm{rad}(K)$ является подгруппой группы G индекса p^r. Следовательно, $|\mathrm{rad}(K)|=1$ тогда и только тогда, когда $K\cap A_{2,p}=\{1\}$. В силу (27) это доказывает утверждение (1). Если $p=2$, то по (27) при $|K|\geqslant 8$ мы имеем $|K\cap A_{2,p}|\geqslant 4$, и потому $|\mathrm{rad}(K)|\geqslant 4$. Таким образом, неравенство $|\mathrm{rad}(K)|\leqslant 2$ влечет, что $|K|\leqslant 4$. Теперь утверждение (2) проверяется прямым вычислением. •

В завершение пункта упомянем еще один факт о группах автоморфизмов циклических групп. Пусть H — подгруппа циклической группы G. Тогда естественные гомоморфизмы

$$\pi_H : \mathrm{Aut}(G)\to\mathrm{Aut}(H),\quad \pi_{G/H} : \mathrm{Aut}(G)\to\mathrm{Aut}(G/H) \tag{28}$$

являются сюръекциями.

5.2. Для описания структуры S-колец над конечной циклической группой нам потребуется следующее определение.

Определение 5.2. Пусть $\mathcal{A}$ — S-кольцо над группой G и L,U — ее подгруппы. Будем говорить, что $\mathcal{A}$ удовлетворяет *U/L-условию*, если выполнены следующие три условия:

(1) $L\leqslant U$ и L нормальна в G;
(2) $L,U\in\mathcal{H}(\mathcal{A})$;
(3) $L\leqslant\mathrm{rad}(X)$ для всех $X\in\mathcal{S}(\mathcal{A})$ таких, что $X\subset G\setminus U$.

Если, кроме того, $L \neq \{1\}$ и $U \neq G$, то мы говорим, что $\mathcal{A}$ удовлетворяет U/L-условию нетривиально.

S-кольцо $\mathcal{A}$, удовлетворяющее U/L-условию, было названо в статьях [11, 12] „wedge product" S-колец $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$. Следует отметить, что в работе [9] авторы независимо ввели операцию обобщенного сплетения двух S-колец, с помощью которой получаются в точности все S-кольца, удовлетворяющие U/L-условию.

Описание всех S-колец над циклической группой было получено в [11, 12]. В следующих двух теоремах мы переформулируем эти результаты в виде, удобном для последующего использования. Ниже S-кольцо $\mathcal{A}$ над группой G называется *плотным*,[5] если множество $\mathcal{H}(\mathcal{A})$ содержит все подгруппы группы G. Легко видеть, что любое орбитное S-кольцо плотно.

Теорема 5.3. *Пусть $\mathcal{A}$ — S-кольцо над конечной циклической группой G. Предположим, что оно не является плотным. Тогда справедливо по крайней мере одно из следующих двух утверждений*:

(1) *$\mathcal{A}$ нетривиально удовлетворяет U/L-условию для некоторых подгрупп L, U группы G таких, что произведение $|L| \cdot |G/U|$ не является квадратом простого числа*;

(2) *$\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1$ — S-кольцо ранга 2 над подгруппой составного порядка группы G.*

Доказательство. Заметим, что в контексте теоремы утверждение (2) можно заменить на следующее: либо $\mathrm{rk}(\mathcal{A}) = 2$, либо $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1 \neq \mathcal{A}$ и $\mathcal{A}_2 \neq \mathcal{A}$. Действительно, если $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, то $\mathcal{A}_1 = \mathcal{A}_{G_1}$, $\mathcal{A}_2 = \mathcal{A}_{G_2}$ для некоторых подгрупп $G_1, G_2 \in \mathcal{H}(\mathcal{A})$ таких, что $G = G_1 \times G_2$. Поскольку кольцо $\mathcal{A}$ не является плотным, то по крайней мере одно из S-колец $\mathcal{A}_1$, $\mathcal{A}_2$, скажем $\mathcal{A}_1$, также не является плотным, и потому по индукции можно считать, что для $\mathcal{A}_1$ выполнено утверждение (1) или утверждение (2). В последнем случае требуемое утверждение очевидно. В первом же случае кольцо $\mathcal{A}_1$ нетривиально удовлетворяет U_1/L_1-условию для некоторых подгрупп L_1, U_1 группы G_1 таких, что $|L_1| \cdot |G_1/U_1|$ не равно квадрату простого числа. Но тогда, очевидно, кольцо $\mathcal{A}$ нетривиально удовлетворяет U/L-условию для $U = U_1 \times G_2$ и $L = L_1$. Поскольку $|G/U| = |G_1/U_1|$, требуемое утверждение доказано.

Выведем теорему из результатов статьи [12], сохраняя используемую в ней нумерацию утверждений. Не умаляя общности, будем считать, что $\mathrm{rk}(\mathcal{A}) > 2$. Предположим, что некоторая силовская подгруппа группы G не принадлежит множеству $\mathcal{H}(\mathcal{A})$. Тогда легко видеть, что выполнено условие следствия 4.3 или теоремы 4.5. В первом случае по следствию 4.3 получаем, что либо $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1 \neq \mathcal{A}$, $\mathcal{A}_2 \neq \mathcal{A}$, либо $\mathcal{A}$ нетривиально удовлетворяет U/L-условию так, что число $|G/U|$ является составным, и потому $|L| \cdot |G/U|$ не

[5]Этот термин был предложен М. Музычуком.

может быть квадратом простого числа. Во втором случае по теореме 4.5 кольцо $\mathcal{A}$ нетривиально удовлетворяет U/L-условию так, что $|G/U| = p$ — простое число. Согласно предложению 4.4, группа L может быть выбрана так, чтобы число $|L|$ не являлось степенью p, откуда снова следует требуемое утверждение. Пусть, наконец, множество $\mathcal{H}(\mathcal{A})$ содержит все силовские подгруппы группы G. Тогда по теореме 5.2 либо $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1 \neq \mathcal{A}$, $\mathcal{A}_2 \neq \mathcal{A}$, либо кольцо $\mathcal{A}$ нетривиально удовлетворяет U/L-условию так, что одно из чисел $|L|$, $|G/U|$ делится на p^2 для некоторого простого p. Таким образом, теорема полностью доказана. •

Для формулировки второй теоремы нам потребуется еще одно определение. Пусть $\mathcal{A}$ — S-кольцо над абелевой группой G. Тогда по теореме Шура [20, теорема 23.9] имеет место включение

$$\mathrm{Aut}(G) \leqslant \mathrm{Iso}(\mathcal{A}). \tag{29}$$

Предположим, что группа G циклическая. Тогда $\mathrm{Aut}(G)$ действует транзитивно на множестве ее образующих. Отсюда следует, что группа $\mathrm{rad}(X)$ не зависит от выбора множества $X \in \mathcal{S}(\mathcal{A})$, для которого $\langle X \rangle = G$. Мы называем ее *радикалом* кольца $\mathcal{A}$ и обозначаем через $\mathrm{rad}(\mathcal{A})$. Из определения 5.2 следует, что если $\mathcal{A}$ удовлетворяет U/L-условию, то $\mathrm{rad}(\mathcal{A}) \geqslant L$. Легко видеть также, что $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(K)$, когда $\mathcal{A} = \mathcal{O}(K, G)$ для некоторой группы $K \leqslant \mathrm{Aut}(G)$.

Теорема 5.4. *Пусть $\mathcal{A}$ — плотное S-кольцо над конечной циклической группой G. Тогда справедливо в точности одно из следующих двух утверждений:*

(1) $|\mathrm{rad}(\mathcal{A})| \geqslant 2$ *и $\mathcal{A}$ удовлетворяет U/L-условию для некоторых подгрупп L, U группы G таких, что $|L| = |G/U| = p$, где p — максимальный простой делитель числа $|\mathrm{rad}(\mathcal{A})|$,*

(2) $|\mathrm{rad}(\mathcal{A})| = 1$ *и $\mathcal{A}$ — орбитное S-кольцо.*

Доказательство. Следует из [11, теоремы 3.4, 3.6]. •

В качестве простого следствия теорем 5.3 и 5.4 мы получаем характеризацию S-колец, нетривиально удовлетворяющих U/L-условию.

Следствие 5.5. *S-кольцо над конечной циклической группой нетривиально удовлетворяет некоторому U/L-условию тогда и только тогда, когда его радикал нетривиален.* •

5.3. В этом пункте мы приводим в терминах U/L-условия сильное необходимое условие нормальности S-кольца над конечной циклической группой.

Пусть G (соответственно G') — группа и L, U (соответственно L', U') — подгруппы группы G (соответственно группы G') такие, что $L \leqslant U$ и L нормальна в G (соответственно $L' \leqslant U'$ и L' нормальна в G'). Пусть далее

$f_1 : U \to U'$ и $f_2 : G/L \to G'/L'$ — изоморфизмы групп, совпадающие на U/L. Для каждого левого класса смежности T группы G по подгруппе U выберем биекцию $f_T : T \to T'$, согласованную с f_2 и такую, что $f_T(ux) = f_1(u)f_T(x)$ для всех $u \in U$, $x \in T$, где T' — образ класса T относительно биекции из множества всех левых классов смежности группы G по подгруппе U на множество всех левых классов смежности группы G' по подгруппе U', индуцированной изоморфизмом f_2. Предположим, что $f_U = f_1$. Тогда отображение

$$f : G \to G', \quad x \mapsto f_T(x),$$

где $T = T(x)$ — класс смежности, содержащий элемент x, является биекцией. Обозначим через $\mathcal{F} = \mathcal{F}(f_1, f_2)$ множество всех таких f. Легко видеть, что $|\mathcal{F}| = |L|^{[G:U]-1}$.

Лемма 5.6. *Пусть $\mathcal{A}$ (соответственно $\mathcal{A}'$) — S-кольцо над группой G (соответственно G'), удовлетворяющее U/L-условию (соответственно U'/L'-условию), и f_1, f_2 — изоморфизмы Кэли из $\mathcal{A}_U$ в $\mathcal{A}'_{U'}$ и из $\mathcal{A}_{G/L}$ в $\mathcal{A}'_{G'/L'}$. Тогда $\mathcal{F} \subset \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$, причем $f_U = f_1$, $f_{G/L} = f_2$ для всех $f \in \mathcal{F}$.*

Доказательство. Пусть $f \in \mathcal{F}$. Тогда из определения множества $\mathcal{F}$ немедленно следуют равенства $f(xy) = f(x)f(y)$ для $x \in U$, $y \in G$ и $f(LxLy) = f(Lx)f(Ly)$ для всех $x, y \in G$. Первое из них показывает, что равенство (17) выполняется для всех $x \in U$ и $y \in G$. Если $x \notin U$, то по условию леммы множества $[x]$ и $[f(x)]$ являются объединениями классов смежности соответственно по L и L' (см. определение 5.2). Поэтому второе равенство показывает, что равенство (17) выполнено для всех $x \notin U$ и $y \in G$. Таким образом, $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ по лемме 4.3. Поскольку равенства $f_U = f_1$ и $f_{G/L} = f_2$ очевидны, лемма доказана. •

Применим лемму 5.6 для изучения нормальных S-колец над циклической группой.

Теорема 5.7. *Пусть $\mathcal{A}$ — нормальное S-кольцо над циклической группой G. Предположим, что $\mathcal{A}$ нетривиально удовлетворяет U/L-условию для некоторых подгрупп L и U группы G. Тогда $|L| = |G/U| = 2$.*

Доказательство. Применяя лемму 5.6 к $\mathcal{A} = \mathcal{A}'$ и тождественным отображениям f_1, f_2, получаем, что для каждого элемента $l \in L \setminus \{1\}$ группа $\mathrm{Aut}(\mathcal{A})$ содержит автоморфизм f, тождественный на U и переводящий x в lx при $x \in G \setminus U$. Поскольку кольцо $\mathcal{A}$ нормально, $f \in \mathrm{Aut}(G)$ по теореме 4.7. Поэтому для $x \in G \setminus U$ мы имеем

$$x^2 l^2 = f(x)^2 = f(x^2) = \begin{cases} x^2 l, & \text{если } x^2 \notin U, \\ x^2, & \text{в противном случае.} \end{cases} \tag{30}$$

С другой стороны, если $|G/U| \neq 2$, то цикличность группы G влечет, что существует $x \in G$, для которого $x^2 \notin U$. Таким образом, в силу (30) $l = 1$, что противоречит выбору l. Аналогично если $|L| \neq 2$, то существует $l \in L$, для которого $l^2 \neq 1$, что противоречит (30). •

Используя результаты этого параграфа, можно получить следующее несколько неожиданное утверждение.

Теорема 5.8. *Пусть $\mathcal{A}$ — S-кольцо над циклической группой G. Тогда* $\mathrm{Aut}(\mathcal{A}) = \{1\}$ *в том и только в том случае, если* $\mathcal{A} = \mathbb{Z}[G]$.

Доказательство. Достаточность очевидна. Пусть $\mathrm{Aut}(\mathcal{A}) = \{1\}$. Тогда лемма 5.6 показывает, что $\mathcal{A}$ не может нетривиально удовлетворять никакому U/L-условию. Таким образом, по теоремам 5.3 и 5.4 либо $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1$ — S-кольцо ранга 2 над группой составного порядка, либо $\mathcal{A} = \mathcal{O}(K, G)$, где $K \leqslant \mathrm{Aut}(G)$. Однако в первом случае, очевидно, $|\mathrm{Aut}(\mathcal{A})| \geqslant |\mathrm{Aut}(\mathcal{A}_1)| > 1$. Во втором же случае $\mathrm{Aut}(\mathcal{A}) \geqslant K$, и потому $|K| = 1$. Это означает, что $\mathcal{A} = \mathbb{Z}[G]$. •

§6. Критерий нормальности и его следствия

6.1. Сформулируем основной результат этой статьи о нормальных S-кольцах над циклической группой G, который будет доказан в §7. С этой целью для группы $K \leqslant \mathrm{Aut}(G)$ положим

$$\mathcal{P}^*(K) = \{p \in \mathcal{P}(G) : |G_p| = p,\ \mathrm{Aut}(G_p) \leqslant K\}.$$

Легко видеть, что условие $\mathrm{Aut}(G_p) \leqslant K$ равносильно равенству $K = \mathrm{Aut}(G_p) \times \pi_{G_{p'}}(K)$, где $G_{p'} = \prod_{l \in \mathcal{P}(G) \setminus \{p\}} G_l$ (см. (28)).

Теорема 6.1. *Пусть W — кольцо Кэли над циклической группой G и $\mathcal{A}$ — соответствующее ему S-кольцо. Тогда следующие утверждения эквивалентны:*

(1) *W — нормальное кольцо Кэли (эквивалентно, $\mathcal{A}$ — нормальное S-кольцо);*
(2) *$W_v = \mathcal{Z}(K, G)$ для некоторой группы $K \leqslant \mathrm{Aut}(G)$, где $v = 1_G$;*
(3) *$\mathcal{A} = \mathcal{O}(K, G)$ для некоторой группы $K \leqslant \mathrm{Aut}(G)$ такой, что $|\mathrm{rad}(K)| \leqslant 2$ и $\mathcal{P}^*(K) \subset \{2, 3\}$.*

Пусть W — нормальное кольцо Кэли над циклической группой G. Тогда по теореме 6.1 найдется группа $K \leqslant \mathrm{Aut}(G)$, для которой $W_v = \mathcal{Z}(K, G)$. Поскольку любая образующая группы G, очевидно, является регулярной точкой кольца $\mathcal{Z}(K, G)$, кольцо W_v является 1-регулярным (см. §9). В силу транзитивности группы $\mathrm{Aut}(W)$ это влечет, что любое одноточечное расширение кольца W является 1-регулярным. Таким образом, по лемме 9.2 при $s \geqslant 1$ расширение кольца W относительно произвольных точек $v_1, \ldots, v_s \in G$ также 1-регулярно, и мы приходим к следующему утверждению.

Следствие 6.2. *Любое s-точечное расширение нормального кольца Кэли над циклической группой является 1-регулярным при $s \geqslant 1$.* •

Из теоремы 6.1 ((1) $\Longrightarrow$ (3)) следует, что каждое нормальное кольцо Кэли над циклической группой шурово. Таким образом, следствие 4.6 влечет следующее утверждение.

Следствие 6.3. *Пусть G — циклическая группа. Тогда отображения*

$$\Gamma \mapsto \mathcal{Z}(\Gamma), \quad W \mapsto \mathrm{Aut}(W)$$

определяют биекцию между 2-замкнутыми подгруппами голоморфа группы G, содержащими G, и нормальными кольцами Кэли над G. •

Поскольку S-кольцо с тривиальным радикалом, очевидно, не может нетривиально удовлетворять никакому U/L-условию, теоремы 5.3, 5.4 и 6.1 ((3) $\Longrightarrow$ (1)) влекут в силу (12) следующее утверждение.

Следствие 6.4. *Радикал S-кольца над циклической группой тривиален тогда и только тогда, когда это кольцо равно тензорному произведению нормального S-кольца с тривиальным радикалом и S-колец ранга 2.* •

Из теоремы 6.1 ((1) $\Longrightarrow$ (3)) следует, что порядок радикала нормального S-кольца над циклической группой не превосходит 2. Если он равен 2, то структура соответствующего S-кольца может быть описана следующим образом.

Следствие 6.5. *Пусть $\mathcal{A}$ — нормальное S-кольцо над циклической группой G. Предположим, что $|\mathrm{rad}(\mathcal{A})| = 2$. Тогда $\mathcal{A}$ удовлетворяет U/L-условию, где L и U — подгруппы группы G такие, что $|L| = |G/U| = 2$ (в частности, $|G|$ делится на 4). Более того, $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ являются изоморфными по Кэли нормальными S-кольцами с тривиальным радикалом.*

Доказательство. По теореме 6.1 кольцо $\mathcal{A}$ орбитно и потому плотно. Поскольку $|\mathrm{rad}(\mathcal{A})| = 2$, из теоремы 5.4 следует, что это кольцо удовлетворяет U/L-условию так, что $|L| = |G/U| = 2$. Пусть $\mathcal{A} = \mathcal{O}(K, G)$, где $K \leqslant \mathrm{Aut}(G)$. Тогда $\mathcal{A}_U = \mathcal{O}(\pi_U(K), U)$ и $\mathcal{A}_{G/L} = \mathcal{O}(\pi_{G/L}(K), G/L)$ (см. (28)). Изоморфизм $G/L \to U$, переводящий Lg в g^2, где g — образующая группы G, индуцирует изоморфизм $\mathrm{Aut}(G/L) \to \mathrm{Aut}(U)$, переводящий $\pi_{G/L}(K)$ в $\pi_U(K)$. Поэтому он является изоморфизмом Кэли из $\mathcal{A}_{G/L}$ в $\mathcal{A}_U$. Для завершения доказательства достаточно проверить, что $\mathcal{A}_{G/L}$ является нормальным S-кольцом с тривиальным радикалом. Однако равенство $\mathrm{rad}(\mathcal{A}) = L$ влечет, что $\mathrm{rad}(\mathcal{A}_{G/L}) = \{1\}$. Далее, если $\pi_{G/L}(K) = \mathrm{Aut}((G/L)_p) \times K'$, где p — нечетное простое число и $K' \leqslant \mathrm{Aut}((G/L)_{p'})$, то

$$K = \pi_{G/L}^{-1}(\pi_{G/L}(K)) = \pi_{G/L}^{-1}(\mathrm{Aut}((G/L)_p) \times K') = \mathrm{Aut}(G_p) \times \pi_{G/L}^{-1}(K')$$

и $|G_p| = |(G/L)_p|$. Поэтому $\mathcal{P}^*(\pi_{G/L}(K)) \setminus \{2\} \subset \mathcal{P}^*(K)$. Таким образом, нормальность кольца $\mathcal{A}_{G/L}$ следует из нормальности $\mathcal{A}$ по теореме 6.1 ((1) $\Longleftrightarrow$ (3)). •

6.2. Как было доказано в [9], не каждый слабый изоморфизм S-колец над циклической группой индуцируется сильным изоморфизмом. Следующая теорема показывает, что для нормальных S-колец ситуация иная. Более того, в этом случае утверждение (2) этой теоремы может рассматриваться как уточнение включения (29). Принимая во внимание тот факт, что слабоизоморфные S-кольца над циклической группой являются изоморфными по Кэли (см. [15]), мы ограничиваемся рассмотрением изоморфизмов S-колец на себя.

Теорема 6.6. *Пусть $\mathcal{A}$ — нормальное S-кольцо над циклической группой G. Тогда*

(1) *каждый слабый изоморфизм кольца $\mathcal{A}$ индуцируется сильным изоморфизмом*;
(2) $[\mathrm{Iso}(\mathcal{A}) : \mathrm{Aut}(G)] \leqslant 2$; *более того,* $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(G)$ *тогда и только тогда, когда либо* $|\mathrm{rad}(\mathcal{A})| = 1$, *либо* $|\mathrm{rad}(\mathcal{A})| = 2$ *и порядок силовской 2-подгруппы группы G равен 4.*

Доказательство. Из теоремы 6.1 ((1) $\Longleftrightarrow$ (3)) следует, что S-кольцо $\mathcal{A}$ является орбитным и $|\mathrm{rad}(\mathcal{A})| \leqslant 2$. Если $|\mathrm{rad}(\mathcal{A})| = 1$, то достаточно доказать следующее утверждение.

Лемма 6.7. *В обозначениях и предположениях теоремы 6.6 пусть* $\mathrm{rad}(\mathcal{A}) = \{1\}$. *Тогда*

(1) *каждый слабый изоморфизм кольца $\mathcal{A}$ индуцируется изоморфизмом Кэли*;
(2) $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(G)$.

Доказательство. Зафиксируем базисное множество X кольца $\mathcal{A}$, содержащее образующую группы G. Мы покажем, что наименьшее S-кольцо $\mathcal{A}'$, содержащее элемент $\xi(X)$, совпадает с $\mathcal{A}$. С этой целью заметим, что $\mathrm{rad}(X) = \mathrm{rad}(\mathcal{A}) = \{1\}$. Поскольку, очевидно, $X \in \mathcal{S}(\mathcal{A}')$, то $\mathrm{rad}(\mathcal{A}') = \mathrm{rad}(X) = \{1\}$. Поэтому кольцо $\mathcal{A}'$ не может нетривиально удовлетворять никакому U/L-условию. По теореме 5.3 это влечет, что кольцо $\mathcal{A}'$ плотно. Действительно, в противном случае для кольца $\mathcal{A}'$ выполнено утверждение (2) этой теоремы. Но тогда множество X не является орбитой никакой подгруппы группы $\mathrm{Aut}(G)$, и потому S-кольцо $\mathcal{A}$ не является орбитным, что противоречит его нормальности по теореме 6.1 ((1) $\Longrightarrow$ (3)). Так что по теореме 5.4 кольцо $\mathcal{A}'$ является орбитным и потому совпадает с $\mathcal{A}$.

Для доказательства утверждения (1) рассмотрим $\varphi \in \mathrm{Isow}(\mathcal{A})$. Поскольку $\langle X\rangle = G$, то по лемме 2.1 и теореме 4.2 имеем $X^\varphi \in \mathcal{S}(\mathcal{A})$ и $\langle X^\varphi\rangle = G$. Отсюда, учитывая, что кольцо $\mathcal{A}$ орбитно, мы заключаем, что множество X^φ содержит образующую группы G. Поэтому $X^\varphi = X^\sigma$ для некоторого автоморфизма $\sigma \in \mathrm{Aut}(G)$. Таким образом, слабый изоморфизм φ совпадает на $\mathcal{A}'$ со слабым изоморфизмом кольца $\mathcal{A}$, индуцированным изоморфизмом σ. В силу равенства $\mathcal{A}' = \mathcal{A}$ утверждение (1) доказано. Для доказательства утверждения (2) пусть $f \in \mathrm{Iso}(\mathcal{A})$. Тогда из утверждения (1) следует, что существует изоморфизм $\sigma \in \mathrm{Aut}(G)$, для которого $f\sigma^{-1} \in \mathrm{Aut}(\mathcal{A})$. В силу нормальности кольца $\mathcal{A}$ это доказывает утверждение (2). •

Пусть теперь $|\mathrm{rad}(\mathcal{A})| = 2$. Тогда существуют подгруппы L и U группы G, для которых выполнены все утверждения следствия 6.5. Пусть $\varphi \in \mathrm{Isow}(\mathcal{A})$. Тогда, поскольку $\mathcal{A}_U$ и $\mathcal{A}_{G/L}$ — нормальные S-кольца с тривиальным радикалом, по утверждению (1) леммы 6.7 слабые изоморфизмы φ_U и $\varphi_{G/L}$ индуцированы соответственно автоморфизмами $\sigma_1 \in \mathrm{Aut}(U)$ и $\sigma_2 \in \mathrm{Aut}(G/L)$. В силу сюръективности гомоморфизмов π_U и $\pi_{G/L}$ (см. (28)), не умаляя общности, можно считать, что автоморфизмы σ_1 и σ_2 совпадают на U/L. Тогда по лемме 5.6 найдется изоморфизм $f \in \mathrm{Iso}(\mathcal{A})$ такой, что $f_U = \sigma_1$ и $f_{G/L} = \sigma_2$. Поскольку f, очевидно, индуцирует φ, утверждение (1) полностью доказано. Для доказательства утверждения (2) заметим, что 4 делит n, где $n = |G|$. Пусть $f \in \mathrm{Iso}(\mathcal{A})$. По утверждению (2) леммы 6.7 мы имеем $f_U \in \mathrm{Aut}(U)$ и $f_{G/L} \in \mathrm{Aut}(G/L)$. Поэтому $f_{U/L} \in \mathrm{Aut}(U/L)$, где $f_{U/L} = (f_U)_{U/L} = (f_{G/L})_{U/L}$. Из сюръективности отображений (28) заключаем, что существует автоморфизм $\sigma \in \mathrm{Aut}(G)$, для которого $\sigma_{U/L} = f_{U/L}$. Таким образом, заменяя f на $f\sigma^{-1}$, не умаляя общности, можно считать, что

$$f_{U/L} = \mathrm{id}_{U/L}, \quad f_U \in \mathrm{Aut}(U), \quad f_{G/L} \in \mathrm{Aut}(G/L). \tag{31}$$

Если $n/4$ нечетно, то это влечет, что $f_U = \mathrm{id}_U$ и $f_{G/L} = \mathrm{id}_{G/L}$. Тогда $f \in \mathrm{Aut}(\mathcal{A})$ и потому $f \in \mathrm{Aut}(G)$ в силу нормальности кольца $\mathcal{A}$ (на самом деле $f \in \Gamma_0$, где $\Gamma_0 = \{\sigma_{1+in/2,G} : i = 0, 1\}$). Предположим, что 8 делит n. Тогда формула (31) показывает, что $f_U \in \Gamma_1$ и $f_{G/L} \in \Gamma_2$, где $\Gamma_1 = \{\sigma_{1+in/4,U} : i = 0, 1\}$, $\Gamma_2 = \{\sigma_{1+in/4,G/L} : i = 0, 1\}$. Обозначим через Γ группу всех $f \in \mathrm{Iso}(\mathcal{A})$, удовлетворяющих последнему условию. Для завершения доказательства достаточно проверить, что $[\Gamma : \Gamma \cap \mathrm{Aut}(G)] = 2$. С этой целью используем еще раз нормальность кольца $\mathcal{A}$. Имеем

$$\Gamma = \{f_{\gamma_1,\gamma_2}\gamma_0 : \gamma_j \in \Gamma_j,\ j = 0, 1, 2\},$$

где f_{γ_1,γ_2} — фиксированный элемент группы $\mathrm{Iso}(\mathcal{A})$, для которого $(f_{\gamma_1,\gamma_2})_U = \gamma_1$ и $(f_{\gamma_1,\gamma_2})_{G/L} = \gamma_2$ (здесь мы воспользовались леммой 5.6 и тем, что $(\gamma_1)_{U/L} = (\gamma_2)_{U/L} = \mathrm{id}_{U/L}$ для всех $\gamma_1 \in \Gamma_1$ и $\gamma_2 \in \Gamma_2$). Легко видеть, что $\Gamma_0 \leqslant \mathrm{Aut}(G)$ и что $f_{\gamma_1,\gamma_2} \in \mathrm{Aut}(G)$ тогда и только тогда, когда $\gamma_1 = \sigma_{1+in/4,U}$, $\gamma_2 = \sigma_{1+in/4,G/L}$, $i = 0, 1$. Таким образом, $[\Gamma : \Gamma \cap \mathrm{Aut}(G)] = 2$, и теорема доказана. •

§7. Доказательство теоремы 6.1

Мы покажем, что (2) $\Longrightarrow$ (1) $\Longrightarrow$ (3) $\Longrightarrow$ (2). Для доказательства импликации (2) $\Longrightarrow$ (1) предположим, что $W_v = Z(K, G)$, где $K \leqslant \mathrm{Aut}(G)$. Стабилизатор любой образующей группы G в группе K, очевидно, тривиален. Поэтому K является 2-замкнутой подгруппой группы $\mathrm{Sym}(G)$ [21, теорема 5.12]. Отсюда следует, что $\mathrm{Aut}(W_v) = \mathrm{Aut}(Z(K, G)) = K$. Так что $\mathrm{Aut}(\mathcal{A}) = K$ в силу (18) и кольцо $\mathcal{A}$ нормально по теореме 4.7.

Докажем импликацию (1) $\Longrightarrow$ (3). Нам потребуется следующая лемма.

Лемма 7.1. *Каждое нормальное S-кольцо над циклической группой является орбитным кольцом, порядок радикала которого не превосходит* 2.

Доказательство. Пусть $\mathcal{A}$ — нормальное S-кольцо над циклической группой G. Тогда оно плотно. (Действительно, в противном случае выполнено по крайней мере одно из двух утверждений теоремы 5.3. Однако в первом случае кольцо $\mathcal{A}$ не может быть нормальным по теореме 5.7, а во втором — по теореме 4.7.) Если $\mathrm{rad}(\mathcal{A}) = \{1\}$, то кольцо $\mathcal{A}$ не может нетривиально удовлетворять никакому U/L-условию. Поэтому в этом случае по теореме 5.4 оно орбитно, и лемма доказана. Пусть $\mathrm{rad}(\mathcal{A}) \neq \{1\}$. Тогда по теореме 5.4 кольцо $\mathcal{A}$ удовлетворяет U/L-условию для некоторых подгрупп L, U группы G таких, что $|L| = |G/U| = p$, где p — максимальный простой делитель числа $|\mathrm{rad}(\mathcal{A})|$. В силу теоремы 5.7 отсюда следует, что $p = 2$ и $\mathrm{rad}(\mathcal{A})$ — нетривиальная 2-группа.

Докажем, что S-кольца $\mathcal{A}_{G/L}$ и $\mathcal{A}_U$ — суть орбитные S-кольца с тривиальным радикалом. Из плотности кольца $\mathcal{A}$ следует, что эти кольца также плотные. Поэтому по теореме 5.4 достаточно доказать, что радикал каждого из них тривиален. Предположим, что $\mathrm{rad}(\mathcal{A}_{G'}) \neq \{1\}$, где $G' = G/L$. Тогда, поскольку $\mathrm{rad}(\mathcal{A})$ — нетривиальная 2-группа, таковой же является и $\mathrm{rad}(\mathcal{A}_{G'})$. По теореме 5.4 это влечет, что кольцо $\mathcal{A}_{G'}$ удовлетворяет U'/L'-условию так, что $|L'| = |G'/U'| = 2$. Но тогда кольцо $\mathcal{A}$ удовлетворяет $U/\pi^{-1}(L')$-условию, где $\pi : G \to G'$ — естественная сюръекция. Однако поскольку $|\pi^{-1}(L')| = 4$, то по теореме 5.7 это противоречит нормальности кольца $\mathcal{A}$. Так что $\mathrm{rad}(\mathcal{A}_{G'}) = \{1\}$. Для доказательства аналогичного утверждения о кольце $\mathcal{A}_U$ достаточно проверить, что $\mathrm{rad}(\mathcal{A}_U)$ — 2-группа. Действительно, если в этом случае $\mathrm{rad}(\mathcal{A}_U) \neq \{1\}$, то по теореме 5.4 кольцо $\mathcal{A}_U$ удовлетворяет U_1/L-условию так, что $|U/U_1| = 2$. Но тогда кольцо $\mathcal{A}$ также удовлетворяет U_1/L-условию. Однако поскольку $|G/U_1| = 4$, то по теореме 5.7 это противоречит нормальности кольца $\mathcal{A}$. Докажем, что $\mathrm{rad}(\mathcal{A}_U)$ — 2-группа. Для этого рассмотрим базисное множество X кольца $\mathcal{A}$, содержащее образующую группы G. Тогда в силу (13) множество $X' = \pi(X)$ является базисным множеством кольца $\mathcal{A}_{G'}$ и содержит образующую группы G'. Поскольку кольцо $\mathcal{A}_{G'}$ орбитно, мы заключаем, что множество $Y' = \{(x')^2 : x' \in X'\}$ — базисное множество этого кольца. Отсюда следует, что $\pi^{-1}(Y') = Y \cup Yh$, где Y —

базисное множество кольца $\mathcal{A}_U$, содержащее образующую группы U и h — элемент группы G порядка 2. Поскольку, очевидно, $\mathrm{rad}(Y) = \mathrm{rad}(Yh)$, мы получаем, что $\mathrm{rad}(Y) \leqslant \mathrm{rad}(\pi^{-1}(Y'))$. Таким образом, достаточно доказать, что $\mathrm{rad}(Y')$ является 2-группой. Однако если $a'Y' = Y'$ для некоторого элемента $a' \in G'$ нечетного порядка, то, очевидно, $b'X' \subset Z'$, где $Z' = X' \cup h'X'$, b' — элемент группы G' такой, что $(b')^2 = a'$ и h' — элемент группы G' порядка 2. Тогда $H' \leqslant \mathrm{rad}(Z')$, где $H' = \langle b' \rangle$. Поэтому Z' является дизъюнктным объединением классов смежности по группе H'. Поскольку X' и $h'X'$ — орбиты одной и той же подгруппы группы $\mathrm{Aut}(G')$ и $\sigma_{1+n'/2}(X') = h'X'$, где $n' = |G'|$, то мощности непустых пересечений $g'H' \cap X'$ и $g'H' \cap h'X'$ не зависят от выбора элемента $g' \in G'$, и равны между собой. В силу нечетности числа $|H'|$ это влечет, что множество X' является объединением классов смежности по группе H', т.е. $H' \leqslant \mathrm{rad}(X')$. Учитывая, что $\mathrm{rad}(X') = \{1\}$, мы заключаем, что $H' = \{1\}$, и потому $a' = b' = 1$.

Как доказано выше, $\mathrm{rad}(\mathcal{A})$ является нетривиальной 2-группой и $\mathrm{rad}(\mathcal{A}_{G/L}) = \{1\}$. Поэтому $|\mathrm{rad}(\mathcal{A})| = 2$, и для завершения доказательства леммы достаточно проверить, что кольцо $\mathcal{A}$ шурово (тогда в силу нормальности оно орбитно). Поскольку кольца $\mathcal{A}_{G/L}$ и $\mathcal{A}_U$ орбитны, то $\mathcal{A}_U = \mathcal{O}(K_1, U)$ и $\mathcal{A}_{G/L} = \mathcal{O}(K_2, G/L)$ для некоторых групп $K_1 \leqslant \mathrm{Aut}(U)$ и $K_2 \leqslant \mathrm{Aut}(G/L)$. Обозначим через Γ группу, порожденную множеством $\bigcup_{f_1,f_2} \mathcal{F}(f_1, f_2)$, где объединение берется по всем парам $(f_1, f_2) \in K_1 \times K_2$, для которых $(f_1)_{U/L} = (f_2)_{U/L}$ (см. лемму 5.6). Поскольку гомоморфизмы π_U и $\pi_{G/L}$ сюръективны (см. (28)), группа Γ действует на U, как K_1, и на G/L, как K_2. Кроме того, легко видеть, что вне U орбиты подгруппы $\mathcal{F}(1,1)$ группы Γ совпадают с классами смежности по L. Так что $\mathrm{Orb}(\Gamma, G) = \mathcal{S}(A)$, и потому кольцо $\mathcal{A}$ шурово. •

Пусть $\mathcal{A}$ — нормальное S-кольцо. Тогда из леммы 7.1 следует, что $\mathcal{A} = \mathcal{O}(K, G)$ для некоторой группы $K \leqslant \mathrm{Aut}(G)$ такой, что $|\mathrm{rad}(K)| \leqslant 2$. Пусть $p \in \mathcal{P}^*(K)$. Тогда $K = \mathrm{Aut}(G_p) \times \pi_{G_{p'}}(K)$. В силу (12) это влечет, что $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, где $\mathcal{A}_1$ — S-кольцо ранга 2 над группой G_p и $\mathcal{A}_2$ — S-кольцо над группой $G_{p'}$. Поэтому $\mathrm{Aut}(\mathcal{A}) \geqslant \mathrm{Aut}(\mathcal{A}_1)$. Поскольку группа $\mathrm{Aut}(\mathcal{A}_1)$ изоморфна симметрической группе степени $p-1$, а группа $\mathrm{Aut}(\mathcal{A})$ абелева в силу нормальности кольца $\mathcal{A}$, то мы заключаем, что $p \leqslant 3$. Это доказывает импликацию (1) $\Longrightarrow$ (3).

Проверим, что (3) $\Longrightarrow$ (2). Доказательство опирается на два утверждения (см. теорему 7.3 и теорему 7.4). Первое из них показывает, что эта импликация справедлива в случае, когда G является p-группой, в то время как второе сводит к нему общий случай. Пусть $\mathcal{A} = \mathcal{O}(K, G)$, где $K \leqslant \mathrm{Aut}(G)$. Тогда $W = \mathcal{Z}(G \cdot K, G)$. Следующая лемма сводит проверку утверждения (2) к проверке 1-регулярности одноточечного расширения кольца W (по поводу 1-регулярности см.§9).

Лемма 7.2. *$W_v = \mathcal{Z}(K, G)$ тогда и только тогда, когда клеточное кольцо W_v*

является 1*-регулярным.*

Доказательство. Необходимость следует из леммы 9.1 ($m = 1, \Gamma = K$). Обратно, пусть W_v — 1-регулярное кольцо и x — его регулярная точка. Тогда, очевидно, $\mathrm{Aut}(W_v)_x = \{1\}$. Поэтому $|\mathrm{Aut}(W_v)| = |X|$, где X — орбита группы $\mathrm{Aut}(W_v)$, содержащая x. Из шуровости кольца W следует, что множество X является окрестностью точки v в базисном отношении кольца W и потому $X \in \mathrm{Orb}(K, G)$. Это влечет, что $|X| \leqslant |K|$. Следовательно, $|\mathrm{Aut}(W_v)| \leqslant |K|$. Поскольку, очевидно, $K \leqslant \mathrm{Aut}(W_v)$, мы заключаем, что $\mathrm{Aut}(W_v) = K$. С другой стороны, из теоремы 9.3 следует, что кольцо W_v шурово. Таким образом, $W_v = \mathcal{Z}(\mathrm{Aut}(W_v)) = \mathcal{Z}(K, G)$. •

Теорема 7.3. *Предположим, что G — p-группа, а группа K удовлетворяет следующим двум условиям*:

(1) $|\mathrm{rad}(K)| = 1$ *при* $p \geqslant 3$ *и* $|\mathrm{rad}(K)| \leqslant 2$ *при* $p = 2$;

(2) *если* $p \geqslant 5$ *и* $|G| = p$, *то* $K \neq \mathrm{Aut}(G)$.

Тогда кольцо W_v является 1*-регулярным.*

Доказательство. Зафиксируем образующую g группы G и покажем, что она является регулярной точкой кольца W_v. Обозначим через $n = p^k$ порядок группы G.

Пусть $p = 2$. Из условия (1) и леммы 5.1 следует, что группа K принадлежит одному из шести семейств, перечисленных в таблице. Поэтому $\mathcal{R}(W) = \{R_c : c \in \mathbb{Z}\}$ и $\mathrm{Cel}(W) = \{X_c : c \in \mathbb{Z}\}$, где

$$R_c = \{(g^a, g^b) : b - a = mc \,(\mathrm{mod}\, n),\ m \in M,\ a, b \in \mathbb{Z}\},$$
$$X_c = \{g^a : a = mc \,(\mathrm{mod}\, n),\ m \in M\}$$

и M имеет тот же смысл, что и в таблице. Прямое вычисление показывает, что $|R_c(g) \cap X_d| \leqslant 1$ для всех групп K и пар (R_c, X_d), исключая группы, принадлежащие семействам 4 или 6, и пары, которые могут быть получены при $(c, d) \in \{(n/4, 1 + n/4), (-1 + n/4, n/4)\}$. Поскольку любое отношение вида $R_c \cap (X_1 \times X_d)$, очевидно, принадлежит множеству $\mathcal{R}^*(W_v)$, мы видим, что g является регулярной точкой кольца W_v для групп K, принадлежащих семействам $1, 2, 3$ и 5. В оставшихся случаях имеем

$$R_{n/4}(g) \cap X_{1+n/4} = \{g^{1+n/4}, g^{1+3n/4}\}, \quad R_{-1+n/4}(g) \cap X_{n/4} = \{g^{n/4}, g^{3n/4}\}.$$

Однако в силу изложенного выше $R_2(g) \cap X_3 = \{g^3\}$ и $R_{-2+n/4}(g^3) \cap X_{1+n/4} = \{g^{1+n/4}\}$. Поэтому $\{g^{1+n/4}\} = S(g)$ для некоторого базисного отношения S кольца W_v. Аналогично $R_1(g) \cap X_2 = \{g^2\}$ и $R_{-2+n/4}(g^2) \cap X_{n/4} = \{g^{n/4}\}$, и потому $\{g^{n/4}\} = T(g)$ для некоторого базисного отношения T кольца W_v. Поэтому g является регулярной точкой кольца W_v также и для семейств 4 и 6.

Пусть $p > 2$. Тогда из условия (1) и леммы 5.1 следует, что клеточное кольцо W является 3/2-однородным, т.е. что любые два его нерефлексивных базисных отношения имеют одну и ту же степень (равную в нашем случае $|K|$). Более того, если $k \geqslant 2$, то множество $\mathcal{E}(W)$ содержит нетривиальную эквивалентность (например, эквивалентность, все классы которой имеют мощность p), т.е. кольцо W является импримитивным клеточным кольцом в смысле [4]. Однако ограничение одноточечного расширения произвольного импримитивного 3/2-однородного клеточного кольца на множество всех его точек, отличных от зафиксированной, является полурегулярным [4, лемма 5.13]. Поэтому при $k \geqslant 2$ любой элемент группы G, отличный от v, является регулярной точкой кольца W_v. Если $k = 1$, отождествим кольцо W с нормальным циклотомическим кольцом над полем $\mathbb{F}$ из p элементов, используя изоморфизм группы G на аддитивную группу поля $\mathbb{F}$. Из условия (2) следует, что $\mathrm{rk}(W) \geqslant 3$, за исключением случая $p = 3$. Если $p = 3$, то требуемое утверждение очевидно. В противном случае, согласно утверждению (1) теоремы 4.8, клеточное кольцо W^*, определенное в (22), является нормальным кольцом Кэли над группой $G = \mathbb{F}^\times$, причем $\mathrm{Aut}(W^*) = G$. Отсюда по лемме 7.1 и равенствам (18) следует, что S-кольцо, соответствующее кольцу W^*, равно $\mathbb{Z}[G]$. Так что кольцо W^* регулярно. Поскольку $(W_v)_G \geqslant W^*$, мы заключаем, что g — регулярная точка кольца W_v. •

Для $p \in \mathcal{P}(G)$ и $R \subset G^2$ положим

$$\mathrm{pr}_p(R) = \{(g_p, h_p) : (g, h) \in R\}, \tag{32}$$

где g_p и h_p — p-компоненты элементов g и h. Пусть $E_p = (G_p)^{\rho_G}$ и $E_{p'} = (G_{p'})^{\rho_G}$ (см. теорему 4.2). Если W — клеточное кольцо на G такое, что $E_{p'} \in \mathcal{E}(W)$, то любые два множества вида $\mathrm{pr}_p(R)$, $R \in \mathcal{R}(W)$, не пересекаются или совпадают и, более того, множество их всех образует стандартный базис некоторого клеточного кольца на G_p, обозначаемого здесь через $\mathrm{pr}_p(W)$. В действительности, согласно [3, лемма 2.1], при естественном отождествлении множеств G_p и $G/E_{p'}$ описанное выше множество образует стандартный базис фактор-кольца кольца W по эквивалентности $E_{p'}$ в соответствии с [3, п. 2.2].

Теорема 7.4. *Пусть* $p \in \mathcal{P}(G)$, $K_p = K \cap \mathrm{Aut}(G_p)$, $W_p = \mathcal{Z}(K_p, G_p)$ *и* $\pi_p = \pi_{G_p}$. *Тогда если* $(W_p)_v = \mathcal{Z}(K_p, G_p)$, *то* $\mathrm{pr}_p(W_v) = \mathcal{Z}(\pi_p(K), G_p)$.

Доказательство. Пусть g — образующая группы $G_{p'}$. Предположим, что $(W_p)_v = \mathcal{Z}(K_p, G_p)$. Докажем сначала, что

$$(W_v)_{G_p g} = \mathcal{Z}(K_p, G_p g). \tag{33}$$

Очевидно, что $K_p \leqslant \mathrm{Aut}(W_v)$ и $(G_p g)^{K_p} = G_p g$. Поэтому $(W_v)_{G_p g} = \mathcal{Z}(K_p, G_p g)$. С другой стороны, из предположения следует, что $\mathcal{Z}(K_p, G_p g) = \widetilde{W}_{\widetilde{v}}$, где $\widetilde{W} = \mathcal{Z}(G_p \cdot K_p, G_p g)$ и $\widetilde{v} = g$. Так что равенство (33) является следствием включения

$$\widetilde{W}_{\widetilde{v}} \leqslant (W_v)_{G_p g}. \tag{34}$$

Для доказательства последнего пусть $\widetilde{R} \in \mathcal{R}(\widetilde{W})$. Тогда $\widetilde{R}$ является 2-орбитой группы $G_p \cdot K_p$, действующей на множестве $G_p g$. Это влечет, что множество $\{(x_p, y) : (x, y) \in \widetilde{R}\}$ является орбитой той же группы на множестве $G_p \times G_p g$. Однако из равенства

$$\{R \cap G_p \times G_p g : R \in \mathcal{R}(W),\ R \cap G_p \times G_p g \neq \varnothing\} = \mathrm{Orb}(G_p \cdot K_p, G_p \times G_p g), \quad (35)$$

доказываемого ниже, вытекает, что это множество имеет вид $R \cap (G_p \times G_p g)$ для некоторого отношения $R \in \mathcal{R}(W)$. Прямое вычисление показывает, что

$$A(\widetilde{R}) = (A(E_{p'}) I_{G_p} A(R))_{G_p g}. \quad (36)$$

Поскольку, очевидно, $G_p \in \mathrm{Cel}^*(W_v)$ и $E_{p'} \in \mathcal{E}(W)$, матрица $A(E_{p'}) I_{G_p} A(R)$ принадлежит кольцу W_v. Поэтому матрица в правой части равенства (36) принадлежит кольцу $(W_v)_{G_p g}$. Так что $\widetilde{R} \in \mathcal{R}((W_v)_{G_p g})$. Это доказывает формулу (34) по модулю равенства (35). Для доказательства последнего достаточно проверить включение „$\subset$“. Пусть $R \in \mathcal{R}(W)$ и $R \cap G_p \times G_p g \neq \varnothing$. Тогда $R = \{(x^\sigma, y^\sigma g^\sigma) : \sigma \in G \cdot K\}$, где $x, y \in G_p$. Представляя элемент $\sigma \in G \cdot \mathrm{Aut}(G)$ в виде $\sigma = \sigma_p \sigma_{p'}$, где $\sigma_p \in G_p \cdot \mathrm{Aut}(G_p)$ и $\sigma_{p'} \in G_{p'} \cdot \mathrm{Aut}(G_{p'})$, имеем

$$\begin{aligned} R \cap (G_p \times G_p g) &= \{(x^\sigma, y^\sigma g) :\ \sigma \in G \cdot K,\ 1^{\sigma_{p'}} = 1,\ g^{\sigma_{p'}} = g\} \\ &= \{(x^\sigma, y^\sigma g) : \sigma \in G \cdot K,\ \sigma_{p'} = 1\} = \{(x^\sigma, y^\sigma g) : \sigma \in G_p \cdot K_p\}. \end{aligned}$$

(Здесь используется определение группы K_p и тот факт, что лишь единица группы $G_{p'} \mathrm{Aut}(G_{p'})$ фиксирует как 1, так и g.) Это доказывает требуемое включение.

Вернемся к доказательству теоремы. Пусть $W' = (W_v)^{\pi_p(K)}$. Из равенства (33) и очевидного включения $K_p \leqslant \pi_p(K)$ следует, что

$$W'_{G_p g} = ((W_v)^{\pi_p(K)})_{G_p g} = ((W_v)_{G_p g})^{\pi_p(K)} = \mathcal{Z}(K_p, G_p g)^{\pi_p(K)} = \mathcal{Z}(\pi_p(K), G_p g). \quad (37)$$

Кроме того, имеет место равенство

$$\mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_p x}), \quad x \in G_{p'}. \quad (38)$$

Действительно, пусть $X \in \mathrm{Orb}(\pi_{p'}(K), G_{p'})$, где $\pi_{p'} = \pi_{G_{p'}}$. Множество $G_p X$ совпадает с окрестностью точки v в отношении $\{(a, b) \in G^2 : a^{-1} b \in G_p X\}$, очевидно, принадлежащем множеству $\mathcal{R}^*(W)$, и потому является клеточным множеством кольца W_v. Поскольку $(G_p X)^{\pi_p(K)} = G_p X$, мы заключаем, что $G_p X \in \mathrm{Cel}^*(W')$. Отсюда по определению кольца $\mathrm{pr}_p(W')$ имеем

$$\mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_p X}). \quad (39)$$

С другой стороны, группа $\mathrm{Aut}(W')$, очевидно, содержит группы K и $\pi_p(K)$, и потому $\pi_{p'}(K)$. Следовательно, множество $\mathrm{pr}_p(W'_{G_p x})$ не зависит от выбора

точки $x \in X$. Так что равенство (38) следует из равенства (39). Используя формулы (37), (38) и тот факт, что действия групп K и $\pi_p(K)$ на G_p совпадают, мы получаем цепочку равенств

$$\begin{aligned}\mathrm{pr}_p(W_v) = (W_v)_{G_p} = W'_{G_p} = \mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_pg}) = \mathrm{pr}_p(\mathcal{Z}(\pi_p(K), G_pg)) \\ = \mathcal{Z}(\pi_p(K), G_p),\end{aligned}$$

что завершает доказательство теоремы. •

Для доказательства импликации (3) $\Longrightarrow$ (2) предположим, что выполнено утверждение (3) теоремы 6.1. Пусть $p \in \mathcal{P}(G)$. Тогда для группы K_p выполнены условия теоремы 7.3: условие (1) является следствием очевидного включения $\mathrm{rad}(K_p) \leqslant \mathrm{rad}(K)$, а условие (2) следует из определения множества $\mathcal{P}^*(K)$. Поэтому из этой теоремы и леммы 7.2 вытекает равенство $(W_p)_v = \mathcal{Z}(K_p, G_p)$ и, следовательно, в силу теоремы 7.4 равенство $\mathrm{pr}_p(W_v) = \mathcal{Z}(\pi_p(K), G_p)$. Так что

$$W_v \geqslant \bigotimes_{p\in\mathcal{P}(G)} \mathrm{pr}_p(W_v) = \bigotimes_{p\in\mathcal{P}(G)} \mathcal{Z}(\pi_p(K), G_p). \tag{40}$$

Каждый сомножитель в правой части формулы (40) является, очевидно, 1-регулярным кольцом. Поэтому тензорное произведение и кольцо W_v также 1-регулярны (см. лемму 9.2). По лемме 7.2 отсюда следует, что $W_v = \mathcal{Z}(K, G)$. Теорема 6.1 полностью доказана. •

§8. Шуровость колец Кэли W^* и $\widehat{W}^*$

Основной результат этого параграфа касается клеточных колец W^* и $\widehat{W}^*$, определенных формулами (22).

Теорема 8.1. *Клеточные кольца W^* и $\widehat{W}^*$ шуровы.*

Доказательство. По утверждению (1) теоремы 4.8 W^* является нормальным кольцом Кэли над группой G. Поскольку эта группа циклическая, из теоремы 6.1 ((1) $\Longrightarrow$ (3)) следует, что S-кольцо, соответствующее W^*, является орбитным, и потому шуровым. Так что кольцо W^* шурово.

Из определения следует, что $\widehat{W}^*$ — кольцо Кэли над группой Γ; соответствующее ему S-кольцо обозначим через $\widehat{\mathcal{A}}^*$. Поскольку $E_G = G^{\rho_\Gamma}$ и $R_s = \{s\}^{\rho_\Gamma}$ (см. п. 4.4), формула (23) и теорема 4.2 влекут, что $G \in \mathcal{H}(\widehat{\mathcal{A}}^*)$ и $\{s\} \in \mathcal{S}(\widehat{\mathcal{A}}^*)$ (и потому $sGs \in \mathcal{H}(\widehat{\mathcal{A}}^*)$). Более того, из теоремы 4.8, утверждения (1) леммы 4.4 и теоремы 4.2 следует, что $\widehat{\mathcal{A}}^*_G$ — нормальное S-кольцо над группой G. По теореме 6.1 ((1) $\Longrightarrow$ (3)) найдется группа $K \leqslant \mathrm{Aut}(\mathbb{F})$, для которой $\widehat{\mathcal{A}}^*_G = \mathcal{O}(K, G)$. Отсюда следует, что

$$\widehat{\mathcal{A}}^*_{sGs} = \xi(s)\widehat{\mathcal{A}}^*_G\xi(s) = \xi(s)\mathcal{O}(K, G)\xi(s) = \mathcal{O}(K, sGs).$$

Таким образом, шуровость кольца $\widehat{W}^*$ вытекает из следующего утверждения.

Теорема 8.2. *Пусть $\mathbb{F}$ — конечное поле из $q = p^d$ элементов, $\Gamma = A \cdot G$ — полупрямое произведение аддитивной группы A поля $\mathbb{F}$ на его мультипликативную группу G и s — элемент группы Γ с A-компонентой $1_{\mathbb{F}}$ и G-компонентой $-1_{\mathbb{F}}$.*[6] *Предположим, что $\mathcal{A}$ — S-кольцо над группой Γ такое, что*

(1) $G, sGs \in \mathcal{H}(\mathcal{A})$,

(2) $\mathcal{A}_G = \mathcal{O}(K, G)$, $\mathcal{A}_{sGs} = \mathcal{O}(K, sGs)$, *где* $K \leqslant \mathrm{Aut}(\mathbb{F})$.

Тогда $\mathcal{A} = \mathcal{O}(K, \Gamma)$.

Замечание 8.3. Отметим, что группы G и sGs являются стабилизаторами точек $0_{\mathbb{F}}$ и $1_{\mathbb{F}}$ в группе Γ, действующей на $\mathbb{F}$ согласно (20).

Доказательство. Мы выведем теорему из лемм 8.4, 8.5 и 8.6, доказываемых ниже. При этом мы будем часто использовать равенство $\mathcal{A}_{\Gamma_0} = \mathbb{Z}[\Gamma_0]$, где Γ_0 — подгруппа группы Γ, состоящая из всех элементов, обе компоненты которых принадлежат простому подполю $\mathbb{F}_0$ поля $\mathbb{F}$. Оно следует из равенств $\mathcal{A}_{G \cap \Gamma_0} = \mathbb{Z}[G \cap \Gamma_0]$ и $\mathcal{A}_{sGs \cap \Gamma_0} = \mathbb{Z}[sGs \cap \Gamma_0]$ (см. условие (2)) с учетом того, что группа Γ_0 порождена группами $G \cap \Gamma_0$ и $sGs \cap \Gamma_0$.

Пусть $g \in \mathbb{F}$. В доказательстве леммы 8.4 и ниже мы называем g нормальным элементом поля $\mathbb{F}$, если аддитивная группа этого поля порождена элементами g^σ, $\sigma \in \mathrm{Aut}(\mathbb{F})$. Известно [13, теорема 2.40], что $\mathbb{F}$ всегда содержит примитивный нормальный элемент.

Лемма 8.4. *Справедливы следующие утверждения:*

(1) $A \in \mathcal{H}(\mathcal{A})$ *и* $\mathcal{A}_A = \mathcal{O}(K, A)$,

(2) *если* $X \in \mathcal{S}(\mathcal{A})$, *то* $\mathrm{pr}_G(X), \mathrm{pr}_A(X) \in \mathcal{S}(\mathcal{A})$.

Доказательство. Для $x \in \mathbb{F}$ положим $\eta(x) = x \cdot 1 \in \Gamma$. Докажем сначала, что для любого примитивного элемента g поля $\mathbb{F}$ имеет место равенство

$$Y^{-1}X \cap tX^{-1}Yt = (\eta(g-1))^K, \tag{41}$$

где $X = (0 \cdot g)^K$, $Y = ((1-g) \cdot g)^K$ и $t = 0 \cdot (-1)$. Пусть $\gamma = a \cdot h$ принадлежит левой части формулы (41). Тогда прямая проверка показывает, что

$$a = (1 - g^{-1})^\sigma g^\tau = g^{\sigma'} - 1, \quad h = (g^{-1})^\sigma g^\tau = (g^{-1})^{\tau'} g^{\sigma'}$$

для некоторых $\sigma, \tau, \sigma', \tau' \in K$. Поскольку $K \leqslant \mathrm{Aut}(\mathbb{F})$, то автоморфизмы $\sigma, \tau, \sigma', \tau'$ определяются возведением соответственно в степени $p^i, p^j, p^{i'}, p^{j'}$, где $0 \leqslant i, j, i', j' \leqslant d-1$. Поэтому $h = g^{-p^i + p^j} = g^{-p^{j'} + p^{i'}}$. Используя примитивность элемента g, мы находим отсюда, что $p^i + p^{i'} = p^j + p^{j'} \pmod{q-1}$. Это влечет, что либо $i = j$, $i' = j'$, либо $i = j'$, $j = i'$. В первом случае,

[6] Ниже мы отождествляем группы A и G с подгруппами группы Γ. Так что $A = \{x \cdot 1 : x \in \mathbb{F}\}$, $G = \{0 \cdot x : x \in \mathbb{F}^\times\}$ и $sGs = \{(1-x) \cdot x : x \in \mathbb{F}^\times\}$, где $0 = 0_{\mathbb{F}}$ и $1 = 1_{\mathbb{F}}$.

очевидно, $h = 1$. Во втором случае $(1 - g^{-p^i})g^{p^j} = g^{p^j} - 1$ или эквивалентно $g^{p^i} = g^{p^j}$. Поэтому $i = j$ и снова $h = 1$. Таким образом, $\gamma \in (\eta(g-1))^K$. Это доказывает равенство (41), поскольку, очевидно, его левая часть инвариантна относительно группы K.

Докажем, что $A \in \mathcal{H}(\mathcal{A})$. Пусть g — примитивный элемент поля $\mathbb{F}$. Тогда из равенства (41) и условия теоремы 8.2 следует, что $(\eta(g-1))^K \in \mathcal{S}^*(\mathcal{A})$. Поскольку $(\eta(g))^K = (\eta(g-1))^K \cdot \eta(1)$ и $\{\eta(1)\} \in \mathcal{S}(\mathcal{A})$, мы имеем $(\eta(g))^K \in \mathcal{S}^*(\mathcal{A})$. Предположим, не умаляя общности, что g — нормальный элемент поля $\mathbb{F}$. Тогда множество $(\eta(g))^{\mathrm{Aut}(\mathbb{F})}$ порождает подгруппу A группы Γ. С другой стороны, если $\mathrm{Aut}(\mathbb{F}) = \bigcup_\tau \tau K$, то $(\eta(g))^{\mathrm{Aut}(\mathbb{F})} = \bigcup_\tau (\eta(g^\tau))^K$. Поскольку g^τ — примитивный элемент поля $\mathbb{F}$ при всех τ, то из сказанного выше следует, что $(\eta(g))^{\mathrm{Aut}(\mathbb{F})} \in \mathcal{S}^*(\mathcal{A})$. Таким образом, $A \in \mathcal{H}(\mathcal{A})$, что доказывает первую часть утверждения (1).

Для доказательства утверждения (2) заметим прежде всего, что поскольку $A, G \in \mathcal{H}(\mathcal{A})$ и $\mathcal{A}_{\Gamma/A} = \mathcal{A}_G$ (см. (13)), то $\mathrm{pr}_G(X) \in \mathcal{S}(\mathcal{A})$ для всех $X \in \mathcal{S}(\mathcal{A})$. Далее, для $X \subset \Gamma$ мы, очевидно, имеем

$$\mathrm{pr}_A(X) = X\,\mathrm{pr}_G(X)^{-1} \cap A.$$

Отсюда следует, что $\mathrm{pr}_A(X) \in \mathcal{S}^*(\mathcal{A})$ при $X \in \mathcal{S}^*(\mathcal{A})$. Более того, если $\mathrm{pr}_A(X) = Y_1 \cup Y_2$, где $Y_i \in \mathcal{S}^*(\mathcal{A})$ — собственное подмножество множества $\mathrm{pr}_A(X)$, $i = 1, 2$, то $X = X_1 \cup X_2$, где $X_i = (Y_i\,\mathrm{pr}_G(X)) \cap X$ — собственное подмножество множества X, $i = 1, 2$. Ясно, что $X_i \in \mathcal{S}^*(\mathcal{A})$. Так что, если $X \in \mathcal{S}(\mathcal{A})$, то $\mathrm{pr}_A(X) \in \mathcal{S}(\mathcal{A})$, что завершает доказательство утверждения (2). Поскольку $\mathrm{pr}_A(sGs) = A \setminus \{1_\Gamma\}$, из этого утверждения следует, что

$$\mathcal{S}(\mathcal{A}_A) = \{1_\Gamma\} \cup \{\mathrm{pr}_A(X) : X \in \mathcal{S}(\mathcal{A}_{sGs})\}.$$

Учитывая равенство $\mathcal{S}(\mathcal{A}_{sGs}) = \mathrm{Orb}(K, sGs)$, мы заключаем, что $\mathcal{A}_A = \mathcal{O}(K, A)$, откуда вытекает вторая часть утверждения (1). Лемма доказана. •

Лемма 8.5. *Пусть g — примитивный элемент поля $\mathbb{F}$. Тогда*

(1) *если $a \in \mathbb{F}$ и $[a \cdot g] \in \mathrm{Orb}(K, \Gamma)$, то $[a \cdot g^\sigma] \in \mathrm{Orb}(K, \Gamma)$ для всех $\sigma \in \mathrm{Aut}(\mathbb{F})$;*

(2) *если g — нормальный элемент поля $\mathbb{F}$, то $[a \cdot g] \in \mathrm{Orb}(K, \Gamma)$ для всех $a \in \mathbb{F}$.*

Доказательство. Докажем утверждение (1). Пусть $a \in \mathbb{F}$ и $[a \cdot g] \in \mathrm{Orb}(K, \Gamma)$. Достаточно доказать, что $[a \cdot g^p] \in \mathrm{Orb}(K, \Gamma)$. Однако поскольку $[0 \cdot g^i] \in \mathrm{Orb}(K, G)$ при всех i, то

$$[0 \cdot g^{p-1}][a \cdot g] \cap A[0 \cdot g^p] = \{a^\tau \cdot (g^{p-1})^\sigma g^\tau : (g^{p-1})^\sigma g^\tau \in (g^p)^K,\ \sigma, \tau \in K\}. \quad (42)$$

С другой стороны, если $(g^{p-1})^\sigma g^\tau = g^p$, где $\sigma, \tau \in \mathrm{Aut}(\mathbb{F})$, то $g^{(p-1)p^i + p^j} = g^p$ для некоторых $i, j \in \{0, 1, \ldots, d-1\}$, и потому $(p-1)p^i + p^j = p \pmod{q-1}$. Это

влечет, что $i = j = 0$. Следовательно, $\sigma = \tau = \mathrm{id}_{\mathbb{F}}$. Так что множество в правой части равенства (42) совпадает с $X = (a \cdot g^p)^K$. Поскольку $A \in \mathcal{H}(\mathcal{A})$ (см. утверждение (1) леммы 8.4), мы заключаем, что левая часть равенства (42) принадлежит множеству $\mathcal{S}^*(\mathcal{A})$. Поэтому $X \in \mathcal{S}^*(\mathcal{A})$. Учитывая, что $|X| = |\mathrm{pr}_G(X)| = |K|$ и $\mathrm{pr}_G(X) \in \mathrm{Orb}(K, G)$, и используя утверждение (2) леммы 8.4, мы получаем, что $X \in \mathcal{S}(\mathcal{A})$. Утверждение (1) доказано.

Для доказательства утверждения (2) пусть g — нормальный элемент поля $\mathbb{F}$ и $a \in \mathbb{F}$. Тогда $a = \sum_{i=0}^{d-1} x_i g_i$, где $x_i \in \mathbb{F}_0$ и $g_i = g^{p^i}$ для всех i. Докажем индукцией по $k = 0, 1, \ldots, d$, что $[a_k \cdot g_k] \in \mathrm{Orb}(K, \Gamma)$, где $a_k = \sum_{i=0}^{k-1} x_i g_i$. Тогда требуемое утверждение получается при $k = d$. Если $k = 0$, то $a_k = 0$ и база индукции следует из условия теоремы 8.2. Пусть $k > 0$ и $[a_{k-1} \cdot g_{k-1}] \in \mathrm{Orb}(K, \Gamma)$. Тогда по утверждению (1) мы имеем $[a_{k-1} \cdot g_k] \in \mathrm{Orb}(K, \Gamma)$. Поскольку, очевидно,

$$[a_k \cdot g_k] = [x_k \cdot 1][a_{k-1} \cdot g_k],$$

мы заключаем, что $[a_k \cdot g_k] \in \mathrm{Orb}(K, \Gamma)$. •

Ниже элемент $x \in \mathbb{F}$ называется максимальным, если $|x^{\mathrm{Aut}(\mathbb{F})}| = |\mathrm{Aut}(\mathbb{F})|$.

Лемма 8.6. *Если равенство* $[\gamma] = \gamma^K$ *выполнено для тех* $\gamma \in \Gamma$, *у которых* A*-компонента является максимальным элементом поля* $\mathbb{F}$, *то оно выполнено и для всех* $\gamma \in \Gamma$.

Доказательство. Пусть g — примитивный элемент поля $\mathbb{F}$. Докажем сначала, что если элемент $a \in \mathbb{F}$ немаксимален и $\sigma, \tau, \sigma', \tau' \in \mathrm{Aut}(\mathbb{F})$, то

$$a^\sigma g^\tau = a^{\sigma'} g^{\tau'} \iff a^\sigma = a^{\sigma'},\ g^\tau = g^{\tau'}. \tag{43}$$

Для доказательства нетривиальной импликации „ $\Longrightarrow$ “ пусть $a^\sigma g^\tau = a^{\sigma'} g^{\tau'}$. Предположим, не умаляя общности, что $\tau' = \mathrm{id}_{\mathbb{F}}$. Из немаксимальности a следует, что этот элемент принадлежит подполю поля $\mathbb{F}$ порядка p^{d_1} для некоторого делителя d_1 числа d, отличного от d. Тогда это подполе содержит элемент $g^\tau / g = a^{\sigma'} / a^\sigma$, и потому $(g^\tau / g)^{p^{d_1}-1} = 1$. Поскольку $g^\tau = g^{p^i}$ для некоторого $i \in \{0, 1, \ldots, d-1\}$, мы имеем $g^{(p^i-1)(p^{d_1}-1)} = 1$, откуда следует, что число $(p^i - 1)(p^{d_1} - 1)$ делится на $p^d - 1$. С другой стороны, поскольку $p^d - 1 = p^{d-i}(p^i - 1) + p^{d-i} - 1$, мы находим, что

$$\mathrm{НОД}\,(p^d - 1, p^i - 1) = \mathrm{НОД}\,(p^d - 1, p^{d-i} - 1).$$

Поэтому $(p^{d-i} - 1)(p^{d_1} - 1)$ делится на $p^d - 1$. Таким образом, $(p^{i_0} - 1)(p^{d_1} - 1)$ делится на $p^d - 1$, где $i_0 = \min(i, d - i)$. Кроме того, первое число меньше второго, поскольку $i_0 \leqslant d/2$ и $d_1 \leqslant d/2$. Это означает, что $i_0 = 0$, откуда $i = 0$. Следовательно, $g^\tau = g$ и потому $a^\sigma = a^{\sigma'}$. Формула (43) доказана.

Пусть $\gamma = a \cdot h$ — элемент группы Γ с немаксимальным a. Тогда из (43) следует, что ag — максимальный элемент поля $\mathbb{F}$ и

$$(a \cdot h)^M (0 \cdot g)^K \cap (ag)^K \cdot G = (ag \cdot hg)^M, \quad (ag \cdot hg)^K (0 \cdot g^{-1})^K \cap a^K \cdot G = (a \cdot h)^K, \tag{44}$$

где M — объединение классов смежности группы K по стабилизатору элемента γ в K. Более того, $(ag\cdot hg)^K \in \mathcal{S}(\mathcal{A})$ по условию леммы, $(0\cdot g)^K, (0\cdot g^{-1})^K \in \mathcal{S}(\mathcal{A})$ по условию теоремы, а $a^K\cdot G, (ag)^K\cdot G \in \mathcal{S}^*(\mathcal{A})$ по лемме 8.4. Так что второе равенство из (44) влечет, что $(a\cdot h)^K \in \mathcal{S}^*(\mathcal{A})$, в то время как первое равенство показывает, что, более того, $(a\cdot h)^K \in \mathcal{S}(\mathcal{A})$, поскольку $(ag\cdot hg)^M$ является собственным подмножеством базисного множества $(ag\cdot hg)^K$ для любого собственного подмножества M группы K. •

Для завершения доказательства теоремы в силу леммы 8.6 достаточно проверить, что $[a\cdot h] = (a\cdot h)^K$, где a — максимальный элемент поля $\mathbb{F}$ и $h\in\mathbb{F}^\times$. С этой целью покажем, что

$$\Big(\bigcap_{\sigma\in \mathrm{Aut}(\mathbb{F})} (0\cdot h/g^\sigma)^K (a\cdot g^\sigma)^K\Big)\cap A\cdot h^K = (a\cdot h)^K, \tag{45}$$

где g — примитивный нормальный элемент поля $\mathbb{F}$. Тогда $(a\cdot h)^K\in\mathcal{S}^*(\mathcal{A})$. Действительно, $(0\cdot h/g^\sigma)^K\in\mathcal{S}(\mathcal{A})$ по условию теоремы, $(a\cdot g^\sigma)^K\in\mathcal{S}(\mathcal{A})$ — по утверждению (2) леммы 8.5 и $A\in\mathcal{S}^*(\mathcal{A})$ — по утверждению (1) леммы 8.4. Так что в силу максимальности a из утверждения (2) леммы 8.4 следует, что $(a\cdot h)^K\in\mathcal{S}(\mathcal{A})$.

Очевидно, правая часть равенства (45) содержится в левой части этого равенства. Обратно, пусть γ принадлежит последней. Тогда легко видеть, что $\gamma = a^\tau\cdot h^\rho$, где $\tau,\rho\in K$. Выберем целые числа s и k так, чтобы $h = g^s$ и $a^\tau = a^{p^k}$. Предположим, не умаляя общности, что $\rho = \mathrm{id}_{\mathbb{F}}$. Тогда из вида левой части (45) следует, что найдутся целые числа j_i, для которых

$$s = (s-p^i)p^{j_i} + p^{i+k} \pmod{q-1}, \quad i = 0,1,\dots,d-1. \tag{46}$$

(Тот факт, что в равенствах (46) целое число k может быть выбрано независимо от i, следует из максимальности элемента a.) Если теперь

$$sp^k = s \pmod{q-1}, \tag{47}$$

то $\gamma = a^\tau\cdot h = a^{p^k}\cdot g^s = a^{p^k}\cdot g^{sp^k} = (a\cdot h)^\tau$, что и требовалось доказать.

Докажем (47). Для числа $t\in\{0,1,\dots,q-2\}$ существуют единственным образом определенные числа $t_0,t_1,\dots,t_{d-1}\in\{0,1,\dots,p-1\}$ такие, что $t = \sum_{i=0}^{d-1} t_i p^i$. Для произвольных целых чисел t,i положим $t_i = t'_{i'}$, где t' (соответственно i') — наименьшее неотрицательное целое число такое, что $t' = t \pmod{q-1}$ (соответственно $i' = i \pmod{q-1}$). Из определения следует, что $t = \widetilde{t} \pmod{q-1}$ тогда и только тогда, когда $t_i = \widetilde{t}_i$ для всех i, принадлежащих некоторой полной системе вычетов по модулю d. Легко видеть, что

$$(tp^j)_{i+j} = t_i \tag{48}$$

для всех целых чисел t,i,j. Таким образом, для доказательства (47) достаточно проверить, что $s_i = s_{i+k}$ для всех $i\in\{0,1,\dots,d-1\}$. Пусть

$i \in \{0, 1, \dots, d-1\}$. Тогда из (46) следует, что $(s-p^i)p^{j_i} = s - p^{i+k} \pmod{q-1}$. В силу (48) это влечет, что

$$c(l, s-p^i) = c(l, s-p^{i+k}), \quad l \in \{0, 1, \dots, p-1\}, \tag{49}$$

где $c(l,t) = |\{j \in \{0,1,\dots,d-1\} : t_j = l\}|$. Предположим, что $s_i \neq s_{i+k}$. Тогда по крайней мере одно из чисел s_i, s_{i+k}, скажем s_i, отлично от 0. Если $s_{i+k} \neq 0$, то $c(s_i - 1, s-p^i) = c(s_i-1, s) - 1$, откуда $c(s_i-1, s-p^{i+k}) = c(s_i-1, s)$, что противоречит равенству (49) при $l = s_i - 1$. Если же $s_{i+k} = 0$, то легко видеть, что

$$c(p-1, s-p^i) \leqslant c(p-1, s) \leqslant c(p-1, s-p^{i+k}).$$

Отсюда и из равенства (49) при $l = p-1$ следует, что

$$c(p-1, s-p^i) = c(p-1, s), \quad c(p-1, s-p^{i+k}) = c(p-1, s).$$

Первое из этих равенств влечет, что $s_i \neq p-1$, а второе, что $s_{i+k-1} = p-1$. Поэтому

$$c(s_i - 1, s-p^i) = c(s_i-1, s) - 1, \quad c(s_i-1, s-p^{i+k}) = c(s_i-1, s),$$

что противоречит равенству (49) при $l = s_i - 1$. •

§9. 1-регулярные клеточные кольца

Клеточное кольцо $W \leqslant \mathrm{Mat}_V$ называется *1-регулярным*, если существует точка $v \in V$ такая, что $|R(v)| \leqslant 1$ для всех $R \in \mathcal{R}(W)$. Любая такая точка называется *регулярной* точкой кольца W. В этом случае $W_v = \mathrm{Mat}_V$. Множество X всех регулярных точек, очевидно, является клеточным множеством кольца W, причем кольцо W_X полурегулярно. Легко видеть, что централизаторное кольцо группы перестановок 1-регулярно тогда и только тогда, когда базовое число этой группы не превосходит 1. Более общо, имеет место следующее утверждение.

Лемма 9.1. *Пусть* $\Gamma \leqslant \mathrm{Sym}(V)$ — *группа перестановок и* m — *натуральное число. Тогда следующие утверждения эквивалентны*:

(1) $b(\Gamma) \leqslant m$,
(2) $\mathcal{Z}(\Gamma_{v_1,\dots,v_{m-1}})$ — 1-*регулярное кольцо для некоторых* $v_1, \dots, v_{m-1} \in V$,
(3) $\mathcal{Z}_m(\Gamma)$ — 1-*регулярное кольцо.*

Доказательство. Лемма сводится к случаю $m = 1$, поскольку $b(\Gamma) \leqslant m$ тогда и только тогда, когда $b(\Gamma_{v_1,\dots,v_{m-1}}) \leqslant 1$ для некоторых точек $v_1, \dots, v_{m-1} \in V$, или что то же самое, когда $b(\widehat{\Gamma}^{(m)}) \leqslant 1$, где $\widehat{\Gamma}^{(m)}$ — группа перестановок на V^m, индуцированная действием группы Γ на упорядоченных m-множествах точек. •

Следующая лемма вытекает непосредственно из определения 1-регулярности.

Лемма 9.2. *Класс всех* 1*-регулярных колец замкнут относительно перехода к надкольцам и тензорным произведениям.* •

Теорема 9.3. *Любое* 1*-регулярное кольцо отделимо и шурово.*

Доказательство. Пусть W — 1-регулярное кольцо. Обозначим через X множество всех его регулярных точек. Тогда $X \in \mathrm{Cel}^*(W)$, причем кольцо W_X полурегулярно. Согласно [7, теорема 4.4], каждое полурегулярное кольцо отделимо и шурово. Поэтому теорема вытекает из следующей леммы.

Лемма 9.4. *Пусть* $W \leqslant \mathrm{Mat}_V$ *— клеточное кольцо,* $\mathcal{R} = \mathcal{R}(W)$ *и* $X \in \mathrm{Cel}^*(W)$. *Предположим, что для каждого множества* $Y \in \mathrm{Cel}(W_{V\setminus X})$ *существует отношение* $R_Y \in \mathcal{R}_{X,Y}$ *такое, что* $d_{\mathrm{out}}(R_Y) = 1$. *Тогда*

(1) *для каждого* $\varphi \in \mathrm{Isow}(W, W')$ *отображение ограничения*

$$\mathrm{Iso}(W, W', \varphi) \to \mathrm{Iso}(W_X, W'_{X^\varphi}, \varphi_X), \quad f \mapsto f_X$$

является биекцией. В частности, отображение $\mathrm{Aut}(W) \to \mathrm{Aut}(W_X)$ *является изоморфизмом групп*;

(2) *если кольцо* W_X *отделимо (соответственно шурово), то отделимо (соответственно шурово) и кольцо* W.

Доказательство. Для каждой клетки Y кольца $W_{V\setminus X}$ зафиксируем базисное отношение $R_Y \in \mathcal{R}_{X,Y}$ такое, что $d_{\mathrm{out}}(R_Y) = 1$. Если $Y \in \mathrm{Cel}(W_X)$, то положим $R_Y = \Delta^{(2)}(Y)$. Пусть $Y \in \mathrm{Cel}(W)$. Тогда $A_Y A_Y^T = A(E_Y)$ для некоторой эквивалентности $E_Y \in \mathcal{E}(W)$, где $A_Y = A(R_Y)$. Поэтому отображение $h : Y \to X/E_Y$, определенное равенством $v^h = R_Y(v)$, является биекцией и

$$R_Y = \bigcup_{v \in Y} v^h \times \{v\}. \tag{50}$$

Пусть $R \in \mathcal{R}_{Y,Z}$ для некоторых клеток $Y, Z \in \mathrm{Cel}(W)$. Выберем отношение $S \in \mathcal{R}_{X,X}$ так, чтобы матрица $A(S)$ входила с ненулевым коэффициентом в разложение произведения $A_Y A(R)(A_Z)^T$ по базисным матрицам кольца W. Тогда, очевидно, $S \cap (U_Y \times U_Z) \neq \varnothing$ для некоторых классов $U_Y \in X/E_Y$, $U_Z \in X/E_Z$ только в том случае, когда $(u, v) \in R$, где $u = h_Y^{-1}(U_Y)$ и $v = h_Z^{-1}(U_Z)$. Поэтому

$$A_Y^T A(S) A_Z = c(S) A(R) \tag{51}$$

для некоторого положительного рационального числа $c(S)$.

Для доказательства утверждения (1) рассмотрим слабый изоморфизм $\varphi \in \mathrm{Isow}(W, W')$, где $W' \leqslant \mathrm{Mat}_{V'}$. Положим $X' = X^\varphi$. Кроме того, для $Y \in \mathrm{Cel}(W)$ положим $Y' = Y^\varphi$, $R_{Y'} = (R_Y)^\varphi$ и $E_{Y'} = (E_Y)^\varphi$ (см. лемму 2.1). Тогда $d_{\mathrm{out}}(R_{Y'}) = 1$ и, следовательно,

$$R_{Y'} = \bigcup_{v' \in Y'} (v')^{h'} \times \{v'\},$$

где $h' : Y' \to X'/E_{Y'}$ — биекция, для которой $(v')^{h'} = R_{Y'}(v')$. Пусть теперь $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$. Для $Y \in \mathrm{Cel}(W)$ обозначим через $f_Y : X/E_Y \to X'/E_{Y'}$ биекцию, индуцированную отображением f_0. Тогда, очевидно, отображение

$$f : V \to V', \quad v \mapsto v^{hf_Y(h')^{-1}},$$

где Y — клетка кольца W, содержащая точку v, является биекцией. Из формулы (50) следует, что $(R_Y)^f = R_{Y'}$ для всех $Y \in \mathrm{Cel}(W)$. Поэтому в силу равенства (51) мы имеем $R^f = R^\varphi$ для всех $R \in \mathcal{R}(W)$. Таким образом, $f \in \mathrm{Iso}(W, W', \varphi)$. Поскольку $R_Y = \Delta^{(2)}(Y)$ для всех $Y \in \mathrm{Cel}(W_X)$, то $f_X = f_0$ для всех $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$. С другой стороны, для произвольного сильного изоморфизма $f \in \mathrm{Iso}(W, W', \varphi)$ биекция $V \to V'$, построенная выше для $f_0 = f_X$, совпадает с f. Это доказывает утверждение (1).

Для доказательства утверждения (2) предположим сначала, что кольцо W_X отделимо. Пусть $\varphi \in \mathrm{Isow}(W, W')$ для некоторого кольца W'. Тогда из отделимости кольца W_X следует, что существует сильный изоморфизм $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$, где $X' = X^\varphi$. По утверждению (1) $f_0 = f_X$ для некоторого сильного изоморфизма $f \in \mathrm{Iso}(W, W', \varphi)$. Так что кольцо W отделимо. Предположим теперь, что кольцо W_X шурово. Пусть $R \in \mathcal{R}_{Y,Z}$, где $Y, Z \in \mathrm{Cel}(W)$. Положим

$$\overline{S} = \{(U_Y, U_Z) \in X/E_Y \times X/E_Z : S \cap (U_Y \times U_Z) \neq \varnothing\},$$

где отношение S такое же, как и в формуле (51). Тогда по этой формуле отображение $(U_Y, U_Z) \mapsto (u, v)$, где $u = (h_Y)^{-1}(U_Y)$, $v = (h_Z)^{-1}(U_Z)$, является биекцией из $\overline{S}$ на R. Используя формулу (50) и инвариантность отношений R_Y и R_Z относительно группы $\mathrm{Aut}(W)$, мы видим, что эта биекция определяет эквивалентность между действиями группы $\mathrm{Aut}(W)$ на множествах $\overline{S}$ и R. С другой стороны, в силу шуровости кольца W_X группа $\mathrm{Aut}(W_X)$ действует транзитивно на множестве $\overline{S}$. По утверждению (1) отсюда следует, что группа $\mathrm{Aut}(W)$ также действует транзитивно на множестве $\overline{S}$, а потому в силу сказанного выше и на множестве R. Таким образом, отношение R является 2-орбитой группы $\mathrm{Aut}(W)$ и, следовательно, кольцо W шурово. •

Следствие 9.5. *Отображения* $W \mapsto \mathrm{Aut}(W)$, $\Gamma \mapsto \mathcal{Z}(\Gamma)$ *определяют биекцию между* 1*-регулярными клеточными кольцами и группами перестановок с базовым числом, не превосходящим* 1. •

Теорема 9.6. *Пусть* W *— клеточное кольцо и* $m \geqslant 1$ *— натуральное число. Если кольцо* $W_{v_1,\ldots,v_{m-1}}$ *является* 1*-регулярным для некоторых точек* $v_1, \ldots, v_{m-1}$*, то кольцо* $\widehat{W}^{(m)}$ *также является* 1*-регулярным.*

Доказательство. Поскольку $W_{v_1,\ldots,v_{m-1}}$ является 1-регулярным кольцом, то по леммам 9.2 и 3.1 кольцо $\widehat{W}_U$, определенное в последней лемме, также

является 1-регулярным. Обозначим через $\overline{v} = (v_1, \dots, v_{m-1}, v_m)$ какую-нибудь регулярную точку кольца $\widehat{W}_U$ и докажем, что она является регулярной точкой кольца $\widehat{W}$. Для $i \in \{1, \dots, m\}$ положим $E_i = \{(\overline{u}, \overline{u}') \in V^m \times V^m : u_i = u_i'\}$. Тогда достаточно доказать, что

$$\forall i \in \{1, \dots, m\}\ \forall U_i \in V^m/E_i\ \exists R_i \in \mathcal{R}^*(\widehat{W}) : \quad R_i(\overline{v}) = U_i. \tag{52}$$

Действительно, если $\overline{u} \in V^m$, то, очевидно, $\{\overline{u}\} = \bigcap_{i=1}^m U_i$, где U_i — класс эквивалентности E_i, содержащий точку $\overline{u}$. Согласно (52), $U_i = R_i(\overline{v})$, где $R_i \in \mathcal{R}^*(\widehat{W})$, для всех i. Поэтому $\{\overline{u}\} = R(\overline{v})$, где $R = \bigcap_{i=1}^m R_i$. Таким образом, $R \in \mathcal{R}^*(\widehat{W})$ и $d_{\mathrm{out}}(R) = 1$. Отсюда следует, что $R \in \mathcal{R}(\widehat{W})$, и потому $\overline{v}$ — регулярная точка кольца $\widehat{W}$.

Докажем формулу (52). Предположим сначала, что $i = m$. Для $U' \in V^m/E_m$ существует точка $v \in V$ такая, что $U' = \{\overline{u} \in V^m : u_m = v\}$. Обозначим через R базисное отношение кольца $\widehat{W}$, содержащее пару $(\overline{v}, v^\varsigma)$. Тогда $d_{\mathrm{out}}(R) = 1$, поскольку $R \subset E$ и $\overline{v}$ является регулярной точкой кольца $\widehat{W}_U$. Поэтому $U' = R'(v)$, где R' — бинарное отношение на множестве V^m, матрица смежности которого равна $A(R') = A(R)A(E_m)$. Поскольку $E_m \in \mathcal{E}(\widehat{W})$, мы имеем $R' \in \mathcal{R}(\widehat{W})$. Пусть теперь i произвольно. Обозначим через G образ естественного представления симметрической группы степени m перестановочными матрицами кольца Mat_{V^m}. Тогда из [5] следует, что $G \subset \widehat{W}$. Поскольку действие группы G правыми умножениями на множестве $\{A(E_i) : i = 1, \dots, m\}$ транзитивно, то общий случай сводится к случаю $i = m$. •

Теорема 9.3 и теорема 9.6 влекут следующее утверждение.

Следствие 9.7. *Пусть W — клеточное кольцо и $b = b(W)$ — его базовое число. Тогда при $m \geqslant b + 1$ кольцо $\widehat{W}^{(m)}$ отделимо и шурово.* •

Список литературы

[1] Brouwer A. E., Cohen A. M., Neumaier A., *Distance-regular graphs*, Ergeb. Math. Grenzgeb. (3), vol. 18, Springer-Verlag, Berlin-New York, 1989.

[2] Dixon J. D., Mortimer B, *Permutation groups*, Grad. Texts in Math., No. 163, Springer-Verlag, New York, 1996.

[3] Evdokimov S., Ponomarenko I., *Isomorphism of coloured graphs with slowly increasing multiplicity of Jordan blocks*, Combinatorica **19** (1999), 321-333.

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

[5] Evdokimov S., Karpinski M., Ponomarenko I., *On a new high-dimensional Weisfeiler-Leman algorithm*, J. Algebraic Combin. **10** (1999), 29-45.

[6] Evdokimov S., Ponomarenko I., *On highly closed cellular algebras and highly closed isomorphisms*, Electron. J. Combin. **6** (1999), no. 1, Research Paper 31.

[7] Evdokimov S., Ponomarenko I., *Separability number and Schurity number of coherent configurations*, Electron. J. Combin. **7** (2000), no. 1, Research Paper 31.

[8] Evdokimov S., Ponomarenko I., Tinhofer G., *Forestal algebras and algebraic forests (on a new class of weakly compact graphs)*, Discrete Math. **225** (2000), 149-172.

[9] Евдокимов С., Пономаренко И., *Об одном семействе колец Шура над конечной циклической группой*, Алгебра и анализ **13** (2001), №3, 139–154.
[10] Higman D. G., *Coherent configurations.* I, Rend. Sem. Mat. Univ. Padova **44** (1970), 1–25.
[11] Leung K. H., Man S. H., *On Schur rings over cyclic groups.* II, J. Algebra **183** (1996), 273–285.
[12] Leung K. H., Man S. H., *On Schur rings over cyclic groups*, Israel J. Math. **106** (1998), 251–267.
[13] Lidl R., Niederreiter H., *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge–New York, 1986.
[14] McConnel R., *Pseudo-ordered polynomials over a finite field*, Acta Arith. **8** (1963), 127–151.
[15] Muzychuk M. E., *On the structure of basic sets of Schur rings over cyclic groups*, J. Algebra **169** (1994), 655–678.
[16] Pöschel R., *Untersuchungen von S-Ringen insbesondere im Gruppenring von p-Gruppen*, Math. Nachr. **60** (1974), 1–27.
[17] Виноградов И. М., *Основы теории чисел*, Наука, М., 1972.
[18] Вейсфейлер Б. Ю., Леман А. А., *Приведение графа к каноническому виду и возникающая при этом алгебра*, НТИ. Сер. 2. Информ. анализ. **1968**, №9, 12–16.
[19] Weisfeiler B. (ed.), *On construction and identification of graphs*, Lecture Notes in Math., vol. 558, Springer-Verlag, Berlin–New York, 1976.
[20] Wielandt H., *Finite permutation groups*, Academic Press, New York–London, 1964.
[21] Wielandt H., *Permutation groups through invariant relations and invariant functions*, Ohio State Univ. Columbus, Dep. Math., Ohio, 1969.

С.-Петербургский институт
информатики и автоматизации РАН
E-mail: evdokim@pdmi.ras.ru

Поступило 15 октября 2001 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