Полукольца цикловых типов

А. В. МИХАЛЁВ, А. А. НЕЧАЕВ, А. В. ПРУДНИКОВ,
М. С. СТАРОВЕРОВ, А. В. ВЫДРИН
Московский государственный университет
им. М. В. Ломоносова

УДК 512.53+512.55

Ключевые слова: цикловой тип, полукольцо цикловых типов, подгруппа конечного индекса свободной абелевой группы, локальные преобразования Фурье, коэффициент Фурье.

Аннотация

Авторы исследуют полукольца цикловых типов с алгебраической точки зрения. Для совершенствования и упрощения анализа вводится понятие локального преобразования Фурье. Описаны делители нуля, нильпотентные элементы, обратимые элементы, идемпотенты и радикал Джекобсона.

Abstract

A. V. Mikhalev, A. A. Nechaev, A. V. Prudnikov, M. S. Staroverov, and A. S. Vydrin, Semirings of cyclic types, Fundamentalnaya i prikladnaya matematika, vol. 12 (2006), no. 2, pp. 175—192.

The authors investigate semirings of cyclic types from the algebraic point of view. To simplify and facilitate the analysis, local Fourier transform of these semirings is introduced. The authors describe zero divisors, nilpotent elements, invertible elements, idempotents, and the Jacobson radical.

1. Введение

Понятие циклового типа (цикловой структуры) появилось впервые, видимо, в теории подстановок. Пусть g — подстановка на множестве Ω, разложение которой в произведение независимых циклов содержит c_s^g циклов длины s для $s \in \mathbb{N}$. Тогда многочлен

$$C_g = \sum_{s \in \mathbb{N}} c_s^g x^s$$

назовём *цикловым типом* подстановки g. Нас интересует алгебраическая операция $*$ *композиции цикловых типов*, позволяющая описать цикловой тип прямого произведения подстановки g и подстановки h на множестве Δ, которое определяется как подстановка $g \times h$, действующая естественным образом, покоординатно, на множестве $\Omega \times \Delta$. Нетрудно проверить, что

$$C_{g \times h} = C_g * C_h = \sum_{s,t \in \mathbb{N}} (s,t) c_s^g c_t^h x^{[s,t]}, \tag{1.1}$$

где (s,t), $[s,t]$ — соответственно НОД и НОК чисел s и t.

Фундаментальная и прикладная математика, 2006, том 12, № 2, с. 175—192.

В [2] проведено дальнейшее обобщение этих понятий: введены понятия циклового типа реверсивного семейства полилинейных рекуррент, циклового типа прямой суммы таких семейств (композиция исходных цикловых типов) и полукольца цикловых типов. Мы рассмотрим их в более общем виде.

Пусть $\mathfrak{A}$ — абелева группа и $\sigma\colon \mathfrak{A} \to S(\Omega)$ — представление группы $\mathfrak{A}$ подстановками на конечном множестве Ω, т. е. гомоморфизм группы $\mathfrak{A}$ в симметрическую группу $S(\Omega)$. Пусть $\Omega_1, \ldots, \Omega_m$ — орбиты группы $\sigma(\mathfrak{A})$ на множестве Ω, $\sigma_i\colon \mathfrak{A} \to S(\Omega_i)$ — гомоморфизм, индуцируемый σ на орбите Ω_i, и $K_i = \operatorname{Ker}\sigma_i$, $i \in \{1, \ldots, m\}$. Заметим, что в таком случае $\sigma_i(\mathfrak{A}) \cong \mathfrak{A}/K_i$ есть транзитивная абелева группа подстановок на Ω_i и потому регулярная группа подстановок мощности $|\Omega_i|$, в частности, индекс подгруппы K_i в группе $\mathfrak{A}$ равен $|\Omega_i|$. Пусть $\mathcal{H} = \mathcal{H}(\mathfrak{A})$ — множество всех подгрупп конечного индекса группы $\mathfrak{A}$. Очевидно, что $\mathcal{H}$ относительно операции пересечения является полугруппой с единицей $\mathfrak{A}$. Для $K, L \in \mathcal{H}$ будем в дальнейшем использовать сокращённую запись: $KL = K \cap L$. Рассмотрим полугрупповое полукольцо $\mathbb{N}\mathcal{H}$ над полукольцом $(\mathbb{N}, +, \cdot)$ и назовём *цикловым типом представления* σ элемент $Z_\sigma \in \mathbb{N}\mathcal{H}$ вида

$$Z_\sigma = \sum_{i \in \{1,\ldots,m\}} K_i = \sum_{K \in \mathcal{H}} z_K^\sigma K, \tag{1.2}$$

где z_K^σ — кратность появления ядра K в наборе $K_1, \ldots, K_m$. Допустим, дано ещё одно представление $\tau\colon \mathfrak{A} \to S(\Delta)$, имеющее цикловой тип

$$Z_\tau = \sum_{L \in \mathcal{H}} z_L^\tau L.$$

Тогда цикловой тип $Z_{\sigma\times\tau}$ прямого произведения этих представлений

$$\sigma \times \tau\colon \mathfrak{A} \to S(\Omega \times \Delta)$$

выражается через исходные цикловые типы по формуле

$$Z_{\sigma\times\tau} = Z_\sigma * Z_\tau = \sum_{K,L \in \mathcal{H}} z_K^\sigma z_L^\tau \psi(K,L) KL, \quad \psi(K,L) = \frac{\operatorname{ind} K \cdot \operatorname{ind} L}{\operatorname{ind} KL}. \tag{1.3}$$

Для вывода этой формулы достаточно рассмотреть случай, когда σ и τ — транзитивные представления с ядрами соответственно K и L, и убедиться, что $\sigma\times\tau$ разбивает множество $\Omega\times\Delta$ мощности $\operatorname{ind} K \cdot \operatorname{ind} L$ на равномощные орбиты:

$$\Omega \times \Delta = W_1 \cup \ldots \cup W_r,$$

где $|W_i| = \operatorname{ind} KL$, $r = \psi(K,L)$, причём ограничение представления $\sigma \times \tau$ на каждой орбите есть представление с ядром KL.

Нетрудно проверить, что операция *композиции* $*$ на $\mathbb{N}\mathcal{H}$, определяемая по правилу (1.3), ассоциативна и для любых $F, G, H \in \mathcal{H}$ выполняются равенства

$$(F * G) * H = \psi(F,G) \cdot \psi(FG,H) \cdot FGH = \frac{\operatorname{ind} F \cdot \operatorname{ind} G \cdot \operatorname{ind} H}{\operatorname{ind} FGH} \cdot FGH =$$
$$= \psi(F,GH) \cdot \psi(G,H) \cdot FGH = F * (G * H). \tag{1.4}$$

Алгебра $(\mathbb{N}\mathcal{H}, +, *)$ есть коммутативное полукольцо с единицей $\mathfrak{A}$, которое мы далее обозначаем $\mathbb{N}^{\psi}\mathcal{H}(\mathbb{Z})$ и называем *полукольцом цикловых типов группы* $\mathfrak{A}$.

Нетрудно увидеть, что выведенная в самом начале формула (1.1), описывающая цикловой тип прямого произведения подстановок, соответствует вычислениям в полукольце $\mathbb{N}^{\psi}\mathcal{H}(\mathbb{Z})$. Если цикловому типу C^g подстановки g поставить в соответствие цикловой тип Z_σ представления $\sigma\colon \mathbb{Z} \to S(\Omega)$, такого что $\sigma(1) = g$, то получим

$$Z_\sigma = \sum_{\langle s\rangle \in \mathcal{H}} c_s^g \langle s\rangle,$$

где $\langle s\rangle$ — циклическая подгруппа группы $\mathbb{Z}$, порождённая s. Аналогично, рассматривая представление $\tau\colon \mathbb{Z} \to S(\Delta)$, такое что $\tau(1) = h$, получаем

$$Z_\tau = \sum_{\langle t\rangle \in \mathcal{H}} c_t^h \langle t\rangle.$$

Теперь ясно, что цикловому типу $C_{g\times h}$ соответствует $Z_\sigma * Z_\tau$.

Несколько более громоздкие выкладки с использованием результатов [2] показывают, что вычисления цикловых типов прямых сумм реверсивных семейств полилинейных рекуррент сводятся к вычислениям в полукольце $\mathbb{N}^{\psi}\mathcal{H}_k$, где $\mathcal{H}_k = \mathcal{H}(\mathbb{Z}^k)$ — полугруппа подгрупп конечного индекса свободной абелевой группы $\mathbb{Z}^k$ ранга k. Изучение свойств этого полукольца представляется первоочередным, в частности потому, что это — основной этап при изучении полукольца $\mathbb{N}^{\psi}\mathcal{H}(\mathfrak{A})$, соответствующего произвольной конечно порождённой абелевой группе $\mathfrak{A}$.

С точки зрения описанной конструкции (1.3) основной прикладной задачей является описание в $\mathbb{N}^{\psi}\mathcal{H}_k$ неразложимых элементов и построение разложения произвольного элемента из $\mathbb{N}^{\psi}\mathcal{H}_k$ в произведение неразложимых элементов.

В связи с этим представляется интересным изучение полуколец $R^{\psi}\mathcal{H}_k$ при различных R с алгебраической точки зрения, в частности описание обратимых элементов, делителей нуля и радикала Джекобсона (в случае, если R — кольцо).

2. Коэффициенты и локальные преобразования Фурье

Для любых подгрупп $G, H \leqslant \mathbb{Z}^k$ будем по-прежнему обозначать $G \cap H$ через GH. Будем говорить, что G *делит* H, и писать $G \mid H$, если $H \leqslant G$, т. е. если $GH = H$. Для $G, H \in \mathcal{H}_k$ последнее равносильно условию $\operatorname{ind} GH = \operatorname{ind} H$. Множество всех делителей в $\mathcal{H}_k$ подгруппы $H \leqslant \mathbb{Z}^k$ обозначим через $\mathcal{D}(H)$. Заметим, что если $H \in \mathcal{H}_k$, то $\mathcal{D}(H)$ — конечная подполугруппа $\mathcal{H}_k$, и более того, любая конечно порождённая подполугруппа $[G_1, \ldots, G_t\rangle$ полугруппы $\mathcal{H}_k$ также конечна, поскольку она лежит в $\mathcal{D}(G_1 \cap \ldots \cap G_t)$.

Всюду далее термин полукольцо (кольцо) будет означать коммутативное полукольцо (кольцо) R с единицей и без делителей нуля, удовлетворяющее

условию $\operatorname{char} R = 0$. При этом соответствующее полукольцо (кольцо) цикловых типов $R^{\psi}\mathcal{H}_k$ есть также коммутативное полукольцо (кольцо) с единицей $1 \cdot \mathbb{Z}^k$, причём $\operatorname{char} R^{\psi}\mathcal{H}_k = 0$.

Зафиксируем $H \leqslant \mathbb{Z}^k$ и назовём отображение

$$R^{\psi}\mathcal{H}_k \xrightarrow{\|\cdot\|_H} R,$$

определяемое для

$$A = \sum_{G \in \mathcal{H}_k} a_G \cdot G$$

равенством

$$\|A\|_H = \sum_{G \in \mathcal{D}(H)} a_G \cdot \operatorname{ind} G,$$

H-коэффициентом Фурье элемента A. Определение корректно, поскольку лишь конечное число коэффициентов a_G отлично от нуля. Для $H = \{0\}$ вместо $\|A\|_{\{0\}}$ будем писать $\|A\|$.

Теорема 2.1. *Для любой подгруппы $H \leqslant \mathbb{Z}^k$ отображение $R^{\psi}\mathcal{H}_k \xrightarrow{\|\cdot\|_H} R$ является гомоморфизмом полуколец.*

Доказательство. Согласованность с операцией сложения очевидна. Докажем согласованность с операцией умножения. Пусть $\mathbb{I}(G) = \mathbb{I}_{\mathcal{D}(H)}(G)$ — характеристическая функция множества $\mathcal{D}(H)$. Тогда $\mathbb{I}(G_1) \cdot \mathbb{I}(G_2) = \mathbb{I}(G_1 G_2)$ для любых $G_1, G_2 \in \mathcal{H}_k$. Докажем теперь, что для любых элементов

$$A = \sum_{i=1}^{n} a_i \cdot F_i, \quad B = \sum_{j=1}^{m} b_j \cdot G_j$$

из $R^{\psi}\mathcal{H}_k$ выполняется равенство

$$\|A * B\|_H = \|A\|_H \cdot \|B\|_H.$$

Нетрудно заметить, что

$$\|A\|_H = \sum_{i=1}^{n} a_i \cdot \mathbb{I}(F_i) \cdot \operatorname{ind} F_i, \tag{2.1}$$

аналогичные равенства выполняются для $\|B\|_H$ и $\|A * B\|_H$. Имеем цепочку равенств

$$\begin{aligned}
\|A\|_H \cdot \|B\|_H &= \left(\sum_{i=1}^{n} a_i \cdot \mathbb{I}(F_i) \cdot \operatorname{ind} F_i \right) \cdot \left(\sum_{j=1}^{m} b_j \cdot \mathbb{I}(G_j) \cdot \operatorname{ind} G_j \right) = \\
&= \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j \cdot \mathbb{I}(F_i) \cdot \mathbb{I}(G_j) \cdot \operatorname{ind} F_i \cdot \operatorname{ind} G_j = \\
&= \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j \cdot \mathbb{I}(F_i G_j) \cdot \operatorname{ind} F_i \cdot \operatorname{ind} G_j =
\end{aligned}$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \cdot b_j \cdot \mathbb{I}(F_iG_j) \cdot \frac{\operatorname{ind} F_i \cdot \operatorname{ind} G_j}{\operatorname{ind}(F_iG_j)} \cdot \operatorname{ind}(F_iG_j) =$$

$$= \left\| \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \cdot b_j \cdot \frac{\operatorname{ind} F_i \cdot \operatorname{ind} G_j}{\operatorname{ind}(F_iG_j)} \cdot F_iG_j \right\|_H =$$

$$= \left\| \sum_{i=1}^{n}\sum_{j=1}^{m} a_i \cdot b_j \cdot \psi(F_i, G_j) \cdot F_iG_j \right\|_H = \left\| \Big(\sum_{i=1}^{n} a_i \cdot F_i \Big) * \Big(\sum_{j=1}^{m} b_j \cdot G_j \Big) \right\|_H =$$

$$= \|A * B\|_H.$$

Итак, H-коэффициент Фурье есть гомоморфизм. □

Коэффициенты Фурье являются основным инструментом изучения полуколец в этой статье. В рассматриваемом случае (полукольца нулевой характеристики с единицей и без делителей нуля) верны два утверждения.

Предложение 2.2. *Равенство нулю коэффициентов Фурье $\|A\|_H$ элемента $A \in R^\psi\mathcal{H}_k$ для всех $H \leqslant \mathbb{Z}^k$ равносильно равенству нулю самого элемента A.*

Предложение 2.3. *Из равенство произведения элементов A и B нулю следует, что для любой группы $H \leqslant \mathbb{Z}^k$ либо $\|A\|_H = 0$, либо $\|B\|_H = 0$.*

В этом разделе демонстрируются преимущества рассмотрения коэффициентов Фурье элемента по сравнению с изучением его коэффициентов. Для начала заметим, что ненулевых коэффициентов у некоторого конечного множества элементов конечное число, а коэффициентов Фурье — бесконечное. Однако оказывается, что число *различных* коэффициентов Фурье также конечно.

Определим *носитель* элемента $A \in R^\psi\mathcal{H}_k$ равенством

$$\operatorname{supp} A = \{\mathbb{Z}^k\} \cup \{H \in \mathcal{H}_k \mid a_H \neq 0\}.$$

Пусть $M = \{A^1, A^2, \ldots, A^n\}$ — конечное подмножество $R^\psi\mathcal{H}_k$. Назовём *базой множества* M подполугруппу $[\operatorname{supp} A^1 \cup \operatorname{supp} A^2 \cup \ldots \cup \operatorname{supp} A^n\rangle$ полугруппы $\mathcal{H}_k$ и обозначим её $\mathfrak{B}(M) = \mathfrak{B}(A^1, A^2, \ldots, A^n)$. Это конечная подполугруппа в $\mathcal{H}_k$.

Назовём *цоколем* конечного подмножества $\mathcal{S} \subset \mathcal{H}_k$ пересечение $K(\mathcal{S})$ всех подгрупп $G \in \mathcal{S}$ и будем говорить, что подполугруппа $\mathcal{H}(\mathcal{S}) = \mathcal{D}(K(\mathcal{S})) < \mathcal{H}_k$ есть *оболочка* $\mathcal{S}$. Для конечного подмножества $M = \{A^1, A^2, \ldots, A^n\}$ полукольца $R^\psi\mathcal{H}_k$ также определим *цоколь* и *оболочку* в $\mathcal{H}_k$ равенствами $K(M) = K(A^1, \ldots, A^n) = K(\mathfrak{B}(M))$ и $\mathcal{H}(M) = \mathcal{H}(A^1, \ldots, A^n) = \mathcal{H}(\mathfrak{B}(M))$ соответственно. Заметим, что $R^\psi\mathcal{H}(A^1, \ldots, A^n)$ — конечно порождённое подполукольцо полукольца $R^\psi\mathcal{H}_k$, содержащее единицу, элементы $A^1, A^2, \ldots, A^n$ и результаты всех алгебраических операций над ними. Цоколь $K(M)$ является максимальным по индексу элементом и базы $\mathfrak{B}(M)$, и оболочки $\mathcal{H}(M)$, следовательно, база содержится в оболочке: $\mathfrak{B}(M) \subset \mathcal{H}(M)$. Обратное верно не всегда, что показывает следующий пример.

Пример 2.4. Пусть F, G, H — группы индекса 2, такие что $FG = GH = FH = FGH$, и $A = 1 \cdot F + 1 \cdot G$. Тогда $\mathfrak{B}(A) \neq \mathcal{H}(A)$.

Доказательство. Действительно,

$$\mathfrak{B}(A) = \{\mathbb{Z}^k, F, G, FGH\} \neq \{\mathbb{Z}^k, F, G, H, FGH\} = \mathcal{H}(A). \qquad \square$$

Для каждой группы $H \in \mathcal{H}_k$ и любой подполугруппы $\mathcal{S} < \mathcal{H}_k$ назовём цоколь пересечения полугрупп $\mathcal{S}$ и $\mathcal{D}(H)$

$$\operatorname{pr}_{\mathcal{S}} H = K(\mathcal{S} \cap \mathcal{D}(H))$$

проекцией H на $\mathcal{S}$. Очевидно, что проекция группы H из $\mathcal{S}$ на $\mathcal{S}$ совпадает с исходной группой: $\operatorname{pr}_{\mathcal{S}} H = H$. В случае, если $\mathcal{S}$ является базой некоторого конечного подмножества $M = \{A^1, A^2, \ldots, A^n\}$ полугруппы $R^{\psi}\mathcal{H}_k$, мы будем также говорить, что $\operatorname{pr}_{\mathfrak{B}(M)} H$ является *проекцией группы на множество M*, и использовать обозначение

$$\operatorname{pr}_M H = \operatorname{pr}_{A^1, A^2, \ldots, A^n} H.$$

Таким образом, база $\mathfrak{B}(M)$ есть множество всех проекций $\operatorname{pr}_M H$, где $H \in \mathcal{H}_k$. Важность понятия проекции показывает следующая теорема.

Теорема 2.5. *Пусть $M \subset R^{\psi}\mathcal{H}_k$ и $\mathfrak{B}(M) \subseteq \mathcal{S} \subset \mathcal{H}_k$. Тогда для каждого элемента $A \in M$ и любой группы $H \in \mathcal{H}_k$ справедливо равенство*

$$\|A\|_H = \|A\|_{\operatorname{pr}_{\mathcal{S}} H}.$$

Доказательство. Для доказательства теоремы достаточно подставить в равенство определение коэффициентов Фурье и воспользоваться определением проекции. Из того, что $\operatorname{supp} A \subset \mathfrak{B}(M) \subset \mathcal{S}$, следует, что

$$\|A\|_H = \sum_{G \in \mathcal{D}(H)} a_G \cdot \operatorname{ind} G = \sum_{G \in \mathcal{S} \cap \mathcal{D}(H)} a_G \cdot \operatorname{ind} G.$$

Пользуясь определением проекции, получаем, что

$$\mathcal{S} \cap \mathcal{D}(H) = \mathcal{S} \cap \mathcal{D}(\operatorname{pr}_{\mathcal{S}} H).$$

Носитель элемента A лежит в $\mathcal{S}$, следовательно,

$$\sum_{G \in \mathcal{S} \cap \mathcal{D}(\operatorname{pr}_{\mathcal{S}} H)} a_G \cdot \operatorname{ind} G = \sum_{G \in \mathcal{D}(\operatorname{pr}_{\mathcal{S}} H)} a_G \cdot \operatorname{ind} G = \|A\|_{\operatorname{pr}_{\mathcal{S}} H}.$$

Теорема доказана. $\square$

Тем самым для фиксированного множества $M \subset R^{\psi}\mathcal{H}_k$ мы разбили множество *всех* групп $H \leqslant \mathbb{Z}^k$ на *конечное* число классов эквивалентности: из того, что $H \sim G$, т. е. $\operatorname{pr}_M H = \operatorname{pr}_M G$, следует, что $\|A\|_H = \|A\|_G$ при всех $A \in M$.

В дальнейшем нам понадобится перечислять элементы различных подмножеств $\mathcal{S} \in \mathcal{H}_k$ в порядке неубывания индексов. Поскольку групп фиксированного конечного индекса в $\mathcal{H}_k$ конечное число, мы можем определить на $\mathcal{H}_k$ отношение порядка $\preceq$ так, что для любых $F, G \in \mathcal{H}_k$

$$(F \prec G) \implies (\operatorname{ind} F \leqslant \operatorname{ind} G). \tag{2.2}$$

Тогда элементы любого конечного подмножества $\mathcal{S} = \{F_1, \dots, F_m\}$ однозначно упорядочиваются так, что для любых $i, j \in \{1, \dots, m\}$

$$(i < j) \iff (F_i \prec F_j). \tag{2.3}$$

Связь между коэффициентами элемента и его коэффициентами Фурье демонстрирует следующая теорема.

Теорема 2.6. *Пусть $A \in R^{\psi}\mathcal{H}_k$, $\mathcal{S} = \{F_1, \dots, F_m\}$ — конечное подмножество $\mathcal{H}_k$, элементы которого упорядочены согласно отношению $\preceq$. Тогда справедливо равенство*

$$\begin{pmatrix} \operatorname{ind} F_1 & 0 & \dots & 0 \\ I_2(F_1)\cdot\operatorname{ind} F_1 & \operatorname{ind} F_2 & 0 \dots & 0 \\ \dots & \dots & \dots & \dots \\ I_m(F_1)\cdot\operatorname{ind} F_1 & I_m(F_2)\cdot\operatorname{ind} F_2 & \dots & I_m(F_{m-1})\cdot\operatorname{ind} F_{m-1} \quad \operatorname{ind} F_m \end{pmatrix} \times$$

$$\times \begin{pmatrix} a_{F_1} \\ a_{F_2} \\ \dots \\ a_{F_m} \end{pmatrix} = \begin{pmatrix} \|A\|_{F_1} \\ \|A\|_{F_2} \\ \dots \\ \|A\|_{F_m} \end{pmatrix}, \tag{2.4}$$

где $I_s(F_t) = \mathbb{I}_{D(F_s)}(F_t)$, $s, t \in \{1, \dots, m\}$.

Доказательство. Очевидно, что если $s, t \in \{1, \dots, m\}$ и $F_t \in D(F_s)$, то $t \leqslant s$. Вспомним определение (2.1) F_s-коэффициента Фурье:

$$\|A\|_{F_s} = \sum_{G \in \mathcal{D}(F_s)} a_G \cdot \operatorname{ind} G.$$

Тем самым

$$\|A\|_{F_s} = \sum_{i}^{m} I_s(F_i) a_{F_i} \cdot \operatorname{ind} F_i.$$

Мы получаем равенство, написанное в s-й строке системы (2.4). □

Назовём целочисленную матрицу $\Phi(\mathcal{S})$ в левой части равенства (2.4) *матрицей локального преобразования Фурье с носителем $\mathcal{S}$*. Эта матрица обратима над $\mathbb{Q}$ и представляется в виде произведения

$$\Phi(\mathcal{S}) = \mathcal{U}(\mathcal{S})\Delta(\mathcal{S}), \tag{2.5}$$

где

$$\mathcal{U}(\mathcal{S}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ I_2(F_1) & 1 & 0 \dots & 0 \\ \dots & \dots & \dots & \dots \\ I_m(F_1) & I_m(F_2) & \dots & I_m(F_{m-1}) \quad 1 \end{pmatrix} - \tag{2.6}$$

обратимая матрица над $\mathbb{Z}$, а

$$\Delta(\mathcal{S}) = \operatorname{diag}(\operatorname{ind} F_1, \dots, \operatorname{ind} F_m) - \tag{2.7}$$

диагональная матрица над $\mathbb{Z}$.

Пусть $\mathcal{K}_{\mathcal{S}}(A) = (a_{F_1}, \ldots, a_{F_m})^{\top} \in R^m$ — столбец коэффициентов элемента A и $\mathcal{N}_{\mathcal{S}}(A) = (\|A\|_{F_1}, \ldots, \|A\|_{F_m})^{\top} \in R^m$ — столбец коэффициентов Фурье элемента A, тогда равенство (2.4) можно коротко записать в виде

$$\Phi(\mathcal{S})\mathcal{K}_{\mathcal{S}}(A) = \mathcal{N}_{\mathcal{S}}(A). \tag{2.8}$$

Так как R — полукольцо без делителей нуля, то верно следующее утверждение.

Предложение 2.7. *Если $\mathcal{S} \supset \mathfrak{B}(A, B)$, то равенство $A = B$ эквивалентно системе равенств $\|A\|_E = \|B\|_E$ при всех $E \in \mathcal{S}$.*

Таким образом, преобразование $\Psi(\mathcal{S})\colon R^m \to R^m$, переводящее столбец $\mathcal{K}_{\mathcal{S}}$ в столбец $N_{\mathcal{S}} = \Phi(\mathcal{S})\mathcal{K}_{\mathcal{S}}$, инъективно, однако при произвольном R оно не сюръективно: уравнение

$$\Phi(\mathcal{S})X = N \tag{2.9}$$

разрешимо не для любого $N \in R^m$, т. е. не к любому столбцу $N \in R^m$ применимо обратное преобразование Фурье. Очевидно, уравнение (2.9) разрешимо в R^m тогда и только тогда, когда

$$N \in \Phi(\mathcal{S})R^m. \tag{2.10}$$

Из (2.5), (2.6) следует также, что уравнение (2.9) разрешимо, в точности если разрешимо уравнение

$$\Delta(\mathcal{S})X = \mathcal{U}(\mathcal{S})^{-1}N. \tag{2.11}$$

Последнее условие равносильно условию

$$\mathcal{U}(\mathcal{S})^{-1}N \in \Delta(\mathcal{S})R^m. \tag{2.12}$$

Более того, при условии (2.12) уравнение (2.9) имеет по предложению 2.7 единственное решение, которое мы обозначим $\Phi(\mathcal{S})^{-1}N$. Назовём столбец $N \in R^m$, удовлетворяющий условию (2.10), *$\mathcal{S}$-нормальным* или просто *нормальным*, если ясно, о каком $\mathcal{S}$ идёт речь. Заметим, что ввиду (2.8), (2.5) нормальность N равносильна тому, что $N = \mathcal{N}_{\mathcal{S}}(A)$ для некоторого $A \in R^{\psi}\mathcal{H}_k$, удовлетворяющего условию $\operatorname{supp} A \subseteq \mathcal{S}$, и в таком случае $\Phi(\mathcal{S})^{-1}N = \mathcal{K}_{\mathcal{S}}(A)$. Очевидно также, что если R — поле, то любой столбец над R нормален, поэтому верно следующее утверждение.

Предложение 2.8. *Если $R = P$ — поле характеристики нуль, то в обозначениях теоремы 2.6 для любого $N \in P^m$ существует единственный элемент $A \in P^{\psi}\mathcal{H}_k$, такой что $\operatorname{supp} A \subseteq \mathcal{S}$ и $N = \mathcal{N}_{\mathcal{S}}(A)$.*

3. Решение уравнения $A * X = B$

Для произвольных $A, B \in R^{\psi}\mathcal{H}_k$ рассмотрим уравнение

$$A * X = B. \tag{3.1}$$

Пусть C — некоторое его решение и $\mathcal{S} \subset \mathcal{H}_k$ — конечное множество, содержащее базу A, B, C, $|\mathcal{S}| = m$. Определим операцию $\odot$ на R^m следующим образом:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \odot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} a_1 c_1 \\ \vdots \\ a_m c_m \end{pmatrix}. \tag{3.2}$$

Тогда ввиду теоремы 2.6 справедливо равенство

$$\mathcal{N}_{\mathcal{S}}(A) \odot \mathcal{N}_{\mathcal{S}}(C) = \mathcal{N}_{\mathcal{S}}(B). \tag{3.3}$$

Теорема 3.1. *Пусть $\mathcal{H} = \mathcal{H}(A, B)$ — оболочка элементов $A, B \in R^{\psi}\mathcal{H}_k$, $|\mathcal{H}| = m$. Тогда справедливы следующие утверждения.*

1. *Уравнение* (3.1) *разрешимо в $R^{\psi}\mathcal{H}_k$, в точности если оно разрешимо в $R^{\psi}\mathcal{H}$.*
2. *Уравнение* (3.1) *разрешимо в $R^{\psi}\mathcal{H}$ тогда и только тогда, когда уравнение*

$$\mathcal{N}_{\mathcal{H}}(A) \odot Y = \mathcal{N}_{\mathcal{H}}(B) \tag{3.4}$$

   имеет $\mathcal{H}$-нормальное решение $N \in \Phi(\mathcal{H})R^m$.
3. *Если $N \in \Phi(\mathcal{H})R^m$ — решение* (3.4)*, то $\Phi(\mathcal{H})^{-1}N = \mathcal{K}_{\mathcal{H}}(C)$ — столбец коэффициентов решения $C \in R^{\psi}\mathcal{H}$ уравнения* (3.1)*.*

Доказательство. 1. Пусть $C = \sum\limits_{F \in \mathcal{H}_k} c_F \cdot F$ — решение (3.1). Положим $C_{\mathcal{H}} = \sum\limits_{F \in \mathcal{H}} c_F \cdot F$. Тогда $C = C_{\mathcal{H}} + C'$, где $\operatorname{supp} C' \cap \mathcal{H} = \varnothing$. По предположению справедливо равенство

$$B - A * C_{\mathcal{H}} = A * C'. \tag{3.5}$$

Так как носитель элемента $B - A * C_{\mathcal{H}}$ есть подмножество в $\mathcal{H}$, а носитель $A * C'$ имеет пустое пересечение с $\mathcal{H}$, то обе части равенства (3.5) — нули. Следовательно, $C_{\mathcal{H}}$ также решение (3.1).

Утверждения 2, 3 теоремы следуют из предложения 2.7, применённого к группе $\mathcal{H}$ и элементам $A * C$ и B. □

Следствие 3.2. *Пусть в обозначениях теоремы* 3.1 *$R = P$ — поле. Тогда уравнение* (3.1) *разрешимо в $P^{\psi}\mathcal{H}_k$, если и только если $\mathcal{N}_{\mathcal{H}}(B) \in \mathcal{N}_{\mathcal{H}}(A) \odot P^m$, т. е. для любого $F \in \mathcal{H}$*

$$(\|A\|_F = 0) \implies (\|B\|_F = 0). \tag{3.6}$$

Доказательство. По предложению 2.8 в P^m все столбцы нормальны, поэтому наличие нормального решения уравнения (3.4) эквивалентно тому, что это уравнение разрешимо в P^m. Так как P — поле характеристики 0, последнее условие равносильно (3.6). □

Заметим, что если в условии предыдущей теоремы поменять оболочку $\mathcal{H}(A, B)$ на базу $\mathfrak{B}(A, B)$, утверждение 1 перестанет быть верным. Приведём пример для кольца $\mathbb{Z}^{\psi}\mathcal{H}_k$.

Пример 3.3. Пусть F, G — различные подгруппы индекса 2 в $\mathbb{Z}^k$, элементы $A = 1 \cdot F$, $C = 1 \cdot G$ и $B = 1 \cdot FG$ — элементы $\mathbb{Z}^\psi\mathcal{H}_k$. Тогда $A * C = B$, т. е. решение уравнения (3.1) существует,

$$\mathfrak{B}(A,B) = \{\mathbb{Z}^k, F, FG\}, \quad \mathcal{N}_{\mathfrak{B}}^{\top}(A) = \begin{pmatrix}0 & 2 & 2\end{pmatrix}, \quad \mathcal{N}_{\mathfrak{B}}^{\top}(B) = \begin{pmatrix}0 & 0 & 2\end{pmatrix}.$$

Отсюда следует, что если $N \in \Phi(\mathfrak{B})R^m$ — решение (3.4), то

$$N^{\top} = \begin{pmatrix}a & 0 & 1\end{pmatrix},$$

где $a \in \mathbb{Z}$, но тогда строка коэффициентов решения равна

$$(\Phi(\mathfrak{B})^{-1}N)^{\top} = \begin{pmatrix}a & \frac{a}{2} & \frac{1}{4}\end{pmatrix}.$$

Противоречие.

В случае, если R не поле, из условия

$$\mathcal{N}_{\mathcal{H}}(B) \in \mathcal{N}_{\mathcal{H}}(A) \odot R^m \tag{3.7}$$

разрешимости уравнения (3.4) не следует. Рассмотрим, например, случай $R = \mathbb{Z}$.

Пример 3.4. Пусть G — подгруппа индекса 6 в $\mathbb{Z}^k$, элемент A равен $3 \cdot \mathbb{Z}^k$, элемент B равен $3 \cdot \mathbb{Z}^k - G$. Заметим, что $\mathfrak{B}(A,B) = \{\mathbb{Z}^k, G\}$, $\|A\|_{\mathbb{Z}^k} = 3$, $\|A\|_G = 3$, $\|B\|_{\mathbb{Z}^k} = 3$, $\|B\|_G = -3$ и, следовательно, условие (3.7) выполнено. Если существует элемент $C \in \mathbb{Z}^\psi\mathcal{H}_k$, такой что $A = B * C$, то $\|C\|_G = -1$, а для любой группы $H \in \mathcal{D}(G) \setminus \{G\}$ коэффициент Фурье $\|C\|_H$ равен 1. Тогда $-1 = \|C\|_G = 6 \cdot c_G + c_{\mathbb{Z}^k} = 6 \cdot c_G + 1$ и $c_G = -1/3$, чего быть не может.

Теперь рассмотрим случай $R = \mathbb{N}$.

Пример 3.5. Пусть G и H — подгруппы в $\mathbb{Z}^k$ индексов 2 и 4 соответственно, такие что $\mathcal{D}(H) = \{\mathbb{Z}^k, G, H\}$, элемент A равен $1 \cdot H$, элемент B равен $1 \cdot G$. Заметим, что $\mathfrak{B}(A,B) = \{\mathbb{Z}^k, G, H\}$, $\|A\|_{\mathbb{Z}^k} = 0$, $\|A\|_G = 0$, $\|A\|_H = 4$, $\|B\|_{\mathbb{Z}^k} = 0$, $\|B\|_G = 2$, $\|B\|_H = 2$ и, следовательно, условие (3.7) выполнено. Если существует элемент $C \in \mathbb{Z}^\psi\mathcal{H}_k$, такой что $A = B * C$, то $\|C\|_H = 2$, что может быть либо при $c_{\mathbb{Z}^k} = 2$, $c_G = c_H = 0$, либо при $c_{\mathbb{Z}^k} = c_H = 0$, $c_G = 1$, но в любом случае $0 = \|A\|_G = \|B\|_G \cdot \|C\|_G = 2 \cdot 2 = 4$, чего быть не может.

Для поиска всех решений уравнения 3.1 при известном одном можно воспользоваться следующим утверждением.

Теорема 3.6. *Пусть R — кольцо и $A, B \in R^\psi\mathcal{H}_k$, элемент X_0 — частное решение уравнения $A*X = B$. Тогда множество всех решений уравнения $A*X = B$ в $R^\psi\mathcal{H}_k$ есть $X_0 + \mathrm{Ann}_{R^\psi\mathcal{H}_k} A$.*

4. Делители нуля и нильпотентные элементы

Множество $\mathfrak{N}(R^\psi\mathcal{H}_k)$ всех нильпотентных элементов полукольца $R^\psi\mathcal{H}_k$ равно $\{0\}$. Действительно, пусть существуют элемент $C \in R^\psi\mathcal{H}_k$ и число $n \in \mathbb{N}$, такие что $C^n = 0$. Тогда $\|C^n\|_H = \|C\|_H^n = 0$ для любой группы $H \in \mathcal{H}_k$, следовательно, по предложению 2.7 $C = 0$.

Описание делителей нуля оказывается далеко не таким простым. Докажем вспомогательное утверждение.

Лемма 4.1. *Если коэффициент Фурье $\|C\|$ элемента $A \in \mathbb{N}^{\psi}\mathcal{H}_k$ равен нулю, то и сам элемент C равен нулю.*

Доказательство. По условию $\sum\limits_{H} c_H \cdot H = \|C\| = 0$, но тогда все коэффициенты c_H нулевые и $C = 0$. □

Теперь нахождение делителей нуля в полукольце $\mathbb{N}^{\psi}\mathcal{H}_k$ тривиально.

Теорема 4.2. *В полукольце $\mathbb{N}^{\psi}\mathcal{H}_k$ не существует делителей нуля.*

Доказательство. Пусть $A \in \mathbb{N}^{\psi}\mathcal{H}_k \setminus \{0\}$ — делитель нуля в $\mathbb{N}^{\psi}\mathcal{H}_k$. Тогда существует элемент $B \in \mathbb{N}^{\psi}\mathcal{H}_k \setminus \{0\}$, такой что $A * B = 0$. Значит, $\|A\| \cdot \|B\| = \|A * B\| = 0$. Поэтому либо $\|A\| = 0$, либо $\|B\| = 0$, откуда по предыдущей лемме либо $A = 0$, либо $B = 0$. Противоречие. □

В произвольном *полукольце* R верна лишь следующая теорема.

Теорема 4.3. *Если элемент $A \in R^{\psi}\mathcal{H}_k$ есть делитель нуля в $R^{\psi}\mathcal{H}_k$, то существует группа $E \in \mathfrak{B}(A)$, такая что $\|A\|_E = 0$.*

Доказательство. По условию существует элемент $B \in R^{\psi}\mathcal{H}_k \setminus \{0\}$, такой что $A * B = 0$. Следовательно, для любой группы $H \in \mathcal{H}_k$ выполняется равенство $\|A * B\|_H = \|A\|_H \cdot \|B\|_H = 0$. Если $\|A\|_E \neq 0$ для любой группы $E \in \mathfrak{B}(A)$, то $\|A\|_H = \|A\|_{\mathrm{pr}_A H} \neq 0$ для любой группы $H \in \mathcal{H}_k$, поэтому $\|B\|_H = 0$ для любой группы $H \in \mathcal{H}_k$, т. е. $B = 0$. Противоречие. □

Теперь мы можем описать все делители нуля в *кольце*.

Теорема 4.4. *Пусть R — кольцо. Элемент $A \in R^{\psi}\mathcal{H}_k$ есть делитель нуля в $R^{\psi}\mathcal{H}_k$ тогда и только тогда, когда существует группа $E \in \mathfrak{B}(A)$, такая что $\|A\|_E = 0$.*

Доказательство. 1. Пусть $A \in R^{\psi}\mathcal{H}_k$ — делитель нуля в $R^{\psi}\mathcal{H}_k$, тогда по теореме 4.3 существует группа $E \in \mathfrak{B}(A)$, такая что $\|A\|_E = 0$.

2. Пусть существует группа $E \in \mathfrak{B}(A)$, такая что $\|A\|_E = 0$. Упорядочим согласно $\preceq$ полугруппу $\mathcal{H} = \mathcal{H}(A)$. Построим элемент $A^{\perp}_E \in R^{\psi}\mathcal{H}_k \setminus \{0\}$, такой что $\mathfrak{B}(A^{\perp}_E) \subset \mathcal{H}$, $\|A^{\perp}_E\|_E = \det \Delta(\mathcal{H})$, $\|A^{\perp}_E\|_H = 0$ при $H \in \mathcal{H} \setminus \{E\}$ и $A * A^{\perp}_E = 0$. Рассмотрим такой элемент $A^{\perp}_E \in R^{\psi}\mathcal{H}_k$, что $\operatorname{supp} A^{\perp}_E \subset \mathcal{H}$ и

$$\Delta(\mathcal{H})\mathcal{K}_{\mathcal{H}}(A^{\perp}_E) = \mathcal{U}^{-1}(\mathcal{H})N,$$

где

$$N^{\top} = \begin{cases} \begin{pmatrix} \det \Delta(\mathcal{H}) & 0 & \dots & 0 \end{pmatrix}, & \text{если } E = \mathbb{Z}^k, \\ \begin{pmatrix} 0 & \det \Delta(\mathcal{H}) & 0 & \dots & 0 \end{pmatrix}, & \text{если } E \neq \mathbb{Z}^k. \end{cases}$$

Он существует и определён однозначно, так как в столбце $\mathcal{U}^{-1}(\mathcal{H})N$ все элементы делятся на $\det \Delta(\mathcal{H})$. Заметим, что $\mathfrak{B}(A, A^{\perp}_E) \subset \mathcal{H}$. Рассмотрим произвольную группу из $\mathcal{H}_k$. Если $\mathrm{pr}_{\mathcal{H}} H \in \mathcal{H} \setminus \{E\}$, то из определения элемента $A^{\perp}_E$ следует

равенство $\|A_E^{\perp}\|_H = \|A_E^{\perp}\|_{\mathrm{pr}_{\mathcal{H}} H} = 0$. В случае, если $\mathrm{pr}_{\mathcal{H}} H = E$, верно равенство $\|A\|_H = \|A\|_E = 0$. Итак, $\|A * A_E^{\perp}\|_H = \|A\|_H \cdot \|A_E^{\perp}\|_H = 0$ при всех H, т. е. $A * A_E^{\perp} = 0$. □

В поле легко описывается даже аннулятор произвольного элемента.

Теорема 4.5. *Если P — поле, то идеал $\mathrm{Ann}_{P^{\psi}\mathcal{H}_k}(A)$ порождается системой элементов*

$$\left\{A_E^{\perp}\right\}_{E\in\mathfrak{B}(A),\,\|A\|_E=0}.$$

Доказательство. Пусть $A * B = 0$, где B — элемент $R^{\psi}\mathcal{H}_k$ и $|\mathfrak{B}(A,B)| = n$. Укажем способ выражения элемента B через элементы системы. Для этого положим $C^0 = B$ и построим цепочку $C^0, C^1, \ldots, C^n$ элементов $P^{\psi}\mathcal{H}_k$, аннулирующих A, рекурсивно определяемую по следующему правилу: если $C^i = 0$, положим $C^{i+1} = 0$, в противном случае выберем в $\operatorname{supp} C^i$ группу с минимальным индексом и обозначим её через H^i. Тогда $\|A\|_{H^i} = 0$, так как $\|C\|_{H^i} = c_{H^i} \neq 0$, и $\|A\|_{H^i} \cdot \|C\|_{H^i} = \|A * C\|_{H^i} = 0$. Положим

$$C^{i+1} = C^i - \frac{c_{H^i}}{\operatorname{ind}\mathrm{pr}_A H^i} \cdot H^i * \frac{A^{\perp}_{\mathrm{pr}_A H^i}}{a^{\perp}_{\mathrm{pr}_A H^i}}.$$

Заметим, что

$$c_{H^i}^{i+1} = c_{H_i} - \frac{c_{H^i}}{\operatorname{ind}\mathrm{pr}_A H^i} \cdot \psi(H_i, \mathrm{pr}_A H^i) \cdot \frac{a^{\perp}_{\mathrm{pr}_A H^i}}{a^{\perp}_{\mathrm{pr}_A H^i}} = 0,$$

$c_F^{i+1} = c_F^i = 0$ при $\operatorname{ind} F \leqslant \operatorname{ind} H$, $F \neq H$, и C^{i+1} является элементом, аннулирующим A, так как

$$A * \left(H^i * A_G^{\perp}\right) = H^i * \left(A * A_G^{\perp}\right) = H^i * 0 = 0.$$

Далее, $\operatorname{supp} C^i \subset \mathfrak{B}(A,B)$, и если

$$n(F) = |\{G \in \mathfrak{B}(A,B)\colon\ \operatorname{ind} G \leqslant \operatorname{ind} F\}|,$$

то $c_F^{n(F)} = c_F^{n(F)+1} = \ldots = c_F^n = 0$. Поэтому $C^n = 0$. Итак, мы получили, что

$$B = \sum_{i=0}^{n-1}(C^i - C^{i+1}) = \sum_{i=0}^{n-1} \frac{c_{H^i}}{\operatorname{ind}\mathrm{pr}_A H^i} \cdot H^i * \frac{A^{\perp}_{\mathrm{pr}_A H^i}}{a^{\perp}_{\mathrm{pr}_A H^i}}.$$

Теорема доказана. □

5. Обратимые элементы

Теорема 5.1. *Пусть R — полукольцо. Если элемент $A \in R^{\psi}\mathcal{H}_k$ обратим в $R^{\psi}\mathcal{H}_k$, то коэффициент Фурье $\|A\|_H$ обратим в R для всех $H \in \mathcal{H}_k$.*

Доказательство. Пусть $B \in R^{\psi}\mathcal{H}_k$ — элемент, обратный к A. Тогда $\mathbb{Z}^k = A*B$, а значит, и $\|A\|_H \cdot \|B\|_H = 1$, поэтому для любой группы H коэффициент Фурье $\|A\|_H$ обратим в R. □

Следствие 5.2. *В $\mathbb{N}^{\psi}\mathcal{H}_k$ обратимым элементом является только $\mathbb{Z}^k$.*

Доказательство. Пусть элемент $A \in \mathbb{N}^{\psi}\mathcal{H}_k$ обратим. По теореме 5.1 коэффициент Фурье $\|A\|_{\mathbb{Z}^k} = a_{\mathbb{Z}^k}$ обратим в $\mathbb{N}$. Значит, $a_{\mathbb{Z}^k} = 1$. Если ещё какой-то коэффициент a_H отличен от 0, то $\|A\|_H \geqslant (1+2\cdot a_H) > 2$, а значит, коэффициент Фурье $\|A\|_H$ не может быть обратим в $\mathbb{N}$. □

Пусть R — кольцо. Следующая важная теорема сводит описание делителей произвольного элемента кольца $R^{\psi}\mathcal{H}_k$ к описанию делителей элемента вида $r \cdot \mathbb{Z}^k$, где $r \in R$.

Теорема 5.3. *Элемент $A \in R^{\psi}\mathcal{H}_k$ делит элемент $\Big(\prod\limits_{E\in\mathfrak{B}(A)} \|A\|_E\Big) \cdot \mathbb{Z}^k$.*

Доказательство. 1. Если элемент A является делителем нуля в кольце $R^{\psi}\mathcal{H}_k$, то по теореме 4.4 элемент $\Big(\prod\limits_{E\in\mathfrak{B}(A)} \|A\|_E\Big) \cdot \mathbb{Z}^k$ равен нулю, следовательно, утверждение верно.

2. Пусть элемент A не является делителем нуля в кольце $R^{\psi}\mathcal{H}_k$. Упорядочим элементы базы $\mathfrak{B}(A) = \{G_1, \ldots, G_n\}$ согласно отношению $\preceq$. Заметим, что $G_1 = \mathbb{Z}^k$. Рассмотрим элемент

$$B = \sum_{i=1}^{n} b_{G_i} \cdot G_i,$$

где

$$b_{G_i} = \bar{b}_{G_i} \cdot \prod_{j=i+1}^{n} \|A\|_{G_j},$$

а последовательность $\bar{b}_{G_i}$ определяется рекурсивно следующим образом: $b_{G_1} = 1$, и если для некоторого $i \in \{2, \ldots, n\}$ уже определены $\bar{b}_{G_1}, \ldots, \bar{b}_{G_{i-1}}$, то

$$\bar{b}_{G_i} = -\sum_{\substack{G_{k_1} G_{k_2} = G_i \\ k_2 < i}} a_{G_{k_1}} \cdot \psi(G_{k_1}, G_{k_2}) \cdot \bar{b}_{G_{k_2}} \cdot \prod_{j=k_2+1}^{i-1} \|A\|_{G_j}.$$

Покажем, что

$$A * B = \Big(\prod_{j=1}^{n} \|A\|_{G_j}\Big) \cdot \mathbb{Z}^k.$$

Из того, что $\operatorname{supp} B \subset \mathfrak{B}(A)$, следует, что $\operatorname{supp}(A * B) \subset \mathfrak{B}(A)$, т. е.

$$A * B = C = \sum_{j=1}^{n} c_{G_j} G_j.$$

Коэффициент c_{G1} равен

$$a_{G_1} \cdot b_{G_1} = a_{G_1} \cdot \bar{b}_{G_1} \cdot \prod_{j=2}^{n} \|A\|_{G_j} = \prod_{j=1}^{n} \|A\|_{G_j}.$$

Теперь покажем индукцией по $i \in \{2, \ldots, r\}$, что $c_{G_i} = 0$. Действительно, имеем

$$\begin{aligned} c_{G_i} &= \sum_{G_{k_1} G_{k_2} = G_i} a_{G_{k_1}} \cdot b_{G_{k_2}} \cdot \psi(G_{k_1}, G_{k_2}) = \\ &= \sum_{G_{k_1} | G_i} a_{G_{k_1}} \cdot b_{G_i} \cdot \psi(G_{k_1}, G_i) + \sum_{\substack{G_{k_1} G_{k_2} = G_i \\ k_2 < i}} a_{G_{k_1}} \cdot b_{G_{k_2}} \cdot \psi(G_{k_1}, G_{k_2}) = \\ &= b_{G_i} \cdot \|A\|_{G_i} + \sum_{\substack{G_{k_1} G_{k_2} = G_i \\ k_2 < i}} a_{G_{k_1}} \cdot \psi(G_{k_1}, G_{k_2}) \cdot \bar{b}_{G_{k_2}} \cdot \prod_{j=k_2+1}^{n} \|A\|_{G_j} = \\ &= \|A\|_{G_i} \cdot \prod_{j=i+1}^{n} \|A\|_{G_j} \cdot \bar{b}_{G_i} + \\ &+ \prod_{j=i}^{n} \|A\|_{G_j} \cdot \sum_{\substack{G_{k_1} G_{k_2} = G_i \\ k_2 < i}} a_{G_{k_1}} \cdot \psi(G_{k_1}, G_{k_2}) \cdot \bar{b}_{G_{k_2}} \cdot \prod_{j=k_2+1}^{i-1} \|A\|_{G_j} = 0. \end{aligned}$$

Итак, мы нашли такой элемент $B \in R^{\psi}\mathcal{H}_k$, что

$$A * B = \left(\prod_{j=1}^{n} \|A\|_{G_j} \right) \cdot \mathbb{Z}^k = \left(\prod_{E \in \mathfrak{B}(A)} \|A\|_E \right) \cdot \mathbb{Z}^k,$$

причём $\mathfrak{B}(B) \subset \mathfrak{B}(A)$. □

Следствие 5.4. *Пусть R — кольцо. Элемент $A \in R^{\psi}\mathcal{H}_k$ обратим в $R^{\psi}\mathcal{H}_k$ тогда и только тогда, когда все коэффициенты Фурье $\|A\|_E$, где $E \in \mathfrak{B}(A)$, обратимы в R.*

Доказательство. 1. Если элемент A обратим в $R^{\psi}\mathcal{H}_k$, то по теореме 5.1 коэффициент Фурье $\|A\|_E$ обратим в R при всех $E \in \mathfrak{B}(A)$.

2. Пусть все коэффициенты Фурье $\|A\|_E$, где $E \in \mathfrak{B}(A)$, обратимы в R, B — элемент, построенный в предыдущей теореме. Тогда

$$A * \left(B \cdot \prod_{j=1}^{n} \|A\|_{G_j}^{-1} \right) = 1$$

и A обратим в кольце $R^{\psi}\mathcal{H}_k$. □

Следствие 5.5. *Пусть P — поле. Тогда в кольце $P^{\psi}\mathcal{H}_k$ любой элемент либо является делителем нуля, либо обратим.*

Доказательство. Это утверждение непосредственно вытекает из теоремы 4.4 и следствия 5.4. □

Следствие 5.6. *Пусть P — поле частных кольца R. Тогда кольцо $P^\psi\mathcal{H}_k$ является кольцом частных кольца $R^\psi\mathcal{H}_k$.*

Доказательство. 1. Если $A \in P^\psi\mathcal{H}_k$, то $s \in R$ — произведение знаменателей всех коэффициентов a_H, $H \in \mathcal{H}_k$, — не является делителем нуля в кольце $R^\psi\mathcal{H}_k$ согласно теореме 4.3. Тогда $C = \sum\limits_{H\in\mathcal{H}_k} s \cdot a_H \cdot H \in R^\psi\mathcal{H}_k$ и $A = \frac{C}{s\cdot\mathbb{Z}^k}$ лежит в кольце частных кольца $R^\psi\mathcal{H}_k$.

2. Пусть $A = \frac{B}{C}$ — элемент кольца частных кольца $R^\psi\mathcal{H}_k$, $B, C \in R^\psi\mathcal{H}_k$, C не является делителем нуля в $R^\psi\mathcal{H}_k$. Тогда C не является делителем нуля и в кольце $P^\psi\mathcal{H}_k$, значит, обратим в $P^\psi\mathcal{H}_k$. Пусть $D \in P^\psi\mathcal{H}_k$ — его обратный, следовательно, $A = B * D \in P^\psi\mathcal{H}_k$. □

Пусть $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{2^k-1}$ — все подгруппы индекса 2 в $\mathbb{Z}^k$, упорядоченные в соответствии с соотношением $\preceq$. Заметим, что

$$(\mathbb{Z}^k - \mathbf{H}_i) * (\mathbb{Z}^k - \mathbf{H}_i) = \mathbb{Z}^k + (2 - 1 - 1) \cdot \mathbf{H}_i = \mathbb{Z}^k$$

при всех $i \in \{1, \ldots, 2^k - 1\}$ и тем самым все элементы $\mathbb{Z}^k - \mathbf{H}_i$ являются обратимыми в $\mathbb{Z}^\psi\mathcal{H}_k$. Для элемента $A \in \mathbb{Z}^\psi\mathcal{H}_k$ положим

$$\hat{A} = \operatorname{sign}(\|A\|_{\mathbb{Z}^k}) * \prod_{i=1}^{2^k-1} (\mathbb{Z}^k - n_i \cdot \mathbf{H}_s) * A,$$

где

$$n_i = \begin{cases} 1, & \operatorname{sign}(\|A\|_{\mathbf{H}_i} \cdot \|A\|_{\mathbb{Z}^k}) = -1, \\ 0 & \text{иначе.} \end{cases}$$

Элемент $\hat{A}$ является произведением обратимых элементов и, следовательно, обратим в $\mathbb{Z}^\psi\mathcal{H}_k$, более того, $\hat{A} * \hat{A} = \mathbb{Z}^k$. У элемента $\tilde{A} = A * \hat{A}$ все коэффициенты Фурье совпадают по модулю с соответствующими коэффициентами Фурье элемента A, причём $\|\tilde{A}\|_{\mathbb{Z}^k} \geqslant 0$, $\|\tilde{A}\|_{\mathbf{H}_i} \geqslant 0$ при всех $i \in \{1, \ldots, 2^k - 1\}$.

Теперь покажем, что верна следующая теорема.

Теорема 5.7. *$\mathbb{Z}^\psi\mathcal{H}_k^*$ — элементарная абелева 2-группа порядка 2^{2^k} с системой образующих*

$$-\mathbb{Z}^k,\ \mathbb{Z}^k - \mathbf{H}_1,\ \mathbb{Z}^k - \mathbf{H}_2, \ldots,\ \mathbb{Z}^k - \mathbf{H}_{2^k-1}.$$

Всего обратимых элементов в $\mathbb{Z}^\psi\mathcal{H}_k$ существует ровно 2^{2^k}.

Доказательство. Если элемент A обратим в $\mathbb{Z}^\psi\mathcal{H}_k$, то по теореме 5.1 все коэффициенты Фурье $\|A\|_H$, где $H \leqslant \mathbb{Z}^k$, равны ± 1. Пусть $\tilde{A} \neq \mathbb{Z}^k$. Выберем в $\operatorname{supp}(\tilde{A} - \mathbb{Z}^k)$ элемент G минимального индекса, тогда $\operatorname{ind} G > 2$, так как $\|\tilde{A}\|_{\mathbb{Z}^k} = \|\tilde{A}\|_{\mathbf{H}_i} = 1$ при всех $i \in \{1, \ldots, 2^k - 1\}$, но

$$|\pm 1| = |\,\|\tilde{A}\|_G| = |1 + \operatorname{ind} G \cdot \tilde{a}_G^{2^k}| \geqslant \operatorname{ind} G - 1 = 2.$$

Противоречие.

Итак, первое утверждение теоремы доказано, а второе следует из того, что разложение обратимого в $\mathbb{Z}^\psi\mathcal{H}_k$ элемента $C \in \mathbb{Z}^\psi\mathcal{H}_k$ в произведение элементов

$$-\mathbb{Z}^k,\ \mathbb{Z}^k - \mathbf{H}_1,\ \mathbb{Z}^k - \mathbf{H}_2, \dots,\ \mathbb{Z}^k - \mathbf{H}_{2^k-1}$$

однозначно задаётся его коэффициентами

$$c_{\mathbb{Z}^k},\ c_{\mathbf{H}_1},\ c_{\mathbf{H}_2}, \dots,\ c_{\mathbf{H}_{2^k-1}}.$$

Теорема доказана. □

6. Идемпотенты

Лёгким следствием предложения 2.7 является следующая теорема.

Теорема 6.1. *Пусть R — полукольцо. Элемент $A \in R^\psi\mathcal{H}_k$ является идемпотентом тогда и только тогда, когда $\|A\|_E$ является идемпотентом в R для любой группы $E \in \mathfrak{B}(A)$.*

Доказательство. 1. Пусть $\|A\|_E = \|A\|_E^2 = \|A^2\|_E$ для любой группы $E \in \mathfrak{B}(A)$, тогда по предложению 2.7 верно, что $A^2 = A$, и A — идемпотент.

2. Пусть элемент $A \in R^\psi\mathcal{H}_k$ является идемпотентом: $A = A^2$. Возьмём любую группу $H \in \mathcal{H}_k$, тогда $\|A\|_H = \|A^2\|_H = \|A\|_H^2$, т. е. коэффициент Фурье $\|A\|_H$ — идемпотент в R, для любой группы $H \in \mathcal{H}_k$. □

Пусть R — кольцо без собственных идемпотентов. Тогда верна следующая теорема.

Теорема 6.2. *Если A, B, $A + B$ — идемпотенты кольца $R^\psi\mathcal{H}_k$, то $A * B = 0$.*

Доказательство. Пусть $H \in \mathcal{H}_k$. Тогда

$$\|A\|_H,\ \|B\|_H,\ \|A + B\|_H = \|A\|_H + \|B\|_H \in \{0, 1\},$$

что возможно либо при $\|A\|_H = 0$, $\|B\|_H = 1$, либо при $\|A\|_H = 1$, $\|B\|_H = 0$. В любом случае $\|A\|_H * \|B\|_H = 0$ при всех $H \in \mathcal{H}_k$, из чего в силу следствия 2.7 получаем, что $A * B = 0$. □

Следствие 6.3. *В $\mathbb{Z}^\psi\mathcal{H}_k$ идемпотентами являются только 0 и $\mathbb{Z}^k$.*

Доказательство. Пусть A — идемпотент в $\mathbb{Z}^\psi\mathcal{H}_k$, $A \neq 0$ и $A \neq \mathbb{Z}^k$. Тогда $\|A\|_{\mathbb{Z}^k}$ есть либо 0, либо 1. Рассмотрим группу $H \in \operatorname{supp} A$, такую что для любой группы $G \in \operatorname{supp} A$ верно $\operatorname{ind} H \leqslant \operatorname{ind} G$. Тогда $\|A\|_H = \operatorname{ind} H \cdot a_H + \|A\|_{\mathbb{Z}^k}$ и уравнения $\|A\|_H = 0$ и $\|A\|_H = 1$ не имеют решений при $\operatorname{ind} H \geqslant 2$ и $a_H \neq 0$. Противоречие. □

Полукольцо $\mathbb{N}^\psi\mathcal{H}_k$ является подполукольцом $\mathbb{Z}^\psi\mathcal{H}_k$ поэтому верно такое следствие.

Следствие 6.4. *В $\mathbb{N}^\psi\mathcal{H}_k$ идемпотентами являются только 0 и $\mathbb{Z}^k$.*

Доказательство. Если A — идемпотент в $\mathbb{N}^\psi\mathcal{H}_k$, то A — идемпотент и в $\mathbb{Z}^\psi\mathcal{H}_k$, т. е. либо $A = 0$, либо $A = \mathbb{Z}^k$. □

Пусть P — поле. В кольце $R^{\psi}\mathcal{H}_k$ идемпотентов существует бесконечно много, однако каждый из них лежит в кольце $R^{\psi}\mathcal{S}$ при некоторой конечной подгруппе $\mathcal{S} < \mathcal{H}_k$, причём верна следующая теорема.

Теорема 6.5. *В кольце $P^{\psi}\mathcal{S}$ существует ровно $2^{|\mathcal{S}|}$ идемпотентов.*

Доказательство. Если A — идемпотент в $P^{\psi}\mathcal{S}$, то для любой группы $E \in \mathcal{S}$ число $\|A\|_E$ — идемпотент в P, т. е. либо 0, либо 1. С другой стороны, по предложению 2.8 для любого столбца

$$N = \begin{pmatrix} n_1 & \dots & n_{|\mathcal{S}|} \end{pmatrix}^{\top} \in P^{|\mathcal{S}|}, \quad n_i \in \{0, 1\},$$

существует единственный элемент $A \in P^{\psi}\mathcal{S}$, такой что $N = \mathcal{N}_{\mathcal{S}}(A)$. Всего таких столбцов $2^{|\mathcal{S}|}$, следовательно, идемпотентных элементов в $P^{\psi}\mathcal{S}$ тоже $2^{|\mathcal{S}|}$. □

Приведём пример идемпотента C в $\mathbb{Z}^{\psi}\mathcal{H}_k$, у которого коэффициент $c_{\mathcal{K}(C)}$ равен нулю.

Пример 6.6. Пусть $k \geqslant 3$, F, G, H — группы индекса 2 в $\mathbb{Z}^k$, порождаемые соответственно тождествами $x_i \equiv 0 \pmod 2$, $i \in \{1, 2, 3\}$. Тогда группы FG, GH, HF попарно различны. Положим

$$C = (\mathbb{Z}^k - F) * (\mathbb{Z}^k - G) * (\mathbb{Z}^k - H) + FGH = \mathbb{Z}^k - F - G - H + FG + GH + HF.$$

Заметим, что $\mathfrak{B}(C) = \{\mathbb{Z}^k, F, G, H, FG, GH, HF, FGH\}$. Имеем $\|C\|_{\mathbb{Z}^k} = 1$, $\|C\|_F = -1$, $\|C\|_G = -1$, $\|C\|_H = -1$, $\|C\|_{FG} = 1$, $\|C\|_{GH} = 1$, $\|C\|_{HF} = 1$, $\|C\|_{FGH} = 0$, и по теореме 6.1 C является идемпотентом в $\mathbb{Z}^{\psi}\mathcal{H}_k$.

7. Радикал Джекобсона

Для коммутативного кольца R с единицей e радикал Джекобсона $\mathcal{J}(R)$, или квазирегулярный радикал, является пересечением всех максимальных идеалов и совпадает с наибольшим квазирегулярным идеалом [1, гл. I, § 6]. Радикал Джекобсона $\mathcal{J}(R)$ коммутативного кольца R с единицей e состоит из всех элементов $j \in R$, таких что элемент $e - jr$ обратим при всех $r \in R$ [1, гл. I, § 6].

Теорема 7.1. *Радикал Джекобсона в $\mathbb{Z}^{\psi}\mathcal{H}_k$ нулевой.*

Доказательство. Пусть $A \in \mathcal{J}(\mathbb{Z}^{\psi}\mathcal{H}_k)\backslash\{0\}$. Тогда элемент $\mathbb{Z}^k - A * B$ обратим для любого элемента $B \in \mathbb{Z}^{\psi}\mathcal{H}_k$. Поэтому

$$\|\mathbb{Z}^k - A * B\|_H = 1 - \|A\|_H \cdot \|B\|_H = \pm 1 \tag{7.1}$$

для любой группы $H \in \mathcal{H}_k$. Так как $A \neq 0$, то существует группа $G \in \mathcal{H}_k$, такая что $\|A\|_G \neq 0$. Возьмём $B = 3 \cdot \mathbb{Z}^k$. Тогда из условия (7.1) следует равенство $3 \cdot \|A\|_G = 1 \pm 1$, которое невозможно. Итак, $\mathcal{J}(\mathbb{Z}^{\psi}\mathcal{H}_k) = 0$. □

Теорема 7.2. *Пусть P — поле. Тогда радикал Джекобсона в $P^{\psi}\mathcal{H}_k$ нулевой.*

Доказательство. Пусть $A \in \mathcal{J}(P^{\psi}\mathcal{H}_k) \setminus \{0\}$. Тогда элемент $\mathbb{Z}^k - A * B$ обратим для любого элемента $B \in P^{\psi}\mathcal{H}_k$. Поэтому $\|\mathbb{Z}^k - A * B\|_H \neq 0$ для любой группы $H \in \mathcal{H}_k$. Так как $A \neq 0$, то существует группа $G \in \mathcal{H}_k$, такая что $\|A\|_G \neq 0$. Возьмём $B = \frac{1}{\|A\|_G} \cdot \mathbb{Z}^k$. Тогда получим

$$\|\mathbb{Z}^k - A * B\|_G = 1 - \|A\|_G \cdot \|B\|_G = 1 - \|A\|_G \cdot \frac{1}{\|A\|_G} = 0.$$

Противоречие. Итак, $\mathcal{J}(P^{\psi}\mathcal{H}_k) = 0$. □

Литература

[1] Джекобсон Н. Строение колец. — М.: ИЛ, 1961.

[2] Kuzmin A. S., Kurakin V. L., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. — 1995. — Vol. 76, no. 6. — P. 2793—2915.