Some algorithmic questions of factorization of automorphisms of integer group rings

A. M. Popova, O. V. Bryukhanov

Novosibirsk, Russia

14^{th} International Summer School-Conference
"Problems Allied to Universal Algebra and Model Theory"
in occasion of 75^{th} Birhtday of
Professor Bruno Poizat
Novosibirsk, 25.06.2021

Цассенхаузом была выдвинута

Гипотеза (о факторизации автоморфизмов)

Для любого нормализованного автоморфизма $\theta \in \mathrm{Aut}\mathbb{Z}G$ *существует единица* $s \in \mathbb{Q}G$ *и групповой автоморфизм* $\sigma \in \mathrm{Aut}\,G$ *такие, что* $\theta(g) = s^{-1}\sigma(g)s$, *для любого* $g \in G$.

Цассенхаузом была выдвинута

Гипотеза (о факторизации автоморфизмов)

Для любого нормализованного автоморфизма $\theta \in \mathrm{Aut}\mathbb{Z}G$ *существует единица* $s \in \mathbb{Q}G$ *и групповой автоморфизм* $\sigma \in \mathrm{Aut}\,G$ *такие, что* $\theta(g) = s^{-1}\sigma(g)s$, *для любого* $g \in G$.

Другими словами, определена *факторизация* нормализованного автоморфизма $\theta = \sigma \circ \varphi_s$, где $\sigma \in \mathrm{Aut}\,G$ и φ_s — сопряжение единицей s алгебры $\mathbb{Q}G$

Цассенхаузом была выдвинута

Гипотеза (о факторизации автоморфизмов)

Для любого нормализованного автоморфизма $\theta \in \mathrm{Aut}\mathbb{Z}G$ *существует единица* $s \in \mathbb{Q}G$ *и групповой автоморфизм* $\sigma \in \mathrm{Aut}\,G$ *такие, что* $\theta(g) = s^{-1}\sigma(g)s$, *для любого* $g \in G$.

Другими словами, определена *факторизация* нормализованного автоморфизма $\theta = \sigma \circ \varphi_s$, где $\sigma \in \mathrm{Aut}\,G$ и φ_s — сопряжение единицей s алгебры $\mathbb{Q}G$

Как известно, гипотеза Цассенхауза о факторизации автоморфизмов целочисленных групповых колец не подтвердилась. Известны контрпримеры Хертвика, Роггенкампа и Клинглера.

Мы предложили другую факторизацию, основанную на теории представлений конечных групп.
Пусть $G = \{e, g_2, ..., g_n\}$ — конечная группа, $T_1(G)$,...,$T_s(G)$ — все ее неприводимые неэквивалентные представления степеней $n_1, ..., n_s$.

$$D(G) = \{\mathrm{diag}(T_1(g), ..., T_s(g)), g \in G\}$$

Очевидно, что $\mathbb{Z}G \cong \mathbb{Z}[D(G)]$. Условимся кольца $\mathbb{Z}[T_i(G)]$ называть *клетками* кольца $\mathbb{Z}[D(G)]$.

Мы предложили другую факторизацию, основанную на теории представлений конечных групп.
Пусть $G = \{e, g_2, ..., g_n\}$ — конечная группа, $T_1(G),...,T_s(G)$ — все ее неприводимые неэквивалентные представления степеней $n_1, ..., n_s$.

$$D(G) = \{\mathrm{diag}(T_1(g), ..., T_s(g)), g \in G\}$$

Очевидно, что $\mathbb{Z}G \cong \mathbb{Z}[D(G)]$. Условимся кольца $\mathbb{Z}[T_i(G)]$ называть *клетками* кольца $\mathbb{Z}[D(G)]$.
Рассмотрим отображения

$$\mu_{ij} : \sum \alpha_g T_i(g) \to \sum \alpha_g T_j(g), \alpha_g \in \mathbb{Z}$$

которые либо являются изоморфизмами, либо не являются.

Мы предложили другую факторизацию, основанную на теории представлений конечных групп.
Пусть $G = \{e, g_2, ..., g_n\}$ — конечная группа, $T_1(G)$,..., $T_s(G)$ — все ее неприводимые неэквивалентные представления степеней $n_1, ..., n_s$.

$$D(G) = \{\mathrm{diag}(T_1(g), ..., T_s(g)), g \in G\}$$

Очевидно, что $\mathbb{Z}G \cong \mathbb{Z}[D(G)]$. Условимся кольца $\mathbb{Z}[T_i(G)]$ называть *клетками* кольца $\mathbb{Z}[D(G)]$.
Рассмотрим отображения

$$\mu_{ij} : \sum \alpha_g T_i(g) \to \sum \alpha_g T_j(g), \alpha_g \in \mathbb{Z}$$

которые либо являются изоморфизмами, либо не являются.
Если клетки $\mathbb{Z}[T_p(G)]$,..., $\mathbb{Z}[T_{p+k-1}(G)]$, $k \geq 2$, μ_{ij} -изоморфны, то обозначим

$$D_p(G) = \{\mathrm{diag}(T_p(g), ..., T_{p+k-1}(g)), g \in G\}$$

и кольцо $O_p = \mathbb{Z}[D_p(G)]$ назовем *блоком*.

Таким образом, все кольцо $\mathbb{Z}[D(G)]$ разбивается на блоки, точнее $\mathbb{Z}[D(G)] \leq O_{p_1} \oplus \cdots \oplus O_{p_r}$, где $\mathbb{Q}$-алгебры $\mathbb{Q}[O_p]$ являются простыми.

Таким образом, все кольцо $\mathbb{Z}[D(G)]$ разбивается на блоки, точнее $\mathbb{Z}[D(G)] \leq O_{p_1} \oplus \cdots \oplus O_{p_r}$, где $\mathbb{Q}$-алгебры $\mathbb{Q}[O_p]$ являются простыми. Если автоморфизм φ кольца $\mathbb{Z}[D(G)]$ все блоки оставляет на месте, назовем его *стабилизирующим*, в противном случае — *переставляющим*.

Таким образом, все кольцо $\mathbb{Z}[D(G)]$ разбивается на блоки, точнее $\mathbb{Z}[D(G)] \leq O_{p_1} \oplus \cdots \oplus O_{p_r}$, где $\mathbb{Q}$-алгебры $\mathbb{Q}[O_p]$ являются простыми. Если автоморфизм φ кольца $\mathbb{Z}[D(G)]$ все блоки оставляет на месте, назовем его *стабилизирующим*, в противном случае — *переставляющим*.

Заметим, что если $K = \mathbb{Q}(\xi)$ — конечное алгебраическое расширение, то любой автоморфизм $\tau \in \mathrm{Aut} K$ индуцирует изоморфизм $\hat{\tau}$ кольца матриц над K :

$$\hat{\tau}((a_{ij})) = (a_{ij}^{\tau}).$$

Таким образом, все кольцо $\mathbb{Z}[D(G)]$ разбивается на блоки, точнее $\mathbb{Z}[D(G)] \leq O_{p_1} \oplus \cdots \oplus O_{p_r}$, где $\mathbb{Q}$-алгебры $\mathbb{Q}[O_p]$ являются простыми. Если автоморфизм φ кольца $\mathbb{Z}[D(G)]$ все блоки оставляет на месте, назовем его *стабилизирующим*, в противном случае — *переставляющим*.

Заметим, что если $K = \mathbb{Q}(\xi)$ — конечное алгебраическое расширение, то любой автоморфизм $\tau \in \mathrm{Aut}K$ индуцирует изоморфизм $\hat{\tau}$ кольца матриц над K :

$$\hat{\tau}((a_{ij})) = (a_{ij}^{\tau}).$$

Справедлива следующая

Теорема.

Любой нормализованный автоморфизм кольца $\mathbb{Z}[D(G)]$ есть композиция $\varphi \circ \hat{\tau} \circ \varphi_s$, где φ — некоторый переставляющий автомофизм из выделенного конечного набора Φ, τ — автоморфизм поля представления группы G, φ_s — сопряжение единицей s алгебры $\mathbb{Q}[D(G)]$.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$. Если χ_i — целочисленный, то блок состоит из одной клетки $\mathbb{Z}[T_i(G)]$.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$. Если χ_i — целочисленный, то блок состоит из одной клетки $\mathbb{Z}[T_i(G)]$.Если χ_i содержит алгебраические числа, то блок состоит из k клеток, где $k = |\mathrm{Aut}\mathbb{Q}(\chi_i)|$.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$. Если χ_i — целочисленный, то блок состоит из одной клетки $\mathbb{Z}[T_i(G)]$.Если χ_i содержит алгебраические числа, то блок состоит из k клеток, где $k = |\mathrm{Aut}\mathbb{Q}(\chi_i)|$.
Пусть $\mathrm{Aut}\mathbb{Q}(\chi_i) = \{\tau_1 = \mathrm{id}, \tau_2, ..., \tau_k\}$. Тогда характерами клеток такого блока являются χ_i, $\tau_2(\chi_i)$,...,$\tau_k(\chi_i)$. Соответственно, клетками блока являются клетки $\mathbb{Z}[T_i(G)]$, $\mathbb{Z}[\hat{\tau}_2(T_i(G))]$,...,$\mathbb{Z}[\hat{\tau}_k(T_i(G))]$, то есть любая матрица блока определяется своей первой клеткой, а характер блока $\chi_i + \tau_2(\chi_i) + \cdots + \tau_k(\chi_i)$ является целочисленным.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$. Если χ_i — целочисленный, то блок состоит из одной клетки $\mathbb{Z}[T_i(G)]$.Если χ_i содержит алгебраические числа, то блок состоит из k клеток, где $k = |\mathrm{Aut}\mathbb{Q}(\chi_i)|$.
Пусть $\mathrm{Aut}\mathbb{Q}(\chi_i) = \{\tau_1 = \mathrm{id}, \tau_2, ..., \tau_k\}$. Тогда характерами клеток такого блока являются χ_i, $\tau_2(\chi_i)$,...,$\tau_k(\chi_i)$. Соответственно, клетками блока являются клетки $\mathbb{Z}[T_i(G)]$, $\mathbb{Z}[\hat{\tau}_2(T_i(G))]$,...,$\mathbb{Z}[\hat{\tau}_k(T_i(G))]$, то есть любая матрица блока определяется своей первой клеткой, а характер блока $\chi_i + \tau_2(\chi_i) + \cdots + \tau_k(\chi_i)$ является целочисленным.
Сужение любого стабилизирующего автоморфизма на таком блоке есть композиция $\hat{\tau}_j \circ \varphi_s$, $j = 1, ..., k$.

Разбиение кольца $\mathbb{Z}[D(G)]$ на блоки определяется характерами χ_i представлений $T_i(G)$. Если χ_i — целочисленный, то блок состоит из одной клетки $\mathbb{Z}[T_i(G)]$.Если χ_i содержит алгебраические числа, то блок состоит из k клеток, где $k = |\mathrm{Aut}\mathbb{Q}(\chi_i)|$.
Пусть $\mathrm{Aut}\mathbb{Q}(\chi_i) = \{\tau_1 = \mathrm{id}, \tau_2, ..., \tau_k\}$. Тогда характерами клеток такого блока являются χ_i, $\tau_2(\chi_i)$,...,$\tau_k(\chi_i)$. Соответственно, клетками блока являются клетки $\mathbb{Z}[T_i(G)]$, $\mathbb{Z}[\hat{\tau}_2(T_i(G))]$,...,$\mathbb{Z}[\hat{\tau}_k(T_i(G))]$, то есть любая матрица блока определяется своей первой клеткой, а характер блока $\chi_i + \tau_2(\chi_i) + \cdots + \tau_k(\chi_i)$ является целочисленным.
Сужение любого стабилизирующего автоморфизма на таком блоке есть композиция $\hat{\tau}_j \circ \varphi_s$, $j = 1, ..., k$.
Возникает естественный

Вопрос

Для любого ли автоморфизма $\tau_j \in \mathrm{Aut}\mathbb{Q}(\chi_i)$, $j = 1, ..., k$, найдется единица s алгебры $\mathbb{Q}[T_i(G)]$ такая, что композиция $\hat{\tau}_j \circ \varphi_s$ является автоморфизмом блока?

По поводу этого вопроса заметим следующее. В таблице характеров группы Матье M_{11} есть алгебраические числа, но $\mathrm{Out} M_{11} = 1$.

По поводу этого вопроса заметим следующее. В таблице характеров группы Матье M_{11} есть алгебраические числа, но $\mathrm{Out}\, M_{11} = 1$. Значит, если автоморфизм поля характера "*продолжается*" до автомофизма целочисленного группового кольца этой группы с помощью сопряжения, то она служит контрпримером к гипотезе Цассенхауза.

По поводу этого вопроса заметим следующее. В таблице характеров группы Матье M_{11} есть алгебраические числа, но $\mathrm{Out}\, M_{11} = 1$. Значит, если автоморфизм поля характера "*продолжается*" до автомофизма целочисленного группового кольца этой группы с помощью сопряжения, то она служит контрпримером к гипотезе Цассенхауза.

Дело в том, что по гипотезе Цассенхауза любой нормалиэованный автоморфизм целочисленного группового кольца есть композиция автоморфизма группы и сопряжения единицей групповой алгебры. Но автоморфизм, индуцированный автоморфизмом поля характера, переставляет классы сопряженных элементов группы. Значит, в случае $\mathrm{Out}\, G = 1$ не может реализоваться автоморфизмом группы.

Цель нашей работы — *описать алгоритм, отвечающий на этот вопрос.*

Цель нашей работы — *описать алгоритм, отвечающий на этот вопрос.*

1. Считаем, что индекс Шура равен 1, то есть поле представления блока совпадает с полем характера. Пусть $\mathbb{Z}[T_p(G)]$ — первая клетка блока, χ_p — характер первой клетки блока, n_p —степень представления $T_p(G)$, $\mathbb{Q}(\chi_p)$ —поле характера, $|\mathbb{Q}(\chi_p) : \mathbb{Q}| = k$, $\{\omega\} = \{\omega_1 = 1, \omega_2, ..., \omega_k\}$ — фундаментальный базис расширения $\mathbb{Q}(\chi_p) : \mathbb{Q}$, то есть любое целое алгебраическое число поля $\mathbb{Q}(\chi_p)$ есть целочисленная линейная комбинация элементов $\{\omega\}$.

Цель нашей работы — *описать алгоритм, отвечающий на этот вопрос.*

1. Считаем, что индекс Шура равен 1, то есть поле представления блока совпадает с полем характера. Пусть $\mathbb{Z}[T_p(G)]$ — первая клетка блока, χ_p — характер первой клетки блока, n_p —степень представления $T_p(G)$, $\mathbb{Q}(\chi_p)$ —поле характера, $|\mathbb{Q}(\chi_p) : \mathbb{Q}| = k$, $\{\omega\} = \{\omega_1 = 1, \omega_2, ..., \omega_k\}$ — фундаментальный базис расширения $\mathbb{Q}(\chi_p) : \mathbb{Q}$, то есть любое целое алгебраическое число поля $\mathbb{Q}(\chi_p)$ есть целочисленная линейная комбинация элементов $\{\omega\}$.

2. Пусть K — кольцо целых алгебраических чисел поля $\mathbb{Q}(\chi_p)$. Элементы сопрягающей матрицы можем считать целыми. Можно показать, что если s — сопрягающая матрица, то $|s| = \varepsilon$, где ε — единица K.

3. Пусть m — наименьшее натуральное число такое, что для всех $1 \leq i, j \leq n_p$, $q = 1, \ldots, k$ $m\omega_q e_{ij} \in \mathbb{Z}[T_p(G)]$,
$I_m = I(m\omega_q e_{ij}, 1 \leq i, j \leq n_p, q = 1, \ldots, k)$.

3. Пусть m — наименьшее натуральное число такое, что для всех $1 \leq i, j \leq n_p$, $q = 1, ..., k$ $m\omega_q e_{ij} \in \mathbb{Z}[T_p(G)]$, $I_m = I(m\omega_q e_{ij}, 1 \leq i, j \leq n_p, q = 1, ..., k)$.

4. Нетрудно доказать, что для любого $\tau \in \mathrm{Aut}\mathbb{Q}(\chi_p)$, $\hat{\tau}(I_m) = I_m$. Этот факт и позволяет свести алгоритм к конечному перебору

3. Пусть m — наименьшее натуральное число такое, что для всех $1 \le i, j \le n_p$, $q = 1, ..., k$ $m\omega_q e_{ij} \in \mathbb{Z}[T_p(G)]$, $I_m = I(m\omega_q e_{ij}, 1 \le i, j \le n_p, q = 1, ..., k)$.

4. Нетрудно доказать, что для любого $\tau \in \mathrm{Aut}\mathbb{Q}(\chi_p)$, $\hat{\tau}(I_m) = I_m$. Этот факт и позволяет свести алгоритм к конечному перебору

5.Ищем сопрягающую матрицу s в виде $s = s_1 + ms_2$, где коэффициенты элементов s_1 в разложении по базису $\{\omega\}$ по модулю меньше m.

6. Сопрягающая матрица s существует тогда и только тогда, когда для s_1 выполняются следующие условия:
1) $|s_1| = \varepsilon + m\alpha$, ε — единица K, $\alpha \in K$;
2) для любого $g \in \mathbb{Z}[T_p(G)]$, $g \notin I_m$ найдется $h \in \mathbb{Z}[T_p(G)]$, $h \notin I_m$ такой, что выполняется сравнение $\hat{\tau}(g)s_1 \equiv s_1 h \pmod{m}$;
3) для s_1 найдется s_2 такая, что $|s_1 + ms_2| = \varepsilon$.

6. Сопрягающая матрица s существует тогда и только тогда, когда для s_1 выполняются следующие условия:
1) $|s_1| = \varepsilon + m\alpha$, ε — единица K, $\alpha \in K$;
2) для любого $g \in \mathbb{Z}[T_p(G)]$, $g \notin I_m$ найдется $h \in \mathbb{Z}[T_p(G)]$, $h \notin I_m$ такой, что выполняется сравнение $\hat{\tau}(g)s_1 \equiv s_1 h \pmod{m}$;
3) для s_1 найдется s_2 такая, что $|s_1 + ms_2| = \varepsilon$.

Алгоритм сводится к перебору всех s_1 и проверке для каждой s_1 условий 1) – 3).

Literature

[1] **А. М. Ивлева, О. В. Брюханов, Е. В. Грачев**, *Единицы целочисленных групповых колец: монография*, (Russian) Новосибирск: Изд-во НГТУ, 2018. – 190 с.

[2] **A. M. Ivleva, O. V. Bryukhanov, E. V. Grachev**, *Units of Integral Group Rings: monograph*, (Russian) Novosibirsk:NSTU Publisher, 2018. –190 pp. ("NSTU Monographs" series).

[3] **O. V. Bryukhanov**, www.researchgate.net in [Your profile] *Units of Integral Group Rings*, .

THANK YOU!