

К-14038

П 249455

К-14038

МИНИСТЕРСТВО
ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ УССР

ВЕСТНИК ХАРЬКОВСКОГО УНИВЕРСИТЕТА

№ 26

СЕРИЯ МЕХАНИКО-МАТЕМАТИЧЕСКАЯ

**ЗАПИСКИ
МЕХАНИКО-МАТЕМАТИЧЕСКОГО
ФАКУЛЬТЕТА И ХАРЬКОВСКОГО
МАТЕМАТИЧЕСКОГО ОБЩЕСТВА**

ТОМ 33

ИЗДАТЕЛЬСТВО ХАРЬКОВСКОГО УНИВЕРСИТЕТА

Цена 68 коп.

V.N. Karazin Kharkiv National University



00195811

5

МИНИСТЕРСТВО
ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ УССР

ВЕСТНИК ХАРЬКОВСКОГО УНИВЕРСИТЕТА

№ 26

СЕРИЯ МЕХАНИКО-МАТЕМАТИЧЕСКАЯ

ЗАПИСКИ
МЕХАНИКО-МАТЕМАТИЧЕСКОГО
ФАКУЛЬТЕТА И ХАРЬКОВСКОГО
МАТЕМАТИЧЕСКОГО ОБЩЕСТВА

ТОМ 33

к-14038



ИЗДАТЕЛЬСТВО
ХАРЬКОВСКОГО ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА имени А. М. ГОРЬКОГО
Харьков

1967

СОДЕРЖАНИЕ

	Стр.
Э. М. Жмудь. Об изоморфизмах структуры нормальных делителей конечной нильпотентной группы	3
Э. М. Жмудь. Верхние и нижние дополнения в конечных модулярных структурах и теория линейных представлений конечных групп	8
Э. М. Жмудь. О конечных группах, обладающих единственным минимальным нормальным делителем и единственным классом изоморфных неприводимых представлений	16
Э. М. Жмудь, Г. К. Куренной. О конечных группах единиц целочисленного группового кольца	20
Л. Н. Пронин. О целочисленных бинарных эрмитовых формах над телом кватернионов	27
Л. В. Потемкин. О разложении полугрупповых колец в прямые суммы идеалов	42
А. М. Калманович. Полугруппа взаимно-однозначных частичных эндоморфизмов графа	54
В. Д. Головин. О некоторых модулях над кольцом ограниченных функций	65
В. С. Гринберг. Асимптотические оценки мощностей классов для одной классификации конечных графов	78
М. А. Перельман. Локальная асимптотическая формула для полиномов, ортогональных на дуге окружности	83
Г. В. Щербина. Краевая задача на полуоси для нелинейного дифференциального уравнения второго порядка	94
А. Г. Боев. О преобразовании Крокко в теории пограничного слоя	103
А. Г. Боев. Пограничное течение вязкого сжимаемого газа на полубесконечной пластине с учетом влияния ведущего края	109
Ю. В. Гандель. Об одной паре сумматорных уравнений с функциями Бесселя	115
А. А. Янцевич. Распространение электромагнитных волн в пуазейдовском потоке вязкой несжимаемой жидкости	120
Ж. С. Ажажа, А. А. Янцевич. Двойное лучепреломление в турбулентных потоках вязкой несжимаемой жидкости	125

Редакционная коллегия:

проф. Н. И. Ахиезер (ответственный редактор),
проф. В. А. Марченко, проф. А. В. Погорелов.

Редактор Л. Ф. Кизилова
Техредактор Г. П. Александрова
Корректоры З. И. Иванова, А. П. Гужва

Сдано в набор 12/VII 1967 г. Подписано к печати 27/XII 1967 г. БЦ 50623.
Формат 70×108¹/₁₆. Объем 8,25 физ. печ. л., 11,6 усл. печ. л. 10,2 уч.-изд. л. Зак. 7-452.
Тираж 500. Цена 68 коп..

Отпечатано с матриц Книжной ф-ки им. Фрунзе в Тип. № 16 Обл. Управления по печати. Харьков, 3, Университетская, 16. Зак. 568.

ОБ ИЗОМОРФИЗМАХ СТРУКТУРЫ НОРМАЛЬНЫХ ДЕЛИТЕЛЕЙ КОНЕЧНОЙ НИЛЬПОТЕНТНОЙ ГРУППЫ

Э. М. Жмудь

В настоящей работе рассматривается некоторый подкласс класса конечных нильпотентных групп и доказывается, что всякая конечная группа $\bar{G}$, структура нормальных делителей которой изоморфна структуре нормальных делителей некоторой группы G этого подкласса, также принадлежит последнему. Если, в частности, группа G абелева, то $\bar{G} \cong G$.

Все группы, рассматриваемые в дальнейшем, конечные.

Определение 1. LN -изоморфизмом группы G на группу $\bar{G}$ называется изоморфизм структуры $L_N(G)$ нормальных делителей группы G на структуру $L_N(\bar{G})$ нормальных делителей группы $\bar{G}$. Группы G и $\bar{G}$, имеющие изоморфные структуры $L_N(G)$ и $L_N(\bar{G})$, называются LN -изоморфными.

Если σ — LN -изоморфизм группы G на группу $\bar{G}$ и $H \triangleleft G$, то H^σ обозначает образ подгруппы H при отображении σ .

Определение 2. LN -изоморфизм σ группы G на группу $\bar{G}$ называется сильным, если $|H^\sigma| = |H|$ для каждого $H \triangleleft G$.

Определение 3. Абелева группа называется ациклической, если она не имеет циклических силовских подгрупп.

Определение 4. Центральный ряд нильпотентной группы называется ациклическим, если все его факторы ациклически.

Определение 5. Нильпотентная группа называется ациклической, если она имеет хотя бы один ациклический центральный ряд.

Целью настоящей статьи является доказательство следующих двух утверждений.

Теорема 1. Если группа $\bar{G}$ LN -изоморфна ациклической* абелевой группе G , то $\bar{G} \cong G$.

Теорема 2. Если группа $\bar{G}$ LN -изоморфна ациклической нильпотентной группе G , то группа $\bar{G}$ также нильпотентна. Всякий LN -изоморфизм нильпотентной группы G на группу $\bar{G}$ является сильным.

При доказательстве теорем 1 и 2 используются некоторые свойства так называемых когерент Ремака конечной группы.

Конечную группу G можно естественным образом рассматривать в качестве области операторов каждого ее нормального делителя N : если $x \in N$, $g \in G$, то $g \circ x = gxg^{-1}$. В этом смысле нормальные делители группы G являются G -группами. В частности, цокль $S_c(G)$ группы G является вполне приводимой G -группой. Однородные компоненты цокля называются когерентами [1] группы G : каждая когерента группы G является композитом всех минимальных нормальных делителей группы G G -изо-

* Условие ациклическости группы G является существенным. Действительно, циклическая группа G простого порядка, очевидно LN -изоморфна любой простой группе $\bar{G}$, между тем как, вообще говоря, $\bar{G} \not\cong G$.

морфных некоторому фиксированному ее минимальному нормальному делителю. Когерента K разлагается в прямое произведение некоторого числа n минимальных нормальных делителей группы G , которое мы будем называть G -рангом когеренты K .

Когеренту будем называть *существенной*, если ее G -ранг > 1 , т. е. если она не является минимальным нормальным делителем группы G . Существенные когеренты являются, как можно показать [1, 2, 3], элементарными абелевыми группами. Следовательно, они примарны.

Имеет место следующее утверждение*:

Лемма 1. Образ K^σ когеренты K группы G при LN -изоморфизме σ последней на группу $\bar{G}$ является когерентой группы $\bar{G}$. Если K — существенная когерента порядка p^x (p — простое число), то K является p -группой.

Пусть G — конечная абелева группа. Подгруппу I группы G будем называть *ядром* последней, если факторгруппа G/I циклическа**.

Если I — ядро группы G , то всякая подгруппа, содержащая I , также, очевидно, является ядром. Ядро I группы G назовем *минимальным*, если его собственные подгруппы уже не являются ядрами.

Лемма 2. Если $\{I_\alpha\}_{1 \leq \alpha \leq k}$ — полная система минимальных ядер нециклической абелевой p -группы G , то

$$I_1 \cdot I_2 \cdot \dots \cdot I_k = G.$$

Доказательство. Пусть $I_1 \cdot \dots \cdot I_k = H$. Так как G/I_α — циклическая p -группа, то I_α содержится в одной и только одной максимальной подгруппе M_α группы G . (Очевидно, возможен случай, когда $\alpha \neq \beta$ и $M_\alpha = M_\beta$). Каждая максимальная подгруппа группы G является, очевидно, ядром и, следовательно, содержит некоторое минимальное ядро. Поэтому в системе $\{M_\alpha\}_{1 \leq \alpha \leq k}$ содержатся все максимальные подгруппы группы G .

Если бы оказалось, что $H \neq G$, то нашлась бы максимальная подгруппа M_α , содержащая H . Но тогда $M_\alpha \supset I_\beta$ для всех $\beta = 1, \dots, k$. Так как ядро I_β содержится только в одной максимальной подгруппе, то отсюда вытекает, что $M_1 = \dots = M_k$. Таким образом, группа G имела бы только одну максимальную подгруппу и, следовательно, была бы циклической, что противоречит предположению. Таким образом, $H = G$ и лемма доказана.

Лемма 3. Пусть σ LN -изоморфизм конечной абелевой p -группы G на группу $\bar{G}$ и пусть H — подгруппа группы G , не являющаяся ее ядром. Тогда цоколь группы $\bar{G}/H^\sigma$ является p -группой.

Доказательство. Отображение σ естественным образом индуцирует LN -изоморфизм σ^* группы $\bar{G}^* = \bar{G}/H$ на группу $\bar{G}^* = \bar{G}/H^\sigma$. Так как G^* — p -группа, то ее цоколь $Sc(G^*)$ является когерентой, а так как группа G^* не является циклической, то $Sc(G^*)$ — существенная когерента. В силу леммы 1 цоколь $Sc(\bar{G}^*) = [Sc(G^*)]^\sigma$ группы $\bar{G}^*$ есть когерента последней и является p -группой.

Лемма 4. Пусть σ — LN -изоморфизм конечной абелевой p -группы G на конечную группу $\bar{G}$; I — минимальное ядро группы G . Тогда I^σ есть p -группа.

Доказательство. Построим для I композиционный ряд:

$$I = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_l = \{1\}. \quad (1)$$

* Доказательство см. в [2] (теоремы 2.1 и 2.2).

** В общем случае произвольной конечной группы под ядрами последней мы понимаем ядра гомоморфизмов ее неприводимых комплексных представлений.

Тогда

$$I^\sigma = H_0^\sigma \supset H_1^\sigma \supset H_2^\sigma \supset \dots \supset H_l^\sigma = \{\bar{1}\}^* \quad (2)$$

— отрезок главного ряда группы $\bar{G}$. Так как (в силу минимальности ядра I) подгруппа H_α ($\alpha \geq 1$) не является ядром группы G , то на основании леммы 3 цоколь группы G/H_α^σ есть p -группа.

Отсюда следует, так как $H_{\alpha-1}^\sigma/H_\alpha^\sigma \subset Sc(\bar{G}/H_\alpha^\sigma)$, что $H_{\alpha-1}^\sigma/H_\alpha^\sigma$ — p -группа. Таким образом, все факторы ряда (2) являются p -группами. Следовательно, и I^σ — p -группа.

Лемма 5. *Всякий LN-изоморфизм конечной p -группы G на конечную p -группу $\bar{G}$ является сильным LN-изоморфизмом.*

Доказательство. Пусть $H \triangleleft G$. Проведем через H главный ряд группы G :

$$\{1\} = N_0 \subset N_1 \subset \dots \subset N_k = H \subset N_{k+1} \subset \dots \subset N_r = G, \quad (3)$$

LN-изоморфизм σ группы G на $\bar{G}$ переводит ряд (3) в главный ряд

$$\{\bar{1}\} = N_0^\sigma \subset N_1^\sigma \subset \dots \subset N_k^\sigma = H^\sigma \subset N_{k+1}^\sigma \subset \dots \subset N_r^\sigma = \bar{G}$$

группы $\bar{G}$. Так как G и $\bar{G}$ p -группы, то $|N_i/N_{i-1}| = |N_i^\sigma/N_{i-1}^\sigma| = p$ ($1 \leq i \leq r$). Следовательно, $|N_i| = |N_i^\sigma| = p^i$ и, в частности, $|H| = |H^\sigma|$. Лемма доказана.

Доказательство теоремы 1. Пусть σ — LN-изоморфизм конечной ациклической абелевой группы G на конечную группу $\bar{G}$.

Рассмотрим сначала случай, когда G является p -группой. Если $\{I_\alpha\}_{1 \leq \alpha \leq k}$ — полная система минимальных ядер группы G , то в силу леммы 4 $I_1^\sigma, \dots, I_k^\sigma$ — инвариантные p -подгруппы группы $\bar{G}$. Поэтому $I_1^\sigma \dots I_k^\sigma$ также является инвариантной p -подгруппой группы $\bar{G}$. Так как в силу леммы 2 $I_1^\sigma \dots I_k^\sigma = (I_1 \dots I_k)^\sigma = G^\sigma = \bar{G}$, то $\bar{G}$ — p -группа.

Пусть

$$G = L_1 \times \dots \times L_s \quad (4)$$

— разложение группы G в прямое произведение циклических подгрупп. Тогда, очевидно,

$$\bar{G} = L_1^\sigma \times \dots \times L_s^\sigma. \quad (5)$$

Так как L_i имеет только одну максимальную подгруппу, то L_i^σ покрывает только один нормальный делитель группы $\bar{G}$. Но в силу (5) каждый нормальный делитель подгруппы L_i^σ является вместе с тем нормальным делителем группы $\bar{G}$. Поэтому L_i^σ имеет только один максимальный нормальный делитель. Так как Z_i^σ p -группа, то отсюда следует **, что Z_i^σ — циклическая группа. Наконец, так как σ в силу леммы 5 — сильный LN-изоморфизм, то $|Z_i^\sigma| = |Z_i|$. Поэтому $Z_i^\sigma \cong Z_i$, откуда $\bar{G} \cong G$. Таким образом, теорема 1 доказана для частного случая, когда группа G примарна.

Рассмотрим теперь общий случай, когда ациклическая абелева группа G имеет более одной силовской подгруппы. Обозначив через $P, Q, \dots, L$ силовские подгруппы группы G , будем иметь $G = P \times Q \times \dots \times L$, откуда $\bar{G} = P^\sigma \times Q^\sigma \times \dots \times L^\sigma$. Так как $P, Q, \dots, L$ нециклически, то на основании доказанного выше частного случая теоремы 1, $P^\sigma \cong P, Q^\sigma \cong Q, \dots, L^\sigma \cong L$. Следовательно, $\bar{G} \cong G$. Таким образом, теорема 1 доказана полностью.

* $\bar{1}$ — единичный элемент группы $\bar{G}$.

** См., например, [4, гл. 12, теорема 12.5.3].

Доказательству теоремы 2 предположим два предложения, являющиеся обобщениями лемм 3 и 4.

Лемма 3а. Пусть G — конечная p -группа и σ — LN -изоморфизм группы G на конечную группу $\bar{G}$. Если H_1 — подгруппа центра группы G и H — подгруппа группы H_1 не являющаяся ее ядром, то цокль фактор-группы $\bar{G}/H^\sigma$ есть p -группа.

Доказательство. Так как абелева группа $H_1^* = H_1/H$ нециклическа, то нециклическа и ее цокль. Далее, так как H_1^* содержится в центре группы $G^* = G/H$, то $Sc(H_1^*) \leq Sc(G^*)$. Следовательно, цокль группы G^* нециклическа. Наконец, так как цокль p -группы G^* содержится в ее центре, то он является когерентной и притом, существенной. Так как отображением σ индуцируется некоторый LN -изоморфизм σ^* группы G^* на группу $\bar{G}/H^\sigma$, то в силу леммы 1 цокль группы $\bar{G}/H^\sigma$ является p -группой. Лемма доказана.

Дословным повторением доказательства леммы 4 с помощью леммы 3а получается

Лемма 4а. Пусть G — ациклическая p -группа; $\{1\} \subset H_1 \subset H_2 \subset \dots \subset H_m = G$ — ациклический центральный ряд группы G ; I — минимальное ядро подгруппы H_1 ; σ — LN -изоморфизм группы $\bar{G}$ на группу G . Тогда I^σ есть p -группа.

Доказательство теоремы 2. Пусть σ — LN -изоморфизм ациклической нильпотентной группы G на группу $\bar{G}$. Как и при доказательстве теоремы 1 рассмотрим сначала случай, когда G — p -группа. Пусть

$$\{1\} \subset H_1 \subset H_2 \subset \dots \subset H_m = G$$

ациклический центральный ряд группы G . Если $\{I_\alpha\}_{1 \leq \alpha \leq k}$ — система всех минимальных ядер подгруппы H_1 , то в силу леммы 2 $I_1 I_2 \dots I_k = H_1$. Отсюда вытекает на основании леммы 4а, что $H_1^\sigma = I_1^\sigma \dots I_k^\sigma$ есть p -группа. Так как отображение σ индуцирует LN -изоморфизм σ_1 группы G/H_1 на группу $\bar{G}/H_1^\sigma$ и так как

$$H_1/H_1 \subset H_2/H_1 \subset \dots \subset H_m/H_1 = G/H_1$$

— ациклический центральный ряд группы G/H_1 , то, как и выше, мы убедимся в том, что фактор H_2^σ/H_1^σ является p -группой. Повторяя это рассуждение, мы в конце концов покажем, что все факторы нормального ряда

$$\{1\} \subset H_1^\sigma \subset H_2^\sigma \subset \dots \subset H_m^\sigma = \bar{G}$$

группы $\bar{G}$ являются p -группами. Следовательно, $\bar{G}$ — p -группа.

В общем случае разложим ациклическую нильпотентную группу G в прямое произведение ее силовских подгрупп $P, Q, \dots$. Все они, как легко видеть, ациклически. Поэтому, на основании доказанного выше, $P^\sigma, Q^\sigma, \dots$ — силовские подгруппы группы $\bar{G}$. Так как $\bar{G} = P^\sigma \times Q^\sigma \times \dots$, то группа $\bar{G}$ нильпотентна. В силу леммы 5 σ индуцирует сильные LN -изоморфизмы подгрупп $P, Q, \dots$ соответственно на $P^\sigma, Q^\sigma, \dots$. Отсюда легко вытекает, что σ — сильный LN -изоморфизм группы G на $\bar{G}$. Теорема 2 доказана.

Примечание. Существуют пары конечных групп G и $\bar{G}$, удовлетворяющие следующим условиям:

- (I). G — нильпотентная ациклическая группа.
- (II). Группы G и $\bar{G}$ LN -изоморфны.
- (III). $\bar{G} \not\cong G$.

Так, например, группы G и $\bar{G}$ 16-го порядка, заданные определяющими соотношениями

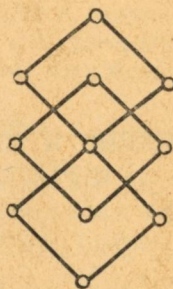
$$a^4 = b^4 = 1, \quad b^{-1}ab = a^{-1}$$

и соответственно

$$r^4 = s^2 = t^2 = 1, \quad t^{-1}rt = rs, \quad rs = sr, \quad ts = st$$

ацикличны, LN -изоморфны, но неизоморфны.

Диаграмма Хассе структуры нормальных делителей каждой из них имеет вид, показанный на приведенном ниже рисунке. Узел, расположенный в центре диаграммы, соответствует центру каждой из групп G и $\bar{G}$. Верхний центральный ряд любой из этих групп имеет два фактора, каждый из которых является элементарной абелевой группой типа $(2,2)$. Таким образом, обе группы ацикличны.



ЛИТЕРАТУРА

1. R. Remak. Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen, *Trans. reine und angew. Math.* 162 (1930), 1—16.
2. Э. М. Жмудь. О ядрах гомоморфизмов линейных представлений конечных групп. Ст. в настоящем сборнике.
3. Э. М. Жмудь. О теоретико-структурных свойствах ядер гомоморфизмов неприводимых линейных представлений конечных групп. Сб. «Алгебра и математическая логика», К., 1966., стр. 98—110.
4. W. Burnside, *The theory of groups of finite order*, Cambridge, 1911.

ВЕРХНИЕ И НИЖНИЕ ДОПОЛНЕНИЯ В КОНЕЧНЫХ МОДУЛЯРНЫХ СТРУКТУРАХ И ТЕОРИЯ ЛИНЕЙНЫХ ПРЕДСТАВЛЕНИЙ КОНЕЧНЫХ ГРУПП

Э. М. Жмудь

ВВЕДЕНИЕ

Настоящая работа примыкает к статье [2], в которой изучается поведение ядер гомоморфизмов неприводимых линейных представлений (сокращено «ядер») конечной группы при изоморфизмах структуры ее нормальных делителей.

В [2] было показано, что ядра конечной группы не определяются, вообще говоря, структурой ее нормальных делителей. Это имеет место также и для антиядер* — объекта двойственного по отношению к ядрам.

В настоящей работе доказывается, что несмотря на то, что ядра и антиядра конечной группы не являются инвариантными объектами структуры ее нормальных делителей, между ними существуют структурно-инвариантные связи. Благодаря этому при заданной структуре нормальных делителей конечной группы ядра и антиядра последней взаимно определяют друг друга.

В основе доказательства этого факта лежат понятия верхнего и нижнего дополнений элемента конечной модулярной структуры, введенные С. Аванном в [1]**.

Основной результат работы: *при любом натуральном k k -антиядра конечной группы являются верхними дополнениями k -ядер***, а k -ядра — нижними дополнениями k -антиядер.*

Отмеченное выше свойство ядер и антиядер взаимно определять друг друга в структуре нормальных делителей группы является простым следствием этого результата (при $k=1$). Кроме того, из него при помощи одного результата Аванна получается новое, чисто комбинаторное доказательство теоремы автора о равенстве числа k -ядер конечной группы числу ее k -антиядер.

Первый параграф статьи содержит сокращенное изложение части результатов статьи [1], дополненное одним результатом автора (теорема С). Во втором параграфе устанавливается связь между этими результатами и теорией представлений конечных групп.

* Определение антиядер см. в [2, 4], а также во втором параграфе настоящей статьи

** Независимо от Аванна эти понятия (под названием N -дополнений 1-го и 2-го рода) были введены автором настоящей статьи в частном случае структуры нормальных делителей конечной группы. Не зная о работе Аванна, автор имел в виду изложить свои результаты об N -дополнениях во 2-й части статьи [2], о чем было анонсировано во введении последней. Ознакомление с работой Аванна побудило автора отказаться от опубликования 2-й части статьи [2] в ее прежнем виде. Настоящая статья является ее переработкой.

*** Определение k -ядер и k -антиядер см. ниже (а также в [4]).

§ 1. ВЕРХНИЕ И НИЖНИЕ ДОПОЛНЕНИЯ В КОНЕЧНЫХ МОДУЛЯРНЫХ СТРУКТУРАХ

1. Пусть L — конечная модулярная структура. Если $a \in L$, то согласно [1], через a^* обозначается объединение всех элементов структуры L , покрывающих элемент a , а через a_* — пересечение всех элементов, покрываемых элементом a . При этом, по определению, $1^* = 1$, $0_* = 0$. Элементы a^* и a_* мы будем в дальнейшем называть соответственно верхней и нижней оболочками элемента a .

Факторы a^*/a и a/a_* являются модулярными структурами с дополнениями.

Пусть $a, a', b', b \in L$, $a' \leq a$, $b' \leq b$. Если факторы a'/a и b/b' перспективны, причем $a' = a \cup b$, $b' = a \cap b$, то фактор b/b' называется нижним транспонированным с a'/a , а фактор a'/a — верхним транспонированным с b/b' .

Фактор b/a называется минимальным (максимальным), если он не имеет отличных от самого себя нижних (верхних) транспонированных факторов.

Если фактор b/a является структурой с дополнениями, то, как показано в [1], он является максимальным (минимальным) тогда и только тогда когда $b = a^*$ ($a = b_*$).

Согласно определению, данному в [1], элемент b называется верхним дополнением элемента $a \in L$, а элемент a — нижним дополнением элемента b , если факторы a^*/a и b/b_* проективны. (Обозначение: $a^*/a \sim b/b_*$).

Иначе говоря, b является верхним дополнением элемента a , если b — числитель минимального фактора проективного a^*/a ; a является нижним дополнением элемента b , если a — знаменатель максимального фактора, проективного b/b_* .

Кроме понятий верхнего и нижнего дополнений в [1] вводится понятие верхнего и нижнего элементов ассоциированных с элементом $a \in L$.

Элемент $c \in L$ называется верхним (нижним) ассоциированным с a , если $c^*/c \sim a^*/a$ ($c/c_* \sim a/a_*$). Другими словами, элемент c является верхним (нижним) ассоциированным с a , если c является знаменателем (числителем) максимального (минимального) фактора проективного a^*/a (a/a_*). Отношения верхней и нижней ассоциированности являются отношениями эквивалентности на L . Каждому из этих отношений отвечает поэтому разбиение множества L на классы. Классы верхних и нижних ассоциированных с элементом a обозначим соответственно через $A_u(a)$ и $A_l(a)$. Полное множество верхних дополнений и полное множество нижних дополнений элемента a обозначим соответственно через $C_u(a)$ и $C_l(a)$. Можно, очевидно, рассматривать C_u и C_l как отображения (многоточные) структуры L на себя. Если $S \subseteq L$, то по определению

$$C_u(S) = \bigcup_{x \in S} C_u(x), \quad C_l(S) = \bigcup_{x \in S} C_l(x).$$

Так как $b \in C_u(a)$ влечет $a \in C_l(b)$ и, наоборот, из $a \in C_l(b)$ следует $b \in C_u(a)$, то отображения C_u и C_l взаимно обратны.

Из данных выше определений нижних и верхних дополнений и ассоциированных непосредственно вытекает, что если $b \in C_u(a)$, то

$$\begin{aligned} C_u(x) &= A_l(b) \text{ для каждого } x \in A_u(a), \\ C_l(y) &= A_u(a) \text{ для каждого } y \in A_l(b). \end{aligned}$$

Таким образом, если b — верхнее дополнение элемента a , то C_u отображает класс $A_u(a)$ на класс $A_l(b)$, а C_l — класс $A_l(b)$ на класс $A_u(a)$, причем каждый из этих классов является образом уже одного элемента

другого класса. Тем самым устанавливается взаимно однозначное соответствие $K_i^{(u)} \leftrightarrow K_i^{(l)}$ между классами $K_i^{(u)}$ верхних ассоциированных и классами $K_i^{(l)}$ нижних ассоциированных структуры L :

$$K_i^{(l)} = C_u(K_i^{(u)}), \quad K_i^{(u)} = C_L(K_i^{(l)}) \quad (i = 1, 2, \dots)$$

Эти факты дополняются следующим, глубоко лежащим утверждением, доказанным в [1]:

Теорема А*. Если L — конечная модулярная структура, $a, b \in L$ и b — верхнее дополнение элемента a , то число верхних дополнений элемента a равно числу нижних дополнений элемента b :

$$|C_u(a)| = |C_l(b)|.$$

Иначе говоря, если $K_i^{(u)}$ и $K_i^{(l)}$ — взаимно соответствующие классы верхних и нижних ассоциированных, то $|K_i^{(u)}| = |K_i^{(l)}|$.

Теорема В.** Если $S \subset L$, $T \subset L$, причем $T = C_u(S)$, $S = C_l(T)$, то $|T| = |S|$.

Доказательство. Так как $S = C_L(T)$, и так как образами элементов структуры L при отображении как образами элементов структуры L при отображении C_L являются классы $K_i^{(u)}$ верхних ассоциированных, то S есть объединение некоторого множества классов $K_{a_j}^{(u)}: S = \bigcup_j K_{a_j}^{(u)}$. Отсюда вытекает, что $T = C_u(S) = \bigcup_j C_u(K_{a_j}^{(u)}) = \bigcup_j K_{a_j}^{(l)}$. Следовательно, $|T| = \sum_j |K_{a_j}^{(l)}| = \sum_j |K_{a_j}^{(u)}| = |S|$.

Наряду с понятием верхних и нижних дополнений в статье [1] вводится понятие прямых верхних и нижних дополнений элемента конечной модулярной структуры L .

Элемент b называется верхним прямым дополнением элемента a структуры L , а элемент a — нижним прямым дополнением элемента b , если фактор b/b_* является нижним транспонированным с a^*/a , т. е. если

$$a \cup b = a^*, \quad (1.1)$$

$$a \cap b = b_*. \quad (1.2)$$

Очевидно, прямые верхние и нижние дополнения являются вместе с тем верхними и нижними дополнениями в прежнем смысле.

В случае, если L является модулярной структурой с дополнениями, прямые верхние и нижние дополнения превращаются в обычные дополнения в структуре L .

Пусть L — конечная модулярная структура. Для каждого элемента $a \in L$ определим множества X_a и Y_a , полагая

$$X_a = \{x \in L \mid a \cup x = a^*\},$$

$$Y_a = \{y \in L \mid y \cap a = a_*\}.$$

Теорема С*.** Элемент $b \in L$ ($a \in L$) тогда и только тогда является верхним (нижним) прямым дополнением элемента $a \in L$ ($b \in L$), когда b (a) есть минимальный (максимальный) элемент множества X_a (Y_b).

Доказательство. 1) Пусть b — верхнее прямое дополнение элемента a . Тогда имеют место соотношения (1.1) и (1.2). Из (1.1) и (1.2)

* Для теорем о модулярных структурах применяется буквенная нумерация, для остальных — численная.

** В явном виде это утверждение в [1] не содержится.

*** Этот результат является, по-видимому, новым.

вытекает, что a^* является прямым объединением элементов a и b в структуре $1/b_*$:

$$a^* = a \times b \text{ (в } 1/b_*\text{)} \quad (1.3)$$

Если бы b не являлся минимальным элементом множества X_a , то последнее содержало бы элемент b_1 , покрываемый элементом b . Условие $b_1 \in X_a$ означает, что

$$a \cup b_1 = a^*. \quad (1.4)$$

Кроме того, очевидно,

$$b_* \leq b_1 < b. \quad (1.5)$$

Так как b/b_* — структура с дополнениями и так как в силу (1.5) $b_1 \in b/b_*$, то элемент b_1 дополняем в b/b_* до b , т. е. существует такой элемент $b' \in L$, что

$$b = b_1 \cup b', \quad (1.6)$$

$$b_1 \cap b' = b_*. \quad (1.7)$$

Из (1.6) и (1.7) вытекает, что b является прямым объединением элементов b_1 и b' в структуре $1/b_*$:

$$b = b_1 \times b' \text{ (в } 1/b_*\text{)}. \quad (1.8)$$

Из (1.3) и (1.8) следует

$$a^* = a \times (b_1 \times b') = (a \times b_1) \times b' = (a \cup b_1) \times b',$$

где прямые объединения берутся в структуре $1/b_*$. Отсюда вытекает в силу (1.4)

$$a^* = a^* \times b' \text{ (в } 1/b_*\text{)}.$$

Следовательно,

$$a^* \cap b' = b_*. \quad (1.9)$$

Так как в силу (1.6), (1.5) и (1.1) $b' \leq b < a^*$, то $a^* \cap b' = b'$, откуда на основании (1.9)

$$b' = b_*. \quad (1.10)$$

Из (1.10), (1.6) и (1.5) вытекает

$$b = b_1 \cup b_* = b_1,$$

что противоречит неравенству $b > b_1$.

Итак, если b — верхнее прямое дополнение элемента a , то b — минимальный элемент множества X_a . Отсюда вытекает двойственное утверждение: если a — нижнее прямое дополнение элемента b , то a — минимальный элемент множества Y_b .

2) Пусть, обратно, b — минимальный элемент множества X_a . Покажем, что тогда b является верхним прямым дополнением к a .

Пусть $\{b_i\}_{1 \leq i \leq r}$ — элементы структуры L , покрывающие элемент b_* . Так как b/b_* структура с дополнениями, а элементы $\{b_i\}_{1 \leq i \leq r}$ являются ее атомами, то

$$b = \bigcup_{i=1}^r b_i. \quad (1.11)$$

Далее, так как $a \cup b = a^*$, $b \geq b_*$, $b_i > b_*$ ($i = 1, \dots, r$), то элементы a, b, a^*, b_i ($i = 1, \dots, r$) принадлежат структуре $1/b_*$. Так как элементы $\{b_i\}_{1 \leq i \leq r}$ являются атомами последней, то

$$a^* = a \cup b = a \cup b_1 \cup \dots \cup b_r = a \times b_{a_1} \times \dots \times b_{a_s},$$

где $1 \leq a_1 < a_2 < \dots < a_s \leq r$ и прямое объединение берется в $1/b_*$. Полагая

$$b' = b_{a_1} \times \dots \times b_{a_s}, \quad (1.12)$$

получаем

$$a^* = a \times b' \quad (\text{в } 1/b_*). \quad (1.13)$$

Из (1.13) вытекает

$$a^* = a \cup b; \quad (1.14)$$

$$a \cap b' = b_*. \quad (1.15)$$

Соотношение (1.14) показывает, что $b' \in X_a$. Так как в силу (1.12) и (1.11) $b' \leq b$ и b — минимальный элемент множества X_a , то $b' = b$. Соотношение (1.15) поэтому принимает вид

$$a \cap b = b_*. \quad (1.16)$$

Так как, кроме того, $a \cup b = a^*$, то элементы a и b удовлетворяют соотношениям (1.1) и (1.2), а это и означает, что b — верхнее прямое дополнение к a .

Итак, доказано, что если b — минимальный элемент множества X_a , то b — верхнее прямое дополнение элемента a . Отсюда вытекает двойственное утверждение: если a — максимальный элемент множества Y_b , то a — нижнее прямое дополнение элемента b . Теорема доказана.

Теорема С приводит к новому определению прямых дополнений, имеющему то преимущество перед определением Авана, что из него становится непосредственно очевидным существование верхних и нижних прямых дополнений для каждого элемента структуры L : элемент $b \in L$ ($a \in L$) называется верхним (нижним) прямым дополнением элемента $a \in L$ ($b \in L$), если $b(a)$ является минимальным элементом множества $X_a(Y_b)$.

§ 2. ТЕОРЕТИКО-СТРУКТУРНЫЕ СВЯЗИ МЕЖДУ ЯДРАМИ И АНТИЯДРАМИ КОНЕЧНОЙ ГРУППЫ

В дальнейшем G означает конечную группу. Допустимым полем называется всякое поле P такое, что $\text{char } P = 0$, либо $\text{char } P = |G|$. Линейные представления группы G над любым допустимым полем, распадающиеся на k неприводимых компонент, называются k -компонентными и представлениями группы G . Через $G^{(k)}$ обозначается декартово произведение k экземпляров группы G . Если $X = (x_1, \dots, x_k) \in G^{(k)}$, то через $\langle\langle X \rangle\rangle$ обозначается пересечение всех нормальных делителей группы G , содержащих множество $\{x_1, \dots, x_k\}$. Через $L_N(G)$ обозначается структура нормальных делителей группы G .

Определение 1. Нормальный делитель H группы G называется k -ядром, если H является ядром гомоморфизма k -компонентного представления группы G .

В частности, 1-ядра называются ядрами группы G .*

Определение 2. Нормальный делитель H группы G называется k -антиядром, если $H = \langle\langle X \rangle\rangle$, где $X \in G^{(k)}$.

В частности, 1-антиядра называются антиядрами группы G .

Нормальный делитель I тогда и только тогда является k -ядром, когда $I = \bigcap_{\alpha=1}^k I_\alpha$, где $\{I_\alpha\}_{1 \leq \alpha \leq k}$ — ядра (не обязательно различные) группы G . Нормальный делитель H группы G тогда и только тогда является k -антиядром, когда $H = \prod_{\alpha=1}^k H_\alpha$, где $\{H_\alpha\}_{1 \leq \alpha \leq k}$ — антиядра (не обязательно различные) группы G .

Каждый нормальный делитель группы G является k -ядром (k -антиядром), если только k достаточно велико. Поэтому множество ядер (анти-

* Ядра группы G не зависят от поля представлений.

ядер) группы G является системой образующих структуры $L_N(G)$ относительно операции пересечения (теоретико-группового объединения $\equiv$ умножения)*.

В статьях [3] и [4] были получены необходимые и достаточные условия для того, чтобы заданный нормальный делитель конечной группы являлся k -ядром (k -антиядром). Приведем один из этих результатов ([4, § 3, теоремы 15 и 15a]).

Теорема 1. *Нормальный делитель H группы G тогда и только тогда является k -ядром (k -антиядром), когда $\varphi_I^{(k)}(G/H) \neq 0$ ($\varphi_{II}^{(k)}(H) \neq 0$), где $\varphi_I^{(k)}(\cdot)$ и $\varphi_{II}^{(k)}(\cdot)$ — теоретико-групповые функции Эйлера I-го и II-го рода и k -го порядка группы G ([4, § 3]).*

Докажем теперь следующее утверждение.

Теорема 2. *Если H — верхнее дополнение нормального делителя I в структуре $L_N(G)$, то для любого натурального k имеет место равенство*

$$\frac{\varphi_I^{(k)}(G/I)}{|G/I|^k} = \frac{\varphi_{II}^{(k)}(H)}{|H|^k}. \quad (2.1)$$

Доказательство. Применим соотношения (3'.3) и (3".3) статьи [4] к группам G/I и H . Так как цокль группы G/I совпадает с факторгруппой I^*/I , где I^* — верхняя оболочка нормального делителя I в структуре $L_N(G)$, то соотношение (3'.3) статьи [4] принимает вид:

$$\frac{\varphi_I^{(k)}(G/I)}{|G/I|^k} = \frac{\varphi^{(k)}(I^*/I)}{|I^*/I|^k}, \quad (2.2)$$

где $\varphi^{(k)}(\cdot)$ — ограничение любой из функций $\varphi_I^{(k)}(\cdot)$, $\varphi_{II}^{(k)}(\cdot)$ на классе вполне приводимых G -групп**.

Аналогичное равенство получается из соотношения (3".3) статьи [4]:

$$\frac{\varphi_I^{(k)}(H)}{|H|^k} = \frac{\varphi^{(k)}(H/H_*)}{|H/H_*|^k}. \quad (2.3)$$

Здесь H_* — нижняя оболочка нормального делителя H в структуре $L_N(G)$.

Заметим теперь, что транспонированные, а потому и проективные факторы структуры $L_N(G)$ являются G -изоморфными G -группами. Так как в силу определения верхних дополнений факторы I^*/I и H/H_* проективны, то $I^*/I \cong H/H_*$ (G — изоморфизм). Следовательно***,

$$\frac{\varphi^{(k)}(I^*/I)}{|I^*/I|^k} = \frac{\varphi^{(k)}(H/H_*)}{|H/H_*|^k},$$

откуда, в силу (2.2) и (2.3) вытекает (2.1).

Теорема 3. *Если H — верхнее дополнение нормального делителя I группы G , то I является k -ядром тогда и только тогда, когда H является k -антиядром.*

Так как единственным верхним дополнением единичной подгруппы E группы G является цокль группы G , то при $I = E$ теорема 3 переходит в предложение, полученное ранее автором в [3].

* Эти системы образующих, вообще говоря, не являются минимальными, т. е. ядра в общем случае разложимы в пересечение больших, а антиядра — в объединение меньших нормальных делителей. Существуют, однако, группы с неразложимыми ядрами и антиядрами (например, все p -группы).

** Областью определения теоретико-групповых функций Эйлера группы G являются G -группы, т. е. группы с областью операторов G , порождающей в каждой из них все внутренние автоморфизмы.

*** Теоретико-групповые функции Эйлера группы G постоянны на классах G -изоморфных G -групп.

Теорема 4. *Группа G тогда и только тогда допускает точные k -компонентные линейные представления, когда цокль группы G является k -антиядром*.*

Теоремой 3, таким образом, дается наиболее общая и законченная формулировка этого результата.

Пусть $\{\Gamma_\alpha\}_{1 \leq \alpha \leq s}$ — полная система представителей классов эквивалентных неприводимых представлений группы G над алгебраически замкнутым полем нулевой характеристики; n_α — степень, I_α — ядро представления Γ_α ; $A = \{1, \dots, k\}$, $A^{(k)}$ — декартова k -я степень множества A ; если $(\alpha) = (\alpha_1, \dots, \alpha_k) \in A^{(k)}$, то

$$n_{(\alpha)} = n_{\alpha_1} \dots n_{\alpha_k}, \\ I_{(\alpha)} = I_{\alpha_1} \cap \dots \cap I_{\alpha_k}.$$

Будем говорить, что элементы $X_1, X_2 \in G^{(k)}$ принадлежат одному и тому же k - N -слою группы G , если $\langle\langle X_1 \rangle\rangle = \langle\langle X_2 \rangle\rangle$. С k -антиядром H группы G сопоставляется порождающий его k - N -слой $F_H^{(k)}$:

$$F_H^{(k)} = \{X \in G^{(k)} \mid \langle\langle X \rangle\rangle = H\}.$$

Порядок $|F_H^{(k)}|$ k - N -слоя $F_H^{(k)}$ обозначим через $f_H^{(k)}$.

Из соотношения (2.1) и результатов статьи [4, § 4, соотношения (2.4) и (12.4)] вытекает следующее предложение.

Теорема 5. *Если H — k -антиядро группы G , являющееся верхним дополнением k -ядра I в структуре $L_N(G)$, то*

$$\sum_{I_{(\alpha)}=I} n_{(\alpha)}^2 = \frac{|G|^k}{|I|^k |H|^k} f_H^{(k)}.$$

Обозначим теперь через Σ_k и Σ_k^* соответственно систему k -ядер и систему k -антиядер группы G . Теорема 3 показывает, что

$$\Sigma_k^* = C_u(\Sigma_k), \quad \Sigma_k = C_L(\Sigma_k^*).$$

Отсюда в силу теоремы В первого параграфа вытекает, что $|\Sigma_k^*| = |\Sigma_k|$.

Таким образом, получено чисто комбинаторное доказательство следующего утверждения, доказанного ранее автором с помощью методов теории представлений.

Теорема 6. *Число k -ядер конечной группы равно числу ее k -антиядер. Наконец, очевидным следствием теоремы 3 является*

Теорема 7. *Пусть G и $\bar{G}$ конечные группы и σ — изоморфизм структуры $L_N(G)$ на структуру $L_N(\bar{G})$. Если образом системы ядер (антиядер) группы G при отображении σ является система ядер (антиядер) группы $\bar{G}$, то образом системы антиядер (ядер) группы G является система антиядер (ядер) группы $\bar{G}$.*

Выше уже отмечалось, что каждый нормальный делитель группы G разлагается в структуре $L_N(G)$ в объединение (пересечение) некоторого множества антиядер (ядер).

Определение 3. N -размерностью ($\dim_N H$) нормального делителя H группы G назовем минимальное число антиядер, объединением которых может являться H ; N -дефектом ($\text{def}_N H$) нормального делителя H назовем минимальное число ядер, пересечением которых может являться H .

Теорема 3, очевидно, равносильна следующему утверждению.

* Частный случай ($k = 1$) этой теоремы был получен Гашнюком [5].

Теорема 3а. Если H — верхнее дополнение нормального делителя I группы G , то

$$\dim_N H = \text{def}_N I. \quad (2.4)$$

Непосредственно очевидны следующие свойства N -размерности и N -дефекта: если $H_1, H_2 \triangleleft G$, то

$$\begin{aligned} \dim_N (H_1 H_2) &\leq \dim_N H_1 + \dim_N H_2, \\ \text{def}_N (H_1 \cap H_2) &\leq \text{def}_N H_1 + \text{def}_N H_2. \end{aligned}$$

В заключение отметим, что если G — аддитивная элементарная абелева p -группа, рассматриваемая как линейное пространство над простым полем характеристики p , то N -размерность и N -дефект каждой ее нетривиальной подгруппы совпадают с обычными размерностью и дефектом этой подгруппы, рассматриваемой как подпространство.

ЛИТЕРАТУРА

1. S. P. Avann. Upper and Lower complementation in a modular lattice, Proc. of the Amer. Math. Soc. Vol. 11, № 1, 1960, 17—22.
2. Э. М. Жмудь, О теоретико-структурных свойствах ядер гомоморфизмов неприводимых линейных представлений конечных групп. Сб. «Алгебра и математическая логика». Изд-во «Наукова думка», Киев, 1966, 98—110.
3. Э. М. Жмудь. О ядрах гомоморфизмов линейных представлений конечных групп. «Матем. сб.», 44 (86) № 3, 1958, 353—408.
4. Э. М. Жмудь. О теоретико-групповой функции Мебиуса. «Зап. мех-матем. ф-та ХГУ и ХМО», т. XXVIII, серия 4. Изд-во ХГУ, Харьков, 1961, 73—96.
5. W. Gaschütz. Endliche Gruppen mit treuen-irreduziblen Darstellungen. Math. Nachr., 12, № 3/4, 1954, 253—255.

**О КОНЕЧНЫХ ГРУППАХ, ОБЛАДАЮЩИХ ЕДИНСТВЕННЫМ
МИНИМАЛЬНЫМ НОРМАЛЬНЫМ ДЕЛИТЕЛЕМ И ЕДИНСТВЕННЫМ
КЛАССОМ ИЗОМОРФНЫХ НЕПРИВОДИМЫХ ПРЕДСТАВЛЕНИЙ**

Э. М. Жмудь

Известно, что конечная группа, обладающая единственным минимальным нормальным делителем, всегда допускает изоморфные неприводимые представления над любым полем, характеристика которого либо равна нулю, либо не делит порядка группы (поля с указанными свойствами мы в дальнейшем будем называть допустимыми по отношению к заданной группе).

В настоящей работе изучаются конечные группы, имеющие единственный минимальный нормальный делитель и единственный класс изоморфных неприводимых представлений над заданным допустимым полем K . Конечные группы, обладающие этими двумя свойствами, мы будем называть K -примитивными.

Напомним введенное С. Д. Берманом понятие K -отдела конечной группы. Пусть G — конечная группа, K — допустимое поле, e — экспонент группы G , ε — первообразный корень e -й степени из единицы 1_K поля K , Γ — группа Галуа поля $K(\varepsilon)/K$.

Каждый автоморфизм $\sigma \in \Gamma$ определяет некоторое взаимно-однозначное отображение Θ_σ группы G на себя: если $\sigma(\varepsilon) = \varepsilon^\nu$ (ν — целое число, $(\nu, e) = 1$), то $\Theta_\sigma(x) = x^\nu$ для всех $x \in G$. Элементы $x, y \in G$ будем называть K -сопряженными (обозначение $x^k y$), если y сопряжен в G с элементом $\Theta_\sigma(x)$, где $\sigma \in \Gamma$. Множество элементов группы G распадается на попарно непересекающиеся классы K -сопряженных элементов — K -отделы группы G (см. [2]).

Согласно известной теореме Витта — Бермана [1] число K -отделов группы G равно числу классов эквивалентных неприводимых K -представлений группы G .

Введем некоторые обозначения. Если H — группа, то $H^* = H \setminus \{1\}$; $|H|$ — порядок группы H ; $C(g)$ — централизатор элемента $g \in G$ в группе G ; $\text{Ord } g$ — порядок элемента g ; $\pi_K(G)$ — число K -отделов группы G .

Теорема 1. Конечная группа G тогда и только тогда является K -примитивной, когда

а) Группа G обладает единственным минимальным нормальным делителем F .

б) Элементы из F^* образуют K -отдел группы G .

в) Если $f \in F^*$, $x \in G \setminus F$, то $f x^K x$.

Доказательство. 1. Докажем необходимость условий а) — в). Пусть $\{\Phi_\nu\}_{1 \leq \nu \leq \pi_K(G)}$ — полная система неэквивалентных неприводимых K -представлений K -примитивной группы G . Представление Φ_1 условимся считать изоморфным. Так как представления $\{\Phi_\nu\}_{2 \leq \nu \leq \pi_K(G)}$ уже не являются изоморфными, то

$$\text{Ker } \Phi_\nu \supsetneq F. \quad (1)$$

Пусть χ_ν — характер представления Φ_ν , m_ν — кратность Φ_ν в регулярном представлении группы G . Вычисление характера элемента x в регулярном K -представлении группы G дает

$$\sum_{\nu=1}^{z_K(G)} m_\nu \chi_\nu(x) = \begin{cases} 1_K |G|, & \text{если } x = 1 \\ 0 & \text{если } x \neq 1. \end{cases} \quad (2)$$

Применяя (2) к фактор-группе G/F , получаем

$$\sum_{\nu=2}^{z_K(G)} m_\nu \chi_\nu(x) = \sum_{\text{Ker } \Phi_\nu \supsetneq F} m_\nu \chi_\nu(x) = \begin{cases} |G/F|, & \text{если } x \in F. \\ 0, & \text{если } x \in F^*. \end{cases} \quad (3)$$

Из (2) и (3) вытекает

$$m_1 \chi_1(x) = \begin{cases} 1_K (|G| - |G/F|), & \text{если } x = 1 \\ -1_K |G/F|, & \text{если } x \in F^* \\ 0 & \text{если } x \in F. \end{cases} \quad (4)$$

Если $x \in F^*$, то в силу (4) $m_1 \chi_1(x) = -1_K \cdot |G/F|$. Отсюда 1) $1_K \cdot m_1 \neq 0$; 2) для любых $f_1, f_2 \in F^*$

$$\chi_1(f_1) = \chi_1(f_2) = -(1_K m_1)^{-1} \cdot |G/F|. \quad (5)$$

Далее, если $\nu > 1$, то в силу а) $f_1, f_2 \in \text{Ker } \Phi_\nu$. Поэтому

$$\chi_\nu(f_1) = \chi_\nu(f_2) = 1_K \cdot n_\nu \quad (\nu > 1), \quad (6)$$

где n_ν — степень Φ_ν .

Из (5) и (6) вытекает, что $\chi_\nu(f_1) = \chi_\nu(f_2)$ для любых $f_1, f_2 \in F^*$ и $\nu = 1, \dots, z_K(G)$. Следовательно, (см., например, [2]) $f_1 \sim^K f_2$. Таким образом, F^* есть K -отдел группы G , т. е. условие б) выполнено.

Пусть теперь $f \in F^*$, $x \in G \setminus F$. Тогда и $fx \in G \setminus F$, а значит в силу (4) $\chi_1(fx) = \chi_1(x) = 0$. Если же $\nu > 1$, то $f \in \text{Ker } \Phi_\nu$ и поэтому $\chi_\nu(fx) = \chi_\nu(x)$. Таким образом, $\chi_\nu(fx) = \chi_\nu(x)$ ($\nu = 1, \dots, z_K(G)$). Следовательно, $fx \sim^K x$. Тем самым необходимость условия в) также доказана.

2. Допустим теперь, что для группы G выполнены условия а) — в). Докажем, что группа G допускает с точностью до эквивалентности единственное изоморфное неприводимое K -представление и, следовательно, является K -примитивной группой.

Из условия а) вытекает, что неизоморфные неприводимые K -представления группы G находятся во взаимно-однозначном соответствии с неприводимыми K -представлениями фактор-группы G/F . Поэтому, обозначив через $\nu_K(G)$ число всех попарно неэквивалентных изоморфных неприводимых K -представлений группы G в силу теоремы Витта — Бермана, будем иметь

$$\nu_K(G) = z_K(G) - z_K(G/F). \quad (7)$$

Пусть $\{T_\nu\}_{1 \leq \nu \leq z_K(G)}$ — K -отделы группы G , причем $T_1 = \{1\}$, $T_2 = F^*$ (в силу условия б) F^* — K -отдел группы G). Тогда $T_\nu \subset G \setminus F$ ($\nu > 2$). Естественный гомоморфизм $x \rightarrow \bar{x} = \varphi(x)$ группы G на $\bar{G} = G/F$ отображает, как легко видеть, K -отдел T_ν в K -отдел $\bar{T}_\nu = \varphi(T_\nu)$ группы $\bar{G}$. При этом $\bar{T}_1 = \bar{T}_2 = \{\bar{1}\}$ ($\bar{1}$ — единичный элемент группы $\bar{G}$). K -отделы $\bar{T}_\nu$ ($\nu \geq 2$) попарно различны.

Действительно, из $\bar{T}_\alpha = \bar{T}_\beta$ ($\beta \geq 2$) вытекает $\bar{t}_\alpha \sim^K \bar{t}_\beta$, где $\bar{t}_\alpha = \varphi(t_\alpha)$, $\bar{t}_\beta = \varphi(t_\beta)$, $t_\alpha \in T_\alpha$, $t_\beta \in T_\beta$. Следовательно, $t_\alpha \sim^K f t_\beta$, где $f \in F$. Но в силу в) $f t_\beta \sim^K t_\beta$. Поэтому $t_\alpha \sim^K t_\beta$, откуда $T_\alpha = T_\beta$ и, таким образом, $\alpha = \beta$.

Итак, группа $\bar{G}$ имеет $\chi_K(G) - 1$ K -отделов: $\bar{T}_1 = \{\bar{1}\}$, $\bar{T}_3$, $\bar{T}_4$, ..., $\bar{T}_{\chi_K(G)}$. Следовательно, $\chi_K(G/F) = \chi_K(G) - 1$, откуда в силу (7) $\chi_K(G) = 1$. Таким образом, G — K -примитивная группа. Достаточность условий а) — в) тем самым доказана.

Теорема 2. Если G — K -примитивная группа и F — ее минимальный нормальный делитель, то

а) F является элементарной абелевой p -группой (p — простое число).

б) Если $f \in F^*$, то $C(f)$ есть силовская p -подгруппа группы G .

Доказательство. 1) По теореме 1 F^* есть K -отдел группы G . Поэтому все элементы из F^* имеют один и тот же порядок. Так как множество F^* содержит элемент простого порядка p , то порядки всех элементов из F^* равны p . Следовательно, F — p -группа. Подгруппа F содержит нетривиальный центр $Z(F)$. Так как $Z(F) \triangleleft G$, то в силу минимальности F имеет место $Z(F) = F$. Таким образом, F — абелева группа. Так как F не содержит нетривиальных характеристических подгрупп, то F — элементарная группа. Таким образом, утверждение а) доказано.

2) Пусть $f \in F^*$. Тогда, в силу а) $\text{Ord } f = p$. Из коммутативности F следует $C(f) \supseteq F$. Порядок любого элемента x из $\{C(f)\}^*$ делится на p . Если $x \in F$ это следует из того, что F — p -группа. Если же $x \notin F$, то в силу утверждения в) теоремы 1 $fx \sim x$. Поэтому $\text{Ord}(fx) = \text{Ord } x$. Таким образом, если $\text{Ord } x = k$, то $(fx)^k = 1$; отсюда $\dot{f}^k = 1$, так как $fx = xf$. Следовательно, $k \equiv 0 \pmod{p}$. Из полученного результата вытекает, что $C(f)$ есть p -группа. Заметим далее, что K -отдел F^* -группы G , как инвариантное ее подмножество, распадается на некоторое число l классов сопряженных элементов группы G . Все эти классы имеют, как легко видеть, одинаковые порядки. Поэтому, полагая $|F| = p^\lambda$, будем иметь

$$l(G : C(f)) = p^\lambda - 1. \quad (8)$$

Из (8) вытекает, что $p \nmid (G : C(f))$. Следовательно, $C(f)$ — силовская p -подгруппа группы G . Таким образом, все утверждения теоремы 2 доказаны.

Если G — K -примитивная группа, F — ее минимальный нормальный делитель и $|F| = p^\lambda$, то простое число p будем называть типом группы G .

Из теоремы 2 вытекает

Следствие. Всякий элемент g K -примитивной группы типа p , не являющийся p -элементом*, индуцирует на минимальном нормальном делителе F группы G регулярный автоморфизм $x \rightarrow g^{-1}xg$ ($x \in F$).

В дальнейшем будут использованы некоторые факты из теории групп Фробениуса. Согласно одному из определений конечная группа G называется группой Фробениуса с ядром N , если

(А). $N \triangleleft G$, $N \neq \{1\}$.

(В). Любой элемент $g \in G \setminus N$ индуцирует на N регулярный автоморфизм $x \rightarrow g^{-1}xg$ ($x \in N$).

Условие (В), очевидно, равносильно следующему: если $x \in N^*$, то $C(x) \subseteq N$.

Порядок ядра N , как известно, взаимно прост с его индексом; поэтому в группе G существует по крайней мере одно полупрямое дополнение H к N ; (1) $N \cap H = \{1\}$; (2) $N \cdot H = G$.

Пусть H — одно из таких дополнений. Имеет место

Теорема Бернсайда [3]. Любая силовская подгруппа группы H либо циклическа, либо является обобщенной группой кватернионов.

Следствие. Если минимальный нормальный делитель F K -примитивной группы G является ее силовской p -подгруппой, то G есть группа Фробениуса с ядром F .

* Элемент $g \in G$ называется p -элементом, если $\text{Ord } g$ есть степень числа p .

Из теоремы Бернсайда и следствия теоремы 2 вытекает кроме того

Теорема 3. Если G — K -примитивная группа типа p и q — простой делитель $|G|$, $q \neq p$, то силовские q -подгруппы группы G либо циклически, либо являются обобщенными группами кватернионов.

Доказательство. Пусть Q — силовская q -подгруппа K -примитивной группы G . Каждый элемент из Q^* индуцирует в минимальном нормальном делителе F группы G регулярный автоморфизм (следствие теоремы 2). Поэтому подгруппа $H = F \cdot Q$ является группой Фробениуса с ядром F и дополнением Q , откуда в силу теоремы Бернсайда вытекает утверждение теоремы 3.

Рассмотрим в заключение случай, когда поле K совпадает с полем C комплексных чисел.

Теорема 4.* Пусть G — C -примитивная группа типа p , F — ее минимальный нормальный делитель, $|F| = p^\lambda$. Тогда

$$|G| = p^\mu (p^\lambda - 1), \quad (9)$$

$$\mu \equiv \lambda \pmod{2}. \quad (10)$$

Доказательство. Так как в рассматриваемом случае F^* является классом сопряженных элементов группы, то множитель l в левой части (8) равен 1. Поэтому

$$(G : C(f)) = p^\lambda - 1, \quad (11)$$

где f — любой элемент из F^* . Так как в силу теоремы 2 $C(f)$ — силовская p -подгруппа группы G , то, полагая $|C(f)| = p^\mu$, получаем из (11) соотношение (9). Полагая в (4) $x = 1$ и учитывая, что в случае $K = C$ $m_\nu = \chi_\nu(1) = n_\nu$ (=степени неприводимого C -представления Φ_ν), с помощью (9) получаем $n_1^2 = p^{\mu-\lambda} (p^\lambda - 1)^2$, откуда вытекает (10). Попутно получено следующее выражение для степени n_1 изоморфного неприводимого C -представления Φ_1 группы G :

$$n_1 = p^{\frac{\mu-\lambda}{2}} (p^\lambda - 1). \quad (12)$$

Следствие. Если G — C -примитивная группа порядка 2^μ , то μ нечетно.

ЛИТЕРАТУРА

1. С. Д. Берман. К теории представлений конечных групп. ДАН СССР, т. 86, № 6 (1952), 885—888.
2. С. Д. Берман. Характеры линейных представлений конечных групп над произвольным полем. «Матем. сб.», Новая серия, т. 44 (86), (1958), 409—456.
3. W. Burnside. Theory of Groups of finite Order, Cambridge, 1911.

* Утверждение этой теоремы остается справедливым, если C — любое алгебраически замкнутое поле, характеристика которого не делит $|G|$.

О КОНЕЧНЫХ ГРУППАХ ЕДИНИЦ ЦЕЛОЧИСЛЕННОГО ГРУППОВОГО КОЛЬЦА

Э. М. Жмудь, Г. Ч. Куренной

Обозначения, основные определения и результаты

- Z — кольцо целых рациональных чисел;
- Q — поле рациональных чисел;
- K — конечное алгебраическое расширение поля Q ;
- C — поле комплексных чисел;
- I — кольцо целых чисел поля K ;
- G — конечная группа;
- $N \triangleleft G$ — N — нормальный делитель группы G ;
- ZG, IG, KG, CG — групповые кольца группы G соответственно над $Z, I, K, \text{ и } C$. Предполагается, что каждое из этих колец естественным образом погружено в следующее: $ZG \subset IG \subset KG \subset CG$;
- $U(G)$ — группа единиц кольца IG ;
- ε — гомоморфизм кольца KG в поле K , порождаемый единичным характером группы G : если $x \in KG$, $x = \sum_{g \in G} \xi(g)g$, $\xi(g) \in K$, то $\varepsilon(x) = \sum_{g \in G} \xi(g)$;
- $V(G)$ — подгруппа тех единиц $V \in U(G)$, для которых $\varepsilon(V) = 1$;
- $|M|$ — число элементов конечного множества M .

Определение 1. Конечную подгруппу H группы $U(G)$ назовем правильной, если H не содержит, кроме единичного элемента, никаких единиц кольца IG , имеющих вид $\zeta 1$, где $\zeta \in I$ и 1 — единичный элемент группы G .

Очевидно, все конечные подгруппы группы $V(G)$ являются правильными. Легко показать [2], что конечная подгруппа группы $U(G)$ тогда и только тогда является правильной, когда ее элементы I -линейно независимы. Отсюда вытекает, в частности, линейная независимость элементов любой конечной подгруппы группы $V(G)$.

Пусть H — конечная подгруппа группы $U(G)$. «Усредняя» подгруппу H в кольце KG (напоминаем, что $IG \subset KG$), получим идемпотент

$$j_H = \frac{1}{|H|} \sum_{h \in H} h \tag{1}$$

этого кольца. Можно показать (§ 2), что подгруппа H является правильной тогда и только тогда, когда $j_H \neq 0$.

Определение 2. Конечную подгруппу H группы $U(G)$ назовем S -подгруппой последней, если

1°. Подгруппа H является правильной.

2°. Идемпотент j_H содержится в центре кольца KG .

Очевидно, S -подгруппой группы $U(G)$ является всякий нормальный делитель любой подгруппы $\bar{G}$ группы $U(G)$, образующий I -базис кольца IG . Если H — S -подгруппа группы $U(G)$ и $H \subset H_1$, где H_1 — правильная подгруппа группы $U(G)$, то, как можно показать, $H \triangleleft H_1$.

Целью настоящей работы является доказательство следующих утверждений:

Теорема 1. Порядок всякой правильной подгруппы группы является делителем порядка группы G^* .

Теорема 2. Существует отображение $\sigma: H \rightarrow H^\sigma$ множества $\mathfrak{S}$ S -подгрупп H группы $V(G)$ на множество $\mathfrak{R}$ всех нормальных делителей группы G , обладающее следующими свойствами:

1°. σ есть структурный гомоморфизм множества $\mathfrak{S}$ на множество $\mathfrak{R}$: из $H_1, H_2 \in \mathfrak{S}$, $H_1 \subset H_2$ следует $H_1^\sigma \subset H_2^\sigma$.

2°. Структурный гомоморфизм σ является сильным, т. е. $|H^\sigma| = |H|$, если $H \in \mathfrak{S}$.

3°. Если $H \in \mathfrak{R}$, то $H^\sigma = H$.

4°. Если $H \in \mathfrak{S}$, то $j_{H^\sigma} = j_H$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Пусть $x \in KG$, $x = \sum_{g \in G} \xi(g)g$, $\xi(g) \in K$

Коэффициент $\xi(1)$ обозначим через $\text{tr}(x)$ («приведенный след» элемента x). Очевидно,

$$\text{tr}(x) = \frac{1}{|G|} S(x),$$

где $S(x)$ — след матрицы, отвечающей элементу x в регулярном представлении алгебры KG .

В дальнейшем нам будет необходим следующий результат С. Д. Бермана [1].

Лемма 1. Если x элемент конечного порядка группы $U(G)$, то либо $x = \zeta 1$, где $\zeta \in I$, либо $\text{tr } x = 0$.

Докажем теперь теорему 1. Пусть H — правильная конечная подгруппа группы $U(G)$. Образует для нее идемпотент $j_H = \frac{1}{|H|} \sum_{h \in H} h$. В силу

леммы Бермана и правильности подгруппы H $\text{tr}(h) = 0$ для каждого $h \in H$, $h \neq 1$. Поэтому $\text{tr}(j_H) = \frac{1}{|H|}$, откуда $S(j_H) = \frac{|G|}{|H|}$. Так как j_H идемпотент, то $S(j_H) \in Z$. Следовательно, $|G|$ делится на $|H|$, что и доказывает теорему **.

Примечание. В процессе доказательства теоремы 1 показано, что для всякой правильной конечной группы единиц H $j_H \neq 0$. Легко убедиться в справедливости обратного утверждения: если H — конечная подгруппа группы $U(G)$ и $j_H \neq 0$, то подгруппа H является правильной. Допустим, что подгруппа H не является правильной. Тогда H содержит элемент $g = \zeta 1$, где $\zeta \in I$, $\zeta \neq 1$. Так как $gj_H = j_H$, то $\zeta j_H = j_H$, откуда ввиду $\zeta \neq 1$ следует $j_H = 0$.

* Для случая циклической группы и при условии $I = Z$ это утверждение переходит в один из результатов С. Д. Бермана [1].

** Приведенное доказательство теоремы 1 по существу не отличается от доказательства леммы 1 статьи [1].

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Определение 3. Высотой $\eta(x)$ элемента x кольца KG назовем наименьшее из натуральных чисел m , обладающих тем свойством, что $mx \in IG$.

Из $mx \in IG$, $m \in \mathbb{Z}$, очевидно, вытекает, что $\eta(x) | m$.

Определим теперь на кольце KG функцию

$$\tau(x) = \eta(x) \operatorname{tr}(x), \quad x \in KG. \quad (2)$$

Очевидно, $\tau(x) \in I$ для всех $x \in KG$. Если e — отличный от нуля идемпотент кольца KG , то, как легко видеть, $\tau(e) \in \mathbb{Z}$, $\tau(e) \geq 1$.

Определение 4. Подгруппу $H_1 \subset U(G)$ назовем ассоциированной с конечной подгруппой $H \subset U(G)$, если элементы подгруппы H_1 имеют вид $\psi(h)h$, где $h \in H$ и ψ — линейный характер подгруппы H .

Лемма 2. ¹⁰. Пусть e — идемпотент центра кольца KG , удовлетворяющий условию $\tau(e) = 1$. Тогда $e = j_H$, где H — S -подгруппа группы $U(G)$. Порядок подгруппы H равен высоте идемпотента e . Среди подгрупп H , дающих представление $e = j_H$ для идемпотента e , одна и только одна ассоциирована с некоторым, зависящим только от e , нормальным делителем группы G .

²⁰. Если H — S -подгруппа группы $U(G)$ и $e = j_H$, то e — идемпотент центра кольца KG , удовлетворяющий условию $\tau(e) = 1$.

Доказательство 1. Пусть $\{e_p\}_{1 \leq p \leq r}$ — минимальные идемпотенты центра кольца CG ; χ_p — комплексный неприводимый характер группы G , отвечающий идемпотенту e_p ($p = 1, \dots, r$); $n_p = \chi_p(1)$ ($p = 1, \dots, r$); θ_p — гомоморфизм центра кольца CG в поле C , отвечающий идемпотенту e_p .

Если z — элемент центра кольца CG , то, как известно [4], $\theta_p(z) = \frac{\chi_p(z)}{n_p}$.

Кроме того, $\theta_p(e_q) = \delta_{pq}$ ($p, q = 1, \dots, r$). Любой идемпотент e центра кольца CG допускает единственное (с точностью до порядка следования слагаемых) представление в виде суммы некоторого множества идемпотентов e_p — компонент идемпотента e . В дальнейшем $e_p \prec e$ будет обозначать, что e_p — компонента идемпотента e . Очевидно,

$$\theta_p(e) = \begin{cases} 1, & \text{если } e_p \prec e \\ 0, & \text{если } e_p \not\prec e. \end{cases} \quad (3)$$

Представим идемпотент e центра кольца KG в виде

$$e = \sum_{g \in G} \xi(g) g, \quad \xi(g) \in K. \quad (4)$$

Из (4) и соотношения $e^2 = e$ вытекает

$$\operatorname{tr}(e) = \sum_{g \in G} \xi(g) \xi(g^{-1}).$$

Далее, так как ([4])

$$e_p = \frac{n_p}{|G|} \sum_{g \in G} \overline{\chi_p(g)} g,$$

то

$$\xi(g) = \frac{1}{|G|} \sum_{e_p \prec e} n_p \overline{\chi_p(g)},$$

откуда вытекает, что

$$\xi(g^{-1}) = \overline{\xi(g)}.$$

Следовательно,

$$\text{tr}(e) = \sum_{g \in G} |\xi(g)|^2. \quad (5)$$

Полагая

$$\psi(g) = \eta(e) \xi(g), \quad g \in G, \quad (6)$$

перепишем (4) и (5) в виде

$$\eta(e)e = \sum_{g \in G} \psi(g)g, \quad (7)$$

$$\eta(e)\tau(e) = \sum_{g \in G} |\psi(g)|^2. \quad (8)$$

Допустим теперь, что $\tau(e) = 1$. Тогда в силу (8)

$$\eta(e) = \sum_{g \in G} |\psi(g)|^2. \quad (9)$$

Здесь, как видно из определения 3, $\psi(g) \in I$ ($g \in G$).

Далее, при $e_p \prec e$ в силу (4) и (3) имеет место

$$1 = \theta_p(e) = \sum_{g \in G} \xi(g) \frac{\chi_p(g)}{n_p},$$

откуда

$$\eta(e) = \sum_{g \in G} \psi(g) \frac{\chi_p(g)}{n_p}. \quad (10)$$

Обозначим через N множество тех элементов g группы G , для которых $\psi(g) \neq 0$. Докажем, что если $g \in N$, то $|\psi(g)| = 1$.

Пусть $K^{(1)} = K$, $K^{(2)}$, ..., $K^{(n)}$ — поля, сопряженные с K относительно поля Q рациональных чисел.

Положим

$$\gamma = \prod_{g \in N} \psi(g)$$

и обозначим через $\{\gamma^{(i)}\}_{1 \leq i \leq n}$ числа, сопряженные с $\gamma = \gamma^{(1)}$. Так как $\gamma \in I$, то $|\gamma^{(1)}| \dots |\gamma^{(n)}| \geq 1$. Поэтому для некоторого i должно иметь место $|\gamma^{(i)}| \geq 1$.

Без ограничения общности можно принять, что $i = 1$ (в противном случае в роли поля K можно было бы взять $K^{(i)}$) и рассмотреть идемпотент $e^{(i)} = \sum_g \xi(g)^{(i)}g$ центра кольца $K^{(i)}G$. Таким образом,

$$\prod_{g \in N} |\psi(g)| \geq 1. \quad (11)$$

Так как

$$\frac{1}{|N|} \sum_{g \in N} |\psi(g)| \geq \left(\prod_{g \in N} |\psi(g)| \right)^{\frac{1}{|N|}},$$

то в силу (11)

$$\frac{1}{|N|} \sum_{g \in N} |\psi(g)| \geq 1. \quad (12)$$

Полагая

$$|\psi(g)| = 1 + \rho(g),$$

с помощью (12) получим

$$\sum_{g \in N} \rho(g) \geq 0. \quad (13)$$

В силу (9) и (13) имеем

$$\begin{aligned}\eta(e) &= \sum_{g \in N} [1 + \rho(g)]^2 = \sum_{g \in N} [1 + \rho(g)] + \sum_{g \in N} \rho(g) + \sum_{g \in N} [\rho(g)]^2 = \\ &= \sum_{g \in N} |\psi(g)| + \sum_{g \in N} \rho(g) + \sum_{g \in N} [\rho(g)]^2.\end{aligned}\quad (14)$$

Замечая, что в силу (10) при $e_p \prec e$ имеет место

$$\eta(e) \leq \sum_{g \in N} \left| \psi(g) \frac{\chi_p(g)}{n_p} \right| \leq \sum_{g \in N} |\psi(g)|. \quad (15)$$

Из (15) получаем

$$\sum_{g \in N} \rho(g) + \sum_{g \in N} [\rho(g)]^2 \leq 0.$$

Отсюда, на основании (14), вытекает

$$\rho(g) = 0, \quad g \in N.$$

Следовательно,

$$|\psi(g)| = 1, \quad g \in N. \quad (16)$$

Из (16) и (9) вытекает

$$|N| = \eta(e). \quad (17)$$

Покажем теперь, что множество N является нормальным делителем группы G .

Из (7), пользуясь соотношением $e^2 = e$, получаем

$$\left(\sum_{g \in N} \psi(g) g \right)^2 = \eta(e) \sum_{g \in N} \psi(g) g. \quad (18)$$

Из (18) вытекает, что для любого элемента $g \in N$

$$\eta(e) \psi(g) = \sum_{x, y \in N, xy=g} \psi(x) \psi(y). \quad (19)$$

Обозначив через M_g множество элементов $x \in N$, удовлетворяющих условию $x^{-1}g \in N$, перепишем (19) в виде

$$\eta(e) \psi(g) = \sum_{x \in M_g} \psi(x) \psi(x^{-1}g), \quad g \in N. \quad (20)$$

Из (20) вытекает

$$\eta(e) = |\eta(e) \psi(g)| \leq \sum_{x \in M_g} |\psi(x) \psi(x^{-1}g)| = |M_g|.$$

Так как, с другой стороны, в силу (17) $|M_g| \leq |N| = \eta(e)$, то $|M_g| = \eta(e)$. Следовательно, $M_g = N$. Это означает, что для любых элементов $x, g \in N$ произведение $x^{-1}g$ содержится в N , поэтому N — группа. Далее, так как функция ψ является постоянной на классах сопряженных элементов группы G , то N — объединение некоторого числа классов сопряженных элементов и, значит, $N \triangleleft G$.

Покажем еще, что ограничение функции ψ на подгруппе N является линейным характером последней. Заметим с этой целью, что в силу (19)

$$\left| \sum_{x, y \in N, xy=g} \psi(x) \psi(y) \right| = \eta(e) = |M_g| = \sum_{x, y \in N, xy=g} |\psi(x) \psi(y)|.$$

Поэтому все слагаемые $\psi(x) \psi(y)$ в правой части (19) имеют один и тот же аргумент и, следовательно, совпадают с $\psi(g)$. Таким образом, при любых $x, y \in N$

$$\psi(x) \psi(y) = \psi(xy),$$

т. е. ψ — линейный характер группы N . Соотношение (7), переписанное в виде

$$e = \frac{1}{|N|} \sum_{g \in N} \psi(g) g, \quad (21)$$

показывает, что $e = j_H$, где H — подгруппа группы $U(G)$, состоящая из элементов $\psi(g)g$, где $g \in N$. Подгруппа H , очевидно, является правильной. Так как e содержится в центре кольца KG , то H является S -подгруппой группы $U(G)$. Подгруппа H ассоциирована с N . Очевидно, подгруппы N и H однозначно определяются идемпотентом e .

Таким образом, первая часть утверждений леммы доказана.

2. Пусть $e = j_H$, где H — S -подгруппа группы $U(G)$. Тогда в силу определения 2 e содержится в центре кольца KG .

Выше было доказано (см. доказательство теоремы 1), что $tr(j_H) = \frac{1}{|H|}$. Следовательно, $|H| \cdot tr(e) \in I$, откуда вытекает, что $|H|$ делится на $\eta(e)$. Так как $|H| \cdot tr(e) = 1$ и $\tau(e) = \eta(e) tr(e) \in I$, то отсюда следует, что $\tau(e) = 1$.

Лемма доказана полностью.

Примечание 1. Линейный характер ψ в правой части (21) не является произвольным. Как было отмечено выше, функция ψ является постоянной на классах сопряженных элементов группы G . Следовательно, $\psi(g^{-1}xg) = \psi(x)$ для любых $x \in N$, $g \in G$. Обозначив через ψ^g линейный характер группы N , определяемый соотношением $\psi^g(x) = \psi(g^{-1}xg)$, мы будем иметь $\psi^g = \psi$. Характеры группы N , обладающие этим свойством, назовем инвариантными. Инвариантность линейного характера ψ является необходимым и достаточным условием для того, чтобы подгруппа H , определяемая нормальным делителем N группы G и ее линейным характером ψ , являлась S -подгруппой группы $U(G)$.

Примечание 2. Если e — идемпотент кольца KG , то, очевидно, $\varepsilon(e) = 1$, либо $\varepsilon(e) = 0$. Если идемпотент e , фигурирующий в условии леммы 2, относится к первому типу, то соответствующий ему линейный характер ψ совпадает с главным характером ψ_0 подгруппы N и, следовательно, $H = N$. Действительно, из (21) следует

$$\varepsilon(e) = \frac{1}{|N|} \sum_{g \in N} \psi(g) = \begin{cases} 1, & \text{если } \psi = \psi_0 \\ 0, & \text{если } \psi \neq \psi_0 \end{cases}$$

Таким образом, если e — идемпотент центра кольца KG , удовлетворяющий условиям $\varepsilon(e) = \tau(e) = 1$, то $e = j_N$, где $N \triangleleft G$ и $|N| = \eta(e)$.

Обратимся теперь к доказательству теоремы 2. Пусть H — S -подгруппа группы $V(G)$. Тогда в силу утверждения 2^о леммы 2 j_H есть идемпотент центра кольца KG , причем $\tau(j_H) = 1$. Кроме того, так как $H \subset V(G)$, то $\varepsilon(j_H) = 1$. Поэтому (см. примечание 2) идемпотенту j_H однозначно соответствует нормальный делитель N группы G , обладающий тем свойством, что $j_H = j_N$. Так как (см. вторую часть доказательства леммы 2) $\eta(j_H) = |H|$, $\eta(j_N) = |N|$, то $|H| = |N|$. Если, в частности, $H \triangleleft G$, то, очевидно, $N = H$.

Таким образом, получено отображение $H \rightarrow N = H^\sigma$ множества $\mathfrak{S}$ S -подгрупп группы $V(G)$ на множество $\mathfrak{N}$ нормальных делителей группы G , обладающее следующими свойствами:

- 1) $j_{H^\sigma} = j_H$;
- 2) $|H^\sigma| = |H|$;
- 3) если $H \triangleleft G$, то $H^\sigma = H$.

Если H_1 и H_2 — S -подгруппы группы $V(G)$ и $H_1 \subset H_2$, то, как легко показать ([4], лемма 2),

$$j_{H_1} j_{H_2} = j_{H_2}. \quad (22)$$

Отсюда вытекает, так как $j_{H_i} = j_{H_i^\sigma}$ ($i = 1, 2$),

$$j_{H_1^\sigma} j_{H_2^\sigma} = j_{H_2^\sigma}. \quad (23)$$

Поскольку $H_i^\sigma \triangleleft G$ ($i = 1, 2$), то в силу леммы 2 статьи [4] $j_{H_1^\sigma} j_{H_2^\sigma} = j_{H_1^\sigma H_2^\sigma}$.

Следовательно, $j_{H_1^\sigma H_2^\sigma} = j_{H_2^\sigma}$, откуда вытекает, что $H_1^\sigma H_2^\sigma = H_2^\sigma$. Это означает, что $H_1^\sigma \subset H_2^\sigma$. Таким образом, отображение σ является структурным гомоморфизмом множества $\mathfrak{S}$ на множество $\mathfrak{N}$. Так как $|H^\sigma| = |H|$ для каждой подгруппы $H \in \mathfrak{S}$, то σ — сильный структурный гомоморфизм.

Теорема 2, таким образом, доказана.

Следствие. Если G и H — конечные группы и $IG \cong IH$, то множества нормальных делителей групп G и H сильно структурно изоморфны.*

Доказательство. Очевидно, достаточно рассмотреть случай, когда $IG = IH$. При этом группу H можно пронормировать (не меняя таблицу умножения классов) так, чтобы имело место $H \subset V(G)$. Построенное выше отображение σ взаимно однозначно отображает множество $\mathfrak{N}_H$ нормальных делителей группы H на множество $\mathfrak{N}_G$ нормальных делителей группы G . Действительно, пусть $H_1, H_2 \in \mathfrak{N}_H$. В силу теоремы 2 $j_{H_i} = j_{H_i^\sigma}$, где $H_i^\sigma \in \mathfrak{N}_G$ ($i = 1, 2$).

Поэтому из $H_1^\sigma = H_2^\sigma$ вытекает $j_{H_1} = j_{H_2}$, откуда $H_1 = H_2$. Таким образом, σ взаимно однозначно отображает множество $\mathfrak{N}_H$ в $\mathfrak{N}_G$. Меняя ролями группы G и H , легко приходим к заключению, что σ отображает $\mathfrak{N}_H$ на $\mathfrak{N}_G$. Таким образом, σ индуцирует сильный структурный изоморфизм множества $\mathfrak{N}_H$ на множество $\mathfrak{N}_G$.

ЛИТЕРАТУРА

1. С. Д. Берман. О некоторых свойствах целочисленных групповых колец. ДАН СССР, т. XCI, № 1, 1953.
2. J. Kohn and D. Livingstone. On the structure of groups algebras, I. Canad. Journ. of Math., 17, № 4. (1965). 583—593.
3. Ван дер Варден. Современная алгебра, Гостехиздат, ч. II, М.—Л., 1947.
4. Э. М. Жмудь. О ядрах гомоморфизмов линейных представлений конечных групп. «Матем. сб.» 44, вып. 3. (1958), 353—408.

* Этот результат не нов: он является простым следствием доказанного С. Д. Берманом совпадения таблиц умножения классов сопряженных элементов групп G и H .

О ЦЕЛОЧИСЛЕННЫХ БИНАРНЫХ ЭРМИТОВЫХ ФОРМАХ НАД ТЕЛОМ КВАТЕРНИОНОВ

Л. Н. Пронин

Настоящая работа посвящена изучению бинарных эрмитовых форм над кольцом Q целых кватернионов (в дальнейшем мы будем называть такие формы для краткости Q -формами) и в смысле постановки задач и применяемой методики примыкает к арифметическим исследованиям Фату [1] и Умбера о целочисленных эрмитовых формах над мнимыми квадратичными полями.

§ 1. ТЕОРИЯ ПРИВЕДЕНИЯ Q -ФОРМ

Пусть K — тело кватернионов над полем рациональных чисел, Q — кольцо целых кватернионов тела K . Как известно [2], целые кватернионы имеют вид $\frac{1}{2}(a_1 \cdot 1 + a_2 i + a_3 j + a_4 k)$, где $a_i (i = 1, 2, 3, 4)$ принадлежат кольцу Z целых рациональных чисел и, кроме того, $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod{2}$.

Бинарной эрмитовой формой над кольцом Q (Q -формой) будем называть функцию кватернионных аргументов x, y

$$f(x, y) = [a, b, c] = xa\bar{x} + xb\bar{y} + y\bar{b}x + yc\bar{y},$$

где $a, c \in Z$, $b \in Q$ и черта обозначает сопряжение в теле K . Если, в частности, $x, y \in Q$, то $f(x, y) \in Z$. Величину $\Delta = b\bar{b} - ac$ назовем *определителем* формы f , а матрицу $F = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$ будем называть *матрицей* формы f .

Если преобразовать переменные x, y формы f линейной подстановкой $x = x'\alpha + y'\beta$, $y = x'\gamma + y'\delta$ с обратимой над телом K матрицей $B = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$, то форма f перейдет в некоторую бинарную эрмитовую форму f_1 над телом K с матрицей

$$F_1 = BFB^*, \quad (1)$$

где B^* — матрица, полученная из B транспонированием и сопряжением элементов. Если $f_1 = [a_1, b_1, c_1]$, то в силу (1) будем иметь

$$\begin{aligned} a_1 &= \alpha\bar{\alpha} + a\bar{\beta} + \gamma\bar{\beta} + c\bar{\gamma} = f(\alpha, \gamma), \\ b_1 &= \alpha\bar{\beta} + a\bar{\delta} + \gamma\bar{\delta} + c\bar{\delta}, \\ c_1 &= \beta\bar{\beta} + b\bar{\delta} + \delta\bar{\beta} + \delta\bar{\delta} = f(\beta, \delta). \end{aligned} \quad (2)$$

В обозначениях мы не будем делать различия между преобразованиями переменных и их матрицами. В случае, если форма f_1 получена из f преобразованием B , будем писать $f_1 = f^B$ или $f \xrightarrow{B} f_1$.

В дальнейшем нас будут интересовать преобразования, матрицы которых обратимы над Q . Такие преобразования образуют некоторую подгруппу U в группе обратимых матриц второго порядка над телом K . Назовем Q -формы f и f_1 эквивалентными, если существует матрица $A \in U$ такая, что $f_1 = f^B$. Легко видеть, что введенное таким образом отношение эквивалентности обладает всеми свойствами равенства, и, следовательно, множество всех Q -форм разбивается на классы эквивалентных Q -форм.

Теорема 1.1. *Определители эквивалентных Q -форм равны.*

Доказательство. Пусть $f_1 = f^B$, $B \in U$. Заметим, что кольцо Q является кольцом главных идеалов; более того, в нем имеет место алгоритм Эвклида. Известно, что любую матрицу над таким кольцом можно представить в виде произведения матриц, отвечающих элементарным операциям над строками и столбцами данной матрицы, и некоторой диагональной матрицы. Поэтому матрицу B можно представить в виде произведения матриц вида $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ и $\begin{pmatrix} \varepsilon & 0 \\ 0 & \eta \end{pmatrix}$, где ε, η — единицы кольца Q ; $t, u \in Q$. Используя формулы (2), легко проверить, что ни одна из этих матриц не меняет определителя формы. Теорема тем самым доказана.

В силу теоремы 1.1 множество Q -форм заданного определителя распадается на классы эквивалентных Q -форм.

Лемма 1.1. (Гурвиц [2]). *Если $a \in Q$ и $m \in Z$, $m \neq 0$, то $a = mb + r$, где $b, r \in Q$, причем норма $N(r)$ элемента r в теле K удовлетворяет условию*

$$N(r) \leq \frac{13}{16} N(m).$$

Назовем Q -форму $f = [a, b, c]$ приведенной, если ее коэффициенты удовлетворяют условию

$$\frac{16}{13} N(b) \leq N(a) \leq N(c). \quad (3)$$

Лемма 1.2. *Каждая Q -форма эквивалентна некоторой приведенной Q -форме.*

Доказательство. Пусть $f = [a_0, b_1, a_1]$ — произвольная Q -форма. Применяя к форме f преобразование $B = \begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix}$, $t \in Q$ получим

$$f^B = [a_1, \bar{b}_1 + a_1 \bar{t}, a_2] = [a_1, b_2, a_2].$$

Применяя лемму 1.1, при подходящем выборе t будем иметь $N(b_2) \leq N(a_1)$. Продолжив этот процесс, получим последовательность эквивалентных форм

$$[a_0, b_1, a_1] \xrightarrow{B_1} [a_1, b_2, a_2] \xrightarrow{B_2} [a_2, b_3, a_3] \xrightarrow{B_3} \dots,$$

для которых при всех $k = 1, 2, \dots$ выполняется условие $N(b_{k+1}) \leq \frac{13}{16} N(a_k)$. В этой последовательности найдется форма $[a_i, b_{i+1}, a_{i+1}]$, для которой $|a_i| \leq |a_{i+1}|$. Действительно, в противном случае мы имели бы бесконечную цепочку неравенств

$$|a_1| > |a_2| > |a_3| > \dots,$$

что невозможно. Форма $[a_i, b_{i+1}, a_{i+1}]$ является приведенной и эквивалентна форме f .

Из леммы 1.2 легко вытекает основная теорема теории приведения.

Теорема 1.2. *Существует лишь конечное число классов эквивалентных Q -форм заданного определителя $\Delta \neq 0$.*

Доказательство. Пусть $f = [a, b, c]$ — Q -форма определителя Δ . В силу леммы 1.2 можно считать f приведенной формой. Если $\Delta > 0$, то $ac < 0$, и, следовательно, $|ac| \leq \Delta$. Если же $\Delta < 0$, то $ac > 0$. В этом случае имеем

$$-\frac{16}{13}\Delta = ac - \frac{16}{13}N(b) + \frac{3}{13}ac,$$

откуда $-\frac{16}{13}\Delta \geq ac$. Следовательно, $|ac| < 6|\Delta|$. Таким образом, всегда

$$N(b) < |ac| < 6|\Delta|. \quad (4)$$

Справедливость утверждения теоремы теперь следует из конечности числа возможных комбинаций элементов a, b и c , удовлетворяющих условию (4).

Рассмотрим в виде примера случай $\Delta = -1$. В силу (3) и (4) существует лишь четыре типа приведенных форм:

- I. $f = [1, 0, 1]$;
- II. $f = [2, b, 2]$; где $N(b) = 3$
- III. $f = [-1, 0, -1]$;
- IV. $f = [-2, b, -2]$.

Легко видеть, что формы типа II эквивалентны форме I. Действительно, из $b \in Q$, $N(b) = 3$ вытекает $b \equiv \varepsilon \pmod{2}$, где ε — единица кольца Q . С помощью приема, использованного при доказательстве леммы 1.2, преобразуем форму $[2, b, 2]$ к форме $[2, \varepsilon, 1]$, которая в свою очередь преобразуется к форме $[1, 0, 1]$. Аналогично доказывается, что формы типа IV эквивалентны форме III. Отсюда вытекает, в частности, что существует лишь один класс эквивалентных положительно определенных Q -форм определителя $\Delta = -1$. Представителем этого класса является, например, форма $[1, 0, 1]$.

§ 2. О ПРЕДСТАВЛЕНИИ ЦЕЛЫХ ЧИСЕЛ Q -ФОРМАМИ

Начиная с этого момента, мы будем рассматривать лишь положительно определенные Q -формы. Если форма $[a, b, c]$ положительно определена, то $a, c > 0$ и $\Delta < 0$.

Пару $\{x, y\}$ элементов кольца Q назовем *представлением* целого положительного числа t формой f , если $f(x, y) = t$. Представление $\{x, y\}$ числа t называется *собственным*, если $(x, y)_l = 1$, где $(x, y)_l$ — левый общий наибольший делитель элементов x и y в кольце Q . Если число t представляется формой f , то оно представляется также всеми формами эквивалентными f .

Преобразование $B \in U$ назовем *автоморфизмом* формы f , если $f^B = f$. Множество автоморфизмов формы f является подгруппой группы U . Группы автоморфизмов эквивалентных форм изоморфны. Порядок группы автоморфизмов формы f в случае его конечности будем обозначать через $t(f)$. Положительно определенные формы имеют, очевидно, конечные группы автоморфизмов. Величину $\frac{1}{t(f)}$ будем называть *измерением* формы f , равно, как и класса, к которому принадлежит f ; будем называть эту величину также *измерением* любого представления числа t формой f .

Пусть S — полная система представителей классов эквивалентных положительно определенных Q -форм определителя Δ , $v_f(t)$ — количество всех представлений числа t формой $f \in S$, $v_f^*(t)$ — количество собственных

представлений числа m формой f . Очевидно, $v_f(m)$ и $v'_f(m)$ не зависят от выбора представителя f в соответствующем классе эквивалентных форм. Обозначим далее через $M(S, m)$ и $M'(S, m)$ соответственно сумму измерений всех представлений числа m и сумму измерений собственных представлений числа m системой Q -форм S :

$$M(S, m) = \sum_{f \in S} \frac{v_f(m)}{t(f)},$$

$$M'(S, m) = \sum_{f \in S'} \frac{v'_f(m)}{t(f)}.$$

В дальнейшем будет использовано также следующее обозначение: пусть $S' \subseteq S$, тогда $M(S', m) = \sum_{f \in S'} \frac{v_f(m)}{t(f)}$.

Теорема 2.1. Если $(m, 2\Delta) = 1$, то

$$M'(S, m) = \frac{m^3}{24} \sum_{d|m} \frac{\mu(d)}{d^2}, \quad (1)$$

где μ — функция Мебиуса.

Доказательство. Пусть $B = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in U$. Тогда $(\alpha, \gamma)_l = 1$. Наоборот, если $\alpha, \gamma \in Q$ и $(\alpha, \gamma)_l = 1$, то существует матрица $B \in U$, в которой α и γ образуют первую строку. Действительно, используя алгоритм Эвклида для элементов α и γ , путем ряда элементарных преобразований над строками и столбцами мы приведем единичную матрицу к матрице, в первой строке которой стоят элементы α и γ .

Сопоставим с каждым собственным представлением $\{x, y\}$ числа m формой $f \in S$ множество $U_{x,y}$ всех матриц группы U , имеющих вид $\begin{pmatrix} \alpha y \\ \beta \delta \end{pmatrix}$.

Легко проверить, что если $B, B' \in U_{x,y}$ и $B = \begin{pmatrix} x & y \\ \beta & \delta \end{pmatrix}$, $B' = \begin{pmatrix} x & y \\ \beta' & \delta' \end{pmatrix}$, то

$$\beta' = \varepsilon\beta + tx, \quad \delta' = \varepsilon\delta + ty, \quad (2)$$

где ε — единица кольца Q , $t \in Q$.

Если $B \in U_{x,y}$, то $f^B = [m, b, c]$, где $b \in Q$ и

$$N(b) \equiv \Delta \pmod{m}. \quad (3)$$

Два решения b и b' сравнения (3) будем называть *однотипными*, если $b' \equiv b\varepsilon \pmod{m}$, ε — некоторая единица кольца Q .

С помощью (2) легко показать, что если $f^B = [m, b, c]$, где $B \in U_{x,y}$, то тип решения b сравнения (3) не зависит от подстановки B , и вполне определяется, следовательно, формой f и представлением $\{x, y\}$ числа m этой формой.

Таким образом, каждому собственному представлению $\{x, y\}$ числа m формой f однозначно соответствует некоторый тип Γ решений сравнения (3). Будем говорить, что представление $\{x, y\}$ определяет тип Γ . При этом каждому представителю b типа Γ соответствует одна и только одна подстановка $B \in U_{x,y}$, переводящая форму f в форму $[m, b, c]$ определителя Δ .

Отсюда следует, что количество собственных представлений числа m заданной формой $f \in S$, определяющих заданный тип Γ решений сравне-

ния (3), равно количеству подстановок $B \in U$, переводящих форму f в форму $[m, b, c]$, где $b \in \Gamma$, $c = \frac{N(b) - \Delta}{m}$. Легко видеть, что это число равно либо нулю, либо $t(f)$.

Пусть теперь Γ — заданный тип решений сравнения (3) и $b \in \Gamma$. Так как формой $[m, b, c]$ определителя Δ , однозначно определяется эквивалентная ей форма $f \in S$, то количество собственных представлений числа m системой форм S , определяющих тип Γ , равно $t(f)$. Поэтому $M'(S, m)$ равно числу типов решений сравнения (3).

Пусть $(m, 2\Delta) = 1$, $m \neq 1$ и

$$b(\varepsilon_1 - \varepsilon_2) \equiv 0 \pmod{m}, \quad (4)$$

где b — решение сравнения (3), $\varepsilon_1, \varepsilon_2$ — единицы кольца Q . Можно полагать, что $N(b) < m^2$. Из (4) следует, что $N(b)N(\varepsilon_1 - \varepsilon_2) = nm^2$, где $n \in \mathbb{Z}$, $n > 0$. Легко проверить, что $N(\varepsilon_1 - \varepsilon_2)$ может принимать лишь значения 0, 1, 2, 3, 4, а отсюда в силу (3) вытекает, что $\varepsilon_1 = \varepsilon_2$. Так как число единиц кольца Q равно 24, то отсюда следует, что каждый тип решений сравнения (3) распадается на 24 класса вычетов $\bmod m$.

Итак,

$$M'(S, m) = \frac{1}{24} h(m), \quad (5)$$

где $h(m)$ — количество решений сравнения (3).

Ввиду нечетности m сравнение (3) равносильно сравнению в целых числах

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv \Delta \pmod{m} \quad (6)$$

и количество несравнимых по $\bmod m$ решений сравнения (3) равно числу несравнимых между собой решений сравнению (6).

Легко видеть, что

$$mh(m) = \sum_{\substack{x_1, x_2, x_3, x_4, s=0 \\ s=0}}^{m-1} e^{2\pi i t \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2 - \Delta}{m} s}.$$

Функция $h(m)$ обладает следующими свойствами:

I. $h(m_1 \cdot m_2) = h(m_1)h(m_2)$, если $(m_1, m_2) = 1$

II. $h(p^2) = p^3 h(p^{2-1})$, $\alpha > 1$, $(p, 2\Delta) = 1$, p — простое число.

Доказательство свойства I функции $h(m)$ не представляет затруднений, и мы докажем лишь свойство II.

Пусть для некоторых целых y_i ($i = 1, 2, 3, 4$) имеет место сравнение

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv \Delta \pmod{p^{2-1}}.$$

Будем искать решение сравнения (6) при $m = p^2$ в виде $x_i = y_i + p^{2-1}z_i$ ($i = 1, 2, 3, 4$), где $z_i \in \mathbb{Z}$. Имеем

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 + 2p^{2-1}(y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4) - \Delta = \\ = \lambda p^{2-1} + 2p^{2-1}(y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4) \equiv 0 \pmod{p^2}. \end{aligned}$$

После сокращения на p^{2-1} получаем

$$\lambda + 2(y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4) \equiv 0 \pmod{p}.$$

Так как одно из чисел y_i (для определенности положим, что y_1) не делится на p , то по произвольному набору z_2, z_3, z_4 среди вычетов $\bmod p$ последнее уравнение определяется однозначно по $\bmod p$ число z_1 . Таким образом, каждому решению сравнения (6) при $m = p^{2-1}$ отвечает p^3 решений сравнения (6) при $m = p^2$. Свойство II функции $h(m)$ тем самым доказано.

Свойства функции $h(m)$ позволяют свести ее вычисление к вычислению $h(p)$, где p — нечетное простое число. Вычислим $h(p)$:

$$ph(p) = \sum_{s=0}^{p-1} e^{-2\pi i \frac{\Delta s}{p}} \left(\sum_{x=0}^{p-1} e^{2\pi i \frac{x^2}{p}} s \right)^4 = p^4 + \sum_{s=1}^{p-1} e^{-2\pi i \frac{\Delta s}{p}} p^2 = p^4 - p^2. \quad (7)$$

При вычислении мы воспользовались значением модуля гауссовой суммы и условием $(p, \Delta) = 1$.

Возвращаемся к вычислению величины $h(m)$ в общем случае. Полагая $m = \prod_{p|m} p^{2p}$, получим, пользуясь доказанными свойствами функции $h(m)$ и соотношением (7),

$$h(m) = \prod_{p|m} h(p^{2p}) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2} \right) = m^3 \sum_{d|m} \frac{\mu(d)}{d^2}.$$

Так как для $m = 1$ справедливость равенства (1) проверяется непосредственно, то теорема доказана полностью.

Теорема 2.2 Если $(m, 2\Delta) = 1$, то

$$M(S, m) = \frac{1}{2^4} \chi(m), \quad (8)$$

где $\chi(m)$ — сумма кубов делителей числа m .

Доказательство. Пусть $\{x, y\}$ — представление числа m формой f и $(x, y)_l = 1$, т. е. $x = px_1$, $y = py_1$ и $(x_1, y_1)_l = 1$. Тогда $\{x_1, y_1\}$ является собственным представлением числа $\frac{m}{N(p)}$ формой f . Таким образом, каждому делителю d числа m отвечает $\psi(d) \nu_f\left(\frac{m}{d}\right)$ представлений числа m формой f , где $\psi(d)$ — количество неассоциированных слева решений уравнения $N(p) = d$ в кольце Q . Известно [3], что $\psi(d)$ равно сумме $\zeta(d)$ нечетных делителей числа d , что в силу нечетности m равно сумме делителей $\zeta(d)$ числа d . Следовательно,

$$\nu_f(m) = \sum_{d|m} \zeta(d) \nu_f\left(\frac{m}{d}\right).$$

Отсюда, используя (5), получаем

$$\begin{aligned} M(S, m) &= \sum_{f \in S} \frac{1}{i(f)} \sum_{d|m} \zeta(d) \nu_f\left(\frac{m}{d}\right) = \\ &= \sum_{d|m} \zeta(d) M'\left(S, \frac{m}{d}\right) = \frac{1}{2^4} \sum_{d|m} \zeta(d) h\left(\frac{m}{d}\right)^*. \end{aligned} \quad (9)$$

Определим на множестве F функций целочисленного аргумента операцию умножения, полагая для функций $f, g \in F$

$$(f * g)(m) = \sum_{d|m} f(d) g\left(\frac{m}{d}\right).$$

По отношению к операции обычного сложения и введенной операции умножения множество F является коммутативно-ассоциативным кольцом. Функция $e(m)$, равная единице, если $m = 1$, и нулю, если $m \neq 1$, яв-

* Соотношение $M(S, m) = \sum_{d|m} \zeta(d) M'\left(S, \frac{m}{d}\right)$ верно также при четном m .

ляется единичным элементом этого кольца. Очевидно, $e = 1 * \rho$, где через 1 обозначена функция, тождественно равная единице, и ρ — функция Мебиуса. Легко проверить, что если функция f вполне мультипликативна, то имеет место соотношение $f * f \cdot g = f \cdot (1 * g)$, где точкой обозначена операция обычного умножения функций.

Из равенства (9) вытекает: $M(S, m) = \frac{1}{24}(\zeta * h)(m)$. Замечая, что $\zeta = 1 * m$ и $h = m \cdot (\rho * m^2)$, находим

$$\zeta * h = 1 * m * m \cdot (\rho * m^2) = 1 * m (1 * \rho * m^2) = 1 * m^3 = \chi.$$

Теорема доказана.

Отметим один частный результат, вытекающий из теоремы 2.2. В конце § 1 мы установили, что все положительно определенные Q -формы определителя $\Delta = -1$ эквивалентны форме $f = [1, 0, 1]$. Нетрудно показать, что элементами группы автоморфизмов формы f являются матрицы вида $\begin{pmatrix} \varepsilon & 0 \\ 0 & \eta \end{pmatrix}$, $\begin{pmatrix} 0 & \varepsilon \\ \eta & 0 \end{pmatrix}$, где ε и η — единицы кольца Q . Порядок $t(f)$ этой группы равен $2 \cdot 24^2 = 1152$. В применении к этому случаю формула (8) приводит к следующему выражению для количества $v_f(m)$ представлений числа m формой f :

$$v_f(m) = 48\chi(m). \quad (10)$$

Соотношение (10) равносильно следующему утверждению:

Теорема 2.3. Пусть m нечетно и N_1 — количество представлений числа m в виде суммы восьми квадратов целых чисел; N_2 — количество представлений числа m в виде суммы $x_1^2 + x_2^2 + x_3^2 + \frac{1}{4}(y_1^2 + y_2^2 + y_3^2 + y_4^2)$, где $x_i, y_i \in \mathbb{Z}$ и $y_i \equiv 1 \pmod{2}$ ($i = 1, 2, 3, 4$); N_3 — количество представлений числа m в виде $\frac{1}{4}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + y_1^2 + y_2^2 + y_3^2 + y_4^2)$, где $x_i \equiv y_i \equiv 1 \pmod{2}$ ($i = 1, 2, 3, 4$). Тогда

$$N_1 + 2N_2 + N_3 = 48\chi(m).$$

Теорема 2.4. Если $(m, \Delta) = 1$, $m = 2^\alpha m'$, $\alpha > 0$, m' нечетно, то

$$M(S, m) = \frac{12 \cdot 2^{3\alpha} - 5}{168} \bar{\chi}(m), \quad (11)$$

где $\bar{\chi}(m)$ — сумма кубов нечетных делителей числа m .

Доказательство. Покажем сначала, что свойство II функции $h(m)$, введенной при доказательстве теоремы 2.2, остается справедливым при $p = 2$, если Δ нечетно. Известно [3], что элементы $\omega_1 = \frac{1}{2}(1 + i + j + k)$, $\omega_2 = \frac{1}{2}(1 - i + j + k)$, $\omega_3 = \frac{1}{2}(1 + i - j + k)$, $\omega_4 = \frac{1}{2}(1 + i + j - k)$ образуют целочисленный базис кольца Q . Каждый элемент из Q единственным образом представляется в виде целочисленной комбинации элементов этого базиса.

Полагая в сравнении (3) $b = \sum_{i=1}^4 x_i \omega_i$, приведем его к равносильному сравнению в целых рациональных числах

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1 x_2 + x_1 x_3 + x_1 x_4 \equiv \Delta \pmod{m}.$$

Проводя теперь для $p = 2$ рассуждения по той же схеме, что и в общем случае, приходим к соотношению

$$h(2^\alpha) = 2^3 h(2^{\alpha-1}), \quad (\alpha > 1). \quad (12)$$

Непосредственный подсчет показывает, что $h(2) = 12$.

Пусть $m = 2^\alpha m'$, $\alpha > 1$, m' нечетно и $(m, \Delta) = 1$. Покажем, что

$$M'(S, m) = \frac{1}{24} h(m). \quad (13)$$

С этой целью необходимо лишь проверить, что два решения $b\varepsilon_1$ и $b\varepsilon_2$ сравнения (3) одного типа несравнимы по $\text{mod } m$ в кольце Q , если $\varepsilon_1 \neq \varepsilon_2$. Проверка этого факта аналогична проделанной при доказательстве теоремы 2.1 и поэтому опускается.

Если $m = 2$, то

$$M'(S, 2) = \frac{1}{2} = \frac{1}{24} h(2), \quad (14)$$

Так как $M(S, m) = \sum_{d|m} \zeta\left(\frac{m}{d}\right) M'(S, d)$ (см. сноску на стр. 12), то

в силу (8), (12), (13) и (14) имеем

$$\begin{aligned} M(S, m) &= \frac{1}{24} \sum_{d|m, d \text{ нечет}} h(d) \zeta\left(\frac{m}{d}\right) + \frac{1}{24} h(2) \sum_{d|m, d \text{ нечет}} h(d) \zeta\left(\frac{m'}{d}\right) + \dots + \\ &+ \frac{1}{24} h(2^\alpha) \zeta\left(\frac{m'}{d}\right) = \frac{1}{24} [1 + h(2) + \dots + \\ &+ h(2^\alpha)] \chi(m') = \frac{12 \cdot 2^{3\alpha} - 5}{168} \bar{\chi}(m). \end{aligned}$$

Формула (11) тем самым доказана.

Если $\Delta = -1$, $f = [1, 0, 1]$, формула (11) дает

$$v_f(m) = \frac{48(12 \cdot 2^{3\alpha} - 5)}{7} \bar{\chi}(m). \quad (15)$$

Соотношение (15) равносильно такому утверждению (при сохранении обозначений теоремы 2.3).

Теорема 2.5. Если $m = 2^\alpha m'$, $\alpha > 0$, m' нечетно, то

$$N_1 + 2N_2 + N_3 = \frac{48(12 \cdot 2^{3\alpha} - 5)}{7} \bar{\chi}(m).$$

§ 3. ИЗМЕРЕНИЕ ПОЛНОЙ СИСТЕМЫ КЛАССОВ ЭКВИВАЛЕНТНЫХ СОБСТВЕННО-ПРИМИТИВНЫХ ПОЛОЖИТЕЛЬНО ОПРЕДЕЛЕННЫХ Q-ФОРМ ОПРЕДЕЛИТЕЛЯ Δ

Во втором параграфе статьи было дано определение измерения класса эквивалентных Q-форм определителя Δ .

Измерением $M(H)$ множества H классов Q-форм назовем сумму измерений классов, входящих в H :

$$M(H) = \sum_{i \in S_H} \frac{1}{i(f)},$$

где S_H — некоторая полная система представителей классов множества H .

Назовем форму $[a, b, c]$ *собственно-примитивной*, если наибольший общий делитель элементов a, b и c в кольце Z равен единице: $(a, b, c)_Z = 1$. Очевидно, собственная примитивность формы есть инвариант отношения эквивалентности.

Целью настоящего параграфа является вывод формул для измерения $M(S_e)$ полной системы S_e классов собственно-примитивных эквивалентных положительно определенных Q -форм определителя Δ . Основную роль при этом будут играть соотношения (8) и (11) предыдущего параграфа.

Лемма 3.1. Пусть $\Delta \neq 2\Delta'$, где Δ' нечетно. Собственно-примитивная форма $f = [a, b, c]$ определителя Δ представляет число взаимно простое с Δ .

Доказательство. Пусть $p \neq 2$ простое число. Если p делит a и c , то p не делит хотя бы одно из чисел $b + \bar{b}, i\bar{b} - bi, j\bar{b} - bj, k\bar{b} - bk$. Если, например, p не делит $i\bar{b} - bi$, то $f(1, -i) \not\equiv 0 \pmod{p}$. Если p не делит a или c , то $f(1, 0)$ или $f(0, 1) \not\equiv 0 \pmod{p}$. Отсюда следует, что f представляет числа взаимно простые с наперед заданным нечетным числом, в частности с Δ , если Δ нечетно.

Пусть $\Delta \equiv 0 \pmod{4}$. Из $(a, b, c)_Z = 1$ тогда вытекает $(a, 2b, c)_Z = 1$. Поэтому если $p = 2$, то одно из чисел a и c не делится на p . Следовательно, в этом случае форма f представляет числа взаимно простые с любым заданным числом. Лемма доказана.

Лемма 3.2: Все пары $\{x, y\}$ элементов кольца Q , для которых $f(x, y, \Delta) \neq 1$, распределяются по нескольким парам арифметических прогрессий вида $\{x^{(k)} + \Delta\xi, y^{(k)} + \Delta\eta\}$ ($k = 1, 2, \dots, l(f)$), где $x^{(k)}, y^{(k)} \in Q$, ξ и η пробегают кольцо Q .

Доказательство этой леммы, ввиду его простоты, мы опускаем.

Пусть t — положительное вещественное число. Рассмотрим совокупность всех пар $\{x, y\}$ элементов кольца Q , удовлетворяющих условиям

$$f(x, x) \leq t, (f(x, y), \Delta) = 1 \quad (1)$$

В силу леммы 3.2 пары $\{x, y\}$, удовлетворяющие условиям (1), содержатся в парах арифметических прогрессий $\{x^{(k)} + \Delta\xi, y^{(k)} + \Delta\eta\}$ ($k = 1, 2, \dots, l(f)$). Каждой паре прогрессий $\{x^{(k)} + \Delta\xi, y^{(k)} + \Delta\eta\}$ отвечают четыре восьмимерные решетки с шагом $D = -\Delta$, ввиду того, что для коэффициентов каждого из кватернионов ξ, η имеются две возможности: 1) все коэффициенты целые, 2) все коэффициенты — половины нечетных чисел. Неравенство $f(x, y) \leq 1$, где x, y — кватернионы с вещественными коэффициентами определяет в восьмимерном евклидовом пространстве ограниченную область $V(f)$. Легко видеть, что число точек каждой решетки, определяемой парой прогрессий $\left\{\frac{1}{\sqrt{t}}(x^{(k)} + \Delta\xi), \frac{1}{\sqrt{t}}(y^{(k)} + \Delta\eta)\right\}$, принадлежащих области $V(f)$, помноженное на объем одной ячейки, асимптотически при $t \rightarrow \infty$ равно объему $v(f)$ области $V(f)$. Если $\lambda^{(k)}(t, f)$ число указанных точек всех четырех решеток, то $\frac{1}{4} \left(\frac{D}{\sqrt{t}}\right)^8 \lambda^{(k)}(t, f)$ асимптотически равно

объему $v(f)$. Полагая $\lambda(t, f) = \sum_{k=1}^{l(f)} \lambda^{(k)}(t, f)$, найдем

$$\lim_{t \rightarrow \infty} \frac{D^8}{4t^4} \lambda(t, f) = l(f) v(f).$$

Ниже будет показано, что $l(f)$ и $v(f)$ не зависят от формы f определителя Δ . Полагая $l(f) = l$, $v(f) = v$, получим

$$\lim_{t \rightarrow \infty} \frac{D^8}{4t^4} \lambda(t, f) = lv.$$

С другой стороны, $\lambda(t, f) = \sum_{m < t, (m, D) = 1} \nu_f(m)$. Таким образом,

$$\lim_{t \rightarrow \infty} \frac{D^3}{4t^4} \sum_{m < t, (m, D) = 1} \nu_f(m) = lv.$$

Разделим обе части последнего равенства на $t(f)$ и просуммируем екак по всем собственным-примитивным формам из системы S . Принимая внимание то обстоятельство, что число m взаимно простое с Δ может представлять лишь собственным-примитивные формы, получим

$$\lim_{t \rightarrow \infty} \frac{D^3}{4t^4} \sum_{m < t, (m, D) = 1} M(S, m) = lv M(S_e)$$

Соотношения (2) и (8), § 2, при $\Delta \equiv 0 \pmod{4}$ дают

$$\lim_{t \rightarrow \infty} \frac{D^3}{96t^4} \sum_{m < t, (m, D) = 1} \chi(m) = lv M(S_e)$$

Обозначим через $\varphi(k|x)$ количество натуральных чисел, взаимно простых с $k \in \mathbb{Z}$, $k > 0$ и не превосходящих положительного числа x . В частности, когда $x = k$, $\varphi(k|x)$ превращается в обычную функцию Эйлера $\varphi(k)$. Легко показать, что

$$\varphi(k|x) = \sum_{d|k} \mu(d) \left[\frac{x}{d} \right],$$

где $\left[\frac{x}{d} \right]$ — символ целой части. С помощью функции $\varphi(k|x)$ преобразуем сумму, стоящую в левой части (3):

$$\begin{aligned} \sum_{m < t, (m, D) = 1} \chi(m) &= \sum_m \sum_{d|m} d^3 = \sum_{d < t, (d, D) = 1} d^3 \varphi\left(D \left| \frac{t}{d} \right.\right) = \\ &= \sum_{\delta|D} \mu(\delta) \sum_{d < \frac{t}{\delta}, (d, D) = 1} d^3 \left[\frac{t}{d\delta} \right] = \sum_{\delta|D} \mu(\delta) G_\delta(t), \end{aligned}$$

где $G_\delta(t) = \sum_d d^3 \left[\frac{t}{d\delta} \right]$. Пусть $a_1, a_2, \dots, a_{\varphi(D)}$ натуральные числа, превосходящие D и взаимно простые с ним. Тогда

$$G_\delta(t) = \sum_{i=1}^{\varphi(D)} G_\delta^{(i)}(t),$$

где

$$G_\delta^{(i)}(t) = \sum_{d < \frac{t}{\delta}, d \equiv a_i \pmod{D}} d^3 \left[\frac{t}{d\delta} \right] = \sum_n (a_i + Dn)^3 \left[\frac{t}{(a_i + Dn)\delta} \right].$$

Имеем

$$\begin{aligned} \frac{1}{t^4} G_\delta^{(i)}(t) &= \frac{1}{D\delta^4} \sum_n \frac{(a_i + Dn)^3 \delta^3}{t^3} \left[\frac{t}{(a_i + Dn)\delta} \right] \frac{D\delta}{t} = \\ &= \frac{1}{D\delta^4} \sum_n x_n^3 \left[\frac{1}{x_n} \right] (x_{n+1} - x_n), \end{aligned}$$

где $x_n = \frac{(a_i + Dn)\delta}{t}$. Отсюда вытекает

$$\lim_{t \rightarrow \infty} \frac{1}{t^4} G_\delta^{(i)}(t) = \frac{1}{D\delta^4} \int_0^1 x^3 \left[\frac{1}{x} \right] dx.$$

Полагая $x = z^{-1}$, получаем

$$\int_0^1 x^3 \left[\frac{1}{x} \right] dx = \int_1^\infty \frac{[z]}{z^5} dz = \frac{1}{4} \sum_{k=1}^{\infty} k \left\{ \frac{1}{k^4} - \frac{1}{(k+1)^4} \right\} = \frac{\pi^4}{360}.$$

Таким образом,

$$\lim_{t \rightarrow \infty} \frac{1}{t^4} G_{\delta}(t) = \frac{\pi^4 \varphi(D)}{360 D \delta^4}.$$

и, следовательно,

$$\begin{aligned} \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{m \leq t, (m, D)=1} \chi(m) &= \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{D \mid \delta} \mu(\delta) G_{\delta}(t) = \\ &= \frac{\pi^4 \varphi(D)}{360 D} \prod_{p \mid D} \left(1 - \frac{1}{p^4} \right). \end{aligned} \quad (4)$$

При Δ нечетном, подставляя значение $M(S, m)$ из (11), § 2, в левую часть равенства (2), получаем

$$\begin{aligned} A &= \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{m \leq t, (m, D)=1} M(S, m) = \frac{1}{24} \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{m \leq t, (m, 2D)=1} \chi(m) + \\ &+ \sum_{\alpha=1}^{\infty} \frac{12 \cdot 2^{3\alpha} - 5}{168} \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{2^{\alpha} m \leq t, (m, 2D)=1} \chi(m). \end{aligned}$$

Замечая, что

$$\lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{2^{\alpha} m \leq t, (m, 2D)=1} \chi(m) = \lim_{s \rightarrow \infty} \frac{1}{2^{4\alpha} s^4} \sum_{m \leq s, (m, 2D)=1} \chi(m) = \frac{1}{2^{4\alpha}} B,$$

где $B = \lim_{t \rightarrow \infty} \frac{1}{t^4} \sum_{m \leq t, (m, 2D)=1} \chi(m)$ легко вычисляется по формуле (4), на-
ходим

$$A = B \left(\frac{1}{24} + \sum_{\alpha=1}^{\infty} \frac{12 \cdot 2^{3\alpha} - 5}{168 \cdot 2^{4\alpha}} \right) = \frac{\pi^4 \varphi(2D)}{6480 D} \prod_{p \mid 2D} \left(1 - \frac{1}{p^4} \right). \quad (5)$$

Вычислим теперь объем $v(f)$ области восьмимерного пространства, определяемой неравенством $f(x, y) \leq 1$, которое мы представим в виде

$$N(ax + y\bar{b}) + DN(y) \leq a. \quad (6)$$

Полагая

$$x' = \frac{1}{\sqrt{a}}(ax + y\bar{b}); \quad y' = \sqrt{\frac{D}{a}} y, \quad (7)$$

приведем (6) к виду $N(x') + N(y') \leq 1$. Отсюда вытекает, что искомый объем равен произведению объема восьмимерного шара единичного радиуса на модуль Якобиана преобразования (7), рассматриваемого как преобразование восьмимерного пространства. Следовательно,

$$v(f) = \frac{\pi^4}{24 D^2} (= v). \quad (8)$$

Остается вычислить величину $l(f)$. Пусть $f = [a, b, c]$ — собственно-примитивная Q -форма определителя Δ . В силу леммы 3.1 можно считать, что $(a, D) = 1$. Так как $af(x, y) = N(ax + y\bar{b}) + DN(y)$, то условия $(f(x, y), D) = 1$ и $(N(ax + y\bar{b}), D) = 1$ равносильны. Рассмотрим мно-

жество пар $\{x, y\}$, где x, y независимо друг от друга пробегают некоторую полную систему вычетов $\text{mod } D$ в Q . Пары $\{x, y\}$, для которых $(f(x, y), D) = 1$, назовем *допустимыми*. Количество допустимых пар, очевидно, равно $l(f)$. Легко видеть, что каждому кватерниону y из полной системы вычетов $\text{mod } D$ отвечает только одно значение x из этой системы, обладающее тем свойством, что $ax + y\bar{b} \equiv \gamma \pmod{D}$, где $(N(\gamma), D) = 1$. Таким образом, количество допустимых пар равно

$$l(f) = D^4 f_Q(D) (= l), \quad (9)$$

где $f_Q(m)$, $m \in \mathbb{Z}$, есть количество классов вычетов $\text{mod } m$ элементов кольца Q , имеющих норму взаимно простую с m .

Функция $\varphi_Q(m)$ обладает следующими свойствами:

$$\text{I. } \varphi_Q(m_1 m_2) = \varphi_Q(m_1) \varphi_Q(m_2), \text{ если } (m_1, m_2) = 1.$$

$$\text{II. } \varphi_Q(p^\alpha) = p^4 \varphi_Q(p^{\alpha-1}), \text{ } p \text{ простое, } \alpha > 1.$$

Свойства I и II функции $\varphi_Q(m)$ позволяет свести ее вычисление к случаю, когда $m = p$, где p — простое число. Пусть сначала $p \neq 2$. Очевидно, $\varphi_Q(p)$ равно разности между количеством всех классов вычетов $\text{mod } p$ кольца Q и количеством классов вычетов $\text{mod } p$ элементов кольца Q , имеющих норму, делящуюся на p . Количество последних равно числу несоразимых по $\text{mod } p$ решений в кольце Z сравнения

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}.$$

Следовательно, $\varphi_Q(p) = p^4 - \frac{1}{p} \sum_{x_1, x_2, x_3, x_4, s=0}^{p-1} e^{2\pi i \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2 + s^2}{p}}$ откуда легко получаем

$$\varphi_Q(p) = p^4 - p^3 - p^2 + p = p^4 \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p}\right). \quad (10)$$

Что касается случая $m = 2$, то непосредственный подсчет дает: $\varphi_Q(2) = 12$.

Из (2), (4), (5), (8), (9) вытекает формула для измерения системы S_e всех классов собственно-примитивных Q -форм определителя Δ :

Теорема 3.1. Если $\Delta = -D \neq 2\Delta'$, где Δ' нечетно, то

$$M(S_e) = \begin{cases} \frac{D^2}{1152} \prod_{p|D} \left(1 + \frac{1}{p^2}\right), & \text{если } \Delta \text{ нечетно.} \end{cases} \quad (11')$$

$$M(S_e) = \begin{cases} \frac{D^2}{2304} \prod_{p|D, p \neq 2} \left(1 + \frac{1}{p^2}\right), & \text{если } \Delta \text{ четно.} \end{cases} \quad (11'')$$

Пусть теперь $\Delta = 2\Delta'$, где Δ' нечетно: S'_e — система всех классов Q -форм $[a, b, c]$ определителя Δ , удовлетворяющих условию $(a, 2b, c) = 1$; S''_e — система всех классов Q -форм $[a, b, c]$ определителя Δ , удовлетворяющих условию $(a, 2b, c)_Z = 2$; S'_e и S''_e — соответственно полные системы представителей классов множеств S'_e и S''_e . Очевидно,

$$S'_e \cup S''_e = S_e \quad (12)$$

Формы множества S'_e представляют целые числа взаимно простые с Δ . Если $(m, \Delta) = 1$, то в силу соотношения (8), § 2,

$$M(S'_e, m) = M(S, m) = \frac{1}{24} \chi(m).$$

Пользуясь методом, примененным выше при выводе соотношения (11"), находим

$$M(S'_e) = \frac{D^2}{2304} \prod_{p \mid D, p \neq 2} \left(1 + \frac{1}{p^2}\right) \quad (13)$$

Пусть $f \in S''_e$. Каждому собственному представлению $\{x, y\}$ числа $m = 2^\alpha m'$, где $\alpha > 1$, m' нечетно, формой f отвечает некоторый тип решений (см. § 2) сравнения

$$N(b) \equiv \Delta \pmod{m} \quad (14)$$

Легко видеть, что решения этого типа удовлетворяют вместе с тем сравнению

$$B(b) \equiv \Delta \pmod{2m} \quad (15)$$

Наоборот, каждому типу решений сравнения (14), удовлетворяющих также сравнению (15) отвечает по крайней мере одно собственное представление числа m одной и только одной из форм $f \in S''_e$ (f эквивалентна форме $[m, b, c]$, где $c = \frac{N(b) - \Delta}{m}$).

Решение b сравнения (14), удовлетворяющее также сравнению (15) назовем допустимым. Каждому типу допустимых решений сравнения (14) отвечает $t(f)$ собственных представлений числа m формой f . Следовательно, измерение множества собственных представлений числа m системой форм S''_e равно количеству типов допустимых решений сравнения (14).

Легко видеть, что каждый класс допустимого решения $b \pmod{m}$ сравнения (14) распадается на 16 классов $\pmod{2m}$. Таким образом, количество допустимых решений сравнения (14) равно 1/16 числа несравнимых по $\pmod{2m}$ решений сравнения (15).

В дальнейшем мы будем предполагать, что $(m, \Delta') = 1$. Как и выше, показывается, что в случае $m \neq 2$ количество типов допустимых решений сравнения (14) равно 1/24 числа его допустимых решений.

Найдем теперь число всех решений сравнения (15). Решение сравнения можно представить в виде $b = b'(1 + i)^*$, где b' является решением сравнения

$$N(b') \equiv \Delta' \pmod{m} \quad (16)$$

Наоборот, каждому решению b' сравнения (16) отвечает решение $b = b'(1 + i)$ сравнения (15). При этом, как легко проверить, каждому решению $b' \pmod{m}$ сравнения (16) отвечают четыре несравнимых по $\pmod{2m}$ решения сравнения (15). Таким образом, при $m \neq 2$ измерение множества собственных представлений числа m системой форм S''_e равно

$$M'(S''_e, m) = \frac{1}{96} h(m), \quad (17)$$

где $h(m)$ — количество решений сравнения (16).

* Элемент $1 + i$ является образующей двухстороннего идеала кольца Q .

Если $m = 2$, то

$$M'(S_e'', 2) = \frac{1}{8} = \frac{1}{96} h(2) \quad (18)$$

Используя (17) и (18), учитывая, что формы системы S_e'' представляют только четные числа, получаем

$$\begin{aligned} M(S_e'', m) &= \sum_{d \mid m, d, \text{ чет}} M'(S_e'', d) \bar{\zeta}\left(\frac{m}{d}\right) = \\ &= \sum_{k=1}^{\alpha} \sum_{d \mid m, d, \text{ нечет}} M'(S_e'', 2^k d) \bar{\zeta}\left(\frac{m}{2^k d}\right) = \\ &= \frac{1}{96} \sum_{k=1}^{\alpha} h(2^k) \sum_{d \mid m, m, \text{ нечет}} h(d) \bar{\zeta}\left(\frac{m}{d}\right) = \frac{2^{3\alpha} - 1}{56} \bar{\zeta}(m). \end{aligned} \quad (19)$$

Приведем без доказательства две леммы аналогичные леммам 3.1 и 3.2.

Лемма 3.3. Форма $f \in S_e''$ представляет число взаимно-простое с Δ' .

Лемма 3.4. Если $f \in S_e''$, то все пары $\{x, y\}$ элементов кольца Q , для которых $(f(x, y), \Delta') = 1$, распределяются по нескольким парам арифметических прогрессий вида $\{x^{(k)} + \Delta'\xi, y^{(k)} + \Delta'\eta\}$ ($k = 1, 2, \dots, l_1(f)$), $x^{(k)}, y^{(k)} \in Q$; ξ, η пробегают кольцо Q .

Подсчет величины $l_1(f)$ аналогичен проведенному выше подсчету величины $l(f)$. При этом оказывается, что

$$l_1(f) = (\Delta')^4 \varphi_Q(\Delta') (= l_1) \quad (20)$$

Таким образом $l_1(f)$ не зависит от формы $f \in S_e''$.

Применяя к формам множества S_e'' изложенный выше метод, приходим к следующему соотношению аналогичному (2)

$$\lim_{t \rightarrow \infty} \frac{(D')^8}{4t^4} \sum_{m \leq t, (m, D')=1} M(S_e'', m) = l_1 v M(S_e''). \quad (21)$$

где $D' = -\Delta'$.

С помощью (4) и (19) показываем, что левая часть (21) равна $\frac{\pi^4 (D')^7 \varphi(D)}{172800} \prod_{p \mid D} \left(1 - \frac{1}{p^4}\right)$. Используя (8) и (20), из (21) получаем

$$M(S_e'') = \frac{D^2}{7680} \prod_{p \mid D, p \neq 2} \left(1 + \frac{1}{p^2}\right). \quad (22)$$

Из (13) и (22), в силу (12), вытекает.

Теорема 3.2. Если $\Delta = -D = 2\Delta'$, где Δ' нечетно, то

$$M(S_e) = \frac{13D^2}{23040} \prod_{p \mid D, p \neq 2} \left(1 + \frac{1}{p^2}\right). \quad (23)$$

Тем самым вопрос об измерении полной системы классов собственно-примитивных форм определителя Δ полностью решен.

В заключение отметим, что формулы (11) и (23) настоящей статьи могут быть получены также с помощью чисто арифметических методов. Изложению этих результатов будет посвящена отдельная статья.

ЛИТЕРАТУРА

1. J. Faïou. Comptes Rendus, 142, Paris, 1900.
2. Hurwitz. Über die Zahlentheorie der Quaternionen. Math. Werke. II, Basel, 1933.
3. Б. Венков. Об арифметике кватернионов. Изв. АН СССР, (6), 16, 1922.