УДК 512.54

На правах рукописи

Грачев Евгений Владимирович

АЛГОРИТМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ В ТЕОРИИ ГРУПП, КОДИРОВАНИИ И КРИСТАЛЛОГРАФИИ

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Красноярск-2010

Работа выполнена в Новосибирском государственном техническом университете

Научный руководитель:

кандидат физико-математических наук,
доцент Ивлева Ася Михайловна

Официальные оппоненты:

доктор физико-математических наук,
доцент Бардаков Валерий Георгиевич

доктор физико-математических наук,
профессор Созутов Анатолий Ильич

Ведущая организация:

Государственное образовательное учреждение высшего профессионального образования "Новосибирский государственный педагогический университет"

Защита состоится 27 апреля 2010 г. в 14 часов на заседании диссертационного совета Д 212.099.02 в Сибирском федеральном университете по адресу: 660041, г. Красноярск, пр. Свободный, 79.

С диссертацией можно ознакомиться в библиотеке Сибирского федерального университета.

Автореферат разослан "____" марта 2010 г.

Ученый секретарь диссертационного совета _____ Бушуева Н.А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В предлагаемой работе с помощью методов компьютерной алгебры исследуются проблемы теории групп, криптографии и кристаллографии. В теории групп методы компьютерной алгебры были применены к изучению строения мультипликативной структуры групповых колец конечных групп малого порядка. Они использованы далее в изучении криптографической проблемы построения защищенных систем связи, основанных на строении конечных групповых колец. Кроме того, в кристаллографии диссертантом были получены новые подходы к изучению строения гидратных каркасов.

Начало изучения строения групповых колец и их мультипликативной структуры было положено в работах Г. Хигмана (1940). В них изучались групповые кольца абелевых групп, их мультипликативная структура и строение группы единиц групповых колец (т.е. группы обратимых элементов группового кольца).

Дальнейшые исследования групп единиц целочисленных групповых колец неабелевых групп основаны на их представлении группами матриц. Укажем на результаты J. Hughers, K.R. Pearson [7], которые описали группу единиц кольца ZS_3 следующим образом:

$$U(ZS_3) \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z) : a + c \equiv b + d (\mathrm{mod}\, 3) \right\}.$$

Аналогичное представление получили P.J. Allen, C.Hobby [1] для кольца ZA_4:

$$U(ZA_4) \cong \{\pm 1\} \times \{X \in SL_3(Z) : X = (x_{ij}) \ \text{ удовлетворяет (1), (2)}\},$$

$$X \equiv \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^i (\mathrm{mod}\, 2), i = 0, 1, 2; \tag{1}$$

$$x_{12} + x_{23} + x_{31} \equiv x_{13} + x_{21} + x_{32} \equiv 0 \pmod 4. \tag{2}$$

В работе E.G. Goodaire, E. Jespers, M.M.Parmenter [5] описаны единицы кольца ZG в случае, когда G – конечная группа, такая, что $G/Z(G) \cong C_2 \times C_2$ и G/G' и $Z(G)$ каждая имеют экспоненту 2,3,4 или 6. В

статье J. Ritter, S.K. Sehgal [10] описаны порождающие для подгрупп конечного индекса группы единиц целочисленного группового кольца ZG, где G принадлежит некоторому классу конечных групп, и приводят пример такой группы $G =< a, b, c : a^4 = [a, b] = [a, c] = 1, a^2 = b^2 = c^2 = [b, c] >$. Кроме того, C.P. Milies [9] описал группы единиц целочисленного группового кольца диэдральной группы восьмого порядка ZD_4 и доказал, что в ней существуют только 2 несопряженные максимальные подгруппы порядка 8. Отметим в заключение, что в работах Р.Ж. Алеева и его учеников изучены центральные единицы целочисленных групповых колец различных конечных групп.

Все эти результаты относятся к описанию порождающих групп единиц целочисленных групповых колец конкретных конечных групп. Они направлены на решение проблемы 17 из монографии S.K. Sehgal [12]: определить представления мультипликативных групп ZG^* различных конечных групп G.

Следует отметить значение для всей теории групповых колец проблемы изоморфизма, сформулированной уже Г.Хигманом: следует ли из изоморфизма групповых колец $ZG_1 \cong ZG_2$ изоморфизм самих групп $G_1 \cong G_2$?

Понятно, что для групповых колец с тривиальной группой единиц, ответ положительный, но Г. Хигман доказал, что и для конечных абелевых групп это так. Были получены положительные результаты во многих других частных случаях. Однако в общем случае ответ на проблему оказался отрицательный, M. Hertweck [6] показал, что существуют две неизоморфные конечные группы G_1 и G_2, групповые кольца которых ZG_1 и ZG_2 изоморфны.

В связи с проблемой изоморфизма для произвольных конечных групп G.H. Cliff, S.K. Sehgal и A.K. Weiss [3] поставили два вопроса.

1) Расщепляемо ли вложение $G \to V(ZG)$?

2) Если расщепляемо, то существует ли нормальное дополнение без кручения?

Отметим, что

$$V(ZG) = \{\sum \alpha_g g \in U(ZG) : \sum \alpha_g = 1\}$$

– нормализованная группа единиц кольца ZG. Здесь через $U(ZG)$ обозначена группа единиц группового кольца ZG.

Очевидно, что $U(ZG) = \{\pm 1\} \times V(ZG)$, поэтому часто вместо $U(ZG)$ рассматривают $V(ZG)$. Вложение группы G в группу H называется расщепляемым, если $H = N \leftthreetimes \breve{G}$, где $G \cong \breve{G}, N \lhd H, N \cap \breve{G} = \{1\}$, при этом N называется нормальным дополнением G. В случае положительных ответов на оба вопроса получаем, что G имеет в $V(ZG)$ нормальное дополнение без кручения, а отсюда следует, что всякая конечная подгруппа группы $V(ZG)$ изоморфна подгруппе G, что ведет к решению проблемы изоморфизма для ZG. Это объясняет интерес к нормальным дополнениям группы G в группе $V(ZG)$. Укажем известные к настоящему времени результаты.

Так P.J. Allen и C. Hobby [2] определили два нормальных дополнения для S_3 в $V(ZS_3)$: одно без кручения, второе содержит элемент порядка 2, при этом дополнение без кручения является свободной группой ранга 3. A E. Jespers и G. Leal [8] описали метод вычисления единиц кольца ZG, в котором G – конечная 2-группа с условием, что $G/Z(G)$ – четверная группа Клейна. Этот класс групп содержит две группы порядка 8, группу кватернионов и диэдральную группу D_4, а также четыре группы порядка 16. Кроме этого, A. Dooms и E. Jespers [4] описали четыре нормальных дополнения к S_3 в $V(ZS_3)$, три из которых изоморфны свободной группе ранга 3, а одно содержит периодические элементы. При этом они показали, что других нормальных дополнений нет.

Укажем, что R.K. Sharma и S. Gangopadhyay [11] доказали, что в $V(ZS_4)$ имеется подгруппа конечного индекса без кручения, но оставили открытым вопрос о существовании нормального дополнения без кручения к S_4 в группе $V(ZS_4)$.

Из этого перечня результатов следует, что на данном этапе исследований интерес представляет изучение строения групп единиц целочисленных групповых колец конкретных конечных групп, что и определяет актуальность темы. В указанных работах описываются группы единиц целочисленных групповых колец конкретных конечных групп малых порядков. Однако для групп существенно больших порядков "ручные" вычисления уже не годятся, для них становится необходимым разработка методов компьютерной алгебры и использование различных фактов теории представлений групп. Решению этих задач отведена первая часть диссертации.

Другой раздел диссертации посвящен построению новой криптосистемы – защищенной системы связи, предложенной С.К. Росошеком.

В таких криптосистемах используются групповые кольца конечных групп над различными кольцами, включая кольцо целых чисел. Для создания открытых и секретных ключей участников сеанса связи в этой криптосистеме необходимо уметь находить единицы групповых колец, автоморфизмы групповых колец и выполнять быстрые операции в таких кольцах. В связи с этим возникла необходимость исследования мультипликативной структуры групповых колец.

Заключительные разделы работы посвящены задачам кристаллографии. Известен широкий класс гидратных соединений включения, т.е. таких соединений, в которых молекулы воды посредством водородных связей образуют трехмерный каркас, имеющий полости различного типа. На данный момент известны следующие типы гидратных каркасов: кубические структуры I, II; гексагональные структуры I, II, III; тетрагональные структуры I, II, III; ромбическая структура. Анализ этих структур показал наличие в них полостей D, D', T, H, P и E -типов. В 2001 году была открыта тетрагональная структура IV с ранее неизвестным типом полости. Строение каркасов с этими структрами сложное, а разбиение каркаса на полости является довольно трудоемким. Поэтому большой интерес вызывает теоретическое обоснование и практическое определение такого разбиения. Предварительным шагом на пути определения этого разбиения служит задача генерации простых многогранников, а также задача о строении групп автоморфизмов точечных кристаллографических групп. Поскольку процесс получения новых гидратных структур продолжается, то решение поставленных задач является крайне актуальным для химии клатратных соединений.

Цель диссертации

Целью настоящей диссертационной работы является разработка и реализация алгоритмов для описания строения мультипликативных групп целочисленных групповых колец групп A_5, S_5, A_6, C_p на языке полупрямых произведений и нахождения линейных представлений этих групп, разработка алгоритмов для построения криптосистем на основе использования целочисленных групповых колец, разработка математического аппарата и алгоритмов для кристаллографического анализа гидратных каркасов.

Методика исследований

Применяются методы теории представлений групп, теории колец, компьютерной алгебры, теории кодирования, теории графов.

Научная новизна

Все основные результаты диссертации являются новыми. Достоверность результатов диссертации обеспечена полными доказательствами всех утверждений, полученных в данной работе, и численными расчетами.

Теоретическая и практическая ценность

Результаты, изложенные в диссертации, имеют теоретическое значение и могут быть использованы в дальнейших исследованиях по теории групп и колец, при разработке криптосистем, при чтении специальных курсов по теории групп, при анализе гидратных каркасов и получении новых гидратных структур.

Апробация работы

Результаты диссертации были представлены на

- Международной конференции ACCMS-2 (Новосибирск, 2004),
- Всероссийском симпозиуме по абелевым группам (Бийск, 2006),
- Международной конференции "Алгебра и ее приложения" (Красноярск, 2007),
- Международной школе "Пограничные вопросы универсальной алгебры и теории моделей" (Эрлагол, 2007),
- Международной конференции "Теория функций, алгебра и математическая логика"(Алма-Ата, 2007),
- Международной конференции "Современные проблемы математики, информатики и управления"(Алма-Ата, 2008),
- Международной научно-практической конференции "Использование экономико-математических методов в науке, управлении и образовании"(Новосибирск, 2009),
- семинаре "Эварист Галуа" (НГУ),
- семинаре кафедры алгебры и математической логики (НГТУ).

Публикации

Основные результаты опубликованы в работах [13]-[24], список которых помещен в конце автореферата. Работа [13] входит в перечень ведущих научных изданий, определенный ВАК.

Структура и объем диссертации

Диссертация состоит из введения, четырех глав, списка литературы. В тексте диссертации имеется 8 рисунков и 6 таблиц. Список литературы включает 47 наименований. Объем работы – 110 страниц.

СОДЕРЖАНИЕ РАБОТЫ

Основными результатами работы являются следующие.

1. Доказаны теоремы, описывающие мультипликативную структуру колец ZA_5, ZS_5, ZA_6, ZCp в терминах полупрямых произведений и найдены линейные представления групп единиц перечисленных выше колец.
2. На основе целочисленного группового кольца группы S_3 построена криптосистема Эль-Гамаля-Росошека.
3. Разработаны алгоритмы и теоретическое обоснование решения задачи о генерации простых многогранников с заданным четным числом вершин.
4. Установлено строение групп автоморфизмов точечных кристаллографических групп.
5. Разработаны алгоритмы и программное обеспечение для решения задачи о разбиении гидратного каркаса на полости.

Во **введении** дается обоснование актуальности темы исследований, определяются основные понятия и терминология, принятая при изложении результатов.

В **главе 1** описаны алгоритмы для решения задач по теории групп. К ним относятся.

1. Генерация группы, заданной порождающими элементами.
2. Построение таблицы неприводимых характеров.
3. Расчет неприводимых неэквивалентных представлений.
4. Описание групп автоморфизмов точечных кристаллографических групп.

В **главе 2** детально описывается строение группы $U(ZG)$ для групп A_5, S_5, A_6 и подгруппы конечного индекса для групп $U(ZCp)$ (p – простое).

Результаты представлены в следующих теоремах.

Теорема 1. *Вложение группы A_5 в $V(ZA_5)$ расщепляемо, при этом нормальное дополнение к группе A_5 является группой без кручения.*

Теорема 2. *Вложение группы S_5 в $V(ZS_5)$ не расщепляемо.*

Пусть $\varphi_m : GL_n(Z) \to GL_n(Z_m)$ – гомоморфизм Минковского, где Z_m – кольцо вычетов по модулю m.

В группе $V(ZD(S_5))$ рассмотрим инвариантный ряд подгрупп

$$V(ZD(S_5)) \rhd B \rhd K_5 \rhd B_1 \rhd K_{10} \rhd B_2 \rhd K_6 \rhd B_3 \rhd K_{12} \rhd B_4 \rhd K_{20}.$$

Тогда справедлива

Теорема 3. $V(Z[D(S_5)])/B \cong C_2$; $B/K_5 \cong C_5^3 \leftthreetimes (C_2 \times L_3(5))$;
$K_5/B_1 \cong Ker\varphi_5$; $B_1/K_{10} \cong C_5^3 \leftthreetimes (C_2 \times L_3(5))$;
$K_{10}/B_2 \cong Ker\varphi_{10}$; $B_2/K_6 \cong C_3^4 \times (C_2^4 \leftthreetimes A_8)$;
$K_6/B_3 \cong Ker\varphi_6$; $B_3/K_{12} \cong C_6 \times C_2^3 \times C_3^3$;
$K_{12}/B_4 \cong Ker\varphi_{12}$; $B_4/K_{20} \cong C_2^5 \times C_5^4 \times C_{10}^5$.

Доказательства этих теорем опубликованы в работах [13] и [15]. Идея построения дополнения и использования теории представлений групп принадлежит научному руководителю диссертанта, а теоретическое обоснование и математическая обработка результатов – автору.

Кроме этого установлены две теоремы о полупрямом разложении группы единиц.

Теорема 4. *Вложение группы A_6 в $V(ZD(A_6))$ не расщепляемо.*

В группе $V(ZD(A_6))$ рассмотрим инвариантный ряд подгрупп

$$V(ZD(A_6)) \rhd K_6 \rhd B \rhd K_6' \rhd B_1 \rhd K_{20} \rhd B_2 \rhd K_{12} \rhd B_3 \rhd K_{45}.$$

Тогда справедлива

Теорема 5. $V(Z[D(A_6)])/K_6 \cong C_6^4 \leftthreetimes GL_4(Z_6)$;
$K_6/B \cong Ker\varphi_6$; $B/K_6' \cong (C_2^4 \leftthreetimes A_8) \leftthreetimes C_3^4$;
$K_6'/B_1 \cong Ker\varphi_6$; $B_1/K_{20} \cong C_2^{40} \times (C_5^8 \leftthreetimes SL_8(5))$;
$K_{20}/B_2 \cong Ker\varphi_{20}$; $B_2/K_{12} \cong C_2^{34} \leftthreetimes (C_3^{24} \leftthreetimes GL_3(Z_3(\sqrt{2})))$;
$K_{12}/B_3 \cong Ker\varphi_{12}$; $B_3/K_{45} \cong C_3^{25} \times C_5^{35} \times C_{15}^{29} \leftthreetimes C_3^7$.

Доказательство этих теорем опубликовано в [16]. В этой работе научному руководителю диссертанта принадлежит идея использования теории представлений групп, а теоретическое обоснование использованных далее алгебраических методов и математическая обработка результатов вычислений принадлежит диссертанту.

Данные теоремы полностью описывают строение групп единиц целочисленных групповых колец соответствующих групп.

В **главе 3** разработаны алгоритмы построения криптосистемы на основе целочисленных групповых колец конечных групп и приведен пример такой системы на основе кольца группы S_3.

Рассмотрим конечную группу G и ее целочисленное групповое кольцо ZG. Пусть S – группа автоморфизмов этого кольца.

Любая криптосистема предполагает наличие не менее двух участников сеанса связи. Участник, который шифрует информацию, и участник, который ее расшифровывает. Пусть B и A такие участники. Создание криптосистемы разобьем на три этапа. Первый этап включает в себя генерацию ключей. Второй этап включает этап шифрования информации и, наконец, третий этап – ее расшифровку.

Этап 1. (Генерация ключей).

Участник A генерирует секретный ключ криптосистемы так: случайно выбирает автоморфизм ϕ, порядок которого есть достаточно большое натуральное число и централизатор которого отличается от циклической группы, порожденной автоморфизмом ϕ. Тогда секретный ключ участника A есть автоморфизм ϕ. Участник A вычисляет свой открытый ключ следующим образом: а) выбирает обратимый $x \in ZG$ тоже высокого порядка, для которого легко вычислить обратный элемент x^{-1}; б) используя секретный ключ ϕ, вычисляет элемент $\phi(x) \in ZG$. Тогда открытый ключ участника A есть пара $(x^{-1}, \phi(x))$.

Этап 2. (Алгоритм шифрования).

После получения открытого ключа участника A, участник B для шифрования своего сообщения действует следующим образом: а) вычисляет случайный сеансовый автоморфизм ψ достаточно высокого порядка, который принадлежит централизатору автоморфизма ϕ; б) вычисляет $\psi(x^{-1})$ и $\psi(\phi(x))$; в) записывает исходный текст в виде $m \in ZG$ и вычисляет $m \cdot \psi(\phi(x))$; г) в результате участник B отправляет участнику A криптограмму $c = (\psi(x^{-1}), m \cdot \psi(\phi(x)))$. Заметим, что в каждом сеансе связи автоморфизм ψ нужно задавать заново.

Этап 3. (Алгоритм расшифрования).

Получив криптограмму c, участник A для расшифрования действует следующим образом: а) используя свой секретный ключ ϕ, вычисляет $z = \phi(\psi(x^{-1}))$; находит m, вычисляя $m \cdot \psi(\phi(x)) \cdot z = m$.

Покажем корректность расшифрования.

$m \cdot \psi(\phi(x)) \cdot z = m \cdot \psi(\phi(x)) \cdot \phi(\psi(x^{-1})) = m \cdot \psi \cdot \phi(x) \cdot \phi \cdot \psi(x^{-1}) = m \cdot \psi \cdot \phi(x) \cdot \psi \cdot \phi(x^{-1}) = m \cdot \psi \cdot \phi(x \cdot x^{-1}) = m \cdot \psi \cdot \phi(1) = m \cdot 1 = m.$

Результаты этой главы принадлежат автору диссертации, они опубликованы в работе [14]. Для построения криптосистем на основе целочисленных групповых колец групп S_4 и $Sl_2(3)$ найдены порождающие и изучено строение групп автоморфизмов этих колец в работах [22] и [24].

В **главе 4** изложены алгоритмы решения следующих задач.

1) Разбиение гидратного каркаса на полости.

2) Генерация всех простых многогранников с заданным четным числом вершин.

Остановимся подробнее на первой задаче. Для этого дадим ряд определений.

Определение. *Многогранником (полиэдром, полостью) будем называть любой планарный трехсвязный граф. Многогранник будем называть простым, если все его вершины трехвалентны.*

Пусть имеется гидратный каркас, каждая молекула которого образует водородные связи ровно с четырьмя другими молекулами. Построим на его основе граф следующим образом. Вершинами графа будем считать молекулы, образующие каркас. Две вершины графа соединим ребром тогда и только тогда, когда соответствующие им молекулы образуют водородную связь. Построенный таким образом граф будем называть графом гидратного каркаса.

В графе гидратного каркаса конечный связный подграф G будем называть разбиваемым на многогранники (полости), если его можно представить в виде объединения многогранников $G = P_1 \cup P_2 \cup \cdots \cup P_k$.

Далее будем предполагать, что мы работаем с разбиваемым на многогранники конечным фрагментом гидратного каркаса, который обладает следуюшими свойствами.

1) Все многогранники P_i простые и не содержат треугольных граней.

2) Все вершины четырехвалентны и принадлежат ровно четырем полостям.

3) Все ребра принадлежат трем многогранникам и трем граням.

4) Каждая грань принадлежит двум многогранникам.

5) Пересечение любых двух граней либо пусто, либо состоит из единственного ребра.

6) Пересечение любых двух многогранников либо пусто, либо состоит из одной грани.

7) Любые два смежных ребра принадлежат ровно одной грани.

8) Любые две смежных грани принадлежат ровно одному многограннику.

Два многогранника, имеющих общую грань, будем называть двухсекционной полостью. Три многогранника, имеющих общее ребро, будем называть трехсекционной полостью. Четыре многогранника, имеющих общую вершину, будем называть четырехсекционной полостью.

В терминах теории графов задача разбиения гидратного каркаса на полости формулируется следующим образом. Имеется гидратный каркас, удовлетворяющий условиям 1) – 8), вершины которого заданы координатами точек в пространстве. Требуется построить все многогранники, вершины которых являются подмножествами заданного множества.

В рамках второй задачи была разработаны алгебраические методы на основе которой создана программа Cavities. Она позволяет находить все имеющиеся полости в гидратном каркасе. С помощью данной программы было изучено строение шести структур клатратных гидратов. Это кубические структуры I и II, тетрагональные структуры I и II, гексагональная структура III и ромбическая структура I. В диссертации подробно рассмотрено строение тетрагональной структуры I. Данная структура содержит следующие полости: D–полость (многогранник 5^{12}), T–полость (многогранник $5^{12}6^2$) и P–полость (многогранник $5^{12}6^3$). В тетрагональной структуре 1 имеются также сдедующие четырехсекционные полости: $T_3D, T_3P, D_3P, D_2T_2, D_2TP, T_2DP, P_2DT$.

Кроме того, автором обоснована и построена база простых многогранников до 32-х вершинников включительно, представленная в диссертации в виде таблицы. С помощью данной базы были решены задачи моделирования фазовых диаграмм различных классов.

Алгебраические методы, указанные в этой главе, принадлежат автору диссертации, а химические приложения выполнены его соавторами. Все эти результаты опубликованы в работах [18 - 21] и [23].

В конце диссертации содержится список программ, реализующих предложенные алгоритмы. Все программы являются оригинальными, они разработаны автором диссертации и иллюстрируют возможности использования полученных алгебраическими методами теоретических результатов. Эти программы являются общедоступными, они размещены в интернете на странице НГТУ. Адрес сайта http://ciu.nstu.ru/kaf/persons/27621/?page=182.

СПИСОК ЛИТЕРАТУРЫ

1. Allen P.J., Hobby C. A Characterization of Units in Z[A_4] // J. of Algebra, 1980, Vol 66, P. 534-543.

2. Allen P.J., Hobby C. A note on the unit group of ZS_3 // Proc. A.M.S., 1987, Vol 99, P. 9-14.

3. Cliff G.H., Sehgal S.K., Weiss A.R. Units of integral Rroup Rings of Metabelian Groups // J. Algebra, 1981, Vol 73, P. 167-185.

4. Dooms A., Jespers E. Normal Complements of the Trivial Units in the Unit Group of Some Integral Group Rings // Commun. Algebra, 2003, Vol 31, № 1, P. 475-482.

5. Goodaire E.G., Jespers E., Parmenter M.M. Determining units in some integral group rings // Canad Math. Bull. 1990. Vol 33, № 2. P. 242-246.

6. Hertweck M. A. Counter-example to the isomorphism problem for integral group rings // Annals of Mathematics, 2001, Vol 154, P. 115-138.

7. Hughers J., Pearson K.R. The group of units of the integral group ring ZS_3// Canad Math. Bull., 1972, Vol 15, № 4, P. 529-534.

8. Jespers E., Leal G. Describing units of integral group rings of some 2-groups // Commun. Algebra, 1991, Vol 19, № 6, P. 1809-1826.

9. Milies P.C. The units of the integral groups ring ZD_4 // Doc. Soc. Brazil. Math., 1972, № 4, P. 85-92.

10. Ritter Y., Sehgal S.K. Construction of units in integral group rings of finite nilpotent groups // Trans. Amer. Mat. Soc., 1991, № 324, P. 603-621.

11. Sharma R.K., Gangopadhyay S. On congruence subgroups and units in ZS_4 // Commun. Algebra, 2004, Vol 32, № 2, P. 663-688.

12. Sehgal S.K. Units in integral group rings // Longman Scientific and Technical Essex, 1993.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

13. Грачев Е.В., Попова А.М. Единицы целочисленного группового кольца группы A_5 // Вестник Красноярского государственного университета. Серия: физ.-мат. науки. 2006. № 4. С. 54-59.

14. Грачев Е.В. Строение группы единиц целочисленного группового кольца циклической группы простого порядка // Algebra and Model Theory 6. Новосибирск. 2007. С. 38–40.

15. Грачев Е.В., Попова А.М. Группа единиц целочисленного группового кольца группы S_5 // Абелевы группы. Материалы всероссийского симпозиума. Бийск. 2006. С. 13.

16. Грачев Е.В., Попова А.М. Мультипликативная группа кольца ZA_6 // Международная конференция «Алгебра и ее приложения». Тезисы докладов. Красноярск. 2007. С. 38-39.

17. Грачев Е.В., Попова А.М., Журков С.В. Некоторые алгоритмические вопросы целочисленных групповых колец // Международная конференция «Теория функций, алгебра и математическая логика». Алматы. 2007. С. 76.

18. Грачев Е.В., Дядин Ю.А. Разбиение гидратных каркасов на полости // Кристаллография. 2005. Том 50, № 3. С. 563-567.

19. Грачев Е.В., Дядин Ю.А., Липковски Я. Построение сечений кристаллических структур с использованием пакета программ CLAT // Журнал структурной химии. 1995. Том 36, № 5. С. 956-959.

20. Грачев Е.В., Комаров В.Ю. Генерация простых многогранников // Сборник материалов Международной научно-практической конференции «Использование экономико-математических методов в науке, управлении и образовании». Новосибирск. 2009. С. 112-116.

21. Косяков В.И., Шестаков В.А., Грачев Е.В. О проблеме перечисления фазовых диаграмм. // Журнал физической химии. 2009. Том 83, № 8. С. 1427–1432.

22. Попова А.М., Грачев Е.В. Группа автоморфизмов кольца ZS_4 // Материалы Международной научной конференции «Современные проблемы математики, информатики и управления». Алматы. 2008. С. 469-470.

23. Komarov V. Yu., Solodovnikov S.F., Grachev E.V., Kosyakov V.I. Phase formation and structure of hight-pressure gas hydrates and modeling of tetrahedral frameworks with uniform polyhedral cavities // Crystallography Reviews. 2007. Vol 13, N 4. P. 257-297.

24. Popova A.M., Grachev E.V. Authomorphisms Group of Ring $ZSL_2(3)$ // Algebra and Model Theory 7. Novosibirsk. 2009. P. 96-103.

25. Косяков В.И., Шестаков В.А., Грачев Е.В. Перечисление диаграмм плавкости трехкомпонентных систем с соединениями постоянного состава // Журнал неорганической химии. 2010, том 55, № 4. С. 1–9 (в печати).