

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»

Р.Х. Вахитов, Е.В. Вахитова

ФУНДАМЕНТАЛЬНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Часть IV

Компьютерная алгебра

Учебно-методическое пособие для вузов

Издательско-полиграфический центр
Воронежского государственного университета
2012

ВВЕДЕНИЕ

Содержание данного учебно-методического пособия «Фундаментальная и компьютерная алгебра. Часть IV. Компьютерная алгебра» составляет материал нескольких тем базовой учебной дисциплины профессионального цикла «Фундаментальная и компьютерная алгебра», изучение которой предусмотрено основной образовательной программой подготовки бакалавра по направлению «Математика и компьютерные науки» для студентов факультета компьютерных наук ФГБОУ ВПО «Воронежский государственный университет». Целью учебной дисциплины является формирование представлений о фундаментальной алгебре: структуры алгебры, линейная алгебра, алгебра многочленов и о компьютерной алгебре. Основными задачами учебной дисциплины являются овладение фундаментальными базовыми знаниями в области фундаментальной и компьютерной алгебры, умением формулировать и доказывать теоремы, самостоятельно решать классические задачи фундаментальной алгебры.

Цель учебно-методического пособия состоит в том, чтобы помочь студентам, изучающим учебную дисциплину «Фундаментальная и компьютерная алгебра», формировать представления о компьютерной алгебре, приобрести навыки и умения практического использования математических методов при решении задач. В результате изучения учебной дисциплины студент должен знать теоретический материал и уметь формулировать результат, строго доказывать утверждение, грамотно пользоваться языком фундаментальной и компьютерной алгебры.

Учебно-методическое пособие состоит из пяти глав. В конце каждой главы приведены вопросы для самоконтроля и упражнения для самостоятельной работы. Определения, теоремы и их доказательства иллюстрируются численными примерами, цель которых – пояснить общую теорию. В каждой главе определения, формулы и теоремы имеют независимую нумерацию.

При изложении глав 1 и 5 приняты за основу сведения из введения и главы 1 книги Е.В. Панкратьева [35].

В первой главе рассмотрены следующие вопросы: отличия компьютерной алгебры, системы компьютерной алгебры, алгоритмы компьютерной алгебры и о представлении данных.

Вторая глава посвящена исследованию вопросов: арифметические операции над целыми систематическими числами, перевод в десятичную систему счисления, перевод из десятичной системы счисления и перевод из g -ичной системы в h -ичную систему.

В третьей главе рассмотрены следующие вопросы: свойства сравнений по натуральному модулю, полная система вычетов, аддитивная группа классов вычетов и кольцо классов вычетов.

кольцо (элементы матрицы принадлежат кольцам общего вида). Даже при арифметических операциях над такими объектами происходит увеличение информации и для записи промежуточных результатов требуется большой объем памяти ЭВМ. Ограничение по времени счета и памяти ЭВМ в символьных вычислениях более неудобно, чем в вычислительных методах.

В следующем параграфе рассмотрим важный продукт исследований символьных вычислений – системы компьютерной алгебры.

§ 2. Системы компьютерной алгебры

Активная разработка систем компьютерной алгебры началась в конце 60-х годов XX века. Системы компьютерной алгебры можно разделить на:

- 1) системы общего назначения (универсальные),
- 2) специализированные системы.

1. Универсальные системы компьютерной алгебры: MACSYMA, REDUCE, MATHEMATICA, MAPLE, AXIOM. Система MACSYMA, как и система REDUCE, является «старой» системой. Система MAPLE (Канада, 80-е годы) в настоящее время широко применяется в Канаде, США, во всем мире. В конце XX века в лидеры выдвинулась также система MATHEMATICA с широкими вычислительными и графическими возможностями, с электронной документацией (как библиотека может быть использована), посвященной различным разделам математики и информатики.

Особое место среди систем компьютерной алгебры занимает система AXIOM. Она имеет высокую степень универсальности, имеет дело с объектами, более привычными для математиков: категории – это ключевое понятие современной математики (например, категории множеств, полугрупп, дифференциальных колец, левых модулей).

Эта система требует для своей реализации мощных компьютеров, у них очень высокая плата (дорогая, имеется только в ограниченном числе мощных университетских и научных центров) в отличие от остальных систем, которые представляют собой пакеты программ, общение осуществляется на некотором алголоподобном языке.

2. Специализированные системы компьютерной алгебры отличаются более высокой эффективностью, но область их применения ограничена: CALEY, GAP – для вычислений в теории групп; MACAULEY, CoCoA, Singular – разной степени универсальности, для вычислений в кольце многочленов; SCHOONSHIP – для вычислений в физике высоких энергий, muMATH и ее правопреемница DERIVE – системы, широко используемые в учебном процессе (например, в Австрии в средних школах).

§ 3. Алгоритмы компьютерной алгебры

Компьютерная алгебра имеет дело с алгоритмами, которые сильно отличаются от алгоритмов, используемых в вычислительной математике. Ал-

горитмы вычислительной математики должны давать возможность решать задачу с требуемой точностью при заданных вычислительных ресурсах, наиболее существенными из которых являются ограничения по используемой памяти и времени счета. В компьютерной алгебре вычисления производятся без округления, мало внимания уделяется анализу сходимости, но используется значительно более широкий набор математических, в первую очередь алгебраических, объектов сложной структуры, и ограничения по времени счета и по используемой памяти становятся более обременительными.

Применение компьютеров в алгебраических исследованиях поставило ряд новых задач перед специалистами и заставило заново пересмотреть задачи, которые считались решенными. К ним относились и задачи, для которых был предложен метод, позволяющий решать их «за конечное число шагов». Методы решения конкретных задач отличались большим разнообразием и не использовались универсальные методы. С применением компьютеров для алгебраических вычислений потребовалось реализовать универсальные алгоритмы в виде программ для ЭВМ и оказалось, что они позволяют решать только небольшие задачи. С увеличением размера задачи резко возрастали время счета и необходимая память компьютера. Это сделало актуальным поиск более эффективных алгоритмов решения алгебраических задач.

В конце XX века бурно развивались исследования в трех областях компьютерной алгебры:

- 1) теории базисов Грёбнера,
- 2) теории факторизации многочленов,
- 3) теории интегрирования в конечном виде.

В компьютерной алгебре рассматриваются арифметические операции, алгоритм вычисления наибольшего общего делителя целых чисел и многочленов, задачи: представления данных для фактор-колец кольца многочленов, разложение многочленов на неприводимые множители, проблемы дифференциальной компьютерной алгебры.

Компьютерная алгебра используется также при нахождении решений дифференциальных уравнений в виде степенных рядов и в других задачах теории дифференциальных уравнений, при построении разностных схем для численного решения дифференциальных уравнений.

§ 4. О представлении данных

Сформулируем проблему представления данных. Имеется множество объектов A и на нем отношение эквивалентности. Требуется в каждом классе эквивалентных объектов выбрать единственного представителя этого класса для основных алгебраических областей: кольца целых чисел, поля рациональных чисел, конечных полей, кольца многочленов и поля рациональных функций, алгебраических и трансцендентных расширений полей.

Примеры. 1. A – множество натуральных чисел > 1 , каждое из которых можно записать в виде арифметического выражения. В качестве канонического выбираем выражение, которое является произведением простых чисел, расположенных в порядке неубывания. Основная теорема арифметики утверждает, что любое натуральное число > 1 представляется в таком виде и такое представление единственно. Поэтому задача разложения натурального числа на простые множители может рассматриваться как задача представления данных.

2. Предыдущий пример обобщается на любое кольцо с однозначным разложением на множители, элементы которого можно упорядочить. В частности, на кольцо $\mathbf{Z}[x]$ (кольцо многочленов над \mathbf{Z}), получается задача факторизации многочленов.

3. Основная теорема алгебры утверждает, что любой многочлен положительной степени от одной переменной x с комплексными коэффициентами может быть представлен в виде $a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$. Поэтому задача представления данных есть задача нахождения корней $\alpha_1, \dots, \alpha_n$ многочлена, то есть задача решения алгебраического уравнения.

Будем требовать, чтобы выбор представления был каноническим, то есть в множестве всех эквивалентных выражений нужно выбрать единственное выражение, которое представляло бы этот класс эквивалентности. При этом предполагаем, что известен алгоритм проверки эквивалентности двух выражений, так как такой алгоритм не всегда существует. Поэтому иногда налагается требование более слабое, чем каноническое.

Условие нормальности, например недопустимо деление на нуль. Тем самым нуль приобретает некоторое особое положение и возрастает значение задачи определения равенства элемента нулю. Нормальное представление – это представление, в котором все эквивалентные нулю выражения представляются одним и тем же образом (0). Отметим, что любое каноническое представление является нормальным, но обратное верно не всегда. Часто, зная нормальное представление, можно построить каноническое. Если рассматриваемая структура данных такая, что в ней, кроме нуля, есть и другие «особые» элементы, то определение нормального представления должно быть усложнено. Отметим, что понятие эквивалентности объектов может быть различным.

Представление называется естественным, если представление каждого элемента определяется одними и теми же правилами, не зависящими от того, в какой последовательности появляется этот элемент.

Будем рассматривать некоторые из основных структур данных, используемых в компьютерной алгебре, для них рассмотрим проблему представления данных. Отметим, что в общем случае эта проблема неразрешима, существуют отношения эквивалентности, для которых нет алгоритма выбора канонического представителя в множестве эквивалентных выражений и даже проверки эквивалентности двух выражений.