МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»

С.В. Напалков
О.М. Абрамова
И.В. Кузнецова
С.А. Тихомиров

МНОГОЧЛЕНЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Учебное пособие

Рекомендовано методической комиссией
Балахнинского филиала
для обучающихся по программам среднего общего образования
Специализированного учебного научного центра ННГУ

Нижний Новгород
2021

УДК 512.622(075.8)
ББК 22.144.77я73
М73

Н 270 Напалков С.В., Абрамова О.М., Кузнецова И.В., Тихомиров С.А. Многочлены от одной и переменной: учебное пособие. – Нижний Новгород: Нижегородский госуниверситет, 2021. – 65 с.

Рецензент: д.ф-м.н., профессор П.Б. Болдыревский

В учебном пособии рассматриваются вопросы теории многочленов от одной переменной, изучаемые в курсе «Математика» программа среднего общего образования. На основе синергетического подхода подробно излагается теория многочленов с использованием математического пакета Mathematica, предложены тесты, задачи для самостоятельного решения и тематика учебных проектов.

Пособие подготовлено для учащихся по программам среднего общего образования, Специализированного учебного научного центра ННГУ.

Ответственный за выпуск:
председатель методической комиссии Балахнинского филиала
к.э.н. С.С. Квашнин

УДК 512.622(075.8)
ББК 22.144.77я73

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Учебное пособие предназначено для учащихся математических и физико-математических направлений подготовки и содержит систематическое изложение важного раздела — теории многочленов с использованием информационно-коммуникационных технологий, конкретно — универсального математического пакета *Mathematica*. Данный пакет является мировым лидером среди подобных систем символьной математики для персональных компьютеров.

В учебном пособии представлены как задачи для самостоятельной работы учащихся, так и тематика учебных проектов по теории многочленов. Это позволит ориентировать учащихся не на получение знаний в готовом виде и запоминание теоретического материала, а на самостоятельный поиск информации, ее осмысление, преобразование и, наконец, синтез на основе имеющейся информации новых знаний.

В данном учебном пособии авторы обеспечивают читателя не только материалами, позволяющими самоорганизовать свою учебную деятельность, но и отражают развивающий потенциал информатики и профессионально ориентированные информационно-коммуникационные технологии, что позволяет выделить данное издание из других существующих изданий аналогичного характера.

Пособие может быть хорошим дополнением к учебному материалу и уже имеющимся пособиям по дисциплине «Математика». Оно состоит из четырех глав, каждая из которых разбита на параграфы. Нумерация параграфов сквозная. При ссылках на определения, теоремы, леммы и формулы первым указывается номер параграфа, вторым — их собственные номера в пределах данного параграфа.

В первой главе изложены основные вопросы работы в специализированном математическом пакете *Mathematica*, подробно описываются понятия и функции компьютерной алгебры, на конкретных примерах иллюстрируется применение процедур для работы с многочленами в данном пакете.

Вторая глава посвящена теории многочленов от одной переменной. В ней излагаются основные сведения и понятия о многочленах.

В третьей главе рассмотрены многочлены над полем комплексных, действительных и рациональных чисел. Особое внимание уделено в ней решению уравнений третьей и четвертой степени.

В четвертой главе представлена теория многочленов от нескольких переменных.

Изложение теоретического материала сопровождается примерами решения типовых задач, раскрывающими суть вводимых понятий и определений, а также иллюстрациями, сделанными с помощью универсального математического пакета *Mathematica*.

Большинство параграфов пособия заканчиваются заданиями для самостоятельной работы. В конце пособия даны ответы на некоторые из них и указания. Перед ответами и указаниями даны тесты для самопроверки.

ВВЕДЕНИЕ

Центральным в школьном курсе алгебры является вопрос о решении уравнений. Изучение уравнений первой степени с одним неизвестным получит свое дальнейшее развитие в курсе высшей алгебры в разделе алгебры многочленов.

Центральным в этом разделе алгебры является уже не вопрос о практическом нахождении корней уравнений, а вопрос об их существовании. Ответ на него дает основная теорема алгебры, согласно которой всякое уравнение с любыми числовыми коэффициентами имеет комплексные корни, причем этих корней столько, какова степень уравнения.

Алгебра многочленов, развивающаяся на протяжении многих десятилетий как наука об одном уравнении произвольной степени от одного неизвестного, в наши дни уже в основном сформирована. При этом аппарат теории многочленов имеет исключительно важное значение как в самой математике, так и в ее приложениях, и входит в основу таких, например, разделов, как линейные операторы, дифференциальные уравнения с постоянными коэффициентами, интегрирование рациональных функций. Кроме того, теория многочленов по своей математической сущности примыкает к теории делимости целых и натуральных чисел, о чем свидетельствует исторический процесс развития математики. Некоторыми вопросами алгебры, в частности решением простейших уравнений, занимались еще вавилонские, а затем древнегреческие математики. Вершиной алгебраических исследований этого периода являются сочинения греческого математика Диофанта (III в.). В дальнейшем эти исследования развивали индийские математики — Ариабхата (VI в.), Брахмагупта (VII в.), Бхаскара (XII в.). Очень рано началась разработка вопросов алгебры в Китае — Чжан Цан (II в. до н. э.), Цзин Чоу-чан (I в.). Весьма крупным китайским алгебраистом был Цинь Цзю-шао (XIII в.).

Большой вклад в развитие алгебры внесли математики средневекового Востока — Мухаммад ал-Хорезми (IX в.) и Омар Хайям (1048–1131). В частности, само слово «алгебра» возникло в связи с заглавием книги ал-Хорезми «Ал-джебр аль-мукабала» (арабское слово «ал-джебр» в Европе стали произносить «алгебра»).

Исследования вавилонских, греческих, индийских, китайских и арабских математиков относились к тем вопросам алгебры, которые лишь иногда касались уравнений третьей степени, но ныне входят в программу курса элементарной алгебры. В этом же круге вопросов оставались в основном и исследования математиков средневековой Западной Европы и затем эпохи Возрождения. Назовем итальянца Леонардо Пизанского (Фибоначчи) (XII в.) и создателя современной алгебраической символики француза Франсуа Виета (1540–1603). В XVI в. были найдены методы решения уравнений третьей и четвертой степени; здесь должны быть названы имена итальянцев Сципион дель Ферро (1465–1526), Никколо Тарталья (1499–1557), Джероламо Кардано (1501–1576) и Лодовико Феррари (1522–1565).

В XVII—XVIII вв. происходила интенсивная разработка общей теории уравнений (то есть алгебры многочленов), в которой принимали участие крупнейшие ученые того времени — Рене Декарт (1596–1650), Исаак Ньютон (1643–1727), Жан Лерон Д'Аламбер (1717–1783) и Жозеф Луи Лагранж (1736–1813). На рубеже XVIII—XIX вв. немецкий математик Иоганн Карл Фридрих Гаусс (1777–1855) доказал основную теорему о существовании корней алгебраических уравнений с числовыми коэффициентами.

Глава 1. СПЕЦИАЛИЗИРОВАННЫЙ МАТЕМАТИЧЕСКИЙ ПАКЕТ MATHEMATICA И ЕГО ПРИМЕНЕНИЕ В ТЕОРИИ МНОГОЧЛЕНОВ

§ 1. История специализированного математического пакета

В настоящее время получили широкое развитие программные средства для численных расчетов — интегрированные системы символьной математики (компьютерной алгебры), такие, как *Mathematica, MatLab, MathCAD, Maple* и другие.

Интегрированные системы компьютерной алгебры для персональных компьютеров (ПК) — отдельное направление в развитии программного обеспечения и применения ПК. В большей степени они ориентированы на сферы деятельности математиков — аналитиков и ученых, занятых решением научно-технических, в частности, математических задач.

Нельзя переоценить значение таких систем в образовании, где они также исполняют роль справочников и математических консультантов, снимают неуверенность перед математическими дисциплинами, существующую у многих обучаемых.

Программное обеспечение такого класса позволяет находить производные и первообразные функции, решать в аналитическом виде сложные алгебраические и дифференциальные уравнения, производить всевозможные символьные преобразования математических выражений. Многие сложные научно-технические проблемы они переводят из категории математического чуда в категорию рутинных задач, быстро и удобно решаемых ПК.

Система *Mathematica* фирмы *Wolfram Research Incorporated* прошла всестороннюю апробацию и тестирование. Она реализована на целом семействе компьютеров — от персональных *IBM PC AT* и *Macintosh* до рабочих станций *Next* и *Sun* и суперкомпьютеров *Cray*. Существует даже версия под операционную систему *OS/2*.

К настоящему времени система *Mathematica* рассматривается как один из лидеров среди систем компьютерной алгебры, обеспечивающих не только возможности выполнения сложных численных расчетов с выводом их результатов в графическом виде, но и проведение особо трудоемких аналитических вычислений и преобразований. Версии системы под *Windows* имеют хороший пользовательский интерфейс и позволяют готовить документы в форме *Notebook* (записная книжка). Они объединяют исходные данные, описание алгоритмов решения задач, программ и результатов решения в самой разнообразной форме (математические формулы, числа, векторы, матрицы, графики). Однако можно сказать, что достойным конкурентом системы *Mathematica* является система *Maple*.

Mathematica была задумана как система, помогающая автоматизировать труд научных работников и математиков-аналитиков. Это мощный и гибкий программный математический инструментарий, который может оказать неоценимую помощь большинству научных работников, преподавателей вузов, студентов и инженеров.

Разумеется, работа с математическими системами требует от пользователя определенных математических знаний. Для решения одних задач достаточно знание школьного курса математики, а для других необходим уровень знания студентов математических направлений вузов.

Ядро системы и синтаксис языка общения с системой одинаковы для всех ее реализаций на различных классах и типах компьютеров.

Эта глава является руководством для пользователя и кратким справочником по системе. Подробно рассматриваются наиболее часто используемые функции и служебные слова, ориентированные в большей степени на работу с многочленами. Примеры иллюстрируют возможности системы.

Рассмотрим историю развития специализированного математического пакета *Mathematica*.

В 1980-х гг. возможностями символьной математики увлекся С. Вольфрам. Его научные интересы были настолько серьезны, что он создал фирму *Wolfram Research Ltd*, приступившую к созданию проекта математической системы *Mathematica*.

Целью нового проекта была разработка мощного и универсального ядра системы, способного работать на различных компьютерных платформах, создание многофункционального языка программирования, ориентированного на математические приложения, подготовка современного пользовательского интерфейса и обширных пакетов применений и расширений системы. Система приобрела свойства адаптации, то есть обучения новым математическим законам и закономерностям. С самого начала большое внимание уделялось двумерной и трехмерной графике, в том числе динамической, и даже возможностям мультимедиа — воспроизведению динамических изображений и синтезу звуков с поддержкой звуковой платы.

Хотя первые версии *Mathematica* под *MS-DOS* имели примитивный пользовательский интерфейс и заметно уступали интерфейсу конкурирующей системы *Maple* под *MS-DOS*, фирма *Wolfram* быстро сумела оценить возможности графической оболочки *Windows* и одной из первых создала версию системы *Mathematica 2 for Windows*.

Из-за понятной сложности системы, первые ее версии имели ряд серьезных недоработок. Тестовые испытания указали на достаточно частую возможность получения неверных результатов и на довольно частые сбои в работе системы, сопровождаемые фатальными ошибками. Частично они были устранены в версии 2.1.

Несмотря на эти ошибки, система быстро заняла ведущие позиции на рынке математического программного обеспечения. Особенно привлекательны были обширные графические возможности системы и реализация интерфейса типа «записная книжка», сочетающего в пределах готовящихся документов объединение программ и команд с данными, представленными в формульном, текстовом, табличном и графическом видах. При этом система обеспечивала динамическую связь между ячейками документов в стиле «записная книжка» даже при решении символьных задач, что принципиально и выгодно отличало ее от других систем.

Mathematica — одна из самых крупных и изощренных математических программных систем. По обилию встроенных в ядро системы функций *Mathematica* уступает системе *Maple*, но вместе с системой *Mathematica* поставляется множество внешних пакетов ее расширения, которые можно пополнять и модифицировать. С учетом включенных в них процедур и функций *Mathematica* почти не уступает *Maple*.

Если рассматривать систему *Mathematica* как язык программирования, то она относится к интерпретирующим системам. Как известно, такие системы последовательно анализируют (интерпретируют) каждое выражение и сразу же исполняют его. Таким образом, работа с системой происходит в интерактивном режиме — пользователь задает системе задание, а она тут же исполняет его. Система содержит достаточный набор управляющих структур для создания условных выражений, ветвления в программах, циклов и некоторых других.

Может показаться, что система *Mathematica* имеет диалог на более примитивном уровне, чем язык программирования интерпретирующего типа. В самом деле, работа с системой *Mathematica* напоминает работу с Бейсиком в режиме непосредственного исполнения команд — в ответ на каждый вопрос тут же следует результат вычислений.

Таким образом, *Mathematica* даже в ходе такого простейшего диалога предоставляет пользователю средства сверхвысокого уровня (например, аналитическое вычисление производных или интегралов), также система имеет все возможности для создания практически любых управляющих структур, организации ввода-вывода, работы с системными возможностями и т.д.

Более того, система имеет ядро, которое используется практически в любой ее реализации — от версий для персональных компьютеров до рабочих станций *Sun* и даже суперкомпьютеров. Это позволяет использовать систему на любой аппаратуре с одинаковым успехом с точки зрения конечных результатов. Таким образом, *Mathematica* состоит из общего для различных реализаций ядра *(Kernel)* и конкретной оболочки пользовательского интерфейса.

§ 2. Интерфейс системы *Mathematica*

Обычно создатели пользовательских интерфейсов математических систем просто копируют стандартный интерфейс программ из комплекса *Microsoft Office*, в частности, самого популярного текстового процессора *MS Word.* Разработчики интерфейса пользователя системы *Mathematica* отошли от этой традиции.

Нетрудно заметить, что пользовательский интерфейс новых версий системы *Mathematica* реализует отдельный вывод своих элементов — окон (включая основное окно редактирования), панелей, палитр знаков и т.д. Это позволяет располагать их в любых местах экрана, что особенно удобно при работе с дисплеями, имеющими большой размер изображения. При работе с дисплеями, имеющими небольшой экран и стандартное разрешение 640×480, 600×800 пикселей, раздельный вывод элементов интерфейса скорее неудобен, поскольку приходится тщательно располагать их в нужных местах и индивидуально подстраивать размеры отдельных окон и палитр. Однако после настройки элементы интерфейса выводятся в том виде, как это было задано.

Главное окно системы имеет скромный вид, поскольку не содержит ничего, кроме строк заголовка и меню. Справа и снизу большого окна редактирования находятся линейки прокрутки с ползунками, управляемыми мышью. Они предназначены для пролистывания текстов больших документов, если последние не помещаются в видимой части окна. Положение ползунка приближенно указывает место в документе, которое в данный момент отображается на экране. В самом низу в начале линейки прокрутки имеется строка состояния (*Status bar*) с информацией о текущем режиме работы. Эта информация (если она есть в данный момент) полезна для оперативного контроля в ходе работы с системой.

Главное меню системы (рис.1) содержит следующие позиции:

File — работа с файлами: создание нового файла, выбор файла из каталога, закрытие файла, запись текущего файла, запись файла с изменением имени, печать документа и завершение работы;

Edit — основные операции редактирования (отмена операции, копирование выделенных участков документа в буфер с их удалением и без удаления, перенос выделенных участков, их стирание);

Cell — работа с ячейками (объединение и разъединение ячеек, установка статуса ячейки, открытие и закрытие);

Format — управление форматом документов;

Input — задание элементов ввода (графиков, матриц, гиперссылок);

Kernel — управление ядром системы;

Find — поиск заданных данных;

Window — операции с окнами и их расположением;

Help — управление справочной системой.

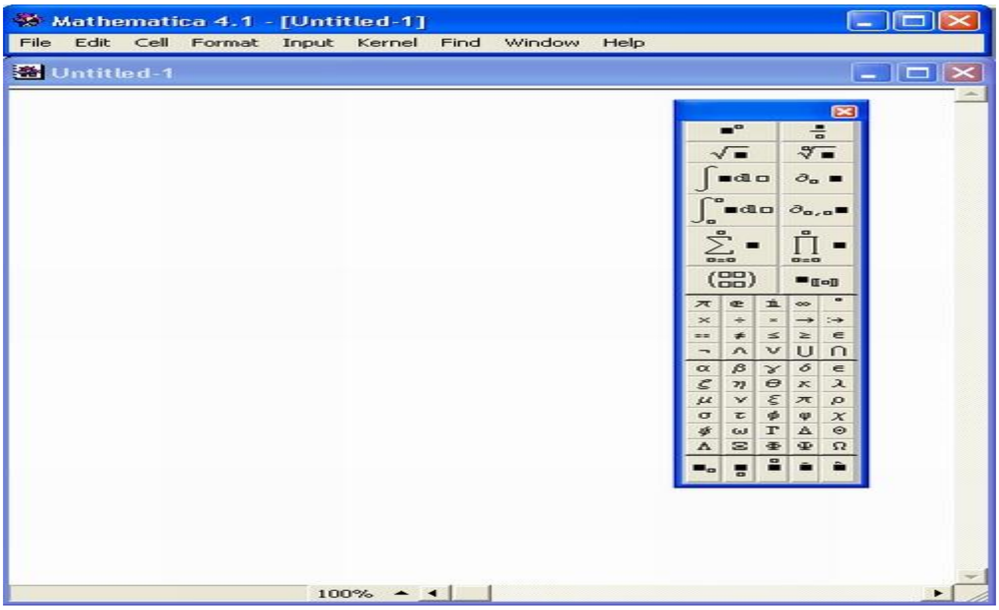

Рис.1. Начало работы с системой *Mathematica 4.1*

Часть команд может быть в данный момент невыполнима. Например, нельзя вычислить значение выражения, если его самого нет в окне редактирования или если ячейка с ним не выделена. Названия таких команд даны серым расплывчатым шрифтом. Четкий шрифт, напротив, характерен для тех команд, которые в данный момент могут исполняться. Управление главным меню обычное.

У многих программ интерфейс предусматривает вывод панелей с кнопками быстрого управления: панели инструментов и панели форматирования.

Если большинство фирм — разработчиков программ компьютерной математики пошло по пути уменьшения числа таких кнопок, то *Wolfram Research* сделала решительный шаг и отказалась от вывода инструментальной панели с такими кнопками.

Причина этого шага очевидна — запомнить назначение множества кнопок по рисункам на них не проще, чем иметь дело со множеством имен команд в обычном меню. Однако, сделав шаг назад, фирма одновременно сделала два шага вперед — она ввела выбираемые пользователем и перемещаемые по экрану в любое место инструментальные палитры со множеством пиктограмм ввода математических символов, функций и команд управления системой. Они выводятся с помощью меню *File* | *Palettes* (*Файл* | *Палитры*).

Если вывести все инструментальные палитры, то они с трудом умещаются в главном окне системы (рис.2):

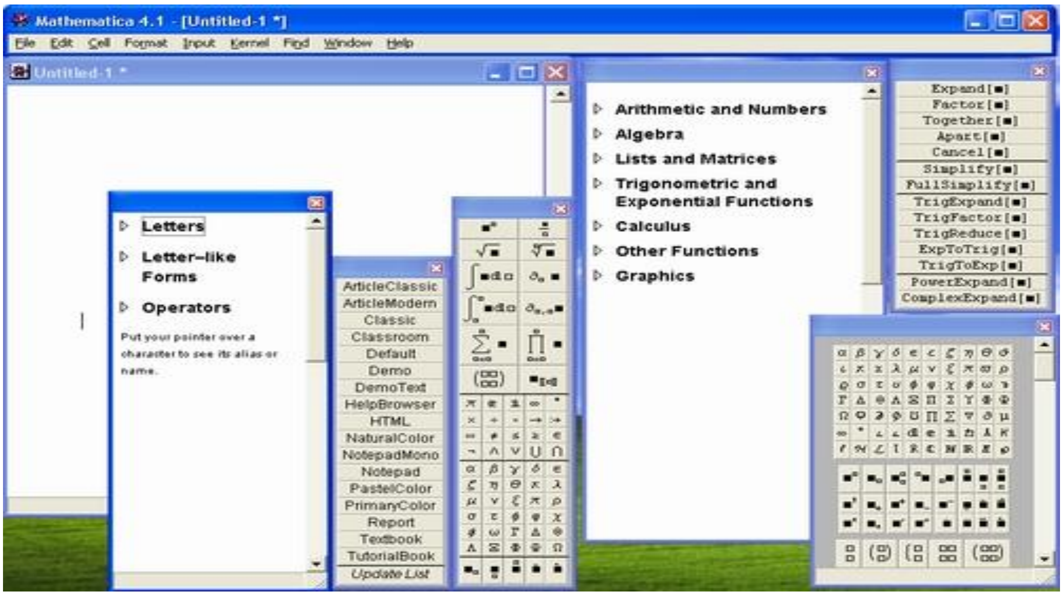

Рис.2. Инструментальные палитры системы *Mathematica 4.1*

Палитры, которые предназначены для ввода математических спецзнаков, намного упрощают работу по подготовке документов. Общее число специальных математических знаков (греческих и латинских букв, операторов, функций и команд), вводимых с помощью палитр, составляет около 700. Многие знаки имеют альтернативные варианты ввода с применением комбинаций клавиш — их можно найти в справочной базе данных системы.

Рисунок 2 наглядно показывает, что целесообразно пользоваться не более чем двумя-тремя панелями одновременно. Для удаления ненужных панелей в правом верхнем углу каждой из них расположены маленькие кнопки со знаком ×. Все панели максимально компактны и могут перетаскиваться мышью в наиболее удобное место экрана.

Если убрать все панели, то интерфейс системы, на первый взгляд, оказывается достаточно простым — остается одна панель с главным меню и висящее отдельно окно документа.

Если завершить работу с системой *Mathematica* при выведенных панелях математических знаков, то в следующем сеансе работы эти панели появятся на тех местах, где они были расположены перед выходом. Таким образом, интерфейс систем *Mathematica* обладает своеобразной памятью.

§ 3. Компьютерная алгебра в системе *Mathematica*

Компьютерная алгебра — это область на стыке математики и информатики, направленная на автоматизацию процесса решения математических задач путем преобразования математических выражений. Ранее в отечественной литературе она получила название аналитических вычислений (преобразований). Первое название отражает положение, когда алгоритмы преобразования математических выражений носят ярко выраженный алгебраический характер. Компьютерная алгебра, как область информатики, включающая в себя системные, алгоритмические и прикладные аспекты, обладает целым рядом специфических особенностей. Вычисления, производимые в компьютерной алгебре, требуют разработки новых алгоритмических и математических методов для их выполнения даже при наличии самого современного и производительного оборудования, оснащенного новейшим программным обеспечением. Методы информатики и программирования, используемые в компьютерной алгебре, также выходят за рамки тех, которые типичны для численных методов. Абстрактные типы данных, объектно-ориентированное программирование, другие передовые методы приобретают здесь особую значимость. Основную сложность по времени используемых алгоритмов компьютерной алгебры составляет арифметика целых чисел неограниченной точности. Понимание и ее правильное использование необходимо при работе с распространенными системами компьютерной алгебры: *Maple, Mathematica, Reduce, ScratchPad, Macsyma, MuPad, Magma* и значительным количеством специализированных программ. Алгоритмы арифметики пришли к нам из глубокой древности. Но, несмотря на возраст, арифметика продолжает свое бурное развитие в связи с увеличением использования компьютеров при проведении научных исследований. Имеется большое количество разработок. Их цель — дать полное для практического применения изложение арифметики в разных алгебраических областях, дать понятие проблематики дисциплины для правильного использования систем компьютерной алгебры, показать на многочисленных примерах методологию разработки алгоритма от математической идеи до формулировки алгоритма, обоснования, оценки сложности алгоритма по времени выполнения и требуемого объема памяти, а также проблемы реализации на конкретном языке. В качестве приложения полученных знаний приводятся криптографические алгоритмы, как применяемые очень давно, так и современные.

Компьютерная алгебра в *Mathematica* включает в себя следующие возможности:

– работа с выражениями;
– выделения и подстановки в функциях;
– рекурсивные функции;
– инверсные функции;
– задание математических отношений;
– упрощение выражений;
– раскрытие и расширение выражений;
– функции преобразования тригонометрических выражений;
– основные операции над многочленами;
– функции для расширенных операций с выражениями.

Математические выражения — основа описания алгоритмов вычислений. Фактически, вся символьная математика основана на тех или иных видах преобразований выражений. Такие преобразования опишем в следующем параграфе.

§ 4. Функции компьютерной алгебры в системе *Mathematica*

Системы компьютерной алгебры имеют несколько характерных для них функций, выполняющих достаточно сложные преобразования выражений. Названия этих функций вполне установились: *Simplify, Expand, Collect, Factor* и т.д. и встречаются практически во всех системах символьной математики. Рассмотрим их более подробно. Прежде всего, рассмотрим упрощение выражений (*Simplify*), раскрытие и расширение выражений (*Expand*), функция приведения (*Collect*), нахождение корней уравнений (*Roots*).

Функция *Simplify*. Упрощение математических выражений — одна из самых важных задач символьной математики. Иногда невероятно сложное математическое выражение является либо просто нулем или единицей, либо сводится к простому выражению после ряда заурядных преобразований. Качество выполнения операции упрощения во многом определяется мощью ядра математической системы, поскольку зависит от числа заложенных в него функций и правил преобразования выражений.

Mathematica всегда старается упростить то или иное выражение, если для этого не требуется каких-либо особых средств. Например, сложные выражения, содержащие элементарные или специальные функции, превращаются в более простые выражения — в том лишь смысле, что они состоят из более простых функций. Следующие примеры иллюстрируют это. Однако так бывает не всегда, и для проведения необходимых преобразований используются различные функции.

Ввод (In)	Вывод (Out)
(Csc[x] Tan[w]) / (Cot[x] Sec[w])	Sec[x] Sin[w]
BesselY[5/2, E]	SQRT(2/л)(Cos[E]- [3Cos[E]+3Sin[E]]/SQRT(E))

Для упрощения выражений используется функция *Simplify* [*expr*]. Она исполняет последовательность алгебраических преобразований над выражением *expr* и возвращает простейшую из найденных форм (обычно это бывает нормальная форма выражения).

Функция *Simplify* работает с самыми различными математическими выражениями: многочленами, рациональными выражениями (состоящими из многочленов и их отношений), расширенными рациональными выражениями (имеющими дробные степени переменных), элементарными и специальными функциями, алгебраическими и тригонометрическими выражениями и так далее. Обычно она приводит выражения к нормальному виду, что автоматически означает и приведение к виду достаточно простых выражений.

Приведем наиболее характерные результаты действия функции *Simplify*.

Ввод (In)	Вывод (Out)
Комбинирование числовых подвыражений Simplify [6x2]	12 x
Приведение подобных множителей у произведений Simplify[x^3 y x^5]	x^8y
Приведение подобных членов суммы Simplify[x + 12 + 4x]	5x + 12
Упрощение тождеств, содержащих 0 или 1	2x

Simplify [2+0] Simplify[l*x]	
Распределение целочисленных показателей степени в произведениях Simplify[(5x^2y^3)^2]	$5x^4 y^6$
Приведение общих знаменателей к выражениям с пониженной степенью или с исключением сокращаемых переменных Simplify [2 x/(x^2 – 1) – 1/(x + 1)]	1/(x+1)
Разложение полиномов и понижение степени выражений Simplify[(x + 1)^2 – x^2]	2x + 1
Сокращение на наибольший полиномиальный делитель Simplify [(x^2 – 2xy + y^2) / (x^2 – y^2)]	(x – y)/(x + y)

Следующие примеры дополнительно поясняют применение функции *Simplify*.

Ввод (In)	Вывод (Out)
Simplify[a*a – 2*a*b + b^2]	$(a – b)^2$
Simplify [Exp[x]^2/x]	E^{2x}/X
Sirnplif y [Sin[x – y] -Sin [x+y]]	2Cos[y] Sin[x]
Simplif y [Exp[x]*Exp [y]/Exp[z]]	E^{x+y-z}
Simplify [Exp[z*Log[b]]]	b^z
Simplify [Log[x/y]]	Log[x/y]
A:=(Cos[4*x]–4*Cos[2*x]+3)/(4*Cos[2*x]+Cos[4*x]+ 3) Simplify [A]	$Tan[x]^4$
Simplify[6*Log[10]]	6Log[10]
Simplify[6 Log[10], Complexity Function -> LeafCount]	Log[1000000]

Операция *Simplify* часто выполняется по умолчанию. Например, это обычно происходит при вычислении выражений, примеры чего приводились выше. Несомненно, это одна из наиболее важных и часто применяемых операций компьютерной алгебры.

Здесь нужно заметить, что понятие упрощения математических выражений не является однозначным. К примеру, некоторые пакеты символьной математики упрощают *sin x/cos x* к единой математической функции *tg x,* тогда как другие упрощают *tgx* к *sinx/cosx,* считая, что функции *sinx* и *cosx* более простые, чем функция *tgx.* Эта неоднозначность часто сбивает неопытных пользователей, пытающихся проверить символьные системы примерами из справочников.

Функция *FullSimplify*, область применения которой в *Mathematica* заметно расширена, обладает заметно большими возможностями, чем функция *Simplify*. В частности, она обеспечивает упрощение выражений, содержащих специальные математические функции.

Функции класса *Expand*. Расширение, или раскрытие, выражений — еще одна типовая операция компьютерной алгебры. По смыслу она противоположна упрощению выражений. Часто компактная форма представления выражений обусловлена определенными операциями по их упрощению. Существует множество выражений, для которых эти правила известны. Например, мы знаем, что выражение $(a - b)^2=(a - b)\cdot(a - b)$ можно представить как $a^2-2ab + b^2$.

Разумеется, такое соответствие существует далеко не всегда. К примеру, выражение в виде числа *1* вовсе не является представлением только выражения $sin^2x + cos^2x$.

Ниже представлены основные функции, производящие раскрытие и расширение выражений.

1. *ComplexExpand* [*expr*] — раскрывает *expr*, полагая все переменные вещественными.

2. *ComplexExpand* [*expr*, $\{x_1, x_2, ..., x_i\}$] — раскрывает *expr*, считая переменные x_i комплексными.

3. *FunctionExpand* [*expr*] — раскрывает выражения *expr,* содержащие специальные функции.

4. *Expand* [*expr*] — раскрывает произведения и положительные целые степени в *expr.*

5. *Expand* [*expr, patt*] — выполняет расширение только для тех элементов *expr*, которые содержат соответствующие шаблону *patt* члены.

6. *ExpandAll* [*expr*] — раскрывает все произведения и целочисленные степени в любой части *expr.*

7. *ExpandAll* [*expr, patt*] — исключает из операции расширения те части *expr*, которые не содержат соответствующие шаблону *patt* члены.

8. *ExpandDenominator* [*expr*] — раскрывает произведение и степени, которые присутствуют в выражении *expr* в роли знаменателей.

9. *ExpandNumerator* [*expr*] — раскрывает произведения и степени в числителе выражения *expr.*

10. *PowerExpand* [*expr*] — раскрывает вложенные степени, степени произведений, логарифмы от степеней и логарифмы от произведений. Осторожно используйте *PowerExpand*, так как эта функция не реагирует на разрывный характер выражения *expr*.

Приведем примеры операций расширения выражений с помощью функции *Expand*.

Пример 4.1

In[56]:=Expand[(x – a)(x – b)*(x – c)]*

Out[56]=$acx - ax^2 - cx^2 - acb + cxb - x^2b$

In[57]:= Simplify[%]

Out[57]:=(a – x)(c – x)(x – b)

Пример 4.2

*In[61]:=Expand[(Sin[x] + Cos[x]) / Cos[x) * Sin[x])]*

Out[61]=Csc[x] + Sec[x]

In[59]:= Simplify[%]

Out[59]:= Csc[x] + Sec[x]

Пример 4.3

In[66]:= Expand[2 + Cos[x] ^2, Trig→True]

Out[66]=2 Cos[x]^2

In[67]:= Simplify[%]

Out[67]=2 Cos[x]^2

Пример 4.4

In[68]:= Expand[Sin [x]^2] + Cos[x]^2]

Out[68]= Cos[x]^2 *+ Sin[x]*^{2}

In[69]:= Simplify[%]

Out[69]= 1

Пример 4.5

In[70]:= Expand[Sin [x]^2] + Cos[y]^2, Trig→True]]

Out[70]=1 – Cos[x]^2*/2 + Cos[y]*^{2}*/2 + Sin[x]*^{2}*/2 – Sin[y]*^{2}*/2*

In[71]:= Simplify[%]

Out[71]=1/2(2 – Cos[2x]+ Cos[2y])

В этих примерах полезно обратить внимание на то, что не всегда последовательное применение функций *Expand* и *Simplify* дает исходное выражение. Чаще получается новое выражение, порой представляющее определенную ценность. При операциях с тригонометрическими выражениями нередко нужно использовать опцию *Trig->True*, намечая тригонометрический путь решения. В противном случае может быть просто выдан отказ от выполнения операции *Expand* с заданным выражением, которое будет просто повторено в ячейке вывода.

Функция приведения *Collect.* К операциям, расширяющим выражения, относится также функция *Collect*:

1. *Collect* [*expr, x*] — выполняет приведение общих членов выражения по степеням переменной x.

2. *Collect [expr,* $\{x_1, x_2, \ldots, x_n\}$*]* — выполняет приведение общих членов выражения по степеням переменных $x_1, x_2, \ldots, x_n$.

Эта операция особенно полезна, если результат можно представить в виде степенных многочленов. Проиллюстрируем это следующими примерами.

Ввод (In)	Вывод (Out)
expr = *(5 + x ^2) * (x – 1)*x*	$(-1 + x)\,x(5 + x^2)$
Collect [*a*x^2 +b*x*y + c*y + d*y^2, y*]	$ax^2 + (c + bx)\,y + dy^2$
Collect [*a*x^2 + b*x*y + c*y+ d*y^2, x*]	$ax^2 + cy + bxy + dy^2$

Следующий пример показывает применение функции *Collect* к выражению с двумя переменными:

Collect [(x – 1)(y – 3)*(x – 2)*(y – 2)*(x – 1), y, x]*

$yx[-5(-2 + x)\,(-1 + x)^2] + y^2x[(-2 + x)(-1+x)^2 + x[6(-2+ x)(-1+ x)^2]$.

Как и в случае упрощения выражений, их расширение не является однозначной операцией и предполагает наличие определенных условностей.

Из школьного курса математики известно, что многочленом (полиномом) называют выражение вида $P(x)=a_0+a_1x+a_2x^2+ a_3x^3+ \ldots + a_nx^n$, *где* a_i – фиксированные коэффициенты, x – переменная.

Хотя термин *полином* не очень прижился в отечественной математической литературе, оставим его здесь ввиду краткости и ради лучшего понимания синтаксиса функций системы, поскольку слова *poly* и *Polynomial* входят в параметры и имена многих функций. При этом полиномы мы будем кратко обозначать как *poly* или p_i (здесь *i* — индекс, или порядковый номер, полинома).

Над полиномами можно выполнять обычные арифметические операции: сложение, вычитание, умножение и деление.

Для получения результата умножения полиномов в обычной форме следует использовать функцию расширения символьных выражений *Expand.* Если один полином делится на другой, то для получения результата надо использовать функцию *Simplify*. В общем случае при делении полиномов может оставаться остаток. Функция, обеспечивающая деление полиномов и вычисляющая остаток, описана ниже.

***Factor* — разложение полиномов.** Разложение чисел, математических выражений и особенно полиномов на простые множители является столь же распространенной операцией, что и функции *Simplify*, *Collect* и *Expand*. Имеется целый ряд функций, в названии которых есть слово *Factor* и которые решают указанные задачи:

1. *Factor* [*poly*] — выполняет разложение полинома над целыми числами.

2. *Factor* [*poly, Modulus->p*] — выполняет разложение полинома по модулю простого числа *p*.

3. *Factorlnteger* [*n*] — возвращает список простых множителей целого числа *n* вместе с их показателями степеней. Опция *FactorComplete* позволяет указать, следует ли выполнять полное разложение.

4. *FactorList* [*poly*] — возвращает список множителей полинома с их показателями степени. Опция *Modulus->p* позволяет представить множители полинома по модулю простого числа *p*.

5. *FactorSquareFree* [*poly*] — записывает полином в виде произведения множителей, свободных от квадратов. Опция *Modulus->p* позволяет представить разложение полинома по модулю простого числа *p.*

6. *FactorSquareFreeList* [*poly*] — возвращает список множителей полинома, свободных от квадратов, вместе с показателями степени. Может использоваться опция *Modulus->p.*

7. *FactorTerms* [*poly*] — извлекает общий числовой множитель в *poly.*

8. *FactorTermsList* [*poly*] — возвращает лист всех общих числовых множителей полинома *poly.*

Далее представлен ряд примеров применения этих функций.

Ввод (In)	Вывод (Out)
Factor [x^$3 - 6$*x^$2 + 11$*$x - 6$] Factor [x^$3 - 6$*x^$2 + 21$*$x - 52$]	$(-3 + x)(-2 + x)(-1+x)(-4+x)$ $(13 - 2x+x^2)$
Factor [x^$5+ 8$*x^$4 + 31$*x ^$3 + 80$*x^2 + + 94*$x + 20$, Modulus -> 3]	$(1 + x)^2 (2 + x)^3$
FactorList[x^$4 - 1$, Modulus -> 2] FactorSquareFree [(x^2 + 1)*(x^4 – 1)]	{{1, 1},{1+ x, 4}} $(-1+x^2)(1+x^2)^2$
FactorSguareFree [$(x$^$2 + l)$*$(x$^$4 - 1)$, Modulus -> 2]	$(1+x)^6$
FactorSquareFreeListt (x^2+1)*(x^4–1), Modulus -> 2] FactorTerms[2*x^$2 + 4$*$x + 6$] FactorTermsList[2*x^$2 + 4$*$x + 6$]	{{1, 1), {1 + x, 6}} 2 (3+$2x+x^2$) {2, 3+ $2x+x^2$}
Factorlnteger [123456789]	{{3, 2), {3607, 1}, {3803, 1}}
FactorList[x^$4 - 1$]	{1, 1}, {–1 + x, 1}, {1+x, 1}, {1+x^2, 1}}
FactorSquareFreeListt [$(x$^$2+1)$*$(x$^$4-1)$]	{{1, 1}, {–1+x^2,1},{1+x^2, 2}}

Обычно функция *Factor* выявляет внутреннюю суть полинома, раскладывая его на множители, содержащие корни полинома. Однако в ряде случаев корни полинома удобнее получать в явном виде с помощью функции ***Roots.*** Ниже даны примеры использования функции.

Пример 4.6 Найти все корни уравнения $x^3 - x - 7 = 0$.

Решение данного примера в среде *Mathematica* будет следующим:

In[50]: = Roots[x³ – x – 7 = 0, x]

$$Out[50] = x = 1/3 \left(\frac{189}{2} - \frac{3\sqrt{3957}}{2}\right)^{1/3} + \frac{\left(\frac{1}{2}\left(63+\sqrt{3957}\right)\right)^{1/3}}{3^{2/3}} \;||$$

$$x = = -1/6 \left(1+i\sqrt{3}\right)\left(\frac{189}{2} - \frac{3\sqrt{3957}}{2}\right)^{1/3} - \frac{\left(1-i\sqrt{3}\right)\left(\frac{1}{2}\left(63+\sqrt{3957}\right)\right)^{1/3}}{23^{2/3}} \;||$$

$$x = = -1/6 \left(1-i\sqrt{3}\right)\left(\frac{189}{2} - \frac{3\sqrt{3957}}{2}\right)^{1/3} - \frac{\left(1-i\sqrt{3}\right)\left(\frac{1}{2}\left(63+\sqrt{3957}\right)\right)^{1/3}}{23^{2/3}}$$

Пример 4.7 Решить уравнение $6x^4 + 19x^3 - 7x^2 - 26x + 12 = 0$.

Используя функцию *Roots*, получим следующее решение:

*In[64]: = Roots[6*x^4+19*x^3 – 7*x^2 – 26*x + 12 = 0, x]*

$$x_1 = 1/3\left(-1-\sqrt{13}\right),\ x_2 = 1/3\left(-1+\sqrt{13}\right), x_3 = 1/2, x_4 = -3$$

Для работы с полиномами имеется еще ряд дополнительных функций.

1. *Decompose* [*poly, x*] — выполняет разложение полинома, если это возможно, на более простые полиномиальные множители.

2. *GroebnerBasis* [{*poly1, poly2, ..., polyn*}, {$x_1, x_2, ..., x_n$}] — возвращает список полиномов, которые образуют базис Гробнера для идеала, порожденного полиномами *poly*.

3. *Polynomial-Division* [*p, q, x*] — возвращает список частного и остатка, полученных делением полиномов *p* и *q* от *x*.

4. *PolynomialGCD* [*poly1, poly2, ..., polyn*] — возвращает наибольший общий делитель ряда полиномов *poly1, poly2* и т.д. С опцией *Modulus->p* функция возвращает наибольший общий делитель по модулю простого числа *p*.

5. *PolynomialLCM* [*poly1, poly2, ..., polyn*] — возвращает наименьшее общее кратное полиномов *poly1, poly2* и т. д. С опцией *Modulus->p* функция возвращает наименьшее общее кратное по модулю простого числа *p.*

6. *PolynomialMod* [*poly, m*] — возвращает полином *poly,* приведенный по модулю *m.*

7. *PolynomialMod* [*poly,* {*m1, m2, ..., mn*}] — выполняет приведение по модулю всех *mi.*

8. *PolynomialQ* [*expr, var*] — возвращает значение *True*, если *expr* является полиномом от *var*, иначе возвращает *False.*

9. *PolynomialQ* [*expr,* {*var1*}] — проверяет, является ли *expr* полиномом от *vari.*

10. *PolynomialQuotient* [*p, q, x*] — возвращает частное от деления *p* и *q* как полиномов от *x*, игнорируя какой-либо остаток.

11. *PolynomialRemainder* [*p, q, x*] — возвращает остаток от деления *p* на *q* как полиномов от *x.*

12. *Resultant* [*poly1, poly2, var*] — вычисляет результант полиномов *poly1* и *poly2* по переменной *var.* С опцией *Modulus->p* функция вычисляет результат по модулю простого числа *p.*

Итак, работа с этими функциями, по существу, сводит операции с таким сложным видом символьных данных, как многочлены, к типовым алгебраическим операциям над обычными символьными переменными.

Далее, в последующих главах, изложение математической теории сопровождается примерами задач, решенными с помощью универсального математического пакета *Mathematica* с применением вышеперечисленных дополнительных функций над многочленами.

Глава 2. МНОГОЧЛЕНЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

§ 5. Основные понятия и определения

Данный параграф будет посвящен краткому изложению элементов абстрактной алгебры.

Определение 5.1. Отношение, при котором каждой упорядоченной паре (a, b) элементов множества M ставится в соответствие единственный элемент c из этого же множества, называется бинарной алгебраической операцией, определяемой на множестве M.

Определение 5.2. *Группой* G называется множество с одной бинарной алгебраической операцией $*$, обладающей следующими свойствами:

1) $(\forall a, \quad b, c \in G)\ a * (b * c) = (a * b) * c$ — ассоциативности;

2) $(\exists n \in G)(\forall a \in G)\ a * n = n * a = a;$

3) $(\forall a \in G)(\exists a' \in G)\ a' * a = a * a' = n.$

Операция $*$, удовлетворяющая свойствам 1—3, иногда называется групповой операцией, а элементы множества G — элементами группы.

Свойством коммутативности группа может не обладать. Если же в группе выполняется свойство коммутативности для любых элементов $(a*b=b*a)$, то она называется коммутативной, или абелевой.

Простейшие свойства групп (на мультипликативном языке) следующие.

1. В каждой группе существует только одна единица e (по теореме о единственности нейтрального элемента).

2. В каждой группе любой элемент g имеет единственный ему обратный элемент $g^{-1} \in G$.

3. Во всякой группе каждое из уравнений $ax=b$ и $ya=b$ при любых $a, b \in G$ имеет решение и притом только одно.

4. Справедливы законы сокращения:

$(\forall a, b, c \in G)\ ab = cb \Rightarrow a = c$ (сокращение справа),

$(\forall a, b, c \in G)\ ba = bc \Rightarrow a = c$ (сокращение слева).

5. $(\forall a, b \in G)\ ab = a \Rightarrow b = 1$ и $(\forall a, b \in G)\ ba = a \Rightarrow b = 1.$

6. $(\forall a, b \in G)\ ab = 1 \Rightarrow a^{-1} = b \wedge b^{-1} = a.$

7. В группе имеет место обобщенный закон ассоциативности

$(a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}) \cdot a_n = (a_1 \cdot a_2 \cdot \ldots \cdot a_{n-2}) \cdot \ldots \cdot a_{n-1} \cdot a_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, а если группа абелева — обобщенный закон коммутативности.

8. $(\forall a \in G)\ (a^{-1})^{-1} = a$.

9. $(\forall a_1, a_2, \ldots, a_n \in G)\ (a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = (a_n)^{-1} \cdot (a_{n-1})^{-1} \cdot \ldots \cdot (a_1)^{-1}$

Определение 5.3. Непустое подмножество H группы $(G,\circ)$ называется подгруппой группы G, если оно само является группой относительно той же операции, что и группа G.

Критерий подгруппы: непустое подмножество H группы G является подгруппой группы G тогда и только тогда, когда

1) $(\forall a, b \in H)\ a \cdot b \in H$; 2) $(\forall a \in H)\ (a^{-1}) \in H$.

Определение 5.4. Пусть имеется две группы $(G_1,\circ)$ и $(G_2,*)$. Отображение f: $G_1 \to G_2$ называется гомоморфизмом групп, если

$(\forall g_1, g_2 \in G_1)\ f(g_1 \circ g_2) = f(g_1) * f(g_2)$.

Определение 5.5. Отображение f: $G_1 \to G_2$ называется изоморфизмом групп $(G_1,\circ)$ и $(G_2,*)$, если

а) f — взаимно однозначное соответствие между множеством элементов первой группы и множеством элементов второй группы;

б) $(\forall g_1, g_2 \in G_1)\ f(g_1 \circ g_2) = f(g_1) * f(g_2)$.

Определение 5.6. Алгебра $(K, +, \cdot)$ — кольцо, если $(K, +)$ — абелева группа; $(K, \cdot)$ — полугруппа (множество с алгебраической и ассоциативной операцией); умножение дистрибутивно относительно сложения.

В развернутом виде определение кольца таково:

Алгебра $(K, +, \cdot)$ – ***кольцо***, если:

1. $(\forall a, b \in K)\ a+b \in K,\ a \cdot b \in K$;
2. $(\forall a, b, c \in K)\ a+(b+c)=(a+b)+c$;
3. $(\forall a, b \in K)\ a+b=b+a$;
4. $(\exists n \in K)\ (\forall a \in K)\ a+n=n+a=a$;
5. $(\forall a \in K)\ (\exists a' \in K)\ a+a'=a'+a=n$;
6. $(\forall a, b, c \in K)\ a \cdot (b \cdot c)=(a \cdot b) \cdot c$;
7. $(\forall a, b, c \in K)\ (a+b) \cdot c=ac+bc$ — левая дистрибутивность умножения относительно сложения, $c \cdot (a+b)=ca+cb$ — правая дистрибутивность умножения относительно сложения.

Кольцо с единицей (то есть нейтральным элементом относительно умножения) называется унитарным. Если умножение коммутативно, то кольцо называется коммутативным.

Свойства колец следующие:

1. Так как $(K, +)$ — абелева группа, то справедливы все свойства групп.

2. Характеристические свойства:

1) $0 \cdot a = a \cdot 0 = 0$ (нуль является поглощающим элементом);

2) правило знаков: $(-a)в = (-ав)$; $a(-в) = (-ав)$; $(-a)(-в) = ав$.

3) $(\forall a, b \in K)\ \left.\begin{aligned} a\,(в - с) &= ав - ас \\ (в - с)\,a &= ва - са \end{aligned}\right\}$ дистрибутивность умножения относительно вычитания

Пусть K — область целостности (коммутативное кольцо с единицей и без делителей нуля). В кольце K можно определить отношение делимости.

Определение 5.7. Элемент a кольца K делится на элемент b того же кольца, если существует такой элемент $q \in K$, что $a = bq$. В этом случае пишут $a \,\vdots\, b$. Элемент b называется делителем элемента a.

Определение 5.8. Элемент ε кольца K называется обратимым, если в кольце K существует такой элемент ε_1, что $\varepsilon \cdot \varepsilon_1 = e$.

Критерий подкольца: непустое подмножество S кольца K является подкольцом тогда и только тогда, когда

1) $(\forall a, в \in S)\ a + в \in S$	или	$(\forall a, в \in S)$
2) $(\forall a \in S)\ \ -a \in S$		1) $a - в \in S$
3) $(\forall a, в \in S)\ \ a \cdot в \in S$		2) $a \cdot в \in S$

Определение 5.9. Кольцо K называется областью целостности, если в нем нет делителей нуля (то есть если $ав = 0$, то $a = 0 \vee в = 0$). Элементы кольца называются ассоциированными, если $a \,\vdots\, в \wedge в \,\vdots\, a$.

Определение 5.10. Пусть имеется два кольца $(K_1, +, \cdot)$ и $(K_2, \oplus, \otimes)$. Отображение $f: K_1 \to K_2$ называется гомоморфизмом колец, если

1) $f(a+в) = f(a) \oplus f(в)$; 2) $f(a \cdot в) = f(a) \otimes f(в)$.

Гомоморфное взаимно однозначное отображение кольца K_1 на кольцо K_2 называют изоморфизмом колец.

Определение 5.11. Алгебра $(P, +, \cdot)$ — поле, если $(P, +)$ — абелева группа, $(P \setminus \{0\}, \cdot)$ — абелева группа, умножение дистрибутивно относительно сложения.

Простейшие свойства поля следующие:

1. Так как поле является кольцом, то для него справедливы все свойства колец.

2. Свойства, специфические для полей:

1) в поле не существует делителей нуля. В поле можно ввести операцию деления: $\frac{a}{b} = a \cdot b^{-1}$;

2) $-a = (-1) \cdot a$; $\frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b}$;

3) $\left(\frac{в}{a}\right)^{-1} = \frac{a}{в}$;

4) $\frac{a}{в} \pm \frac{c}{d} = \frac{ad \pm вc}{вd}$;

5) критерий равенства дробей: $\frac{a}{в} = \frac{c}{d} \Leftrightarrow ad = вc$;

6) $\frac{a}{в} \cdot \frac{c}{d} = \frac{ac}{вd}$;

7) $ac = вc \wedge c \neq 0 \Rightarrow a = в$;

8) $aв = 1 \Rightarrow a \neq 0 \wedge в = a^{-1}$;

9) $aв = 0 \Rightarrow a = 0 \vee в = 0$;

10) $\frac{ac}{вc} = \frac{a}{в}$.

К р и т е р и й п о д п о л я*:* непустое подмножество S поля P является подполем поля P тогда и только тогда, когда

1) $(\forall a, в \in S)\ a + в \in S$; 2) $(\forall a, в \in \mathrm{S})\ a \cdot в \in \mathrm{S}$;

3) $(\exists a \in S) -a \in S$; 4) $(\exists a \in \mathrm{S})\ a^{-1} \in \mathrm{S}$.

Определение 5.12. Числовым полем называется любое подполе поля комплексных чисел.

Определение 5.13. Главным идеалом кольца *K*, порожденным элементом *a* этого кольца, называют множество элементов кольца *K*, кратных *a*. Главный идеал, порожденный элементом *a*, обозначают (*a*). Таким образом, $(a) = \{ra, r \in R\}$. То есть, $b \in (a)$ в том и только в том случае, когда $b \vdots a$.

Свойства главных идеалов следующие:

1. Любой элемент *a* кольца *K* принадлежит порожденному им главному идеалу: $a \in (a)$

2. $(0) = \{0\}, (e) = K$.

3. Если $b, c \in (a)$, то $b - c \in (a)$.

4. Если $b \in (a)$, то для любого $r \in K$ следует, что $br \in (a)$.

Следующее свойство главных идеалов позволяет свести отношение делимости элементов кольца *К* к отношению включения соответствующих главных идеалов.

5. Элемент *a* кольца *К* делится на элемент *b* того же кольца в том и только в том случае, когда $(a) \subset (b)$. Пользуясь свойством 5, можно переформулировать свойства делимости для элементов кольца на языке включения главных идеалов. Например, справедливо следующее утверждение:

6. Ассоциированные элементы кольца *К* порождают один и тот же главный идеал. Частным случаем свойства 6 является следующее свойство:

7. Главный идеал, порожденный обратимым элементом ε кольца *К*, совпадает с *К*. В областях целостности верно и обращение свойства 6:

8. Если главные идеалы, порожденные элементами *a* и *b* области целостности совпадают, то есть $(a) = (b)$, то элементы *a* и *b* ассоциированы в *К*.

Введем теперь общее понятие идеала кольца.

Определение 5.14. Подмножество *I* кольца *К* называется идеалом в *К*, если для любых *a* и *b* из *I* подмножество *I* содержит их разность $a - b$; и для любого *r* из кольца *К* вместе с каждым элементом *a* подмножество *I* содержит все кратные *ra*.

Свойства 3 и 4 главных идеалов показывают, что каждый главный идеал кольца *К* является идеалом этого кольца.

Теорема 5.1. Пусть $a_1,\ a_2, \ldots, a_{\mathrm{n}}$ — некоторые элементы кольца *К*. Тогда множество *I* всех элементов вида $r_1 a_1 + r_2 a_2 + \ldots + r_n a_n$, (1)

где $r_k \in K$, $k = 1, 2, \ldots, n$, образует идеал в кольце *К*.

Теорема 5.2. Пусть *А* — любое подмножество кольца *К*. Множество *I* всех элементов вида

$$r_1 a_1 + r_2 a_2 + \ldots + r_n a_n, \quad (2)$$

где $a_1, a_2, \ldots, a_n$ — некоторые элементы из *А*, а $r_k \in K$, $k = 1, 2, \ldots, n$, является идеалом в *К*.

Идеал *I*, состоящий из всех элементов вида (2), называют идеалом, порожденным множеством *А*, и обозначают (A). В частности, если *А* состоит из одного элемента a, $A=\{a\}$, то порожденный A идеал — это главный идеал, порожденный элементом a. Любой элемент a из A можно представить в виде $a=ae$, то есть имеет вид (2), а поэтому $A\subset(A)$.

Теорема 5.3. Пересечение $I_1\cap I_2$ двух идеалов I_1 и I_2 кольца K является идеалом того же кольца.

Теорему 5.3 можно обобщить на любое множество идеалов.

Теорема 5.3'. Пересечение любого множества идеалов кольца K является идеалом в K.

Теорема 5.4. Наименьший идеал $I(A)$ кольца K, содержащий подмножество A этого кольца, совпадает с идеалом (A), порожденным подмножеством A.

§ 6. Кольцо многочленов

Пусть A — коммутативное кольцо с единицей. Построим новое кольцо B, элементами которого являются бесконечные упорядоченные последовательности

$$f=(f_0,\ f_1,\ f_2...),\ f_i\in\mathrm{A}, \tag{1}$$

в которых все элементы, начиная с некоторого, равны нулю. Такую последовательность назовем псевдобесконечной. Определим на множестве B операции сложения и умножения, полагая

$$f+g=(f_0,\ f_1,\ f_2...)+(g_0,g_1,g_2...)=(f_0+g_0,f_1+g_1,f_2+g_2,...),$$

$$f\cdot g=h=(h_0,h_1,h_2...)=(f_0g_0,\ f_0g_1+f_1g_0,\ ...)=\sum_{i+j=k}f_ig_j, \text{ где } k=0,1,2,...,n.$$

Покажем, что множество B относительно указанных операций является кольцом. Воспользуемся определением кольца.

1. Проверим, что $(B,+)$ — абелева группа. Очевидно:

а) операция сложения алгебраическая, так как в результате сложения двух бесконечных упорядоченных последовательностей вида (1) получается снова последовательность, у которой все элементы, начиная с некоторого, равны нулю;

б) операция сложения ассоциативна и коммутативна, поскольку она ассоциативна и коммутативна в множестве A, которое является коммутативным кольцом;

в) нейтральный элемент $(0,\ 0,\ 0,\ 0,\ ...,\ 0)=\theta$ и верно равенство $f+\theta=\theta+f=f$;

г) противоположный элемент $-f = (-f_0, -f_1, ..., -f_k, 0...)$ и верно равенство $f + (-f) = \theta$.

Таким образом, мы доказали, что $(B, +)$ — абелева группа.

2. Покажем, что $(B, \cdot)$ — полугруппа.

Операция умножения алгебраическая, так как в результате умножения двух бесконечных упорядоченных последовательностей вида (1) получается снова последовательность, у которой все элементы, начиная с некоторого, равны нулю.

Задание 1. Показать, что операция умножения коммутативна и ассоциативна на множестве B.

Задание 2. Показать, что умножение дистрибутивно относительно сложения, то есть $(f + g)\cdot h = f\cdot h + g\cdot h$.

3. Единица кольца — последовательность $1 = (1, 0, 0,...)$, так как $(1, 0, 0,...)\cdot f = f\cdot(1, 0, 0...) = (f_0, f_1, ..., f_k, 0...)$

Из пунктов 1 — 3 и заданий 1, 2 следует, что B — коммутативное кольцо с единицей. Последовательности вида $(a, 0,..., 0...)$ складываются и умножаются так же, как элементы кольца A. Это позволяет отождествить такие последовательности с соответствующими элементами из A, то есть обозначить $a=(a, 0,..., 0,...)$ для всех $a \in A$. Тем самым A становится подкольцом кольца B. Рассмотрим теперь последовательность $(0, 1, 0,..., 0,...)$, обозначив ее x, и назовем переменной над A. Используя введенную на множестве B операцию умножения, находим, что

$$x^2 = x \cdot x = (0, 0, 1, 0, ..., 0...),$$

. . . .

$$x^n = x \cdot x \cdot ... \cdot x = (0, 0, ...0, 1, 0, ..., 0, ...) \qquad (2)$$

Ввиду равенства (2) и так как $A \subset B$, имеем $f = (a_0, a_1, a_2, ..., a_n, 0,...) =$

$$= (a_0, 0, 0, ..., 0, ...) + (0, a_1, 0, ..., 0, 0, ...) + ... + (0, 0, ..., a_n, 0, ...) =$$

$$= a_0 + a_1(0, 1, 0, ...) + a_2(0, 0, 1, 0, ...) + ... + a_n(0, 0, ..., 1, 0, ...) =$$

$$= a_0 + a_1x + a_2x^2 + ... + a_nx^n \qquad (3)$$

Определение 6.1. Введенное выше кольцо B обозначается через $A[x]$ и называется кольцом многочленов над A от одной переменной x, а его элементы — многочленами (или полиномами) от переменной x.

Определение 6.2. Формальное выражение, состоящее из нескольких одночленов, соединенных знаком +, называется многочленом или полиномом от x с коэффициентами из A.

Запись многочлена в виде $f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ называется канонической, или естественной.

Определение 6.3. Пусть $f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, причем $a_n \neq 0$. Одночлен $a_n x^n$ называется старшим членом многочлена $f(x)$, а показатель n называется степенью многочлена $f(x)$ и обозначается *degf,* $a_0, a_1, a_2, \ldots, a_n$ — коэффициенты многочлена *f,* a_0 — свободный член.

Определение 6.4. Многочлен, старший коэффициент которого равен единице, называется нормированным (унитарным).

Многочлен *f* — нулевой, когда все его коэффициенты равны 0. Нулевому многочлену приписывают степень $-\infty$ и считают, что $-\infty < n$. Многочлены степени 1, 2, 3, … называются соответственно линейными, квадратными, кубическими и т.д.

Введем определение равенства многочленов и рассмотрим основные операции над ними.

Определение 6.5. Два многочлена считаются равными, если они составлены в канонической записи из одинаковых одночленов, то есть $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ в том и только в том случае, если $a_i = b_i$, $i = 0, 1, \ldots, n$.

Рассмотрим, как будут складываться и умножаться многочлены в каноническом виде. Пусть $f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_n \neq 0$,

$g(x)=b_s x^s + b_{s-1}x^{s-1} + \ldots + b_0$, $b_s \neq 0$ и $n \geq s$.

Определение 6.6. Суммой двух многочленов *f(x)* и *g(x)* называется многочлен $f(x)+g(x)=c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0$, коэффициенты которого получаются посредством сложения коэффициентов многочленов *f(x)* и *g(x),* стоящих при одинаковых степенях неизвестного, то есть $c_i = a_i + b_i$, где $i = 0, 1, \ldots, n$.

Если многочлены $f(x)$ и $g(x)$ имеют разное число одночленов, то, приписав необходимое число одночленов с нулевыми коэффициентами к одному из них, в котором число одночленов меньше, можно добиться их равенства в обоих многочленах. Поэтому складывать можно многочлены с разным числом одночленов. Например, пусть $f(x)=x^3+1$, $g(x)=x+3$ преобразуем $g(x)$ к виду $g(x)=0\cdot x^3 + 0\cdot x^2 + x + 3$, добавив два нулевых одночлена.

Суммой $f(x)$ и $g(x)$ будет многочлен $f(x)+g(x)=(1+0)x^3+(0+0)x^2+(0+1)x+(1+3)=x^3+x+4$.

Из соотношения

$$c_i = a_i + b_i,\ \mathrm{i}=0,\ 1,\ \ldots,\ n \qquad (4)$$

легко видеть, что операция суммирования (сложения) многочленов обладает такими же свойствами, что и операция сложения элементов кольца A, то есть она ассоциативна и коммутативна.

Многочлен, все коэффициенты которого нули, является нейтральным элементом относительно сложения многочленов; для каждого многочлена существует ему противоположный: противоположным к многочлену $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$ является многочлен $-f(x)=-a_nx^n-a_{n-1}x^{n-1}-\ \ldots\ -a_0$. Итак, множество многочленов с операцией сложения образует коммутативную группу.

Определение 6.7. Произведением двух многочленов называется многочлен, составленный из произведений всех членов первого сомножителя на все члены второго, то есть $f(x)\cdot g(x)=d_{n+s}x^{n+s}+d_{n+s-1}x^{n+s-1}+\ldots+d_0$. Коэффициенты определяются следующим образом: $d_i=\sum\limits_{k+l=i}a_kb_l$, $i\ =\ 0,\ 1, \ldots, n\ +\ s\ -\ 1,\ n\ +\ s$. То есть коэффициент d_i — сумма всевозможных произведений a_k и b_l, где $k+l=i$, в частности $d_0=a_0\cdot b_0,\ d_1=a_0\cdot b_1+a_1\cdot b_0, \ldots,\ d_{n+s}=a_n\cdot b_s$.

Пример 6.1. Найдем произведение многочленов $2x^4-x^3+x^2+x+1$ и x^2-3x+1, используя универсальный математический пакет *Mathematica*:

*In[11]:=Expand[(2*x^4 – x^3 + x^2 + x + 1) * (x^2 – 3*x + 1)]*

$Out[11] = 1-2x-x^2-3x^3+6x^4-7x^5+2x^6$

В результате получим многочлен $2x^6-7x^5+6x^4-3x^3-x^2-2x+1$.

Степень суммы двух многочленов будет равна n, если $n > s$, но при $n = s$ она может оказаться меньше n, а именно в случае $b_n = -a_n$. Кроме того, при сложении многочленов $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$ и $g(x)=b_sx^s+b_{s-1}x^{s-1}+\ldots+b_0$ мы видим, что формула для суммы не содержит членов, степень которых выше, чем $\max\{n,s\}$, а формула для произведения — членов, степень которых выше, чем $n + s$. Поэтому справедливы теоремы 6.1 и 6.2.

Теорема 6.1. Степень суммы двух ненулевых многочленов не больше максимальной степени слагаемых, то есть

$$\deg(f(x)+g(x)) \le \max\{\deg f(x), \deg g(x)\}. \qquad (5)$$

Теорема 6.2. Если A — область целостности, то степень произведения двух ненулевых многочленов равна сумме степеней сомножителей, то есть $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ (6)

Доказательство. Пусть $f(x)=a_n x^n + a_{n-1}x^{n-1}+\ldots+a_0$, $g(x)=b_s x^s + b_{s-1}x^{s-1}+\ldots+b_0$ — многочлены над областью целостности A и $a_n \ne 0$, $b_s \ne 0$. Тогда $f(x)\cdot g(x) = a_0\cdot b_0 + (a_0\cdot b_1 + a_1\cdot b_0)x + \ldots + a_n\cdot b_s x^{n+s}$.

При произведении многочленов $f(x)=a_n x^n + a_{n-1}x^{n-1}+\ldots+a_0$ степени n и $g(x)=b_s x^s + b_{s-1}x^{s-1}+\ldots+b_0$ степени s, старший член равен $a_n b_s$ (это коэффициент при x^{n+s}). Так как A — область целостности, то $a_n b_s \ne 0$, и значит, $f(x)g(x)\ne 0$. Из нашего рассуждения следует, что

$$\deg(f(x)g(x)) = n+s = \deg f(x) + \deg g(x) \square \qquad (7).$$

Формула (6) также справедлива и тогда, когда один из многочленов $f(x)$, $g(x)$ или они оба равны нулю.

Теорема 6.3. Кольцо многочленов над областью целостности само является областью целостности.

Так как $A[x]$ — кольцо, то, как и в любом кольце, можно рассмотреть вопросы делимости многочленов. Вспомним определение отношения делимости в произвольном кольце.

Определение 6.8. Элемент a кольца K делится на элемент b того же кольца, если существует такой элемент $q \in K$, что $a = bq$. В этом случае пишут $a \,\vdots\, b$. Элемент b называется делителем элемента a.

Определение 6.9. Пусть A — некоторая область целостности. Многочлен $f(x)\in A[x]$ делится на многочлен $\varphi(x)\in A[x]$, если в кольце $A[x]$ найдется такой многочлен $q(x)$, что $f(x) = \varphi(x)\cdot q(x)$. В этом случае пишут $f(x)\,\vdots\,\varphi(x)$. При этом многочлен $q(x)$ называют частным от деления $f(x)$ на $\varphi(x)$.

Простейшие свойства отношения делимости в кольце многочленов над областью целостности следующие:

1. Отношение делимости рефлексивно, то есть $f(x) \,\vdots\, f(x)$.
2. Отношение делимости транзитивно: если $f(x)\,\vdots\,g(x)$ и $g(x)\,\vdots\,h(x)$, то $f(x)\,\vdots\,h(x)$.

Доказательство. Если $f(x) \vdots g(x)$ и $g(x) \vdots h(x)$, то по определению 6.9 существуют многочлены $\varphi(x) \in A[x]$ и $\psi(x) \in A[x]$ такие, что $f(x) = g(x) \cdot \varphi(x)$ и $g(x) = h(x) \cdot \psi(x)$. Подставим второе равенство в первое: $f(x) = h(x) \cdot (\varphi(x) \cdot \psi(x))$, что означает $f(x) \vdots h(x)$. □

3. Если $f(x) \vdots \varphi(x)$ и $g(x) \vdots \varphi(x)$, то $(f(x) \pm g(x)) \vdots \varphi(x)$.

Доказательство. Складывая (вычитая) равенства $f(x) = \varphi(x) \cdot \psi(x)$ и $g(x) = \varphi(x) \cdot \lambda(x)$, получаем $f(x) \pm g(x) = \varphi(x) \cdot \psi(x) \pm \varphi(x) \cdot \lambda(x) = \varphi(x)(\psi(x) \pm \lambda(x))$, что влечет $(f(x) \pm g(x)) \vdots \varphi(x)$. □

4. Если $f(x) \vdots \varphi(x)$ и $g(x) \in A[x]$, то $(f(x) \cdot g(x)) \vdots \varphi(x)$.

Доказательство. Действительно, если $f(x) = (\varphi(x) \cdot \psi(x)$, то, умножив обе части равенства на $g(x)$ получим $f(x) \cdot g(x) = \varphi(x) \cdot (\psi(x) \cdot g(x))$, что означает $(f(x) \cdot g(x)) \vdots \varphi(x)$. □

5. Если каждый из многочленов $f_1(x), f_2(x), \ldots, f_k(x)$ делится на $\varphi(x)$, то на этот многочлен будет делиться и многочлен $f_1(x) \cdot g_1(x) + f_2(x) \cdot g_2(x) + \ldots + f_k(x) \cdot g_k(x)$, где $g_1(x), g_2(x), \ldots, g_k(x)$ — произвольные многочлены из кольца $A[x]$.

Задание 3. Доказать пятое свойство отношения делимости.

6. Если $f(x) \vdots \varphi(x)$, то $f(x) \vdots c \cdot \varphi(x)$, где c — обратимая константа.

Доказательство. В самом деле, из равенства $f(x) = \varphi(x) \cdot \psi(x)$ следует, что $f(x) = (c\varphi(x)) \cdot (c^{-1} \psi(x))$, что означает $f(x) \vdots c \cdot \varphi(x)$. □

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Записать в естественном виде многочлен $h(x) = f(x) \cdot g(x)$, где:

а) $f(x) = (2x^4 - x^3 + x^2 + x + 1)$, $g(x) = (x^2 - 3x + 1)$;

б) $f(x) = (x^3 + x^2 - x - 1)$, $g(x) = (x^2 - 2x - 1)$.

2. Найти a, b так, чтобы $f(x) = x^4 + x^3 + 2x^2 + ax + b$ был квадратом некоторого многочлена в кольце $R[x]$.

3. Найти коэффициенты a, b, c, d, при которых многочлен $f(x) = x^4 + ax^3 + bx^2 - 8x + 4$ является квадратом многочлена $\varphi(x) = x^2 + cx + d$ в кольце $Z[x]$?

4. Построить многочлены f и g так, чтобы:

а) $deg\,(f + g) = max(deg\, f, deg\, g)$;

б) $deg\,(f + g) < max(deg\, f, deg\, g)$;

в) $deg\,(f \cdot g) = deg\, f + deg\, g$.

5. Выясните, делится ли $f(x) = x - 3$ на $g(x) = 3x^2 + x - 1$ в кольце $Z[x]$?

6. При каких значениях a, b, c, d равны многочлены

$p(z) = (az + b)(z^2 - z + 1) + (cz + d)(z^2 + 3)$ и $g(z)=2z^3+z^2+5z+1$ из кольца $Z[x]$?

7. Найти сумму коэффициентов многочлена, получающегося из многочлена $f(x) = 1 + (x^2 - 6x + 5)(x^5 + 3x^4 - 2x^3 + x^2 - x - 7)^3 + (x^2 - 3x + +1)^{25} \cdot (x^3+5+7)$ приведением к каноническому виду.

8. При каком условии многочлен $(x^3 + px + q)$ делится на многочлен вида $(x^2 + mx - 1)$ в кольце $R[x]$?

9. При каком условии многочлен $(x^4 + px^2 + q)$ делится на многочлен вида $(x^2 + mx + 1)$ в кольце $R[x]$?

10. При каком соотношении между p и q многочлен $x^3 + px + q$ делится (без остатка) на $(x - \alpha)^2$ в кольце $R[x]$ и чему равно в этом случае α?

11. Найти необходимое и достаточное условие делимости многочлена

$f(x) = x^3 + 2x^2 + ax - 3$ на $\varphi(x) = x^2 + px + q$ в кольце $R[x]$.

12. Многочлен $f(x)$ принимает при всех целых x целые значения. Может ли один из его коэффициентов быть равным $\frac{1}{13}$?

13. Найдите все целые x, при которых многочлен $f(x) = 2x^2 - x - 36$ принимает значения, равные квадратам простых чисел.

§ 7. Корни многочленов

Будем рассматривать кольцо многочленов $A[x]$ над областью целостности A. Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in A[x]$ — произвольный многочлен кольца и c — любой элемент из области целостности A.

Определение 7.1. Сумму $a_n c^n + a_{n-1} c^{n-1} + \ldots + a_0$ будем называть значением многочлена f от c (или в точке c) и обозначать $f(c)$.

Определение 7.2. Элемент c из кольца A называют *корнем* многочлена $f(x)$, если $f(c) = 0$.

Теорема 7.1 (Безу). Пусть $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0\in A[x]$ и $c\in A$. Тогда в кольце $A[x]$ найдется и единственный многочлен $g(x)$ такой, что выполняется равенство $f(x)=(x-c)g(x)+f(c)$.

Доказательство. Пусть многочлен имеет нулевую степень $f = a \neq 0$, тогда $a=(x-c)\cdot 0+a$, $a = f(c)$. Предположим, что многочлен $f(x)$ имеет степень, равную n.

Рассмотрим разность

$f(x) - f(c)=a_n(x^n-c^n)+a_{n-1}(x^{n-1}-c^{n-1})+...+(a_1-c_1)=a_n(x-c)(x^{n-1}+cx^{n-2}+$ $+c^2x^{n-3}+...+c^{n-1})+a_{n-1}(x-c)(x^{n-2}+cx^{n-3}+...+c^{n-2})+..+a_1(x-c)=(x-c)(a_n(x^{n-1}+...+c^{n-1})+$ $+a_{n-1}(x^{n-2}+...+c^{n-2})+...+a_1)=(x-c)(a_nx^{n-1}+...+a_1)=\mathbf{(x-c)g(x)},$ где $g(x)=a_nx^{n-1}+...+a_1$. Таким образом, имеем $f(x)-f(c)=(x-c)g(x)$ или $f(x) = (x-c)g(x)+f(c)$. □

Существует другая формулировка теоремы Безу: остаток от деления многочлена $f(x)$ на двучлен $(x-c)$ равен значению многочлена $f(c)$.

Пользуясь теоремой Безу, можно, не производя деления, найти остаток от деления многочлена на двучлен $(x-c)$.

Теорема 7.2 (критерий корня). Элемент $c\in A[x]$является корнем многочлена $f(x)\in A[x]$ тогда и только тогда, когда $f(x)$ делится на двучлен $(x-c)$ в кольце $A[x]$.

Доказательство.

1. Необходимость. Пусть $f(x)$ — многочлен из кольца $A[x]$ и c — его корень, тогда по определению корня $f(c)=0$. По теореме Безу: $f(x)=(x-c)g(x)+f(c)=(x-c)g(x)$, что означает делимость многочлена $f(x)$ на $(x-c)$.

2. Достаточность. Пусть $f(x)$ делится на $(x-c)$, тогда по определению отношения делимости существует многочлен $g(x)$ такой, что выполняется равенство $f(x)=(x-c)g(x)$. Найдем $f(c)=(c-c)g(x)=0$, то есть $f(c)=0$, значит, c — корень многочлена $f(x)$. □

§ 8. Схема Горнера

В кольце многочленов деление в обычном смысле слова, как правило, невозможно. Например, в кольце $\boldsymbol{R}[x]$ многочлен x^2 нельзя разделить на $x + 1$, то есть не существует такого многочлена $g(x)$, что $x^2 = g(x)(x + 1)$.

Однако всегда осуществимо так называемое деление с остатком: $f(x) = (x - c)h(x) + r$, где $r \in A$. При этом многочлен $h(x)$ называется неполным частным, а r — остатком.

Рассмотрим вопрос о делимости многочлена $f(x) \in A[x]$ на линейный двучлен $(x - c)$ при $c \in A$.

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in A[x]$. Согласно теореме Безу $f(x) = (x - c)g(x) + f(c)$.

Тогда искомый многочлен $g(x)$ будет иметь вид $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$. Подставим вместо $f(x)$ и $g(x)$ их выражения, полагая $r = f(c)$.

Сравнивая коэффициенты многочлена в левой части равенства $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x - c)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0) + r$ с коэффициентами многочлена, полученного после раскрытия скобок и приведения подобных слагаемых в правой части этого равенства, получим цепочку равенств

$$\begin{aligned}
&a_n = b_{n-1}, \\
&a_{n-1} = b_{n-2} - cb_{n-1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&a_2 = b_1 - cb_2, \\
&a_1 = b_0 - cb_1, \\
&a_0 = r - cb_0,
\end{aligned} \tag{1}$$

откуда последовательно определяют коэффициенты $h(x)$ и остаток r:

$$\begin{aligned}
&b_{n-1} = a_n, \\
&b_{n-2} = a_{n-1} + cb_{n-1}, \\
&b_{n-3} = a_{n-2} + cb_{n-2}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&b_1 = a_2 + cb_2, \\
&b_0 = a_1 + cb_1, \\
&r = a_0 + cb_0.
\end{aligned} \tag{2}$$

Равенство $r = f(c)$ непосредственно следует из равенства $f(x) = (x - c)h(x) + r$ после подстановки в него вместо x элемента c.

Кроме того, получен очень удобный способ, который позволяет найти результат от деления многочлена $f(x)$ на двучлен $(x - c)$. Этот способ носит название схемы Горнера. Вычисления удобно располагать в виде таблицы:

	a_n	a_{n-1}	a_{n-2}	...	a_1	a_0
c	b_{n-1}	b_{n-2}	b_{n-3}	. . . . .	b_0	$f(c)$

Элементы нижней строки вычисляются последовательно по формулам (2): $a_n = b_{n-1}$, а каждый последующий элемент равен сумме элемента, находящегося над ним, и предыдущего элемента нижней строки, умноженного на c.

Пример 8.1. Выполним деление с остатком по схеме Горнера многочлена $f(x) = 5x^5 - 19x^4 + x^2 - 5x + 2$ на двучлен $(x - 4)$.

Составим таблицу, в которой в первой строке расположены коэффициенты многочлена $f(x)$, в том числе и нулевые, а во второй — соответствующие коэффициенты частного и остаток, последовательно вычисляемые, а слева сбоку — значение c в данном примере:

	5	–19	0	1	–5	2
4	5	1	4	17	63	254

Таким образом, искомое деление будет следующим: $f(x) = (x-4)(5x^4 + x^3 + 4x^2 + 17x + 63) + 254$.

Замечание. Выполнить деление данного многочлена на двучлен может школьник с помощью другой схемы, называемой «делением углом». Тогда:

$$\begin{array}{l|l}
5x^5 - 19x^4 + x^2 - 5x + 2 & x - 4 \\ \cline{2-2}
-\ \underline{5x^5 - 20x^4} & 5x^4 + x^3 + 4x^2 + 17x + 63 \\
\quad x^4 + x^2 - 5x + 2 & \\
-\ \underline{x^4 - 4x^3} & \\
\quad 4x^3 + x^2 - 5x + 2 & \\
-\ \underline{4x^3 - 16x^2} & \\
\quad 17x^2 - 5x + 2 & \\
-\ \underline{17x^2 - 68x} & \\
\qquad 63x + 2 & \\
\quad -\ \underline{63x - 252} & \\
\qquad\quad 254 &
\end{array}$$

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Докажите, что если многочлен $f(x) \in Z[x]$ принимает при $x = 0$ и при $x = 1$ нечетные значения, то он не имеет целых корней.

2. Докажите, что если многочлен $f(x) \in Z[x]$ при трех различных целых значениях переменной принимает значение 1, то он не имеет целых корней.

3. Существует ли многочлен $f(x) \in Z[x]$, такой, что его свободный член равен 1995, числа 1 и 5 являются его корнями и при некотором целом x значение этого многочлена равно 1994?

4. Выясните, делится ли $f(x) = (x^2 + 3x - 4)^{40} + (x-2)^{11} + 1$ на $(x+1)$?

5. Пользуясь схемой Горнера, разделите с остатком многочлен $f(x) \in R[x]$ на $(x - x_0)$ и вычислите $f(x_0)$:

а) $f(x) = x^4 - 3x^3 + 6x^2 - 10x + 16,\ x_0 = 4;$

б) $f(x) = x^4 + 3x^3 - 3x^2 - 4x + 1,\ x_0 = -1;$

в) $f(x) = 3x^4 + 4x^3 + 5x^2 + x + 33,\ x_0 = -2;$

г) $f(x) = 3x^4 - 2x^3 + 5,\ x_0 = -2;$

д) $f(x) = x^4 - 2x^3 + 4x^2 - 6x + 8,\ x_0 = 1;$

е) $f(x) = 5x^5 - 3x^3 + x,\ x_0 = 1;$

ж) $f(x) = 2x^5 - 5x^3 - 8x,\ x_0 = -3;$

з) $f(x) = 3x^5 + x^4 - 19x^2 - 13x - 10,\ x_0 = 2;$

и) $f(x) = x^4 - 3x^3 - 10x^2 + 2x + 5,\ x_0 = -2;$

к) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1,\ x_0 = -1;$

л) $f(x) = x^4 + 2x^2 + 20x + 7,\ x_0 = -3;$

м) $f(x) = 2x^4 - 3x^3 - 5x^2 + 8x - 3,\ x_0 = 4/$

6. Пользуясь схемой Горнера, найдите значение многочлена $f(x) \in \boldsymbol{C}[x]$ в точке x_0:

а) $f(x) = x^4 + 2ix^3 - (1 + i)x^2 - 3x + 7 + i,\ x_0 = -i;$

б) $f(x) = x^5 + (1 + 2i)x^4 - (1 + 3i)x^2 + 7,\ x_0 = -2 - i;$

в) $f(x) = 4x^3 + x^2,\ x_0 = -1 - i;$

г) $f(x) = x^3 - x^2 - x,\ x_0 = 1 - 2i;$

д) $f(x) = x^6 + (2-i)x^4 + (i-1)x^3 + (1+i)x^2 - (1+i)x + 3 - i,\ x_0 = i;$

е) $f(x) = x^3 + x^2 - 7,\ x_0 = -4 - 4i;$

ж) $f(x) = 3x^5 - x^4 + 2x^3 - x - 1,\ x_0 = -1 + i;$

з) $f(x) = 2x^6 - 4ix^5 + (2 + 4i)x^4 + 4x^3 + 8ix^2 + 16ix - 8 + 4i,\ x_0 = -1+2i;$

и) $f(x)=2x^5-2x^3+x$, $x_0=1+2i$;

к) $f(x) = 3x^5 + ix^4 - (1-i)x^2 + 2 + i$, $x_0=1+2i$.

7. Пользуясь схемой Горнера, проверить, является ли число a корнем многочлена $f(x)$:

а) $f(x)=2x^4+3x^3-4x^2+2x-3$, $a=1$;

б) $f(x)=x^5+2x^4-7x^3-3x^2+12x-20$, $a=2$;

в) $f(x)=x^6+7x^5-6x^3+5x-9$, $a=3$;

г) $f(x)=x^4-3x^3+5x-3$, $a=-3$;

д) $f(x) = 2x^5 - 2x^4 + (1-i)x^3 + 3x^2 + (2-2i)x + 2 + 4i$, $a = 1 + i$.

8. Найдите a и b, если при делении многочлена ax^3+bx-1 на x^2-3x+2 остаток равен 7.

9. Найдите коэффициенты a, b, c многочлена $x^4-x^3+ax^2+bx+c$, если известно, что он делится на многочлен x^3-2x^2-5x+6.

10. Найти многочлен третьей степени такой, что его старший коэффициент равен 1, а остатки от деления многочлена на $(x-2)$, $(x-1)$, $(x+1)$ соответственно равны 13, 21, 13.

11. Найдите многочлен третьей степени такой, что его старший коэффициент равен $(-\frac{1}{2})$, числа i и $-i$ являются его корнями, а остаток от деления многочлена на $(x-1)$ равен 2.

12. Найти $f(x) = a_0 + a_1x + a_2x^2$, если $f(1) = 1$, $f(2) = 2$, $f(3) = 3$.

13. Докажите, что в $Z[x]$:

а) $(100x^{100} - 50x^{50} + 10x^{10} - 5x^5 + x - 56) \vdots (x-1)$;

б) $((x+3)^{25} - (x+1)^5 + x) \vdots (x+2)$.

14. Данные многочлены расположите по степеням двучлена $(x-c)$:

1) $f(x) = 2x^5 - x^2 + 2$, $c = -1$;

2) $f(x) = x^3 + 2x - 5$, $c = 2$;

3) $f(x) = 3x^4 + 2x^2 + x + 1$, $c = 2$;

4) $f(x) = x^4 - 8x^3 + 24x^2 - 50x + 90$, $c = 2$.

15. Вычислить значение многочлена $f(x) = x^4 + 5x^3 - 9x^2 + 7$ при $x = 3{,}01$ и $x = 2{,}98$.

16. Разложить по степеням x многочлен:

а) $(x-4)^4 - 3(x-4)^3 + 2(x-4) - 5$;

б) $(x-2)^4 + 4(x-2)^3 + 6(x-2) + 10(x-2) + 20$.

17. Записать в стандартном виде многочлен $(x+2)^5 - 3(x+2)^3$.

§ 9. Кратные корни многочлена

Пусть $f(x) \in A[x]$, где f — ненулевой многочлен и $c \in A$.

Если c — корень многочлена $f(x)$, то по критерию корня $f(x) \vdots (x-c)$, то есть $f(x)=(x-c)\cdot g(x)$. Может оказаться, что c — корень многочлена $g(x)$, тогда $f(x)=(x-c)^2\cdot h(x)$ и т.д.

Определение 9.1. Элемент $c \in A$ называется *k–кратным корнем многочлена $f(x)$*, если $f(x)$ делится на многочлен $(x-c)^k$, но не делится на многочлен $(x-c)^{k+1}$. Если $k = 1$, то говорят, что c — простой корень многочлена $f(x)$; при $k>1$ говорят о кратном корне.

Л е м м а 9.1. Элемент $c \in A$ является корнем кратности k многочлена $f(x) \in A[x]$ тогда и только тогда, когда $f(x)$ представим в виде $f(x) = (x-c)^k$ $p(x)$, где $p(x) \in A[x]$ и $p(c) \neq 0$.

Теорема 9.1. Пусть $f(x) \in A[x]$ и $c_1, c_2, \ldots, c_s$ — различные корни многочлена $f(x)$, кратность которых соответственно равны $k_1, k_2, \ldots, k_s$. Тогда $f(x) \vdots (x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_s)^{k_s}$.

Д о к а з а т е л ь с т в о. Докажем теорему методом математической индукции по числу корней s.

1. Пусть $s = 1$. По условию имеем, что многочлен $f(x)$ обладает корнем c_1 порядка кратности k_1. Тогда по определению кратного корня многочлена $f(x) \vdots (x-c_1)^{k_1}$. Теорема справедлива.

2. Пусть утверждение справедливо для $s= n-1$, то есть многочлен $f(x) \vdots (x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_{n-1})^{k_{n-1}}$.

3. Докажем, что утверждение справедливо для $s=n$. Из предположения индукции следует, что $f(x)=(x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_{n-1})^{k_{n-1}}\cdot$ $\cdot\varphi$, где $\varphi \in A[x]$. Если c_n — корень многочлена $f(x)$ кратности k_n, то $f(c_n)= 0$. С другой стороны, $f(c_n)=(c_n-c_1)^{k_1}\cdot(c_n-c_2)^{k_2}\cdots(c_n-c_{n-1})^{k_{n-1}}\cdot\varphi(c_n)$. Так как все корни различны, то ни одна из скобок в правой части не равна нулю, следовательно, $\varphi(c_n)=0$, и поэтому c_n является корнем для многочлена φ. Пусть порядок кратности c_n для многочлена φ равен r, тогда $\varphi=(x-c_n)^r\cdot q$, где q не делится на $(x-c_n)$. Имеем $f(x)=(x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_{n-1})^{k_{n-1}}\cdot\ (x-c_n)^r\cdot q$.

Обозначив за $h=(x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_{n-1})^{k_{n-1}}\cdot q$ имеем: $f(x)=(x-c_n)^r\cdot h$, причем $h(c_n)\neq 0$. Тогда по критерию корня h не делится на двучлен $(x-c_n)$. Таким образом, это означает, что c_n — корень многочлена $f(x)$ кратности r, то есть $r=k_n$. Окончательно имеем: $f(x)=(x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_n)^{k_n}\cdot q$, что и означает делимость многочлена $f(x)$ на $(x-c_1)^{k_1}\cdot(x-c_2)^{k_2}\cdots(x-c_n)^{k_n}$. Согласно принципу математической индукции утверждение справедливо для любого натурального числа s. □

Следствия:

1. Многочлен степени n из кольца $A[x]$ имеет в области целостности A не более n корней, даже если каждый корень считать столько раз, какова его кратность.

Доказательство. Пусть многочлен степень многочлена f равна n и $c_1, c_2, \ldots, c_s$ — корни многочлена f в кольце $A[x]$, порядки кратности которых равны $k_1, \ldots, k_s$, соответственно. Многочлен f, согласно доказанной теореме, можно представить в виде $f=(x-c_1)^{k_1}\cdot\ldots\cdot(x-c_s)^{k_s}\cdot g,\quad g\in A[x]$.

По теореме о степени произведения двух ненулевых многочленов имеем $\deg f=k_1+k_2+\ldots+k_s+\deg g$, причем $\deg g\geq 0$. Следовательно, $n\geq k_1+k_2+\ldots+k_s$, и значит, самое большое число корней у многочлена n. □

2. Пусть φ — многочлен из кольца $A[x]$, который записан следующим образом: $\varphi=b_k\cdot x^k+b_{k-1}\cdot x^{k-1}+\ldots+b_1\cdot x+b_0$. Если многочлен φ имеет в области целостности A более k корней, то многочлен φ — нулевой.

Доказательство. Докажем методом от противного. Предположим, что многочлен $\varphi\neq 0$, тогда он имеет вполне определенную степень и из данной записи многочлена φ следует, что степень $\varphi\leq k$. Тогда по предыдущему следствию многочлен φ имеет в области целостности A не более k корней, что противоречит условию. □

Пример 9.1. Является ли число (–1) корнем многочлена $f=2x^6-3x^5-4x^4+2x^2-3$? Если да, то определить его порядок кратности.

Решение. Воспользуемся схемой Горнера:

	2	–3	–4	0	2	0	–3	
–1	2	–5	1	–1	3	–3	0	←остаток, то есть $f(-1) = 0$, значит (–1) — корень многочлена f
–1	2	–7	8	–9	12	–15	← остаток, то есть $g(-1) \neq 0$	

Следовательно: (–1) — корень многочлена f кратности 1 (или простой корень). Приведем решение данного примера с помощью математического пакета *Mathematica:*

In[20]:= Roots[2*x^6 – 3*x^5 – 4*x^4 + 2*x^2 – 3 = = 0, x]

Out[20] = x = = Roots[– 3 + 3#1 – #12 + #13 – 5#14 + 2#15&, 1]//

x = = Roots[– 3 + 3#1 – #12 + #13 – 5#14 + 2#15&, 2] //

x = = Roots[– 3 + 3#1 – #12 + #13 – 5#14 + 2#15&, 3] //

x = = Roots[– 3 + 3#1 – #12 + #13 – 5#14 + 2#15&, 4] //

x = = Roots[– 3 + 3#1 – #12 + #13 – 5#14 + 2#15&, 5] //

x = = – 1

Таким образом, снова получили приведенный выше ответ.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Выяснить, будет ли число 2 корнем и какой кратности для многочлена $f(x) = x^5 - 7x^4 + 12x^3 + 16x^2 - 64x + 48$.

2. С помощью схемы Горнера определить кратность корня

а) –2 для $f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16;$

б) 1 для $f(x) = x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27;$

в) –1 для $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4;$

г) –1 для $f(x) = 3x^5 + 2x^4 + x^3 - 10x - 8;$

д) 2 для $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8;$

е) 3 для $f(x) = x^5 - 6x^4 + 2x^3 + 36x^2 - 27x - 54.$

3. Определите, при каких a, b, c многочлен $f(x)= x^4+ax^3+bx^2+cx - 24$ имеет число (–2) корнем не ниже третьей кратности.

§ 10. Алгебраическое и функциональное равенство многочленов

Определение 10.1. Два многочлена, равные в обычном смысле (равенство соответствующих коэффициентов при одинаковых степенях переменной *x*), будем называть равными алгебраически. Обозначение $(sign)$: $f =^a g$.

Пусть $f \in A[x]$. Зададим отображение $\tilde{f}$, ставящее каждому элементу a из области целостности A значение многочлена f для аргумента a: $(\forall a \in A)(a \xrightarrow{\tilde{f}} f(a))$. Заданное таким образом отображение $A \xrightarrow{\tilde{f}} A$ называют полиномиальной функцией, определяемой многочленом *f*.

Будем говорить, что два многочлена *f*, $g \in A[x]$ равны функционально, если равны определяемые ими полиномиальные функции, $sign: f =^{\Phi} g$.

Таким образом, $f =^{\Phi} g \Leftrightarrow (\forall c \in A)(f(c) = g(c))$.

Задание 1. Доказать, что если две функции равны алгебраически, то они равны и функционально, то есть $(\forall f, g \in A[x]) \quad f =^a g \Rightarrow f =^{\Phi} g$. Обратное утверждение неверно.

Пример 10.1. В качестве области целостности возьмем $Z_2 = \{\bar{0}, \bar{1}\}$. Над этой областью целостности рассмотрим кольцо многочленов: $Z_2[x]$. Выберем в нем произвольно два многочлена:

$$f = x^3 + x + \bar{1} \quad \text{и} \quad g = x^2 + x + \bar{1}.$$

Зададим отображение $\tilde{f}$: $(\forall a \in Z_2) \ a \to f(a)$.

Тогда $\bar{0} \to f(\bar{0}) = (\bar{0})^3 + \bar{0} + \bar{1} = \bar{1}$ и $\bar{1} \to f(\bar{1}) = \bar{1}^3 + \bar{1} + \bar{1} = \bar{1}$.

Отображение $\tilde{g}$: $(\forall a \in Z_2) \ a \to g(a)$. Тогда $\bar{0} \to g(\bar{0}) = (\bar{0})^2 + \bar{0} + \bar{1} = \bar{1}$ и $\bar{1} \to g(\bar{1}) = \bar{1}^2 + \bar{1} + \bar{1} = \bar{1}$. Следовательно, $f =^{\Phi} g$, но $f \neq g$ (алгебраически), поскольку коэффициенты при соответствующих степенях переменной *x* различны.

Задание 2. Как мы убедимся в следующей теореме, существуют области целостности, где понятия алгебраического и функционального равенства многочленов совпадают. Приведите пример!

Теорема 10.1 Если область целостности *A* бесконечна, то понятия алгебраического и функционального равенства многочленов совпадают, то есть $(\forall f, g \in A[x]) \quad f =^a g \Leftrightarrow f =^{\Phi} g$.

Доказательство. Пусть A — бесконечная область целостности. Возьмем два произвольных многочлена $f, g \in A[x]$.

1. Необходимость. Пусть $(\forall f, g \in A[x])$ $f =^{a} g$, тогда очевидно, что $f =^{\Phi} g$.

2. Достаточность. Пусть $(\forall f, g \in A[x])$ $f =^{\Phi} g$, докажем, что $f =^{a} g$.

Рассмотрим разность многочленов $f - g = h$. Возьмем $(\forall c \in A)$ и найдем значение многочлена $h(c)$. Имеем: $h(c) = f(c) - g(c)$. Но $f(c) = g(c)$, так как $f =^{\Phi} g$, тогда $h(c) = 0$.

Таким образом, при любом c имеем $h(c) = 0$. Последнее равенство означает, что каждый элемент области целостности A является корнем многочлена h. Однако A — бесконечное множество, поэтому многочлен h в A имеет бесконечное множество корней, что невозможно, если h — не является нулевым многочленом (по следствию 2 из теоремы 9.1.), значит, $h = 0$, но тогда $f =^{a} g$. □

§ 11. Кольцо многочленов над полем

Пусть P — некоторое поле. Известно, что всякое поле является областью целостности. Следовательно, кольцо многочленов $P[x]$ обладает свойствами отношения делимости, справедливыми в кольце многочленов над областью целостности.

Определение 11.1. Будем говорить, что многочлен f ассоциирован с многочленом g, и обозначать $f \sim g$, если f нацело делится на g и g нацело делится на f, то есть $f \sim g \Leftrightarrow f \,\vdots\, g \wedge g \,\vdots\, f$.

Отношение ассоциированности многочленов обладает следующими свойствами:

1. Рефлексивность: $f \sim f$ (любой многочлен f ассоциирован сам с собой).
2. Симметричность: если $f \sim g$, то $g \sim f$.
3. Транзитивность: если $f \sim g$ и $g \sim q$, то $f \sim q$.

Таким образом, отношение ассоциированности является отношением эквивалентности. Кольцо $P[x]$ можно разбить на классы ассоциированных многочленов.

Теорема 11.1. Два многочлена f и g, принадлежащие кольцу $P[x]$, ассоциированы тогда и только тогда, когда они отличаются некоторым ненулевым множителем из поля P: $(\forall f, g \in P[x]) f \sim g \Leftrightarrow (\exists c \in P) f = c \cdot g$), где $c \neq 0$.

Доказательство.

1. Необходимость. Пусть $f \sim g$. Докажем, что $(\exists c \in P)\ f = c \cdot g$. Если многочлены f и g нулевые, то доказательство очевидно.

Пусть многочлен f — ненулевой. Воспользуемся определением 11.1. Так как $f \sim g \Rightarrow f \vdots g \wedge g \vdots f \Rightarrow (\exists q_1, q_2 \in P[x])$ и выполняется равенство $f = g \cdot q_1 \wedge g = f \cdot q_2 \Rightarrow f = (f \cdot q_1) \cdot q_2 \Rightarrow f = f \cdot (q_1 \cdot q_2)$. Последнее равенство возможно при $q_1 \cdot q_2 = 1 \Rightarrow \deg(q_1 \cdot q_2) = \deg q_1 + \deg q_2 = 0 \Rightarrow \deg q_1 = \deg q_2 = 0$ $\Rightarrow q_1, q_2 \in P$. Таким образом, $(\exists c = q_1 \in P)\ f = c \cdot g$.

2. Достаточность. Пусть $(\exists c \in P)\ f = c \cdot g, c \neq 0$. Докажем, что многочлены f и g — ассоциированы. Так как

$$f = c \cdot g, \tag{1}$$

тогда по определению отношения делимости многочленов $f \vdots g$ и, так как $c \neq 0$, то существует для него в поле P обратный элемент c^{-1}. Умножим обе части равенства (1) на c^{-1} слева: $c^{-1} \cdot f = c^{-1} \cdot c \cdot g \Rightarrow g \vdots f$. По определению ассоциированных многочленов $f \sim g$. □

Из этой теоремы следует, что:

1. Нулевой многочлен ассоциирован сам с собой.
2. Класс многочленов, ассоциированных с единицей, — все элементы из P, кроме нуля.
3. С многочленом f ассоциированы многочлены вида $c \cdot f,\ c \neq 0$.

Рассмотрим специфические свойства отношения делимости в кольце многочленов над полем.

1. $(\forall f \in P[x])\ (\forall c \in P)\ c \neq 0 \Rightarrow f \vdots c$.

Доказательство. Так как $c \neq 0$, то в поле P существует для него обратный элемент c^{-1}, тогда $f = f \cdot c \cdot c^{-1} = c \cdot (f \cdot c^{-1}) \Rightarrow f \vdots c$. □

2. Если $f \vdots g \wedge g \sim g_1 \Rightarrow f \vdots g_1$

Доказательство. Пусть $f \vdots g \wedge g = c \cdot g_1$, где $c \neq 0$, тогда по свойству транзитивности $(f \vdots c \cdot g_1 \wedge c \cdot g_1 \vdots g_1) \rightarrow f \vdots g_1$.

Таким образом, в кольце $P[x]$ всякий многочлен в качестве делителей имеет все ненулевые константы и все ненулевые многочлены, с ним ассоциированные. □

Теорема 11.2 (о делении с остатком). Пусть $\varphi \neq 0 \in P[x]$. Для любого многочлена ($\forall f \in P[x]$) существует единственная пара многочленов q, $r \in P[x]$ такая, что $f = \varphi \cdot q + r$, при этом $\deg r < \deg \varphi$ или $r = 0$. (1)

Доказательство. Докажем возможность данного представления и его единственность. Возможность данного представления доказывается следующим образом:

1. Если f — нулевой многочлен или степень f меньше степени φ, то $f = \varphi \cdot 0 + 0,\ r = 0$, то есть для таких многочленов теорема справедлива.

2. Если $f \neq 0$, тогда он имеет определенную степень. Пусть $deg\ f = n$, $f = a_n \cdot x^n + \ldots + a_1 \cdot x + a_0,\ (a_n \neq 0)$. Если $\deg \varphi > n$, то $f = \varphi \cdot 0 + f$ и, следовательно, можно считать, что $q = 0,\ r = f$ и утверждение справедливо. Поэтому нам остается рассмотреть случай, когда $\deg f \geq \deg \varphi$. Докажем методом математической индукции по степени n многочлена f существование многочленов q, r, удовлетворяющих условиям (1) теоремы.

Базис индукции: $n = 0 \Rightarrow f = a_0 \neq 0$. Тогда $\deg f = 0$, а поскольку $\deg \varphi \leq \deg f$, то $\deg \varphi = 0$, следовательно $\varphi = b_0 \in P$ и $b_0 \neq 0$ и справедливо представление $f = \frac{a_0}{b_0} \cdot b_0 + 0$,где $\frac{a_0}{b_0} = q$, $b_0 = \varphi,\ 0 = r$, и $\frac{a_0}{b_0} \in P$. Теорема верна.

Индукционный шаг: допустим, что наше утверждение справедливо для всех чисел $k<n$. Пусть $\varphi = b_k \cdot x^k + \ldots + b_1 \cdot x + b_0$. Рассмотрим вспомогательный многочлен $h = f - \frac{a_n}{b_k} \cdot x^{n-k} \cdot \varphi$, где $n - k > 0$. Причем $\deg h < \deg f = n$. Тогда по предположению индукции для многочлена h найдутся многочлены q_1 и r_1 в $P[x]$ такие, что $h = \varphi \cdot q_1 + r_1 \wedge (r_1 = 0 \vee \deg r_1 < \deg \varphi)$. Из равенства $f - \frac{a_n}{b_k} \cdot x^{n-k} \cdot \varphi = \varphi \cdot q_1 + r_1$ получим $f = (\frac{a_n}{b_k} \cdot x^{n-k} + q_1) \cdot \varphi + r_1$. Обозначим $(\frac{a_n}{b_k} \cdot x^{n-k} + q_1) = q$, $r_1 = r$ и $deg r_1 < deg \varphi$. Тогда по принципу математической индукции утверждение справедливо для любого натурального числа n.

Единственность представления доказывается следующим образом: пусть для некоторых многочленов f и φ нашлись две пары многочленов q и r с нужными условиями, то есть

$$f=\varphi\cdot q_1+r_1,\ r_1=0\vee\deg r_1<\deg\varphi, \quad (1)$$

$$f=\varphi\cdot q_2+r_2,\ r_2=0\vee\deg r_2<\deg\varphi \quad (2)$$

Вычтем из (1) равенство (2), получим: $\varphi\cdot(q_1-q_2)=r_2-r_1,\ r_2-r_1=0\vee\deg(r_2-r_1)<\deg\varphi$. Пусть $r_2\neq r_1\Rightarrow r_2-r_1\neq 0$, а значит, $\deg(r_2-r_1)$ имеет определенное значение. Следовательно, $\varphi\cdot(q_1-q_2)\neq 0$. Используя теорему о степени произведения многочленов, получим $\deg(r_2-r_1)=\deg(\varphi\cdot(q_1-q_2))=\deg\varphi+\deg(q_1-q_2)\Rightarrow\deg(r_2-r_1)\geq\deg(\varphi)$. С другой стороны, в силу неравенств (1) и (2) $\deg(r_2-r_1)<\deg(\varphi)$. Получили противоречие, значит, допущение неверно, а верно то, что требовалось доказать, то есть $r_2=r_1$, но тогда $\varphi\cdot(q_1-q_2)=0\xrightarrow{\varphi\neq 0}q_1=q_2$. □

С л е д с т в и е 1. $f\,\vdots\,\varphi\Leftrightarrow r=0$.

Область целостности K называется евклидовым кольцом, если существует отображение h множества K в N, удовлетворяющее условиям:

1) $(\forall a,b\in K)(b\neq 0)(\exists\, q,r\in K)\ a=b\cdot q+r\wedge h(r)<h(b)$,

2) $h(a)=0$ тогда и только тогда, когда $a=0$.

С л е д с т в и е 2. Кольцо многочленов $P[x]$ есть евклидово кольцо.

С л е д с т в и е 3. Кольцо многочленов $P[x]$ есть кольцо главных идеалов.

Д о к а з а т е л ь с т в о. Кольцом главных идеалов называется область целостности, в которой каждый идеал является главным, т.е. имеет вид $(f)=\{f\cdot g|g\in P[x]\}$ для некоторого f из $P[x]$. Пусть I – некоторый идеал в $P[x]$. Если $I=\{0\}$, то $I=(0)$. Предположим, что $I\neq(0)$ и выберем многочлен f наименьшей степени, лежащий в I. Покажем, что $I=(f)$. Действительно, включение $I\supseteq(f)$ очевидно. Пусть g – произвольный многочлен из I. Разделим g с остатком на f, получим $g=f\cdot q+r$, где $r=0$ или $\deg r<\deg f$. Если при этом $r\neq 0$, то $r=g-f\cdot q\in I$, что противоречит тому, что f – многочлен наименьшей степени в I. Следовательно, $g=f\cdot q$, т.е. $g\in(f)$, а значит $I=(f)$. □

П р и м е р 11.1. Разделите с остатком многочлены:

а) $f=2x^4-3x^3+4x^2-5x+6$ на $g=x^2-3x+1$;

б) $f=6x^5+13x^4-3x^3-7x^2+6x+2$ на $g=2x^3+x^2-1$;

в) $f=2x^4+3x^3+x-1$ на $g=x^2+x+5$.

Решение. Продемонстрируем решение данного примера с помощью математического пакета *Mathematica.*

а) *In[1]: = PolinomialRemainder[2*x^4 – 3*x^3 + 4*x^2 – 5*x+6, x^2 – 3*x + 1, x]*

Out[1]= –5 + 25x

*In[2]:=PolinomialQuotient[2*x^4–3*x^3+4*x^2–5*x+6,x^2–3*x+1, x]*

Out[2] = 11 + 3x + 2x^2

Ответ: неполное частное от деления многочлена f на φ есть многочлен (*11 + 3x + 2* x^2*)*, а остаток *(–5 + 25x).*

б) *In[1]: = PolinomialRemainder[6*x^5 + 13* x^4 – 3*x^3 – 7*x^2 + 6*x + 2, 2*x^3 + x^2 – 1, x]*

Out[1] = –2 + 11x

Ответ: по теореме о делении с остатком, если *f(x) = g(x)·q(x)+ r(x)*, то *f(x) =* $(2x^3+x^2-1)(3x^2+5x-4)+(11x-2)$.

в) *In[6]:= PolinomialRemainder[2*x^4 + 3*x^3+x –1, x^2 + x + 5, x]*

Out[6] = 54 + 7x

*In[7]: = PolinomialQuotient[2*x^4 + 3*x^3 + x – 1, x^2 + x + 5, x]*

Out[7] = –11 + x + 2x^2

Ответ: остаток равен *(7x+54)*, неполное частное равно $(2x^2+x-11)$.

Пример 11.2. Найти делитель, если известны делимое *f*, неполное частное *q* и остаток *r:* $f=2x^4+x^3+3x^2+1,\ q=2x^2+3x+2,\ r=-4x-3$.

Решение. По теореме о делении с остатком имеем: *f(x)=g(x)·q(x)+r(x).* Выразим из последнего равенства требуемое неизвестное: *g(x) = (f(x) – r(x))/q(x).* Подставив в данное равенство известные многочлены и выполнив деление, найдем ответ задачи с помощью компьютера:

*In[3]: = Expand[((2*x^4 + x^3 + 3*x^2 + 1) – (–4*x – 3))]*

Out[3] = 4 + 4x + 3x^2 *+ x*^{3} *+ 2x*^{4}

In[7]:= PolinomialQuotient[4+4x+3x^2*+x*^{3} *+ 2x*^{4}*, 2*x^2 + 3 *x + 2, x]*

Out[4] = 2 – x + x^2

Ответ: *g (x)=* $2-x+x^2$.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Разделите с остатком:

а) $f(x) = 6x^5 + 13x^4 - 3x^3 - 7x^2 + 6x + 2$ на $g(x) = 2x^3 + x^2 - 1$;

б) $f(x) = 2x^4 + 3x^3 + x - 1$ на $g(x) = x^2 + x + 5$;

в) $f(x) = 10x^4 - 3x^3 + 2x - 1$ на $g(x) = 2x^2 - x + 1$;

г) $f(x) = 7x + 9$ на $g(x) = 3x^{17} + 9x^{10} - 2$;

д) $f(x) = 2x^4 - 3x^3 + 4x^2 - 5x + 6$ на $g(x) = x^2 - 3x + 1$;

е) $f(x) = x^3 - 3x^2 - x - 1$ на $g(x) = 3x^2 - 2x + 1$.

2. Найти делитель, если известны делимое $f(x)$, неполное частное $g(x)$ и остаток $r(x)$:

а) $f(x) = 2x^5 + 3x^4 + 2x^3 + 1$, $g(x) = x^2 + 3x + 1$, $r(x) = 63x + 25$;

б) $f(x) = 2x^5 + 3x^4 + 2x^3 + 1$, $g(x) = 2x^3 - 3x^2 + 9x - 24$, $r(x) = 63x + 25$;

в) $f(x) = 2x^4 + x^3 + 3x^2 + 1$, $g(x) = 2x^2 + 3x + 2$, $r(x) = -4x - 3$;

г) $f(x) = x^4 + 3x^3 - x^2 + 1$, $g(x) = x^2 + (3 - i)x - (4 + 3i)$,
$r(x) = -3(3 - 2i)x + 3(3 + 2i)$.

3. Не производя деление с остатком, найти остаток от деления

а) $f(x) = x^{151} + x^{117} + x^{13} + 10x - 11i$ на $\varphi(x) = x^4 - 1$;

б) $f(x) = 2x^{64} - 5x^{36} - 3x^{27} + 7x^{15} + 2x^6 - 3x^4 + 8$ на $\varphi(x) = x^3 - x$.

4. Разделить с остатком с помощью схемы Горнера:

$f(x) = 2ix^7 + 2x^5 - 2ix + 3i$ на $t(x) = (x - i)(x + 2)$.

5. Многочлен $x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ при делении на $(x - a)$ дает остаток А, а при делении на $(x - b)$ дает остаток В. Найти остаток от деления этого многочлена на $(x - a)(x - b)$, если $a \neq b$.

6. При делении многочлена $f(x)$ на $(x - 1)$ и $(x - 2)$ остатки соответственно равны 1 и 2. Чему равен остаток от деления многочлена $f(x)$ на $(x - 1)\cdot(x - 2)$?

7. При делении $f(x)$ на $g(x)$ получили равенство $f(x) = g(x)\cdot s(x) + r(x)$. Найдите остаток от деления $f^2(x)$ на $g(x)$, если $r(x) = 7x^3 - x + 1$ и степень многочлена $g(x)$ равна 7.

8. Многочлен $f(x)$ делится на $x + 1$, а при делении $f(x)$ на $x^2 - 3x$ остаток равен $7x - 1$. Найдите остаток при делении $f(x)$ на $x^3 - 2x^2$.

9. При каких значениях a и b многочлен
$2x^{35} - 18x^{33} - 5x^{15} + 45x^{13} + ax^2 + bx - 3$ делится на многочлен $x^2 - 1$?

10. Найдите остаток при делении многочлена:

а) $x^{62} - x^{31} + 5$ на $x^2 - 1$; б) $x^{17} - x^{10} + 2x^3 - 1$ на $x^2 + 1$;

в) $x^{100} - 2x^{51} + 1$ на $x^2 - 1$.

11. Найти частное и остаток от деления многочлена $f(x) = 2x^4 + x + 1$ на $g(x) = 2x + 1$ в кольце $Z_3[x]$.

§ 12. Наибольший общий делитель многочленов

Рассматривается кольцо $P[x]$ многочленов над некоторым полем.

Определение 12.1. Общим делителем многочленов $f_1, f_2, \ldots, f_k \in P[x]$ называется многочлен $d \in P[x]$, на который будет делиться каждый из многочленов $f_1, f_2, \ldots, f_k \in P[x]$.

Пример 12.1. Для многочленов $f_1 = x^2 - 4;$ $f_2 = x^3 - 8;$ $f_3 = x^2 - 3x + 2$ $\forall const \neq 0$ является их общим делителем, а также $(x-2)$ и $c \cdot (x-2)$.

Определение 12.2. Наибольшим общим делителем многочленов $f_1, f_2, \ldots, f_k \in P[x]$ называется многочлен $D(x)$, удовлетворяющий условиям:

1. $D(x)$ — общий делитель многочленов $f_1, f_2, \ldots, f_k \in P[x]$.
2. Если $\delta(x)$ — любой общий делитель, то $D(x) \vdots \delta(x)$.

Если многочлен $D(x)$ является наибольшим общим делителем многочленов $f_1, f_2, \ldots, f_k \in P[x]$, то будем записывать: $D(x) \sim$ НОД($f_1, f_2, \ldots, f_k$) или $D(x) =$ НОД($f_1, f_2, \ldots, f_k$).

Теорема 12.1 (о существовании наибольшего общего делителя). Для любых многочленов $f_1, f_2, \ldots, f_k \in P[x]$ наибольший общий делитель существует.

Доказательство

1. Может оказаться, что все многочлены равны нулю: ($f_1 = f_2 = \ldots = f_k = 0$). Легко убедиться, что нулевой многочлен будет их наибольшим общим делителем.

2. Пусть среди многочленов $f_1, f_2, \ldots, f_k \in P[x]$ хотя бы один многочлен не равен нулю. Рассмотрим идеал, порождённый этими многочленами ($f_1, f_2, \ldots, f_k$) $= I$. Очевидно, что он является главным. Если порождающее множество I состоит из одного элемента d, то идеал называется главным идеалом $I = (d)$.

Убедимся в том, что d — наибольший общий делитель многочленов $f_1, f_2, \ldots, f_k$. Прежде всего в том, что каждый из многочленов делится на d. Построим идеал из элементов $f_1, \ldots, f_k$.

$I = \{ f_1 \cdot u_1 + \ldots + f_k \cdot u_k / u_1, \ldots, u_k \in P[x]\}$. Так как идеал главный, то $I = (d) = \{d \cdot u / u \in P[x]\}$. Поскольку $f_1, \ldots, f_k \in I = (d) \Rightarrow$ все они делятся на d. Пусть δ — любой общий делитель многочленов $f_1, \ldots, f_k$. Покажем, что $d \,\vdots\, \delta$. Возьмем $d \in (d) = I$, имеем $d = v_1 \cdot f_1 + \ldots + v_k \cdot f_k$. Так как каждое из $f_1, \ldots, f_k$ делится на $\delta \Rightarrow d \,\vdots\, \delta \Rightarrow d$ — наибольший общий делитель многочленов $f_1, \ldots, f_k$. □

Определение 12.3. Линейным представлением наибольшего общего делителя d многочленов $f_1, f_2, \ldots, f_k$ через данные многочлены называют запись его в виде: $d = f_1 \cdot h_1 + f_2 \cdot h_2 + \ldots + f_n \cdot h_k$, где $h_i \in P[x]$.

Свойства наибольшего общего делителя многочленов следующие:

1. Наибольший общий делитель данных многочленов имеет линейное представление через данные многочлены.

Доказательство. Справедливость свойства вытекает непосредственно из теоремы о существовании наибольшего общего делителя многочленов. Так как $d \in (f_1, f_2, \ldots f_k) = I = \{v_1 \cdot f_1 + v_2 \cdot f_2 + \ldots + v_k \cdot f_k\}$, то $d = v_1 \cdot f_1 + v_2 \cdot f_2 + \ldots + v_k \cdot f_k$, где $v_1, v_2, \ldots, v_k \in P[x]$. □

2. Пусть $f, g \in P[x]$, причем $f \,\vdots\, g$, тогда $(f, g) \sim g$.

Задание 1. Доказать второе свойство наибольшего общего делителя многочленов.

3. Пусть $f, g, h \in P[x]$, тогда $(h{\cdot}f, h{\cdot}g) \sim h{\cdot}(f, g)$.

Доказательство. Пусть $(f, g) \sim d$, тогда требуется доказать, что $(h \cdot f, h \cdot g) = d \cdot h$. Воспользуемся определением наибольшего общего делителя многочленов, то есть докажем, что

а) $h \cdot f \,\vdots\, h \cdot d \wedge h \cdot g \,\vdots\, h \cdot d$. По допущенному обозначению, $f \,\vdots\, d \wedge g \,\vdots\, d$, тогда по 4 свойству отношения делимости многочленов $h \cdot f \,\vdots\, h \cdot d \wedge h \cdot g \,\vdots\, h \cdot d$;

б) пусть общий делитель $h \cdot g,\ h \cdot f$ равен δ, то есть $h \cdot g \,\vdots\, \delta \wedge h \cdot f \,\vdots\, \delta$. Покажем, что $h \cdot d \,\vdots\, \delta$. Так как $(f, g) = d$, то по первому свойству наибольшего общего делителя многочленов $(\exists \varphi, \psi \in P[x])\ d = f \cdot \varphi + g \cdot \psi$. Умножим обе части данного равенства на h: $h \cdot d = h \cdot f \cdot \varphi + h \cdot g \cdot \psi$. Каждое слагаемое правой части последнего равенства делится на δ, а значит, и вся сумма, то есть $h\cdot d \vdots \delta \xrightarrow{\text{по определению НОД}} h\cdot d$ — есть один из наибольших общих делителей многочленов hf, hg. □

4. Ассоциативное свойство НОД многочленов: если $(f_1, f_2, \ldots, f_{k-1}) = d_1$, то $(f_1,\ f_2, \ldots,\ f_k) = (d_1,\ f_k)$.

Доказательство. Обозначим $d = (d_1, f_k)$ и докажем по определению, что d является наибольшим общим делителем многочленов $f_1,\ f_2,\ \ldots,\ f_k$.

1) каждый из многочленов $f_1, f_2, \ldots, f_k$ делится на d, поскольку $f_1, f_2, \ldots, f_{k-1} \vdots d_1$ (по условию теоремы) и $d_1 \vdots d$ (из обозначений), следовательно, в силу свойства транзитивности каждый из многочленов $f_1, f_2, \ldots, f_{k-1} \vdots d$. Кроме того, из обозначений $f_k \vdots d$. Значит d — общий делитель многочленов $f_1, f_2, \ldots, f_k$;

2) докажем, что d — наибольший из общих делителей данных многочленов. Пусть δ — любой общий делитель многочленов $f_1, f_2, \ldots, f_k$; $d \vdots \delta$, так как δ является общим делителем многочленов f_k и d_1. Свойство доказано. Из этой теоремы можно вывести следствие, которое доказывается методом математической индукции.

Следствие. Если $d_1 = (f_1, f_2),\ d_2 = (d_1, f_3), \ldots, d_{k-1} = (d_{k-2}, f_k)$, тогда $(f_1, f_2, \ldots, f_k) = d_{k-1}$.

5. Если среди многочленов $f_1,\ f_2,\ \ldots,\ f_k$ есть ненулевой, то наибольший общий делитель этих многочленов есть их общий делитель наибольшей степени.

§ 13. Алгоритм Евклида

Ассоциативное свойство наибольшего общего делителя показывает, что достаточно научиться находить наибольший общий делитель двух многочленов, и, следовательно, можно будет найти наибольший общий делитель конечного числа многочленов. Аппаратом для нахождения наибольшего общего делителя двух многочленов служит алгоритм Евклида. Он основан на следующем утверждении.

Лемма 13.1. Пусть для некоторых многочленов кольца $P[x]$ выполняется равенство $f = g\cdot h + \varphi$, тогда $(f, g) = (g, \varphi)$.

Доказательство. Обозначим один из наибольших общих делителей *(f, g)*= *d*. Тогда достаточно показать, что один из наибольших общих делителей $(g,\varphi)=d$. Воспользуемся определением наибольшего общего делителя многочленов и получим $f \vdots d \wedge g \vdots d$. Для $\varphi \neq 0 \in P[x]$: $\varphi = f - g \cdot h$ и, так как $f \vdots d \wedge g \cdot h \vdots d \Rightarrow \varphi \vdots d$. Таким образом, d — общий делитель g и φ. Докажем, что он наибольший. Пусть δ таков, что $\varphi \vdots \delta \wedge g \vdots \delta$. Докажем, что $d \vdots \delta$. По условию теоремы $f = g \cdot h + \varphi$. Каждое слагаемое правой части равенства делится на δ, следовательно, $f \vdots \delta \Rightarrow \delta$ — общий делитель многочленов f и g. Но их наибольший общий делитель равен *d*, следовательно, $d \vdots \delta$. □

Решим задачу. Пусть *f, g* — многочлены из кольца $P[x]$. Найти один из их наибольших общих делителей. Необходимо выполнить два шага.

1. Может оказаться, что каждый из многочленов нулевой, тогда их наибольший общий делитель — нулевой многочлен (доказать самостоятельно).

2. Пусть хотя бы один из многочленов ненулевой. Пусть для определенности $g \neq 0$. К многочленам f и g из кольца многочленов $P[x]$ применим теорему о делении с остатком:

$$f = g \cdot q_1 + r_1 \text{ и } r_1 = 0 \vee \deg r_1 < \deg g. \tag{1}$$

Если $r_1 = 0$, то процесс прекращается. В противном случае (если $r_1 \neq 0$), применим теорему о делении с остатком к многочленам g и r_1:

$$(\exists\, q_2, r_2 \in P[x])\ g = r_1 \cdot q_2 + r_2 \text{ и } r_2 = 0 \vee \deg r_2 < \deg r_1. \tag{2}$$

Если $r_2 = 0$, то процесс закончим. Предположим, что $r_2 \neq 0$. Применим теорему о делении с остатком к многочленам r_1, r_2:

$$r_1 = r_2 q_3 + r_3 \text{ и } r_3 = 0 \vee \deg r_3 < \deg r_2. \tag{3}$$

Процесс последовательного деления продолжают до тех пор, пока не будет получен нулевой остаток. Пусть на *k*-шаге имеем:

$$r_{k-2} = r_{k-1} \cdot q_k + r_k \text{ и } r_k = 0 \vee \deg r_k < \deg r_{k-1}. \tag{k}$$

Рассмотрим последовательность полученных остатков:

$$r_1, r_2, \ldots, r_k, r_{k+1} \tag{*}$$

Степени многочленов последовательности (*) строго убывают. Степени многочленов — это целые неотрицательные числа, следовательно, убывающая последовательность (*) не может быть бесконечной, поэтому она заканчивается, по крайней мере, нулевой степенью многочлена. Многочлен нулевой степени это ненулевая константа. Пусть $r_s \neq 0 \wedge r_s = const.$ Но тогда следующее деление выполнится без остатка, так как в кольце $P[x]$ любой многочлен делится на ненулевую константу. А значит, $r_{s+1} = 0$. Таким образом, в нашем процессе последовательного деления мы получим нулевой остаток. Пусть это $r_{s+1} = 0$. Последний ненулевой остаток r_s и есть наибольший общий делитель многочленов f и g.

Действительно:

Из (1) $(f,g) \sim (g,r_1)$

Из (2) $(g,r_1) \sim (r_1,r_2)$

Из (3) $(r_1,r_2) \sim (r_2,r_3)$

....

$(r_{s-1},r_s) \sim (r_s,0) \sim r_s$

А поскольку отношение ассоциированности многочленов обладает свойством транзитивности, то $(f,g) \sim r_s$.

Таким образом, алгоритм Евклида утверждает, что последний ненулевой остаток при делении многочленов это и есть наибольший общий делитель многочленов.

П р и м е р 13.1. Найти наибольший общий делитель многочленов $x^4 + x^3 + 2x^2 + x + 1$ и $x^3 - 1$, пользуясь алгоритмом Евклида. Разделим первый многочлен на второй:

$$
\begin{array}{rl}
x^4 + x^3 + 2\cdot x^2 + x + 1 & \big|\ \underline{x^3 - 1} \\
-\underline{x^4 - x\qquad\qquad\qquad} & \ x + 1 \\
x^3 + 2\cdot x^2 + 2\cdot x + 1 & \\
-\underline{x^3 - 1\qquad\qquad} &
\end{array}
$$

$$
\begin{array}{rl}
x^3 - 1 & \big|\ \underline{2\cdot x^2 + 2\cdot x + 2} \\
-\ \underline{x^3 + x^2 + x} & \ 1/2\cdot x - 1/2 \\
-x^2 - x - 1 & \\
-\ \underline{-x^2 - x - 1} & \\
0 &
\end{array}
$$

Из выполненного деления находим, что наибольший общий делитель равен $\left(x^4 + x^3 + 2x^2 + x + 1,\ x^3 - 1\right) = 2x^2 + 2x + 2$.

Найдем наибольший общий делитель многочленов $x^4 + x^3 + 2x^2 + x + 1$ и $x^3 - 1$ с помощью математического пакета *Mathematica*.

Решение.

*In[7]: = PolynomialGCD[x^4 + x^3 + 2*x^2 + x + 1, x^3 – 1]*

Out[7]= 1 + x + x^2

Замечание: пусть требуется к многочленам f и φ применить теорему о делении с остатком, то есть найти такие многочлены q и r, что $f=\varphi\cdot q+r$, $r=0$ или $\deg r<\deg\varphi$. Возьмем ненулевую константу $c\neq 0$.

1. Умножим f на c, значит, остаток при делении на φ будет равен $c\cdot r$, то есть ассоциирован с r.

2. Изменим делитель: $c\cdot\varphi$. Тогда частное приобретет множитель c^{-1}, а остаток не изменится.

Из сказанного следует, что если в алгоритме Евклида умножить делимые или делители на некоторую ненулевую константу, то полученные остатки либо не изменяются, либо будут приобретать ненулевой постоянный множитель, то есть будут меняться с точностью до ассоциированности. А так как наибольший общий делитель многочленов определен с точностью до ассоциированности, то умножение делимых и делителей на ненулевую константу не изменяет наибольший общий делитель многочленов. Этим часто пользуются на практике.

Пример 13.2. В кольце $\boldsymbol{R}[x]$ многочленов с действительными коэффициентами найдем наибольший общий делитель многочленов $f=x^4+3x^3-x^2-4x-3$, $g=3x^3+10x^2+2x-3$. Делим f на g:

$$\begin{array}{rl|l}
 & x^4+3x^3-x^2-4x-3 & 3x^3+10x^2+2x-3 \\ \cline{3-3}
- & x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x & \frac{1}{3}x-\frac{1}{9} \\ \cline{2-2}
 & -\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3 & \\
- & -\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3} & \\ \cline{2-2}
 & -\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3} &
\end{array}$$

Для удобства умножим полученный остаток на $(-\frac{9}{5})$. При этом последующие остатки также умножатся на некоторые числа, отличные от нуля, что несущественно при нахождении наибольшего общего делителя, так как он находится с точностью до константы. Выполним второе деление:

$$
\begin{array}{r|l}
3x^3+10x^2+2x-3 & x^2+5x+6 \\ \cline{2-2}
-\ 3x^3+15x^2+18x & 3x-5 \\ \cline{1-1}
-5x^2-16x-3 & \\
-\ -5x^2-25x-30 & \\ \cline{1-1}
9x+27 &
\end{array}
$$

Полученный остаток разделим на 9 и выполним третье деление:

$$
\begin{array}{r|l}
x^2+5x+6 & x+3 \\ \cline{2-2}
-\ x^2+3x & x+2 \\ \cline{1-1}
2x+6 & \\
-\ 2x+6 & \\ \cline{1-1}
0 &
\end{array}
$$

Поскольку остаток равен нулю, то $(f,g)=x+3$.

П р и м е р 13.3. Найти наибольший общий делитель многочленов: а) $f=x^6-7x^4+8x^3-7x+7, \quad g=3x^5-7x^3+3x^2-7$.

Р е ш е н и е. Воспользуемся математическим пакетом *Mathematica:*

In[12]: = PolynomialGCD[x^6 –7 x^4 + 8*x^3 –7*x + 7,*

*3*x^5 – 7*x^3 + 3*x^2 – 7]*

Out[12]= 1 + x^3

О т в е т: $(f,g)=x^3+1$

б) $f=x^4-2x^3-4x^2+4x-3, \quad g=2x^3-5x^2-4x+3$

In[13]: = PolynomialGCD[x^4 –2 x^3 – 4*x^2 +4*x – 3,*

*2*x^3 – 5*x^2 – 4*x + 3]*

Out[13]= –3 + x

О т в е т: $(f,g)=x-3$.

П р и м е р 13.4. Найти наибольший общий делитель многочленов $f=x^2+2, \quad g=x^3+x-1$ и его линейное представление. Это означает, что наибольший общий делитель данных многочленов надо представить в виде $f\cdot u+g\cdot v=(f,g)=d$.

Применим алгоритм Евклида:

$$
\begin{array}{r|l}
x^3 + x - 1 & x^2 + 2 \\
-\ \underline{x^3 + 2 \cdot x} & x \ \to q_1
\end{array}
$$

$$
\begin{array}{r|l}
x^2 + 2 & -x - 1 \to r_1 \\
-\ \underline{x^2 + x} & -x + 1 \to q_2
\end{array}
$$

$$
\begin{array}{r}
-x + 2 \\
-\ \underline{-x - 1}
\end{array}
$$

$$
\begin{array}{r|l}
-x - 1 & 3 \to r_2 \\
-\ \underline{-x - 1} & 1/3 \cdot (-x - 1) \\
0 &
\end{array}
$$

Таким образом $(f,g)=3$. Результаты делений с остатком, выполненных при решении примера, показывают, что $g = f \cdot q_1 + r_1,\ f = r_1 \cdot q_2 + r_2$. Выразим r_2 через многочлены f и g. Получаем $r_2 = f - r_1 \cdot q_2 = f - (g - f \cdot q_1) \cdot q_2 =$
$= f - g \cdot q_2 + f \cdot q_1 \cdot q_2 = f \cdot (1 + q_1 \cdot q_2) + g \cdot (-q_2)$, где $1 + q_1 \cdot q_2 = u,\ -q_2 = v$. Найдем u, v: $u = 1 + q_1 \cdot q_2 = 1 + x \cdot (-x+1) = 1 - x^2 + x = -x^2 + x + 1$; $v = -(-x+1) = x - 1$. Окончательно получим: $3 = f \cdot (-x^2 + x + 1) + g \cdot (x - 1)$.

З а м е ч а н и е. На практике линейное выражение многочлена r_2 иногда удобнее искать не с помощью алгоритма Евклида, а методом неопределенных коэффициентов. Запишем искомые многочлены u и v в общем виде с неопределенными (неизвестными) коэффициентами. Приравнивая коэффициенты при одинаковых степенях x в равенстве $r_2 = uf + vg$, получим систему уравнений для коэффициентов многочленов u и v. Легко видеть, что эти уравнения будут линейными. Для применения этого метода необходимо заранее знать оценки степеней многочленов u и v (иначе мы не будем знать, в каком общем виде их записать).

Теорема 13.1. Пусть многочлен h, кратный $d = (f,g)$, удовлетворяет условию $\deg h < \deg f + \deg g$. Тогда он допускает линейное выражение $h = uf + vg$, в котором $\deg u < \deg g, \deg v < \deg f$.

Д о к а з а т е л ь с т в о. Пусть $h = u_0 f + v_0 g$ — линейное выражение многочлена h. Разделим u_0 с остатком на g: $u_0 = qg + u$, $\deg u < \deg g$. Выражение $u_0 f + v_0 g$ может быть преобразовано следующим образом: $u_0 f + v_0 g = uf + (v_0 + qf)g = uf + vg,$ где $v = v_0 + qf$.

Итак, $h = uf + vg,$ причем $\deg u < \deg g$. Так как $vg = h - uf$ и $\deg h < \deg f + \deg g,$ то $\deg vg < \deg f + \deg g$. Отсюда следует, что

$\deg v < \deg f$, и потому многочлены u и v удовлетворяют требованиям теоремы.

Пример 13.5. Найти наибольший общий делитель многочленов и его линейное выражение через многочлены *f*, *g*, если $f = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g = 2x^3 - x^2 - 5x + 4$.

Решение. Запишем общий вид линейного представления наибольшего общего делителя через данные многочлены. Получаем: $fu + gv = (f,g) = d$. Найдем наибольший общий делитель многочленов: $(f,g) = -1 + x$.

$f = g \cdot q_1 + r_1$, $g = r_1 \cdot q_2 + r_2$. Из последней записи выражаем r_2 через g и r_1, подставляем r_1, выраженное через f и g первой записи:

$r_2 = g - r_1 q_2 = g - (f - gq_1) \cdot q_2 = g \cdot (1 + q_1 \cdot q_2) + f \cdot (-q_2)$, где $1 + q_1 \cdot q_2 = u$, $-q_2 = v$.

Решение примера с помощью математического пакета *Mathematica:*

*PolynomialGCD[4*x^4 – 2*x^3 – 16*x^2 + 5*x + 9,*
*2*x^3 – x^2 – 5*x + 4]– 1 + x*
*PolynomialQuotient[4*x^4 – 2*x^3 – 16*x^2 + 5*x + 9,*
*2*x^3 – x^2 – 5*x + 4, x]2x*
*PolynomialRemainder[4*x^4 – 2*x^3 – 16*x^2 + 5*x + 9,*
*2*x^3 – x^2 – 5*x + 4, x]9– 3x – 6x*^{2}
*PolynomialQuotien[2*x^3 – x^2 – 5*x + 4, 9– 3x – 6x*^{2}*, x]*1/3 – x/3
Expand[*(4*x^4 – 2*x^3 – 16*x^2 + 5*x + 9)*(–(1/3 – x/3)) +*
*+ (2*x^3 – x^2 – 5*x + 4)* (1 + (2x)* (1/3 – x/3))]1 – x*

Таким образом, $(1 - x) = f(x)\cdot(x/3 - 1/3) + g(x)\cdot(1+2x\cdot(1/3 - x/3))$.

Пример 13.6. Найти линейное представление НОД(f, g) = $x + 1$ для многочленов $f = x^5 + x^4 + x^3 + x^2 + x + 1$ и $g = x^4 - 1$ методом неопределенных коэффициентов.

Решение. Линейное представление наибольшего общего делителя многочленов будем искать из условия $fu + gv = (f, g) = d$.

Функции u и v запишем в следующем виде:

$u = ax^2 + bx + c$, $v = ex^3 + kx^2 + lx + m$

Имеем:

$$(x^5 + x^4 + x^3 + x^2 + x + 1)\cdot(ax^2 + bx + c) + (x^4 - 1)\cdot(x^3 + kx^2 + lx + m) = x + 1$$

Приравнивая соответствующие коэффициенты, получим систему:

при x^7 $a+e=0$

при x^6 $a+b+k=0$

при x^5 $a+b+c+l=0$

при x^4 $a+b+c+m=0$

при x^3 $a+b+c-e=0$

при x^2 $a+b+c-k=0$

при x $b+c-l=1$

$c-m=1$

Решение данной системы будет следующим:

$$a=-\frac{1}{3}, \mathrm{b}=0, \mathrm{c}=\frac{2}{3}, e=\frac{1}{3}, k=\frac{1}{3}, l=-\frac{1}{3}, m=-\frac{1}{3}$$

Ответ: $u=\frac{1}{3}(-x^2+2), v=\frac{1}{3}(x^3+x^2-x-1)$

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найти наибольший общий делитель многочленов:

а) $x^5+x^4-x^3-2x-1, \; 3x^4+2x^3+x^2+2x-2;$

б) $x^5-2x^4+x^3+7x^2-12x+10, \; 3x^4-6x^3+5x^2+2x-2;$

в) $x^4+7x^3+19x^2+23x+10, \; x^4+7x^3+18x^2+22x+12;$

г) $2x^6-5x^5-14x^4+36x^3+86x^2+12x-31, 2x^5-9x^4+2x^3+10x-14;$

д) $x^6-7x^4+8x^3-7x+7, \; 3x^5-7x^3+3x^2-7;$

е) $x^4-2x^3-4x^2+4x-3, \; 2x^3-5x^2-4x+3.$

2. Найти наибольший общий делитель $(f_1(x), f_2(x))$ и его линейное выражение через $f_1(x)$, $f_2(x)$:

а) $f_1(x)=x^5+3x^4+x^3+x^2+3x+1, \; f_2(x)=x^4+2x^3+x+2;$

б) $f_1(x)=x^4+4x^3-7x+2, \quad f_2(x)=x^3+3x^2-4;$

в) $f_1(x)=x^5-x^4+x^3-x^2+2x-2, \; f_2(x)=x^5-1;$

г) $f_1(x)=3x^5+6x^4+3x^3-x^2-2x-1, \; f_2(x)=x^4-2x^2+1;$

д) $f_1(x)=x^6-x^4+3x^3-2x+2, \; f_2(x)=x^3+2;$

е) $f_1(x)=x^4+2x^3-x^2-4x-2, \; f_2(x)=x^4+x^3-x^2-2x-2.$

3. Пользуясь алгоритмом Евклида, подберите многочлены $M(x)$ и $N(x)$ так, чтобы выполнялось равенство: $f(x)\cdot M(x)+\varphi(x)\cdot N(x)=d(x),$ где $f(x)=x^4-2x^3-4x^2+4x-3, \; \varphi(x)=2x^3+x^2-x-1$ и $d(x)=(f(x), \varphi(x)).$

4. Пользуясь алгоритмом Евклида, найдите полиномы $M_1(x)$ и $M_2(x)$ такие, что $f_1(x)\cdot M_2(x)+f_2(x)\cdot M_1(x)=1$, где:

а) $f_1(x)=3x^3-2x^2+5x+3, f_2(x)=x^4+2x^3+2x^2+x+1;$

б) $f_1(x)=x^5-5x^4-2x^3+12x^2-2x+12, \; f_2(x)=x^3-5x^2-3x+17;$

в) $f_1(x) = 2x^4 + 3x^3 - 3x^2 - 5x + 2,\ f_2(x) = 2x^3 + x^2 - x - 1;$

д) $f_1(x) = x^5 + 5x^4 + 9x^3 + 7x^2 + 5x + 3,\ f_2(x) = x^4 + 2x^3 + 2x^2 + x + 1;$

е) $f_1(x) = x^4 - 4x^3 + 1,\ f_2(x) = x^3 - 3x^2 + 1;$

ж) $f_1(x) = 3x^3 - 2x^2 + x + 2,\ f_2(x) = x^2 - x + 1.$

5. Пользуясь алгоритмом Евклида, подберите полиномы $M_1(x)$ и $M_2(x)$ так, чтобы $f_1(x)\cdot M_2(x) + f_2(x)\cdot M_1(x) = d(x)$, где $d(x) = (f_1(x), f_2(x))$:

а) $f_1(x) = 3x^7 + 6x^6 - 3x^5 + 4x^4 + 14x^3 - 6x^2 - 4x + 4,$

$f_2(x) = 3x^6 - 3x^4 + 7x^3 - 6x + 2;$

б) $f_1(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6,\ f_2(x) = 3x^4 - 4x^3 - x^2 - x - 2.$

6. Сократима ли дробь $f(n)/g(n)$ при каком-нибудь целом n? Если да, то при каких целых n она сократима и на какое число, когда:

1) $f(x) = x^2 + x + 1,\ g(x) = x - 2;$

2) $f(x) = 3x^3 - 2x^2 + x + 2,\ g(x) = x^2 - x - 1.$

7. Решить систему уравнений

$$\begin{cases} x^{15} + x^{13} - 2x^5 - 3x^3 + 3x = 0, \\ x^{11} + x^9 - 2x = 0. \end{cases}$$

§ 14. Унитарные многочлены

Естественная запись унитарного многочлена: $x^n + a_{n-1}\cdot x^{n-1} + \ldots + a_1\cdot x + a_0$.

Унитарный многочлен нулевой степени равен единице.

Утверждение 1. В классе ассоциированных многочленов унитарный многочлен единственен.

Доказательство. Пусть M — некоторый класс ассоциированных многочленов, порожденный многочленом f, $deg\ f = n$. Докажем данное утверждение методом от противного. Пусть в этом классе два унитарных многочлена:

$$g = x^n + a_{n-1}\cdot x^{n-1} + \ldots + a_1\cdot x + a_0 \text{ и } \varphi = x^n + b_{n-1}\cdot x^{n-1} + \ldots + b_1\cdot x + b_0.$$

Так как многочлены g и φ находятся в одном классе ассоциированных многочленов, то $g \sim \varphi$, а поскольку ассоциированные многочлены отличаются на константу, то $\exists c / \varphi = c\cdot g \Rightarrow\ x^n + b_{n-1}\cdot x^{n-1} + \ldots +$ $+ b_1\cdot x + b_0 = c\cdot x^n + c\cdot a_{n-1}\cdot x^{n-1} + \ldots + c\cdot a_1\cdot x + c\cdot a_0 \Rightarrow c = 1 \Rightarrow \varphi = g$. □

Утверждение 2. *Унитарный наибольший общий делитель нескольких многочленов единственный.* Справедливость утверждения следует из предыдущего предложения и из того, что наибольшие общие делители многочленов ассоциированы.

§ 15. Взаимно простые многочлены

Определение 15.1. Многочлены $f_1, f_2, \ldots, f_s \in P[x]$ назовем взаимно простыми, если их наибольший общий делитель ассоциирован с единицей.

Свойства взаимно простых многочленов следующие:

1. Критерий взаимной простоты: $(f,g)\sim 1 \Leftrightarrow (\exists h_1, h_2 \in P[x])$ такие, что $f\cdot h_1 + g\cdot h_2 = 1$.

Доказательство.

Необходимость. $(f,g)\sim 1 \xrightarrow{\text{свойство НОД}} (\exists h_1, h_2 \in P[x])$ такие, что $f\cdot h_1 + g\cdot h_2 = 1$ (линейное представление).

Достаточность. Пусть для многочленов f и g существуют многочлены h_1, h_2 такие, что $f\cdot h_1 + g\cdot h_2 = 1$. Докажем, что $(f,g)\sim 1$ (методом от противного). Пусть f и g не являются взаимно простыми многочленами, тогда $(f,g)=d \Rightarrow$ по определению наибольшего общего делителя $f \vdots d \wedge g \vdots d$, так как $f\cdot h_1 + g\cdot h_2 = 1 \Rightarrow 1 \vdots d \Rightarrow (\exists q \in P[x])$ такое, что $1 = d\cdot q$. По теореме о степени произведения $q\neq 0 \wedge \deg 1 = \deg d + \deg q \Rightarrow$ $\Rightarrow \deg d = \deg q = 0 \Rightarrow$ $d\in P \Rightarrow d\sim 1 \Rightarrow$из полученных равенств имеем $(f,g)\sim 1$.

2. Если $f\cdot g \vdots \varphi \wedge (f,\varphi)\sim 1$, то $g \vdots \varphi$.

Доказательство. Так как $f\cdot g \vdots \varphi \Rightarrow (\exists \psi \in P[x])$ такой, что

$$f\cdot g = \varphi\cdot\psi. \qquad (*)$$

Поскольку $(f,\varphi)\sim 1 \Rightarrow (\exists h_1, h_2 \in P[x]) / \ f\cdot h_1 + \varphi\cdot h_2 = 1 \Rightarrow f\cdot h_1 = 1 - \varphi\cdot h_2$.
Умножим на h_1 равенство (*): $f\cdot g\cdot h = \varphi\cdot\psi\cdot h_1 \Rightarrow (1-\varphi\cdot h_2)\cdot g = \varphi\cdot\psi\cdot h_1 \Rightarrow$
$g - \varphi\cdot h_2\cdot g) = \varphi\cdot\psi\cdot h_1 \Rightarrow g = \varphi\cdot(\psi\cdot h_1 + g\cdot h_2) \Rightarrow g \vdots \varphi$. □

3. Если многочлен f взаимно прост с каждым из многочленов φ и g, то он взаимно прост и с их произведением, то есть $(f,\varphi)\sim 1 \wedge (f,g)\sim 1 \Rightarrow (f,\varphi\cdot g)\sim 1$.

Доказательство. Из критерия взаимной простоты многочленов f и φ, для них существуют многочлены $h_1, h_2 \in P[x]$ такие, что $f\cdot h_1 + \varphi\cdot h_2 = 1$, аналогично для многочленов f и g имеем: $(\exists \psi_1, \psi_2 \in P[x]) \ / \ f\cdot\psi_1 + g\cdot\psi_2 = 1$
$\Rightarrow (f\cdot h_1 + \varphi\cdot h_2)\cdot(f\cdot\psi_1 + g\cdot\psi_2) = 1 \Rightarrow (f\cdot h_1)\cdot$
$\cdot(f\cdot\psi_1) + (f\cdot h_1)\cdot(g\cdot\psi_2) + (\varphi\cdot h_2)\cdot(f\cdot\psi_1) + (\varphi\cdot h_2)\cdot(g\cdot\psi_2) = 1 \Rightarrow f\cdot(f\cdot h_1\cdot\psi_1 +$

$+h_1\cdot g\cdot\psi_2+\varphi\cdot h_2\cdot\psi_1)+g\cdot\varphi\cdot(h_2\cdot\psi_2)=1\xrightarrow{\text{по критерию взаимной простоты}}(f,g\cdot\varphi)\sim 1.$ □

4. Если $f\,\vdots\, g\wedge f\,\vdots\,\varphi\wedge(g,\varphi)\sim 1$, то $f\,\vdots\, g\cdot\varphi$.

Доказательство. Имеем $f\,\vdots\, g\Rightarrow f=g\cdot h$, где $h\in P[x]$, $f\,\vdots\,\varphi\wedge f=g\cdot h\Rightarrow$

$\Rightarrow g\cdot h\,\vdots\,\varphi\wedge(g,\varphi)\sim 1\xrightarrow{\text{по 2 свойству}}h\,\vdots\,\varphi\Rightarrow h=\varphi\cdot q\Rightarrow f=g\cdot\varphi\cdot q\Rightarrow f=(g\cdot\varphi)\cdot q\Rightarrow f\,\vdots\, g\cdot\varphi.$

5. Частные многочленов *f, g* от деления на их наибольший общий делитель взаимно просты, то есть если $(f,g)=d\wedge d\neq 0\Rightarrow(\frac{f}{d};\frac{g}{d})\sim 1.$

Доказательство. По условию $(f,g)=d$. Найдем частные от деления *f*, *g* на *d*: $f=d\cdot f_1$, $g=d\cdot g_1$. В силу линейного представления наибольшего общего делителя через данные многочлены имеем: $f\cdot u+g\cdot v=d\Rightarrow d\cdot f_1\cdot u+d\cdot g_1\cdot v=d$. Сократим обе части последнего равенства на *d*: $f_1\cdot u+g_1\cdot v=1$. Таким образом, по критерию взаимной простоты $(f_1,g_1)\sim 1\Rightarrow(\frac{f}{d},\frac{g}{d})\sim 1.$ □

§ 16. Наименьшее общее кратное

Определение 16.1. Общим кратным многочленов $f_1, f_2,\ldots, f_s\in P[x]$ называют многочлен, кратный каждому из них, то есть тот, который делится на каждый из многочленов $f_1,\ f_2,\ \ldots,\ f_s$.

Пример 16.1. Найти общее кратное многочленов: $f_1=x-2$, $f_2=x^3-8$, $f_3=x^2+2x+4$.

Решение.

$[f_1,f_2,f_3]=k=x^3-8$, так как $k\,\vdots\,(x-2)$, $k\,\vdots\,(x^3-8)$, $k\,\vdots\,(x^2+2x+4)$. Общим кратным данных многочленов будет и $k_1=2\cdot(x^3-8)$. Таким образом, общих кратных для многочленов будет бесконечно много.

Определение 16.2. Многочлен $h\in P[x]$ называется наименьшим общим кратным многочленов $f_1,\ f_2,\ \ldots,f_s$ из кольца $P[x]$, если он является их общим кратным и любое общее кратное делится на многочлен *h*.

Обозначение: $h=[f_1,f_2,\ldots,f_s]$.

Теорема 16.1 (о существовании наименьшего общего кратного). Для любых многочленов $f_1,f_2,\ldots,f_s$ из кольца $P[x]$ наименьшее общее кратное (НОК) в кольце $P[x]$ существует и определено однозначно с точностью до ассоциированности.

Доказательство.

1. Предположим, что среди многочленов $f_1, f_2, \ldots, f_s$ хотя бы один равен нулю, тогда наименьшее общее кратное равно 0 (исходя из определения наименьшего общего кратного многочленов).

2. Пусть среди многочленов нет ни одного нулевого. Рассмотрим идеал, порожденный каждым многочленом $f_1, f_2, \ldots, f_s$, и их пересечение: $(f_1) \cap (f_2) \cap \ldots \cap (f_s) = I = (\gamma)$. Но так как это кольцо евклидово, то каждый идеал главный, следовательно, идеал I будет порождаться одним элементом — γ. И этот порождающий многочлен γ является наименьшим общим кратным данных многочленов. Убедимся в этом. Пересечение не пусто и $I \neq \{0\}$. Например, здесь находится такой многочлен $f_1 \cdot f_2 \cdot \ldots \cdot f_s$. Значит, $\gamma \in I$, а в I находятся многочлены, делящиеся на f_1, f_2, $\ldots$, f_s. Значит, $\gamma \in I \Rightarrow \gamma \vdots f_1, \gamma \vdots f_2, \ldots, \gamma \vdots f_s \Rightarrow \gamma$ — общее кратное многочленов $f_1, f_2, \ldots, f_s$. Возьмём любое общее кратное данных многочленов, например, многочлен k: $k \in I = (\gamma) \Rightarrow k \vdots \gamma$, то есть, доказано, что наименьшее общее кратное существует.

Докажем, что НОК многочленов $f_1, f_2, \ldots, f_s$ определен однозначно с точностью до ассоциированности. Предположим, что f_1, f_2 — два различных наименьших общих кратных многочленов $f_1, \ldots, f_s$. Если j_1 — общее кратное многочленов $f_1, \ldots, f_s$, то $f_1 \vdots f_2$. Если f_2 — общее кратное многочленов $f_1, \ldots, f_s$, то $f_2 \vdots f_1$. Таким образом, $f_1 \vdots f_2 \wedge f_2 \vdots f_1$, следовательно, эти многочлены ассоциированы. Таким образом, наименьшее общее кратное многочленов определяется однозначно с точностью до ассоциированности.

Теорема 16.2 (ассоциативное свойство НОК).
Если $[f_1, \ldots, f_{s-1}] = j_1 \wedge [j_1, f_s] = j$, то $[f_1, \ldots, f_s] = j$.

Доказательство. Воспользуемся определением наименьшего общего кратного многочленов.

1. Покажем, что j — общее кратное, то есть $j \vdots f_1, j \vdots f_2, \ldots, j \vdots f_s$. Так как j_1 — наименьшее общее кратное многочленов $f_1, f_2, \ldots, f_{s-1}$, то

$j_1 \vdots f_1, j_1 \vdots f_2, \ldots, j_1 \vdots f_{s-1} \wedge j \vdots j_1 \wedge j \vdots f_s \xrightarrow{\text{в силу транзитивюсти}} j \vdots f_1 \wedge j \vdots f_2 \wedge \ldots \wedge j \vdots f_s \Rightarrow j$ — общее кратное многочленов $f_1, \ldots, f_s$.

2. Пусть δ — любое общее кратное многочленов $f_1, f_2, \ldots, f_s$. Покажем, что $\delta \vdots j$. Действительно, $\delta \vdots j$, так как оно является общим кратным многочленов j_1 и f_s. Таким образом, j — наименьшее общее кратное многочленов $f_1, f_2, \ldots, f_s$. □

Следствие. Пусть

$$[f_1, f_2] = \gamma_1,$$
$$[\gamma_1, f_3] = \gamma_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[\gamma_{s-2}, f_s] = \gamma_{s-1} \Rightarrow [f_1, \ldots f_s] = \gamma_{s-1}.$$

Свойства наименьшего общего кратного многочленов следующие:

1. $[f \cdot g, f \cdot \varphi] \sim f \cdot [g, \varphi]$.

Доказательство. Обозначим $[g, \varphi] = h$. Докажем, что $[f \cdot g, f \cdot \varphi] = h \cdot f$.

Воспользуемся определением наименьшего общего кратного многочленов. Так как $h \vdots g \wedge h \vdots \varphi \xrightarrow{\text{свойство делимости}} h \cdot f \vdots g \cdot f \wedge h \cdot f \vdots f \cdot \varphi \Rightarrow h \cdot f$ — общее кратное многочленов $f \cdot g$ и $f \cdot \varphi$.

Пусть δ — общее кратное многочленов $f \cdot g$ *и* $f \cdot \varphi \Rightarrow \delta \vdots f \cdot g \wedge \delta \vdots f \cdot \varphi \Rightarrow \delta = f \cdot g \cdot \delta_1 \wedge \delta = f \cdot \varphi \cdot \delta_2 \Rightarrow f \cdot g \cdot \delta_1 = f \cdot \varphi \cdot \delta_2 \Rightarrow g \cdot$ $\cdot \delta_1 = \varphi \cdot \delta_2 \Rightarrow g \cdot \delta_1 \vdots \varphi.$ Так как $g \cdot \delta_1 \vdots g \Rightarrow g \cdot \delta_1$ — общее кратное φ и g, но h — наименьшее многочленов φ и $g \Rightarrow$ $g \cdot \delta_1 \vdots h \Rightarrow g \cdot \delta_1 = h \cdot q \Rightarrow \delta = f \cdot g \cdot$ $\cdot \delta_1 = f \cdot h \cdot q \Rightarrow \delta \vdots f \cdot h$. □

2. Связь между НОК и НОД многочленов:

$$[f, \varphi] = \frac{f \cdot \varphi}{(f, \varphi)}.$$

Доказательство.

Введем обозначения: $(f, \varphi) = d,\ f = f_1 \cdot d,\ \varphi = \varphi_1 \cdot d$. Тогда имеем $\frac{f \cdot \varphi}{(f, \varphi)} =$

$= \frac{f_1 \cdot d \cdot \varphi_1 \cdot d}{d} = f_1 \cdot d \cdot \varphi_1,$ таким образом $[f, \varphi] = f_1 \cdot d \cdot \varphi_1 = \gamma$

По определению наименьшего общего кратного многочленов получаем: $\gamma \vdots f$, так как $\gamma = (f_1 \cdot d) \cdot \varphi_1 = f \cdot d;\ \gamma \vdots \varphi,$ так как $\gamma = f_1 \cdot (d \cdot \varphi_1) = \varphi \cdot f_1$.

3. Возьмем k — любое общее кратное многочленов f *и* φ. Оно делится на f, тогда $k = f \cdot q$, но $k \vdots \varphi \Rightarrow k = f_1 \cdot d \cdot q \vdots \varphi_1 \cdot d \Rightarrow f_1 \cdot q \vdots \varphi_1$. ($f_1, \varphi_1$ — это частные от деления, тогда по свойству взаимно простых многочленов f_1, φ_1 — взаимно просты). По второму свойству взаимно простых

многочленов $q \vdots \varphi_1$. Имеем: $q = \varphi_1 \cdot s$, $k = f \cdot q = f_1 \cdot d \cdot \varphi_1 \cdot s$, так как $f_1 \cdot d \cdot \varphi_1 = \gamma \Rightarrow k \vdots \gamma$. □

3. Если $(f,g)\sim 1 \Rightarrow [f,g] = f \cdot g$.

4. Доказательство. По предыдущему свойству имеем: $[f,g] = \frac{f \cdot g}{(f,g)} = \frac{f \cdot g}{1} = f \cdot g$. □

Пример 16.2. Найти наименьшее общее кратное многочленов.

а) $f = 2x^5 - 5x^3 - 8x$ и $g = x + 3$.

Решение. Найдем наименьшее общее кратное данных многочленов с помощью математического пакета *Mathematica:*

*In[3]:= PolynomiaLLCM[2*x^5 – 5*x^3 – 8*x, x + 3]*

Out[3]= $(3 + x)(-8x - 5x^3 + 2x^5)$

In[4]:= Expand[$(3 + x)(-8x - 5x^3 + 2x^5)$*]*

Out[4]= $-24x - 8x^2 - 15x^3 - 5x^4 + 6x^5 + 2x^6$

Таким образом, $[f,g] = 2x^6 + 6x^5 - 5x^4 - 15x^3 - 8x^2 - 24x$.

б) $f = x^6 - 7x^4 + 8x^3 - 7x + 7$, $g = 3x^5 - 7x^3 + 3x^2 - 7$.

Решение

*In[14]:= PolynomiaLLCM[x^6 – 7*x^4 + 8*x^3 – 7*x + 7,*
*3*x^5 – 7*x^3 + 3*x^2 – 7]*

Out[14]= $(7 - 7x + x^3)(-7 + 3x^2 - 7x^3 + 3x^5)$*]*

In[15]:=Expand[$(7 - 7x + x^3)(-7 + 3x^2 - 7x^3 + 3x^5)$*]*

Out[15]= $-49 + 49x + 21x^2 - 77x^3 + 49x^4 + 24x^5 - 28x^6 + 3x^8$

Ответ: $[f,g] = 3x^8 - 28x^6 + 24x^5 + 49x^4 - 77x^3 + 21x^2 + 49x - 49$.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найти наименьшее общее кратное многочленов:

а) $x^5 + x^4 - x^3 - 2x - 1$, $3x^4 + 2x^3 + x^2 + 2x - 2$;

б) $x^3 + 2x^2 + 3x + 2$, $x^4 + x^3 + x^2 - x - 2$, $x^3 - x^2 - 4$.

§ 17. Приводимые и неприводимые многочлены

Аналогично тому, как в кольце целых чисел существуют простые и составные числа, так и в кольце многочленов существуют приводимые и неприводимые многочлены.

Пусть дан многочлен $f(x)$ из кольца $P[x]$ степени n, $n \geq 1$, с коэффициентами из поля P.

Определение 17.1. Многочлен f положительной степени из кольца $P[x]$ называется неприводимым над полем P, если его нельзя представить в виде произведения двух многочленов положительной степени из этого же кольца:

$$f \neq f_1 \cdot f_2, \qquad \deg f_1 \geq 1, \deg f_2 \geq 1 \text{ над } P.$$

Определение 17.2. Многочлен f положительной степени из кольца $P[x]$ называется приводимым над полем P, если он представляется в виде произведения двух многочленов положительной степени из этого же кольца:

$$f = f_1 \cdot f_2, \qquad \deg f_1 \geq 1, \deg f_2 \geq 1 \text{ над } P.$$

Следует обратить особое внимание на то обстоятельство, что о приводимости или неприводимости многочлена можно говорить лишь по отношению к данному полю P, так как многочлен, неприводимый над данным полем, может оказаться приводимым в некотором его расширении $\overline{P}$.

Более подробно о расширениях полей см. в § 25 главы 3.

Так, например, многочлен $x^2 - 2$ с целыми коэффициентами неприводим над полем рациональных чисел, поскольку он не может быть разложен в произведение двух множителей первой степени с рациональными коэффициентами. Однако в поле действительных чисел этот многочлен оказывается приводимым, как показывает равенство: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Многочлен $x^2 + 1$ неприводим не только в поле рациональных чисел, но и в поле действительных чисел; однако он делается приводимым в поле комплексных чисел, так как $x^2 + 1 = (x - i)(x + i)$.

Поскольку любой многочлен в качестве своих делителей имеет ненулевые константы и многочлены, с ним ассоциированные, то, во-первых, неприводимый многочлен имеет только такие делители, а во-вторых, приводимый многочлен кроме этих имеет, по крайне мере, один делитель, не ассоциированный с данным многочленом и не равный константе. Таким образом, множество $P[x]$ разбивается на 3 класса:

1. Константы.
2. Приводимые многочлены.
3. Неприводимые многочлены.

Свойства неприводимых многочленов следующие:

1. Любой многочлен первой степени над любым полем неприводим. Действительно, этот полином не может иметь никаких делителей, степень которых была бы меньше 1, но больше 0.

2. Если многочлен f неприводим, то неприводим и всякий многочлен, ассоциированный с ним.

Доказательство. Пусть f — неприводим и $f \sim g$. Докажем свойство методом от противного.

Пусть g — приводим. Тогда по определению 17.2 существуют многочлены φ и p такие, что $g = \varphi \cdot p$ и $1 \leq deg\ \varphi < deg\ g$, $1 \leq deg\ p < deg\ g$. Так как $f \sim g \Rightarrow f \vdots g \Rightarrow f = g \cdot s \Rightarrow f = \varphi \cdot p \cdot s = \varphi \cdot (ps)$, причем $1 \leq deg\ \varphi < deg f$ и $1 \leq deg(ps) < deg\ f$, а это означает, что многочлен f приводим, что противоречит условию. □

3. Если $f(x)$ — произвольный многочлен, а $p(x)$ — неприводимый многочлен, то либо $f(x)$ делится на $p(x)$, либо эти многочлены взаимно просты.

Доказательство. Известно, что для любых двух многочленов существует наибольший общий делитель. Обозначим $(f, p) = d$. По определению наибольшего общего делителя многочленов $p \vdots d$, и так как p — неприводимый, то d является многочленом нулевой степени, тогда наибольший общий делитель многочленов f и p является константой. Если $(f, p) = 1$, то многочлены f и p взаимно просты. В другом случае этот делитель d будет ассоциирован с p, тогда $f \vdots p$. □

4. Если произведение двух многочленов делится на неприводимый многочлен p, то хотя бы один из них делится на p: $f_1 \cdot f_2 \vdots p \ \rightarrow\ f_1 \vdots p \ \vee\ f_2 \vdots p$.

Доказательство. Рассмотрим два многочлена f_1 и f_2. Действительно, если f_1 не делится на p, тогда по третьему свойству неприводимых многочленов f_1 и p взаимно просты, а тогда по второму свойству взаимно простых многочленов, так как $f_1 \cdot f_2 \vdots p \wedge (f_1, p) = 1 \ \Rightarrow\ f_2 \vdots p$. Аналогично доказывается, что если f_2 не делится на p, то $f_1 \vdots p$. Это свойство допускает следующее обобщение.

5. Если произведение нескольких многочленов делится на неприводимый многочлен p, то хотя бы один из сомножителей делится на p.

Доказательство. Так как $f_1 \cdot f_2 \cdot \ldots \cdot f_s \vdots p$ и p — неприводимый многочлен $\Rightarrow$ существует $f_i \,/\, f_i \vdots p$. Доказательство методом математической индукции по числу s состоит из двух шагов.

1) $s = 2$. Пусть $f_1 \cdot f_2 \vdots p$ и p — неприводимый, тогда по четвертому свойству неприводимых многочленов утверждение доказано;

2) пусть утверждение справедливо для $s = k$, то есть $f_1 \cdot f_2 \cdot \ldots f_k \vdots p$ и p — неприводим $\Rightarrow \exists f_i /\ f_i \vdots p$.

Докажем справедливость утверждения для $s = k+1$.

Пусть $f_1 \cdot f_2 \cdot \ldots f_k \cdot f_{k+1} \vdots p$ и p — неприводим $\Rightarrow$ $(f_1 \cdot f_2 \cdot \ldots f_k) \cdot f_{k+1} \vdots p$ и p — неприводимый $\Rightarrow$ согласно первому шагу $f_1 \cdot f_2 \cdot \ldots f_k \vdots p$ или $f_{k+1} \vdots p$ $\Rightarrow (\exists i = \overline{1,k})/ f_i \vdots p$ или $f_{k+1} \vdots p$ $\Rightarrow (\exists i = \overline{1,k+1})/ f_i \vdots p$.

Таким образом, методом математической индукции все доказано ($\forall s \in N$).

6. Если степень многочлена $f(x)$ над полем $P > 1$, и он имеет корень α, являющийся числом из P, то $f(x)$ приводим над P. Действительно, $(x - \alpha)$ оказывается делителем многочлена $f(x)$, являющимся многочленом над P (его коэффициенты 1 и $-\alpha$) и имеющими степень (единицу), большую нуля, но меньшую степени $f(x)$.

7. Если степень n многочлена $f(x)$ над полем P равна двум или трем и $f(x)$ не имеет корней, являющихся числами из P, то $f(x)$ неприводим над P.

Действительно, будучи приводимым, многочлен $f(x)$ представлялся бы в виде: $f(x) = \varphi(x) \cdot \psi(x)$, где $\varphi(x)$ и $\psi(x)$ — многочлены над P ненулевой степени. Сумма степеней $\varphi(x)$ и $\psi(x)$ равна 2 или 3. Следовательно, степень хотя бы одного из них равна 1. Пусть $\varphi(x) = ax + b\ (a, b \in P, a \neq 0)$. Тогда число $\alpha = -\dfrac{b}{a} \in P$, будучи корнем $\varphi(x)$, оказалось бы корнем и для $f(x)$. Но это противоречит тому, что $f(x)$ не имеет корней в P.

8. Пусть для полей P_1 и P_2 имеет место $P_1 \subset P_2$. Если многочлен $f(x) \in P(x)$ над полем P_1 является неприводимым над P_2, то он неприводим и над P_1. Действительно, поскольку $P_1 \subset P_2$ и многочлен $f(x)$ одновременно может рассматриваться и многочлен над P_2. Это следует из того, что всякий делитель многочлена $f(x)$, являющийся многочленом над P_1, можно рассматривать как его делитель, являющийся многочленом над P_2.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Разложить на неприводимые множители многочлен $f(x) = x^4 + 4$ над полем R, C.

2. Разложить на неприводимые множители многочлен $f(x) = x^2 + \sqrt{2}$ над полем R, C.

§ 18. Теорема о разложении многочлена на неприводимые множители. Каноническое представление многочленов

Теорема 18.1. Любой многочлен положительной степени из кольца $P[x]$ либо неприводим над P, либо представляется единственным образом в виде произведения константы, не равной нулю, и нормированных неприводимых многочленов над полем P с точностью до порядка следования множителей.

Доказательство. Докажем возможность и единственность разложения.

Возможность разложения доказывается следующим образом: пусть $f \in P[x]$ и $deg\ f \geq 1$, обозначим $deg\ f = n$. Докажем теорему методом математической индукции по числу n.

Базис индукции: $n = 1 \Rightarrow$ многочлен f имеет первую степень, тогда по первому свойству неприводимых многочленов он является неприводимым и имеет вид: $f = ax+b = a(x+\frac{b}{a})$ — это нормированный многочлен первой степени и он неприводим.

Индукционный шаг: предположим, что теорема справедлива для всех многочленов, степень которых меньше n. Докажем справедливость теоремы для n: $f = a_n x^n+a_{n-1} x^{n-1}+\ldots+ a_1x+ a_0$.

1. Если f — неприводим, то его можно представить в виде:

$f = a_n(x^n+\ldots\frac{a_1}{a_n}x+\frac{a_0}{a_n})$, где $a_n = const$, а в скобках нормированный неприводимый многочлен по второму свойству неприводимых многочленов (поскольку f — неприводим, то неприводим и многочлен $c\cdot f$).

2. Пусть f приводим, тогда по определению его можно представить в виде $f = f_1\cdot f_2$, где $1\leq deg\ f_1<deg\ f = n$, $1\leq deg\ f_2<n$, то есть у многочленов f_1 и f_2 степень меньше n, и тогда к ним применимо допущение — они

будут либо неприводимы, либо представляться в виде произведения константы, не равной нулю, и нормированных неприводимых над полем P многочленов. Таким образом, согласно методу математической индукции, утверждение справедливо для любого натурального числа n.

Единственность разложения доказывается следующим образом: если $n = 1$, то $f = ax + b = a(x + \frac{b}{a})$. Единственность данного представления справедлива в силу алгебраичности операций над полем P.

Предположим, что многочлен степени меньше n раскладывается требуемым способом единственным образом. Докажем единственность разложения для многочлена n-ой степени методом от противного. Пусть он представляется не единственным образом, то есть

$$f_1 = a\cdot p_1\cdot p_2\cdot\ldots\cdot p_s, \quad (1)$$

$$f_2 = b\cdot q_1\cdot q_2\cdot\ldots\cdot q_l. \quad (2)$$

Приравняем оба разложения $a\cdot p_1\cdot p_2\cdot\ldots\cdot p_s = b\cdot q_1\cdot q_2\cdot\ldots\cdot q_l \Rightarrow a = b$, так как они являются старшими коэффициентами одного и того же многочлена f. После сокращения обеих частей данного равенства на старший коэффициент имеем:

$$p_1\cdot p_2\cdot\ldots\cdot p_s = q_1\cdot q_2\cdot\ldots\cdot q_l. \quad (3)$$

Правая часть последнего равенства делится на q_1. Но q_1 — неприводимый многочлен, тогда по пятому свойству неприводимых многочленов $\exists\, p_i \,\vdots\, q_1$. Пусть для определенности $p_1 \,\vdots\, q_1$. Но поскольку p_1 и q_1 — нормированные и неприводимые многочлены, то $\boldsymbol{p_1 = q_1}$. Сократим обе части равенства (3) на p_1, q_1:

$$p_2\cdot\ldots\cdot p_s = q_2\cdot\ldots\cdot q_l\,. \quad (4)$$

После сокращения слева и справа в равенстве (4) записан многочлен степени меньше n. Следовательно, к нему применимо индукционное допущение, то есть он раскладывается единственным образом в произведение нормированных неприводимых над полем P многочленов с точностью до порядка следования множителей. Получим $s - 1 = l - 1$, то есть $s = l$. С точностью до порядка следования можно считать, что $\boldsymbol{p_2 = q_2, \ldots, p_s = q_s}$. Из выделенных полужирным равенств следует, что многочлен n-ой степени раскладывается единственным образом в произведение неприводимых нормированных многочленов. Из всего выше сказанного следует единственность представления для всех многочленов степени n. □

Если f — неприводимый, то будем говорить, что он представлен в каноническом виде. Если f — приводим, то по предыдущей теореме его можно представить в виде произведения неприводимых множителей. Пусть множитель p_1 встречается α_1 раз, p_2 — α_2 раз и т.д.: $f = ap_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Запись многочлена f в таком виде называют каноническим разложением многочлена на множители.

Используя каноническое разложение многочленов, можно находить наибольший общий делитель и наименьшее общее кратное многочленов. Очевидно, что два различных многочлена f и φ можно представить в виде произведения одних и тех же нормированных неприводимых многочленов:

$$\left.\begin{array}{l} f = ap_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \\ \varphi = bp_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s} \end{array}\right| \quad \begin{array}{l} \alpha_i \ge 0,\ \beta_i \ge 0 \\ i = \overline{1,\ldots,s} \end{array}$$

Тогда $(f, \varphi) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$, где $\gamma_i = \min(\alpha_i, \beta_i)$ и $[f, \varphi] = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s}$, где $l_i = \max(\alpha_i, \beta_i)$

П р и м е р 18.1. Найти наибольший общий делитель и наименьшее общее кратное многочленов

$f = (x-2)^4(x + 3)^2(2x - 1)$ и $g = (2x - 1)^3(x+3)(x - 5)$.

Р е ш е н и е.

$(f, \varphi) = (x - 2)^0(x+3)^1(2x - 1)(x - 5)^0 = (x+3)(2x - 1)$;

$[f, \varphi] = (x - 2)^4(x+3)^2(2x - 1)^3(x - 5)$.

П р и м е р 18.2. Найти наибольший общий делитель многочленов: $(x - 1)^3(x+2)^2(x - 3)(x - 4),(x - 1)^2(x+2)(x+5)$.

Р е ш е н и е.

Решим задачу средствами математического пакета *Mathematica:*

In[3]:=PolynomialGCD[(x – 1)^3(x + 2^2*(x – 3)*(x – 4),*
(x – 1)^2(x + 2)*(x + 5)]*

Out[3]= $(-1 + x)^2(2 + x)$

О т в е т: $(f, \varphi) = (x-1)^2(x+2)$

П р и м е р 18.3. Найти наименьшее общее кратное многочленов:

а) $f = x^3 - 125$, $g = x^2 - 25$, $s = x - 5$.

Р е ш е н и е.

In[17]:=PolynomialLCM[x^3 – 125, x^2 – 25, x – 5]

Out[17]= $(-5 + x)(5 + x)(25 + 5x + x^2)$

In[18]:=Expand[$(-5 + x)(5 + x)(25 + 5x + x^2)$*]*

Out[18]= – 625 – 125x + 5x³ + x⁴

Ответ: $[f,g,s] = -625-125x+5x^3+x^4$.

б) $f = x^3 - 125$, $g = x^2 - 25$, $s = x^4 + 5$.

Решение.

In[16]:=PolynomialLCM [x^3 – 25, x^2 – 125, x^4 + 5]

Out[16]= $(-125+x)^2(-25+x^3)(5+x^4)$

Ответ: $[f,g,s] = (-125+x^2)(-25+x^3)(5+x^4)$.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найти наибольший общий делитель многочленов:
   а) $(x^2 + 5x + 6)(x^2 - 1)$ и $(x^4 - 2)(x^2 + 2x - 3)$;
   б) (x – 1) 3 (x + 2) 2(x – 3) (x – 4) и (x – 1) 2 (x + 2) (x + 5);
   в) $(x - 1)(x^2 - 1)(x^3 - 1)(x^4 - 1)$ и $(x + 1)(x^2 + 1)(x^3 + 1)(x^4 + 1)$.

§ 19. Характеристика поля

Не все свойства числовых полей сохраняются в случае произвольного поля. К примеру, складывая число 1 само с собой несколько раз, то есть, беря любое целое положительное, кратное единице, мы никогда не получим нуля, и все эти кратные – натуральные числа будут отличны друг от друга. Если же мы будем брать целые кратные единицы в каком-либо конечном поле, то среди них непременно будут равные, поскольку это поле обладает лишь конечным числом различных элементов. Если все целые кратные единицы поля P являются различными элементами поля P, то есть $k\cdot 1 \neq l\cdot 1$ при $k \neq l$, то говорят, что поле P имеет характеристику нуль; таковы, например, все числовые поля. Если же существуют такие целые числа k и l, что $k > l$, но в поле P имеет место равенство $k\cdot 1 = l\cdot 1$, то $(k - l)\cdot 1 = 0$, то есть в P существует такое целое положительное число, кратное единице, которое оказывается равным 0. В этом случае P называется полем конечной характеристики, а именно характеристики p, если p есть тот первый положительный коэффициент, с которым единица поля P обращается в нуль. Примерами полей конечной характеристики служат все конечные поля; существуют, впрочем, и бесконечные поля, имеющие конечную характеристику.

§ 20. Формальная производная многочлена

Пусть поле P имеет характеристику нуль и многочлен $f \in P[x]$.

Если f = const, то ее производную будем считать равной нулю.

Если $f \neq$ const, то в естественном виде $f = a_n x^n + \ldots + a_1 x + a_0, \quad a_n \neq 0.$

Тогда формальной производной многочлена будем называть многочлен $f' = n \cdot a_n x^{n-1} + \ldots + a_1$.

Тот подход, который существует в математическом анализе, к многочленам не применим, так как коэффициенты не всегда числа и теория пределов не годится, поэтому подход к понятию производной формальный.

В любом случае $n \cdot a_n = (\underbrace{a_n + a_n + \ldots + a_n}_{n \text{ раз}})$

Пример 20.1. Пусть многочлен $f \in Z_3$, $f = x^6 + x^3 + \bar{1}$. Найдем для него производную: $f' = 6 \cdot \bar{1} \cdot x^5 + 3 \cdot \bar{1} \cdot x^2 = (\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1}) \cdot x^5 +$ $+(\bar{1} + \bar{1} + \bar{1}) \cdot x^2 = \bar{0}$.

Если коэффициенты не числа, то в результате f' не всегда многочлен степени $(n - 1)$, как показывает этот пример.

Свойства производной следующие:

1. $(\forall f, g \in P[x]) \qquad (f + g)' = f' + g'$.

Доказательство. Запишем многочлены f и g в естественном виде: $f = a_n x^n + \ldots + a_1 x + a_0$, $g = b_n x^n + \ldots + b_1 x + b_0$, тогда $f + g = (a_n + b_n) \cdot x^n + \ldots + (b_1 + a_1) \cdot x + (b_0 + a_0)$.

$(f + g)' = n \cdot (a_n + b_n) \cdot x^{n-1} + \ldots + 2 \cdot (b_2 + a_2) \cdot x + (b_1 + a_1) = n \cdot a_n \cdot x^{n-1} +$ $+ \ldots + a_1 + n \cdot b_n \cdot x^{n-1} + \ldots + b_1 = f' + g'$.

2. $(\forall f, g \in P[x]) \qquad (f \cdot g)' = f' \cdot g + g' \cdot f$.

3. $(\forall f \in P[x])(\forall p \in N) \qquad (f^p)' = p \cdot f^{p-1} \cdot f'$.

Доказательство. Если $p = 1$, то в левой части данного равенства будет f', в правой — $1 \cdot f^{1-1} \cdot f' = f'$. Справедливость равенства очевидна.

Пусть утверждение справедливо для некоторого $k \in N$, то есть $(f^k)' = k \cdot f^{k-1} \cdot f'$. Покажем, что $(f^{k+1})' = (k+1) \cdot f^k \cdot f'$. Действительно: $(f^{k+1})' = (f^k \cdot f)' = (f^k)' \cdot f + f^k \cdot f' = k \cdot f^{k-1} \cdot f' \cdot f + f^k \cdot f' = f^k \cdot f'(k+1)$, что и требовалось доказать. Тогда по принципу математической индукции утверждение справедливо $(\forall p \in N)$.

4. Если c — некоторая константа, то $(c \cdot f)' = c \cdot f'$, $c \neq 0$.

§ 21. Формула Тейлора

Определение 21.1. Производная от производной $f'(x)$ называется производной второго порядка (или второй производной) функции $f(x)$.

Определение 21.2. Производная от производной n-1 порядка называется производной n-го порядка (или n-ой производной) функции $f(x)$.

Пусть имеется многочлен $f \in P[x]$ и c – const, $\deg f = n$, Тогда $f = f(c) + \frac{f'(c)}{1!}(x-c) + \ldots + \frac{f^{n}(c)}{n!}(x-c)^n$.

Доказательство. Пусть многочлен f имеет вид $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, где $a_0 \neq 0$. Разделим его на двучлен $(x - c)$ с помощью схемы Горнера:

$$
\begin{aligned}
f &= (x-c)q_1 + r_0, \\
q_1 &= (x-c)q_2 + r_1, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
q_{n-2} &= (x-c)q_{n-1} + r_{n-2}, \\
q_{n-1} &= (x-c)a_0 + r_{n-1},
\end{aligned}
\tag{1}
$$

где $q_k \in P[x]$ и $r_k \in P$. Если последнее выражение в (1) для q_{n-1} подставить в предыдущее равенство, а затем то, что при этом получится, подставить вместо q_{n-2} и т.д., то получим равенство:

$$f = r_0 + r_1(x-c) + r_2(x-c)^2 + \ldots + r_{n-1}(x-c)^{n-1} + a_0(x-c)^n. \tag{2}$$

Это есть разложение данного многочлена f по степеням $(x - c)$. Дифференцируя обе части равенства (2) и полагая $x=c$, получим $f(c) = r_0$, $f'(c) = r_1$, $f''(c) = 2!r_2$, ..., $f^{(n)}(c) = n!a_0$. Поэтому равенство (2) можно записать в виде:

$$f = f(c) + f'(c)(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n.$$

Это и есть формула Тейлора для многочленов. Все вычисления удобно расположить в одну таблицу:

	a_0	a_1	..	a_{n-1}	a_n
c	b_0	b_1	..	b_{n-1}	$r_0 = f(c)$
c	c_0	c_1	..	$r_1 = f'(c)$	
c	d_0	d_1	..	$r_2 = \frac{f''(c)}{2!}$	
c	...	...	..	...	
c	a_0	$r_{n-1} = \frac{f^{(n-1)}(c)}{(n-1)!}$			

П р и м е р 21.1. Разложим многочлен $2x^5 - x^2 + 2$ по степеням $x+1$. Для этого построим таблицу:

			1		
-1					
	2		3		1
-1					
	4		9	2	
-1					
	6	2	21		
-1					
	8	0			
-1					
	10				
-1					

Используя формулу Тейлора, получим:

$$2x^5 - x^2 + 2 = -1 + 12(x+1) - 21(x+1)^2 + 20(x+1)^3 - 10(x+1)^4 + 2(x+1)^5.$$

З а м е ч а н и е. Процесс получения коэффициентов разложения многочлена по степеням *x + 1* аналогичен переводу записи целого числа из одной позиционной системы счисления в другую. Многочлен в естественном виде есть запись в системе счисления с основанием x. Разложение многочлена по степеням $x+1$ есть запись в системе счисления с основанием $x+1$.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найдите $f(x)$, если:

1) $f(x) = f'(x) + x$;

2) $f'(x) = 3x^3 - 2x^2 + x - 1$ и $f(2) = 2$;

3) $f(x) = [f'(x)]^n$ при некотором $n \in N$.

2. Разложить многочлен по степеням $(x-c)$, пользуясь формулой Тейлора:

а) $f(x) = x^4 - 6x^3 + 12x^2 - 26x + 37$, $c = 2$;

б) $f(x) = x^4 - x^3 - x + 1$, $c = 2$;

в) $f(x) = x^4 + 3x^3 + 5x^2 + 5x + 2$, $c = -2$;

г) $f(x) = x^4 - 5x^3 + 9x^2 - 8x + 4$, $c = 1$;

д) $f(x) = x^4 + 3x^3 + 2x^2 + 4x + 8$, $c = -1$.

3. Пользуясь схемой Горнера, найдите значение многочлена и всех его производных при $x = a$:

а) $f(x) = 2x^5 + 7x^4 - x^3 + 3x - 2$, $a = -3$;

б) $f(x) = 3x^5 + 7x^4 + x^3 - 2x + 3$, $a = -2$;

в) $f(x) = x^4 - 3ix^3 - 4x^2 + 5ix - 1$, $a = 1 + 2i$.

4. Пусть $f(x)$ — многочлен n-й степени над R, $a \in \mathbf{R}$ и $f(a) \geq 0$, $f'(a) \geq 0$, …, $f^{(n-1)}(a) \geq 0$, $f^{(n)}(a) > 0$. Докажите, что действительные корни многочлена $f(x)$ не превосходят a.

§ 22. Корни многочлена и его производных

В этом параграфе все рассмотрения будут происходить над полем нулевой характеристики.

Теорема 22.1. Пусть $f \in P[x]$, $\deg f \geq 1$. Если α — k-кратный корень многочлена f, то он является корнем производной многочлена порядка кратности $k-1$. Если α — простой корень, то он не является корнем производной многочлена f.

Доказательство. Пусть α – корень многочлена f кратности k, тогда f можно представить в виде $f = (x-\alpha)^k\cdot\varphi$, где $\varphi\in P[x]$ и φ не делится на $(x-\alpha)$.

Найдем производную многочлена f, имеем:

$$f'=((x-\alpha)^k\ \varphi)'=((x-\alpha)^k)'\cdot\varphi+(x-\alpha)^k\cdot\varphi'=k\cdot(x-\alpha)^{k-1}\cdot\varphi+(x-\alpha)^k\cdot\varphi'=$$
$$=(x-\alpha)^{k-1}(k\varphi+\varphi'(x-\alpha))=(x-\alpha)^{k-1}\cdot h.$$

Докажем теперь, что h не делится на $(x-\alpha)$.

Имеем $(x-\alpha)\cdot\varphi' \vdots (x-\alpha)$. Но $k\varphi$ не делится на $(x-\alpha)$, так как φ не делится на $(x-\alpha)$ по условию, а k — константа, $(x-\alpha)$ — неприводимый многочлен $\Rightarrow$ h не делится на $(x-\alpha)$. Тогда по определению кратного корня α — корень многочлена f' кратности $k-1$.

Если α — простой корень, то $f=(x-\alpha)\cdot\varphi$, φ не делится на $(x-\alpha)$.

$f'=(x-\alpha)'\cdot\varphi+(x-\alpha)\cdot\varphi'=\varphi+(x-\alpha)\cdot\varphi'$ $\Rightarrow$ f' не делится на $(x-\alpha)$ $\Rightarrow$ α — не является корнем производной многочлена f. □

Следствие. Если α — корень многочлена f' кратности k, то α является корнем производных многочлена f до $(k-1)$ включительно и не является корнем k-й производной.

Доказательство. Допустим, что α — k-кратный корень. Тогда по предыдущей теореме он является $(k-1)$-кратным для f', $(k-2)$ - кратным для f'' и т.д. и нулевым для $f^{(k)}$, что противоречит условию. □

Теорема 22.2. Неприводимый над полем P многочлен не имеет кратных корней над любым расширением этого поля.

Доказательство. Методом от противного. Пусть f — неприводимый многочлен и имеет α — корнем кратности $k\neq 1$. Тогда $f=(x-\alpha)^k\cdot\varphi$ или f запишется в виде $f=(x-\alpha)\cdot[(x-\alpha)^{k-1}\cdot\varphi]$ произведения двух многочленов $f_1=(x-\alpha)$ и $f_2=(x-\alpha)^{k-1}\cdot\varphi$, где $\deg f_1=1$, $\deg f_2\geq 1$, что противоречит тому, что f — неприводимый многочлен. Значит, наше предположение неверно, а верно то, что требуется доказать. □

Теорема 22.3. Если для последовательных производных многочлена $f(x)$ имеет место $f(\alpha)=0$, $f'(\alpha)=0$, $f''(\alpha)=0\ldots f^{(k-1)}(\alpha)=0$, $f^{k}(\alpha)\neq 0$, то число α является для $f(x)$ корнем кратности k.

Пример 22.1. Является ли число 1 корнем для многочлена $f(x)=273x^{10}-100x^9-1830x+1657$, если да, то какой кратности?

Решение.

$f(x)=273x^{10}-100x^9-1830x+1657$,

$f(1) = 0,$

$f'(x) = 2730x^9 – 900x^8 – 1830,$

$f'(1) = 2730 – 900 – 1830 = 0,$

$f''(x)= 24570x^8 – 7200x^7,$

$f''(1)\neq 0,$ тогда 1 является для многочлена $f(x)$ корнем кратности 2.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Определить A и B так, чтобы $f(x)= Ax^{n+1} + Bx^n + 1$ делился на $(x – 1)^2$.

2. При каком значении a многочлен $x^5 – ax^2 – ax + 1$ имеет –1 корнем не ниже второй кратности?

3. Определить, при каких a, $в$, c многочлен $f(x) = x^4 + ax^3 + вx^2 + cx – 24$ имеет число –2 корнем не ниже кратности 3?

4. Определить a и $в$ так, чтобы многочлен $f(x) = x^5 + ax^2 + вx + 1$ имел число –2 корнем не ниже кратности 2.

5. Покажите, что многочлен $1+\frac{x}{1!}+\frac{x^2}{2!}+...+\frac{x^n}{n!}$ не имеет кратных корней.

6. Доказать, что многочлен $x^{2n}-nx^{n+1}+nx^{n-1}-1$ имеет число 1 корнем кратности 3.

§ 23. Неприводимые множители многочлена и его производной

В этом параграфе все рассмотрения будут происходить над полем нулевой характеристики.

Определение 23.1. Говорят, что неприводимый многочлен p является делителем кратности α, если $f \vdots p^{\alpha} \;\wedge\; f$ не делится на $p^{\alpha+1}$.

Докажем теорему об изменении кратности неприводимого делителя при дифференцировании многочлена.

Теорема 23.1. Если неприводимый делитель p входит в многочлен с кратностью α, то в f' он войдет с кратностью $\alpha – 1$.

Доказательство. Пусть многочлен $f = p^{\alpha}\cdot h$, h не делится на p. Продифференцируем данное равенство:

$f'= (p^{\alpha}\cdot h)'= (p^{\alpha})'\cdot h + p^{\alpha}\cdot h'= \alpha\cdot p^{\alpha-1}\cdot p'\cdot h + p^{\alpha}\cdot h' = p^{\alpha-1}\cdot(\alpha\cdot p'\cdot h + p\cdot h').$

$f' \vdots\, p^{\alpha-1}$. Покажем, что выражение $(\alpha\cdot p'\cdot h + p\cdot h')$ не может делиться на p.

Для этого достаточно показать, что $(\alpha \cdot p' \cdot h)$ не делится на p. Действительно, α не делится на p как многочлен нулевой степени, h не делится на p (по условию), p' не делится на p, так как его степень ниже степени p. Поскольку каждый множитель не делится на p, то и все произведение не делится на p. Следовательно, p действительно войдет в производную многочлена f с кратностью $\alpha - 1$. □

С л е д с т в и е. Для того чтобы многочлен f не имел кратных неприводимых делителей, необходимо и достаточно, чтобы $(f; f') = 1$ (то есть чтобы f и f' были взаимно просты).

Теорема 23.2 (отделение кратных неприводимых делителей).

Пусть $f = ap_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. Обозначим через F_1 произведение неприводимых делителей кратности 1 взятых по одному разу; через F_2 — произведение неприводимых делителей кратности 2, взятых тоже по одному разу; через F_3 — произведение неприводимых делителей кратности 3, взятых тоже по одному разу, и так далее: через F_s — произведение неприводимых делителей кратности s, взятых по одному разу. С учетом этого многочлен f примет вид $f = a \cdot F_1 \cdot F_2^2 \cdot F_3^3 \ldots \cdot F_s^s$. Выделим $F_1, F_2, F_3, \ldots, F_s$. Найдем производную $f' = b \cdot F_2 \cdot F_3^2, \ldots, \cdot F_s^{s-1}$.

Найдем наибольший общий делитель f и f', обозначив $(f, f') = d_1$:

$$d_1 = F_2 \cdot F_3^2 \cdot \ldots \cdot F_s^{s-1}, \qquad d_1' = c \cdot F_3 \cdot \ldots \cdot F_s^{s-2},$$

$$d_2 = (d_1, d_1'), \qquad d_2 = F_3 \cdot \ldots \cdot F_s^{s-2},$$

$$d_3 = (d_2, d_2'), \qquad d_3 = F_4 \cdot \ldots \cdot F_s^{s-3},$$

$$\ldots \qquad \ldots$$

$$d_{s-1} = (d_{s-2}, d_{s-2}') = F_s,$$

$$d_s = (d_{s-1}, d_{s-1}') = 1.$$

Найдем следующие отношения:

$$v_1 = \frac{f}{d_1} = a \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_s,$$

$$v_2 = \frac{d_1}{d_2} = F_2 \cdot F_3 \cdot \ldots \cdot F_s,$$

$$v_3 = \frac{d_2}{d_3} = F_3 \cdot F_4 \cdot \ldots \cdot F_s,$$

$$\ldots$$

$$v_{s-1}=\frac{d_{s-2}}{d_{s-1}}=F_{s-1}\cdot F_s,$$

$$v_s=\frac{d_{s-1}}{d_s}=F_s.$$

Теперь найдем $\frac{v_1}{v_2}=a\cdot F_1$:

$$\frac{v_2}{v_3}=F_2,$$

$$\frac{v_3}{v_4}=F_3,$$

. . . .

$$\frac{v_{s-1}}{v_s}=F_{s-1},$$

$$v_s=F_s.$$

Итак, мы выделили все неприводимые делители $f=a\cdot F_1\cdot F_2^2\cdot F_3^3\ldots\cdot F_s^s$.

Пример 23.1. Найти значения многочлена $f=3x^4-2x^3+6x^2-30$ и всех его производных в точке 2.

Решение. Разложим многочлен f по степеням двучлена $x-2$ с помощью схемы Горнера:

	3	–2	6	0	–30
2	3	4	14	28	26
2	3	10	34	96	
2	3	16	66		
2	3	22			
2	3				

Имеем: $f=26+96(x-2)+66(x-2)^2+22(x-2)^3+3(x-2)^4$. Теперь применим к данному многочлену формулу Тейлора: $f=f(c)+\frac{f'(c)}{1!}(x-c)+\frac{f''(c)}{2!}(x-c)^2+$ $+\frac{f'''(c)}{3!}(x-c)^3+\frac{f^{IV}(c)}{4!}(x-c)^4=26+96(x-2)+\frac{132}{2!}(x-2)^2+\frac{132}{3!}(x-2)^3+\frac{72}{4!}(x-2)^4.$

Сравнивая два последних разложения, получаем: $f(2)=26$, $f'(2)=96$, $f''(2)=132$, $f'''(2)=132$, $f^{(IV)}=72$.

Пример 23.2. Найти НОД многочлена f и его производной, если $f=(x-1)^3\cdot(x^2+1)^2\cdot(x-3)$.

Решение. Многочлен f задан в каноническом виде, множитель $(x - 1)$ входит в него с кратностью 3, множитель (x^2+1) с кратностью 2, множитель $(x - 3)$ с кратностью 1, тогда в производную многочлена f они войдут соответственно с кратностью 2, 1 и 0 соответственно.

$f' = (x - 1)^2 \cdot (x^2 + 1) \cdot g$, где $g \in P[x]$ / $\deg f' = \deg f - 1$,

$\deg f = 8 \Rightarrow \deg f' = 7$, следовательно, g имеет степень 3, но g не кратен $(x - 1)$, $(x^2 + 1)$, $(x - 3)$, тогда $(f', f) = (x - 1)^2(x^2 + 1)$.

Пример 23.3. Найти наибольший общий делитель многочлена и его производной, если $f = (x - 1)^3 \cdot (x+1)^2 \cdot (x - 3)$.

Решение. Используем пакет *Mathematica*. Сначала находим производную:

In[4]:= D[(x – 1)^3(x + 1)^2*(x – 3), x]*

Out[4]=2(–3+x)(–1+x)^3(1+x)+3(–3+ x)(–1+ x)^2(1+x)^2+(–1+ x)^3(1 + x)^2]

Затем находим наибольший общий делитель многочленов:

In[5]:=PolynomialGCD[(x – 1)^3(x + 1)^2*(x – 3),*

2(– 3 + x)(–1+ x)^3(1+ x) + 3(–3 + x)(–1 + x)^2(1 + x)^2 + (–1 + x)^3(1 + x)^2]

Out[5] =$1 - x - x^2 + x^3$

Ответ: $(f', f) = x^3 - x^2 - x + 1$.

Пример 23.4. Отделить неприводимые кратные делители многочлена $f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1$.

Решение. Вычислим производную многочлена: $f' = 8x^7 - 6x^5 - 10x^4 + 6x^2 + 2x$. С помощью алгоритма Евклида найдем наибольший общий делитель многочлена f и его производной f': $(f', f) = x^4 - x^3 - x + 1 = x^3(x - 1) - (x - 1) = (x - 1)(x^3 - 1) = (x - 1)(x - 1) \cdot$ $\cdot (x^2 + x + 1) = (x - 1)^2(x^2 + x + 1)$.

Из этого равенства следует, что $f' \vdots (x - 1)^2(x^2 + x + 1) \Rightarrow$ $f \vdots (x - 1)^3(x^2 + x + 1)^2$, $f = (x - 1)^3(x^2 + x + 1)^2(ax + в)$. Подберем a и $в$: $a = 1$, $в = 1$.

Значит, $f = (x - 1)^3 (x^2 + x + 1)^2(x + 1)$.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найдите наибольший общий делитель многочлена $f(x)$ и его производной, если:

а) $f(x) = (x - 1)^3(x + 1)^2(x - 3)$;

б) $f(x) = (x - 1)(x^2 - 1)(x^3 - 1)(x^4 - 1)$.

2. Найдите многочлен, который имеет те же корни, что и многочлен $f(x) = x^7 - 9x^5 + 6x^4 + 15x^3 - 12x^2 - 7x + 6$, только однократные.

3. Отделить кратные множители многочлена:

а) $f(x) = x^7 - x^6 - 4x^5 + 3x^3 + 5x^2 + 8x + 4;$

б) $f(x) = x^6 - 6x^5 + 9x^4 + 12x^3 - 48x^2 + 48x - 16;$

в) $f(x) = x^5 - 10x^3 - 20x^2 - 15x - 4.$

§ 24. Рациональные корни многочленов

Теорема 24.1. Если многочлен $f = a_nx^n + \ldots + a_1x + a_0 \in Z[x]$ имеет несократимую дробь $\frac{p}{q}$ корнем, то p — делитель сводного члена a_0, q — делитель a_n ; $p - mq$ — делитель $f(m)$ $\forall m \in Z$.

Доказательство.

1. $\frac{p}{q}$ — несократимая $\Rightarrow$ $(p, q) \sim 1$. Так как $\frac{p}{q}$ — корень многочлена $f \Rightarrow \frac{\grave{a}_n \cdot p^n}{q^n} + \frac{a_{n-1} \cdot p^{n-1}}{q^{n-1}} + \ldots + \frac{a_1 p}{q} + a_0 = 0$. Умножим последнее равенство на q^n: $a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$ (1)

а) разделим равенство (1) на q:

$$\underset{\in Z}{\frac{a_n p^n}{q}} = \underbrace{-(a_{n-1} p^{n-1} + \ldots + a_1 p q^{n-2} + a_0 q^{n-1})}_{\in Z}$$

Тогда $a_n p^n \vdots q$. Так как $(p, q) \sim 1$ $\Rightarrow$ по свойству взаимно простых чисел $(p^n, q) \sim 1 \Rightarrow a_n \vdots q;$

б) разделим равенство (1) на p:

$$\underset{\in Z}{\frac{a_0 q^n}{p}} = \underbrace{-(a_n p^{n-1} + a_{n-1} p^{n-2} q + \ldots + a_1 q^{n-1})}_{\in Z}$$

Тогда $a_0 q^n \vdots p$. Так как $(p, q) \sim 1$, то $(p, q^n) \sim 1 \Rightarrow a_0 \vdots p$.

2. Расположим многочлен f по степеням $(x - m)$, используя схему Горнера: $f = a_n (x-m)^n + c_{n-1}(x-m)^{n-1} + \ldots + c_1 (x-m) + c_0$, где $c_0, \ldots, c_{n-1}, a_n \in Z$.

Тогда $f(\frac{p}{q}) = a_n (\frac{p}{q} - m)^n + c_{n-1}(\frac{p}{q} - m)^{n-1} + \ldots + c_1(\frac{p}{q} - m) + c_0 = 0$.

Отсюда $\dfrac{a_n(p-mq)^n}{q^n}+\dfrac{c_{n-1}(p-mq)^{n-1}}{q^{n-1}}+\ldots+\dfrac{c_1(p-mq)}{q}+c_0=0.$

Умножим на q^n:

$a_n(p-mq)^n+c_{n-1}(p-mq)^{n-1}q+\ldots+c_1(p-mq)q^{n-1}+c_0q^n=0$.

Разделим последнее равенство на $(p-mq)$:

$$\underbrace{\frac{c_0q^n}{p-mq}}_{\in Z}=-(\underbrace{a_n(p-mq)^{n-1}+\ldots+c_1q^{n-1}}_{\in Z}).$$

Тогда $c_0q^n \,\vdots\, (p-mq)$.

Если $\dfrac{p}{q}$ — несократимая дробь, тогда $(\dfrac{p}{q}-m)$ — несократимая дробь, то есть $\dfrac{p-mq}{q}$ $\Rightarrow (p-mq, q)\sim 1 \Rightarrow (p-mq, q^n)\sim 1$. Следовательно, $c_0 \,\vdots\, (p-mq)$.

Согласно схеме Горнера: $c_0=f(m)$, то есть $f(m) \,\vdots\, p-mq$. □

Следствие. Если $\dfrac{p}{q}$ — корень, то $f(1) \,\vdots\, p-q$, $f(-1) \,\vdots\, p+q$.

Замечание. Данная теорема является лишь необходимым условием существования корня, а потому с помощью первого условия теоремы можно найти все возможные корни, с помощью второго можно отбросить некоторые, но, в конечном счете, они должны быть проверены с помощью схемы Горнера.

Пример 24.1. Найти рациональные корни многочлена:

а) $4x^3-3x-1$.

Решение. Найдем все делители свободного члена: $p=\{\pm1\}$ и положительные делители старшего коэффициента: $q=\{1, 2, 4\}$.

Возможные корни многочлена: $\dfrac{p}{q}=\{\pm1; \pm1/2; \pm1/4\}$.

Пусть $m=1$, тогда $f(1)=0$, то есть число 1 является корнем данного многочлена. Возьмем $m=-1$, тогда $f(-1)=-2$.

Составим таблицу, в которой в первой строке запишем возможные рациональные корни искомого многочлена:

	1/2	–1/2	1/4	–1/4
$\frac{-2}{p+q}\in Z$	ξ	+	ξ	ξ

Итак, возможный рациональный корень равен (–1/2). Убедимся в этом непосредственной подстановкой данного числа в многочлен:

$f(-1/2) = -4\cdot 1/8 + 3\cdot 1/2 - 1 = -1/2 + 3/2 - 1 = 0.$

О т в е т: $\{1; -1/2\}$ – рациональные корни искомого многочлена.

б) $f = 6x^4 + 19x^3 - 7x^2 - 26x - 12.$

Р е ш е н и е. Выпишем делители свободного члена и старшего коэффициента $p = \{\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 12\}$,

$q = \{1; 2; 3; 6\}$.

Если данный многочлен имеет рациональные корни, то они могут быть только среди чисел:

$\frac{p}{q} = \{\pm 1; \pm 1/2; \pm 1/3; \pm 1/6; \pm 2; \pm 2/3; \pm 3; \pm 3/2; \pm 4; \pm 4/3; \pm 6; \pm 12\}.$

Найдем значение многочлена: $f(1) = -20$, $f(-1) = -6$, $f(2) = 156$.

	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{6}$	$-\frac{1}{6}$	$\frac{2}{1}$	$\frac{2}{3}$	$\frac{3}{1}$	$-\frac{3}{1}$	$\frac{3}{2}$	$-\frac{3}{2}$	$\frac{4}{1}$	$-\frac{4}{1}$	$\frac{4}{3}$	$-\frac{4}{3}$	$\frac{6}{1}$	$-\frac{6}{1}$	$\frac{12}{1}$	$-\frac{12}{1}$
$\frac{-20}{p-q} \in Z$	+	ξ	+	+	+	ξ	+	+	+	+	+	+	ξ	+	+	ξ	+	ξ	ξ	ξ
$\frac{-6}{p+q} \in Z$	+	ξ	ξ	+	ξ	ξ	+	ξ	ξ	ξ	ξ	+	ξ	+	ξ	ξ	ξ	ξ	ξ	ξ
$\frac{156}{p-2q} \in Z$	+	ξ	ξ	ξ	ξ	ξ	ξ	ξ	ξ	ξ	ξ	ξ	ξ	+	ξ	ξ	ξ	ξ	ξ	ξ

Окончательную проверку проведем по схеме Горнера:

	6	19	–7	–26	–12
1/2	6	22	4	–24	$-24 \neq 0$
–4	6	–5	13	–78	$300 \neq 0$

О т в е т: рациональных корней нет.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Найти рациональные корни многочлена:

а) $2x^3 - 3x^2 - 3x + 2;$

б) $2x^4 + 3x^3 - 12x^2 + 6x - 6;$

в) $x^4 - 2x^3 - 8x^2 + 13x - 24;$

г) $\frac{1}{8}x^6 - \frac{3}{4}x^5 + \frac{11}{8}x^4 - \frac{1}{8}x^3 - \frac{9}{4}x^2 + \frac{5}{2}x - 1;$

д) $x^4 + x^3 - 11x^2 - 5x + 30;$

е) $x^3 - 6x^2 + 15x - 14;$

ж) $x^5 - 7x^3 - 12x^2 + 6x + 36;$

з) $2x^3 + 3x^2 + 6x - 4;$

и) $x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6.$

2. Доказать, что многочлен $f(x)$ с целыми коэффициентами не имеет целых корней, если $f(0)$, $f(1)$ — нечетные числа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алгебра и теория чисел / Под ред. Н.Я. Виленкина. — М.: Просвещение, 1984. — 192 с.

2. Компьютерная алгебра. Символьные и алгебраические вычисления / Под ред. Б. Бухбергера, Дж. Коллинза, Р. Лооса. – М.: Мир, 1986. – 392 с.

3. *Винберг Э.Б.* Алгебра многочленов. — М.: Просвещение, 1980. — 175 с.

4. *Винберг Э.Б.* Курс алгебры. — М.: Факториал, 2002. — 544 с.

5. *Девенпорт Дж., Сирэ И., Турнье Э.* Компьютерная алгебра. Символьные и алгебраические вычисления. — М: Мир, 1991. — 350 с.

6. *Дьяконов В.П.* Системы символьной математики Mathematica 2 и Mathematica 3. — М: СК-пресс, 1998. — 318 с.

7. *Кострикин А.И.* Введение в алгебру. Основы алгебры. — М.: Физматлит, 1994. — 320 с.

8. *Кузнецова И.В.* Теория многочленов: учебное пособие / И.В. Кузнецова, А.Н. Костиков; Поморский гос. ун-т им.М.В. Ломоносова — Архангельск: Поморский университет, 2006. — 154 с.

9. *Куликов Л.Я.* Алгебра и теория чисел. — М.: Высш. шк. 1979. — 559 с.

10. *Куликов Л.Я., Москаленко А.И., Фомин А.А.* Сборник задач по алгебре и теории чисел. — М.: Просвещение,1993. — 288 с.

11. *Курош А.Г.* Курс высшей алгебры. — М.: Наука, 1971. — 432 с.

12. *Лельчук М.П., Полевченко И.И., Радьков А.М., Чеботаревский Б.Д.* Практические занятия по алгебре и теории чисел. — Минск: Вышэйшая шк., 1986. — 301 с.

13. *Ленг С.* Алгебра. — М.: Мир, 1968. — 564 с.

14. Сборник задач по алгебре / Под ред. А.И. Кострикина. — М.: Физматлит, 2001. — 464 с.

15. *Фаддеев Д.К.* Лекции по алгебре. — М.: Наука, 1984. — 416 с.

16. *Фаддеев Д.К., Соминский И.С.* Задачи по высшей алгебре. — СПб: Лань, 2008. — 298 с.

17. *Шнеперман Л.Б.* Сборник задач по алгебре и теории чисел. — Минск: Дизайн ПРО, 2000. — 240 с.