Федеральное агентство по образованию

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГОУВПО «АмГУ»

Факультет математики и информатики

УТВЕРЖДАЮ

Зав. кафедрой МАиМ

_____Т.В. Труфанова

15 мая 2007г.

АЛГЕБРА

Учебно – методический комплекс дисциплины для специальностей 010101 – математика

Составитель: **Н.В. Кван**

Благовещенск

2007

ББК
К

Печатается по решению редакционно-издательского совета факультета математики и информатики Амурского государственного университета

Кван Н.В.

Алгебра. Учебно – методический комплекс дисциплины для студентов АмГУ 1 и 2 курсов очной формы обучения по специальности 010101 «Математика». – Благовещенск: Амурский гос. ун–т, 2007. − 163 с.

Учебно – методический комплекс дисциплины "Алгебра" содержит рабочую программу дисциплины, краткий курс лекций, материалы для проведения практических занятий, контролирующие материалы для осуществления промежуточного и итогового контроля, справочный материал и библиографический список.

1. ГОСУДАРСТВЕННЫЙ ОБРАЗВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Специальность 010101 – «Математика»

Квалификация – Математик

ОПД.Ф.02 Алгебра

Понятие группы, кольца и поля; поле комплексных чисел; кольцо многочленов; деление многочленов с остатком; теорема Безу; кратность корня многочлена, ее связь со значениями производных; разложение многочлена на неприводимые множители над полями комплексных и действительных чисел; формулы Виета; наибольший общий делитель многочленов, его нахождение с помощью алгоритма Евклида; кольцо многочленов от нескольких переменных; симметрические многочлены. Группа подстановок; четность подстановки; циклические группы; разложение группы на смежные классы по подгруппе; теорема Лагранжа. Системы линейных уравнений; свойства линейной зависимости; ранг матрицы; определители, их свойства и применение к исследованию и решению систем линейных уравнений; кольцо матриц и группа невырожденных матриц. Векторные пространства; базис и размерность; подпространства; сумма и пересечение подпространств; прямые суммы; билинейные и квадратичные формы; приведение квадратичной формы к нормальному виду; закон инерции; положительно определенные квадратичные формы; критерий Сильвестра; ортонормированные базисы и ортогональные дополнения; определители Грама и объем параллелепипеда. Линейные операторы; собственные векторы и собственные значения; достаточные условия приводимости матрицы линейного оператора к диагональному виду; понятие о жордановой нормальной форме; самосопряженные и ортогональные (унитарные) операторы; привидение квадратичной формы в евклидовом пространстве к каноническому виду. Аффинные системы координат; линейные многообразия, их взаимное

расположение; квадрики (гиперповерхности второго порядка); их аффинная и метрическая классификация и геометрические свойства; Примеры групп преобразований: классические линейные группы, группа движений и группа аффинных преобразований, группы симметрии правильных многоугольников и многогранников в трехмерном пространстве; классификация движений плоскости и трехмерного пространства.

2. РАБОЧАЯ ПРОГРАММА

по дисциплине **"Алгебра"**

для специальности 010101–"Математика"

Курс 1, 2 Семестр 2, 3

Лекции 108 (36+72) час. Экзамен 3 семестр

Практические (семинарские) занятия 72 (36+36) час. Зачет 2, 3 семестр

Лабораторные занятия (нет)

Самостоятельная работа 70 час.

Всего 250 часов

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования по специальности 010101–"Математика"

Составитель Н.В. Кван, ст. преподаватель.
Факультет математики и информатики.

Кафедра математического анализа и моделирования.

2007 г.

2. 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ, ЕЁ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ

Дисциплина «Алгебра» ставит своей целью ознакомление студентов с основными алгебраическими структурами (группы, кольца, поля, конечномерные алгебры), их конкретными реализациями (поле комплексных чисел, кольца многочленов, абелевы группы, группы симметрии, линейные группы) и методами их исследования.

В процессе обучения студенты должны получить навыки владения аксиоматическим методом, усвоить и научиться пользоваться основными понятиями теории групп (подгруппы, нормальные делители, смежные классы, фактор группы, гомоморфизм, циклические группы и их представление, абелевы группы, прямые произведения групп), теории колец (обратимые элементы, подкольца, мультипликативная группа, идеалы), теории полей (аддитивная и мультипликативная группы, расширения теории конечномерных алгебр (алгебр гиперкомплексных чисел)).

Студенты должны получить навыки свободной работы в поле комплексных чисел, познакомиться с группой кватернионов и теоремой Фробениуса. Студенты должны знать алгебраическое решение уравнений 3-й и 4-й степени и теорему об алгебраической неразрешимости уравнений степени выше четвертой.

Студенты должны быть ознакомлены с кольцами многочленов от одной и нескольких переменных, знать основные теоремы о делимости, распределении корней и основную теорему алгебры.

Студенты должны знать классические линейные группы, группы движения евклидовых и унитарных пространств, группы аффинных преобразований.

В процессе обучения студенты должны приобрести навыки исследования и решения задач.

Алгебра - один из фундаментальных разделов математики. Ее понятия, результаты и методы широко используются во многих разделах математики:

функциональный анализ, математический анализ, дифференциальная геометрия, во многих разделах теоретической физики и т.д.

2. 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.2.1. Наименование тем, их содержание и объем в часах лекционных занятий

Лекции – 108 часов

Введение — 2 часа.

Основы теории групп — 38 часов.

Определение группы. Примеры групп. Основные свойства групп. Группа подстановок. Основные классические группы: полная линейная, специальная линейная группа, ортогональная группа, специальная ортогональная группа, унитарная группа, специальная унитарная группа. Подгруппы. Циклическая подгруппа. Знакопеременная группа. Гомоморфизмы и изоморфизмы групп. Образ и ядро гомоморфизма. Их свойства. Циклические группы и их подгруппы. Порядок элемента и порядок группы. Свободные элементы и свободные группы. Смежные классы группы по подгруппе. Отношение эквивалентности. Разбиение группы по подгруппе. Теорема Лагранжа. Фактор группа. Нормальные делители группы. Фактор группа. Теорема о гомоморфизме групп. Эндоморфизмы и автоморфизмы групп. Примеры и свойства. Внутренние автоморфизмы. Центр и коммутант группы. Разрешимые группы. Нильпотентные группы. Простые группы. Прямые произведения и прямые суммы групп. Абелевы группы. Строение абелевых групп с конечным числом образующих.

Кольца и поля — 18 часов.

Определение кольца. Примеры. Свойства колец. Понятие тела и поля. Их простейшие свойства. Алгебры Буля и булевы кольца, их свойства, связь с решетками. Гомоморфизмы колец. Идеалы колец. Кольца главных идеалов. Факторкольцо. Кольцо вычетов по данному модулю. Поле вычетов по простому модулю. Простые и полупростые кольца. Радикал кольца. Теорема о гомоморфизме колец. Делители нуля. Теорема о вложении коммутативного кольца в поле частных. Характеристика тела (поля). Простое подполе. Центр

тела. Центральные подполя тела. Векторные пространства и алгебры над полями. Понятие модуля над коммутативным кольцом. Алгебры Ли. Йордановы алгебры. Матричные алгебры Ли.

Кольцо многочленов — 12 часов.

Кольцо многочленов и его целостность. Теорема Безу. Схема Горнера. Ее применение. Число корней многочлена. Многочлены над данным полем. ПОД двух многочленов. Алгоритм Евклида. Приводимые и неприводимые многочлены над данным полем. Производные многочлена. Теорема о неприводимом кратном корне многочлена и его производной. Кратность корня многочлена. Отделение кратных множителей многочлена.

Многочлены от n переменных — 8 часов.

Многочлены от n переменных. Лексикографическое упорядочение. Основная теорема о симметрических многочленах и следствия из нее. Представление симметрических многочленов через основные симметрические. Степенные суммы. Результант двух многочленов. Исключение неизвестных. Дискриминант.

Многочлены над полем C и R — 10 часов.

Леммы о свойствах многочленов над полем С. Основная теорема алгебры. Решение уравнений 3 степени по формулам Кардано. Решение уравнений 4степени методом Феррари. Результаты Руфини, Абеля и Галуа по вопросам решения уравнений высших степеней. Следствия из основной теоремы алгебры. Формулы Виета. Разложение многочлена над полем действительных чисел на неприводимые множители. Границы действительных корней многочлена. Теорема Штурма. Приближенное вычисление действительных корней.

Многочлены над полем Q — 6 часов.

Целые и рациональные корни многочленов. Приводимость многочленов над полем рациональных чисел. Критерий Эйзенштейна.

Поле алгебраических чисел — 6 часов.

Минимальный многочлен алгебраического числа. Строение простого алгебраического расширения. Сопряженные алгебраические числа. Составное алгебраическое расширение поля.

Алгебры с делением — 8 часов.

Алгебры с делением. Алгебра кватернионов. Теорема Фробениуса о конечномерных алгебрах с делением.

2.2. 2. Практические занятия, их содержание и объем в часах - 72 часа

1 курс 2 семестр

1. Определение группы. Примеры групп. Основные свойства групп. - 4 часа.
2. Подгруппы. Циклическая подгруппа. - 4 часа.
3. Гомоморфизмы и изоморфизмы групп. Образ и ядро гомоморфизма. - 4 часа.
4. Циклические группы и их подгруппы. Порядок элемента и порядок группы. -4 часа.
5. Смежные классы группы по подгруппе. Разбиение группы по подгруппе. Теорема Лагранжа. Фактор группа. - 4 часа.
6. Нормальные делители группы. Фактор группа. - 4 часа.
7. Контрольная работа № 1 – 2 часа.
8. Центр и коммутант группы. Разрешимые группы. Нильпотентные группы. Простые группы. Прямые произведения и прямые суммы групп. - 4 часа.
9. Теорема о гомоморфизмах групп. Виды гомоморфизмов – 2 часа.
10. Абелевы группы. Строение абелевых групп с конечным числом образующих - 4 часа.
11. Зачетная контрольная работа. - 2 часа.

2 курс 3 семестр

11.Определение кольца. Примеры. Свойства колец. Понятие тела и поля. - 2 часа.

12.Идеалы колец. Кольца главных идеалов. Факторкольцо. Кольцо вычетов по данному модулю. Поле вычетов по простому модулю. - 2 часа.

13.Кольцо многочленов и его целостность. Теорема Безу. Схема Горнера. Ее применение. - 2 часа.

14.Многочлены над данным полем. НОД двух многочленов. Алгоритм Евклида. - 2 часа.

15.Приводимые и неприводимые многочлены над данным полем. Производные многочлена. - 2 часа.

16.Отделение кратных множителей многочлена. - 2 часа.

17.Контрольная работа №1. - 2 часа.

18.Многочлены от n переменных. Лексикографическое упорядочение. – 2 часа.

19.Представление симметрических многочленов через основные симметрические. Степенные суммы. - 2 часа.

19.Результант двух многочленов. Исключение неизвестных. Дискриминант. - 2 часа.

20.Контрольная работа №2. - 2 часа.

21.Решение уравнений 3 степени по формулам Кардане. Решение уравнений 4 степени методом Феррари. - 2 часа.

22.Следствия из основной теоремы алгебры. Формулы Виета. Разложение многочлена над полем действительных чисел на неприводимые множители. - 2 часа.

23. Границы действительных корней многочлена. Теорема Штурма. Приближенное вычисление действительных корней. - 2 часа.

24.Целые и рациональные корни многочленов. Приводимость многочленов над полем рациональных чисел. Критерий Эйзенштейна. - 2 часа.

25.Контрольная работа №3. - 2 часа.

26.Минимальный многочлен алгебраического числа. Строение простого алгебраического расширения. - 2 часа.

2.3 ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

№	Самостоятельная работа	Часы	Форма контроля
1	Индивидуальное задание №1 по теме «Б.А.О. Группа»	4	Защита работы на консультации
2	Изучение основных классических групп: полная линейная, специальная линейная группа, ортогональная группа, специальная ортогональная группа, унитарная группа, специальная унитарная группа.	4	Лекционный контроль
3	Изучение свойств знакопеременной группы A_n	4	Лекционный контроль
4	Изучение свойств центра и коммутанта группы	4	Лекционный контроль
5	Изучение темы «Прямые произведения групп»	4	Лекционный контроль
6	Индивидуальное задание по теме «Делимость многочленов над полем»	4	Проверочная работа на практич. занятии
7	Индивидуальное задание по теме «Многочлены от n переменных»	4	Защита работы на консультации
8	Индивидуальное задание по теме «Решение уравнений 3 и 4степени»	4	
9	Изучение темы «Отделение действительных корней многочлена»	4	Лекционный

			контроль
10	Индивидуальное задание по теме «Многочлены над полем Q»	4	Защита работы на консульта-ции
11	Индивидуальное задание по теме «Алгебраические числа»	4	Защита работы на консульта-ции
12	Решение задач по каждой теме практических занятий	26	Контроль на каждом практ. занятии

2.4 ВОПРОСЫ К ЭКЗАМЕНУ

3 семестр

1. Определение группы, ее основные свойства. Примеры групп.
2. Основные классы классических групп.
3. Группа подстановок S_n.
4. Подгруппы. Примеры подгрупп.
5. Группа A_n.
6. Порядок элемента и порядок группы. Свободные элементы и свободные группы.
7. Циклические группы.
8. Смежные классы. Разбиение группы по подгруппе.
9. Нормальные делители. Фактор - группа.
10. Теорема о гомоморфизмах.
11. Эндоморфизмы и автоморфизмы групп. Примеры. Свойства. Внутренние автоморфизмы групп.
12. Центр группы.
13. Коммутант группы.
14. Разрешимые группы и их свойства.
15. Нильпотентные группы и их свойства.

16.Простые группы.

17.Прямые произведения групп.

18.Теорема о строении абелевых р - групп.

19.Теорема о строении конечнопорожденных абелевых групп.

20. Определение кольца. Примеры. Основные свойства. Подкольца.

21. Область целостности. Теорема о вложении коммутативного кольца без делителей нуля в поле частных.

22. Алгебры Буля и булевы кольца. Их свойства. Связь с решетками.

23. Кольцо классов вычетов. Поле классов вычетов по простому модулю.

24. Гомоморфизмы колец. Изоморфизмы колец.

25. Теорема о гомоморфизмах колец.

26. Идеалы колец.

27. Кольца главных идеалов

28. Простые и полупростые кольца. Радикал кольца.

29.Характеристика тела (поля). Простое подполе, его строение.

30.Центр тела. Центральные подполе тела.

31.Векторные пространства и алгебры над полями. Понятие модуля над коммутативным кольцом. Примеры.

32.Кольцо многочленов над областью целостности.

33.Деление многочлена на двучлен x-a. Теорема Безу. Схема Горнера.

34.Число корней многочлена в коммутативной области целостности. Теорема о тождестве многочленов.

35.Многочлены над данным полем. Делимость многочленов.

36.НОД многочленов. Алгоритм Евклида.

37.Приводимые и неприводимые многочлены над данным полем.

38.Теорема о кратном множителе многочлена.

39.Выделение кратных множителей.

40.Кольцо многочленов от нескольких переменных.

41.Симметрические многочлены. Основная теорема о симметрических многочленах.

42.Результант многочленов. Исключение неизвестного.

43.Дискриминант многочленов.

44.Уравнения 3 степени. Вывод формул Кардано.

45. Исследование уравнений 3 степени с действительными коэффициентами.

46.Метод Феррари решения уравнения 4 степени.

47.Результаты Руффини, Абеля и Галуа по вопросам решения уравнений высших степеней.

48.Леммы о свойствах полиномов над полем С. Лемма о возрастании модуля полинома на комплексной плоскости. Лемма Даламбера. Основная теорема алгебры

49.Многочлены с действительными коэффициентами. Теорема Виета.

50.Границы корней.

51.Теорема Штурма.

52.Рациональные корни многочленов. Приводимость многочленов над полем Q. Критерий Эйзенштейна.

53.Минимальный многочлен алгебраического числа. Строение простого алгебраического расширения.

54.Сопряженные алгебраические числа. Составное алгебраическое расширение поля.

55.Алгебры с делением.

56.Алгебра кватернионов.

57.Теорема Фробениуса о конечномерных алгебрах с делением.

2.5 ТРЕБОВАНИЯ ПРИ ОЦЕНКЕ ЗНАНИЙ НА ЭКЗАМЕНЕ

При оценивании учитываются: правильность и осознанность изложения содержания ответа на вопросы; полнота раскрытия понятий и закономерностей, точность употребления и трактовки общенаучных и специальных терминов; степень сформированности интеллектуальных и научных способностей экзаменуемого; самостоятельность ответа;

речевая грамотность и логическая последовательность ответа; умение решать предложенные задачи.

Критерии оценок:

отлично - полно раскрыто содержание вопросов в объеме программы и рекомендованной литературы; четко и правильно даны определения и раскрыто содержание концептуальных понятий, закономерностей, корректно использованы научные термины; ответ самостоятельный, без наводящих дополнительных вопросов; полностью решены предложенные задачи.

хорошо - раскрыто основное содержание вопросов; в основном правильно даны определения понятий и использованы научные термины; ответ самостоятельный; определения понятий неполные, допущены нарушения в последовательности изложения, небольшие неточности при использовании научных терминов или в выводах и обобщениях, исправляемые по дополнительным вопросам экзаменатора; предложенные задачи в основном решены.

удовлетворительно — усвоено основное содержание учебного материала, но изложено фрагментарно не всегда последовательно; определение понятий недостаточно четкое; не использованы в качестве доказательства выводы наблюдений и опытов или допущены ошибки при их изложении; допущены ошибки и неточности в использовании научной терминологии, определении понятий; решения задач не доведены до конца.

неудовлетворительно – ответ неправильный, не раскрыто основное содержание программного материала, не даны ответы на вспомогательные вопросы экзаменатора, допущены грубые ошибки в определении основных понятий; предложенные задачи не решены.

2.6 ВОПРОСЫ К ЗАЧЕТУ

2 семестр

1. Определение группы, ее основные свойства. Примеры групп.
2. Основные классы классических групп.

3. Группа подстановок S_n.
4. Подгруппы. Примеры подгрупп.
5. Группа A_n.
6. Порядок элемента и порядок группы. Свободные элементы и свободные группы.
7. Циклические группы.
8. Смежные классы. Разбиение группы по подгруппе.
9. Нормальные делители. Фактор – группа.
10. Теорема о гомоморфизмах.
11. Эндоморфизмы и автоморфизмы групп. Примеры. Свойства. Внутренние автоморфизмы групп.
12. Центр группы.
13. Коммутант группы.
14. Разрешимые группы и их свойства.
15. Нильпотентные группы и их свойства.
16. Простые группы.
17. Прямые произведения групп.
18. Теорема о строении абелевых р - групп.
19. Теорема о строении конечнопорожденных абелевых групп.

2.7 ВАРИАНТ ЗАЧЕТНОЙ РАБОТЫ

1. Проверить, является ли множество всех множеств (включая пустое) группой относительно объединения.
2. В группе подстановок 3 степени найти все смежные классы по подгруппе H={1,(12)}.
3. Доказать, что всякая подгруппа циклической группы сама циклическая.
4. Доказать, что ядро гомоморфизма группы в группу есть нормальный делитель.

2.8 БИЛЕТЫ К ЭКЗАМЕНУ ПО АЛГЕБРЕ

Экзаменационный билет
№1

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Основная теорема алгебры (лемма 1).
2. Нормальный делитель группы. Фактор – группа.

Экзаменационный билет
№2

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Основная теорема алгебры (лемма 2).
2. Гомоморфизм и изоморфизм групп. Ядро гомоморфизма.

Экзаменационный билет
№3

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Симметрические многочлены. Основная теорема о симметрических многочленах.
2. Центр и коммутант группы.

Экзаменационный билет
№4

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Решение уравнений 3 степени по формулам Кардано.
2. Теорема о гомоморфизмах групп.

Экзаменационный билет
№5

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Многочлены над полем. НОД и НОК многочленов. Алгоритм Евклида.
2. Алгебраические числа. Строение простого алгебраического расширения.

Экзаменационный билет
№6

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Многочлены над областью целостности. Делимость многочлена на двучлен. Схема Горнера.
2. Прямая сумма абелевых групп.

Экзаменационный билет
№7

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Корень многочлена. Число корней многочлена. Разложение многочлена по степеням x-a.
2. Идеалы кольца. Кольцо главных идеалов.

Экзаменационный билет
№8

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Производная многочлена. Теорема о неприводимом множителе многочлена. Кратность корней многочлена. Выделение кратных множителей.
2. Смежные классы. Теорема Лагранжа.

Экзаменационный билет
№9

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Приводимые и неприводимые многочлены над данным полем. Разложение многочлена на неприводимые множители.
2. Евклидовы кольца.

Экзаменационный билет
№10

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Следствия из основной теоремы алгебры. Сопряженность мнимых корней многочлена с действительными коэффициентами.
2. Порядок элемента группы. Циклические группы. Изоморфизм конечных и бесконечных циклических групп.

Экзаменационный билет
№11

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Целые и рациональные корни многочлена.
2. Основная теорема о конечных абелевых группах.

Экзаменационный билет
№12

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Отделение действительных корней многочлена. Теорема Штурма.
2. Подгруппы группы. Теорема Кэли.

Экзаменационный билет
№13

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Группа: примеры, свойства. Изоморфизм и гомоморфизм групп.
2. Избавление вот иррациональности в знаменателе дроби. Поле алгебраических чисел.

Экзаменационный билет
№14

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Прямая сумма абелевых групп.
2. Исследование уравнения 3 степени с действительными коэффициентами.

Экзаменационный билет
№15

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1.Эндоморфизмы и автоморфизмы групп.
2. Решение уравнений 4 степени методом Феррари.

Экзаменационный билет
№16

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Модули.
2. Теорема о представлении симметрического многочлена через основные симметрические.

Экзаменационный билет
№17

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Кольцо: примеры, свойства. Подкольцо. Область целостности.
2. Целые и рациональные корни многочлены.

Экзаменационный билет
№18

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Поле отношений.
2. Разложение многочлена в произведение неприводимых множителей.

Экзаменационный билет
№19

Утвержден 12 декабря 2006 ФМиИ

на заседании каф. МАиМ Алгебра

Зав. кафедрой _____Труфанова Т.В. 2 курс

1. Поле. Характеристика поля. Кольцо классов вычетов по простому модулю.

Следствия из основной теоремы алгебры. Сопряженность мнимых корней многочлена с действительными коэффициентами.

3. ПЕРЕЧЕНЬ УЧЕБНИКОВ, УЧЕБНЫХ ПОСОБИЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

Основная литература

1. Кострикин А.И. Введение в алгебру. – М., 1994.
2. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. – М., 1977.
3. Курош А.Г. Теория групп. – М.,1967.
4. Понтрягин Л.С. Неприрывные группы. – М., 1984.
5. Проскуряков И.В. Сборник задач по линейной алгебре. – М., 1970.
6. Сборник задач по алгебре. Под ред. Кострикина А.И. – М.,1995.

Дополнительная литература

1. Ван дер Варден Б.Л. Алгебра – М., 1979.
2. Варпаховский Ф.Л., Солодовников А.С., Стелецкий И.В. Алгебра. – М.,1978.
3. Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел. – М., 1993.
4. Мишина А.П., Проскуряков И.В. Высшая алгебра. – М., 1965.
5. Нечаев В.А. Задачник – практикум по алгебре. – М., 1983.
6. Скорняков Л.А. элементы алгебры. – М., 1980.

Методические материалы

1. Раздаточный материал по расчетно – графическим работам по темам: «Группы», «Многочлены над полями», «Симметрические многочлены».
2. Материалы для контрольных работ.
3. Учебно – методическое пособие Кван Н.В. «Группы. Кольца. Поля» Изд. АмГу, 1999.

4. МАТЕРИАЛЫ ДЛЯ ЧТЕНИЯ ЛЕКЦИЙ

1. БИНАРНАЯ АЛГЕБРАИЧЕСКАЯ ОПЕРАЦИЯ

Упорядоченный набор из n элементов $a_1,...,a_n$ некоторого множества A называется *кортежем* длины n и обозначается $\langle a_1,...,a_n \rangle$, а множество всех таких кортежей называют n-й декартовой степенью множества A и обозначается A^n.

Бинарной алгебраической операцией на непустом множестве A называется отображение $A \times A \to A$, сопоставляющее каждому кортежу $\langle a,b \rangle$ из A^2 определенный элемент c из множества A, т.е. бинарная алгебраическая операция на множестве A – это некоторое правило, по которому любой паре элементов a, b из A (взятых в определенном порядке) ставится однозначно определенный элемент c из A ($c = a * b$).

Под n - местной операцией на множестве A понимают отображение, ставящее каждому кортежу $\langle a_1,...,a_n \rangle$ из A^n определенный элемент из A.

Примеры.

1.Сложение, умножение и операция возведения в степень на множестве $\boldsymbol{Z}^+$ целых положительных чисел – бинарные алгебраические операции.

2.Умножение вещественных квадратных матриц заданного порядка – бинарная алгебраическая операция.

3.Бинарной алгебраической операцией на множестве векторов трехмерного вещественного векторного пространства $\overrightarrow{E^3}$ может служить операция векторного произведения $\left[\vec{a},\vec{b}\right]$, $\vec{a},\vec{b} \in \overrightarrow{E^3}$.

4.Сложение и умножение функций действительного переменного - примеры бинарных алгебраических операций.

5.Не являются бинарными алгебраическими операциями умножение на множестве отрицательных целых чисел, сложение нечетных целых чисел, деление действительных чисел.

Пусть на конечном множестве $A = \{a_1, \dots, a_n\}$ бинарная операция $*$ задана таблицей, состоящей из n строк и n столбцов, в которой на пересечении i-й

строки и *j*-го столбца стоит элемент $a_i * a_j$ множества *A*. Эта таблица называется *таблицей умножения* или *таблицей Кэли*.

Построим, таблицу Кэли для операции нахождения наибольшего общего делителя (НОД) на множестве $A = \{1, 2, 3, 4, 6, 12\}$.

НОД	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

Из этой таблицы видно, что операция нахождения наибольшего общего делителя на множестве *A* является бинарной алгебраической, т.к. все результаты этой операции - числа того же множества *A*.

Задача. Выяснить, являются ли бинарными алгебраическими операции +, -, ×, ÷ на указанном множестве: а) $A=\{x : x \in N_-\}$; б) $A=\{-1,0,1\}$.

Решение. а) Для операции + имеем: $\forall x_1,\ x_2 \in N_-\ x_1 + x_2 \in N_-$; следовательно, операция сложения + является бинарной алгебраической на множестве *A*.

Операция вычитания − не является бинарной алгебраической на множестве *A*, так как найдутся числа x_1 и x_2, для которых $x_1 - x_2 \notin N_-$. Например, при $x_1 < x_2$ разность $x_1 - x_2$ будет числом положительным, а значит, не будет принадлежать множеству N_-.

Операции умножения × и деления ÷ на множестве чисел противоположных натуральным N_- также не являются бинарными алгебраическими, поскольку и произведение и частное двух любых отрицательных чисел является числами положительными.

б) Для данного множества $A=\{-1,0,1\}$ составим таблицы Кэли по каждой из операций:

+	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

-	-1	0	1
-1	0	1	2
0	-1	0	1
1	-2	-1	0

×	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

÷	-1	0	1
-1	1	0	-1
0	-	-	-
1	-1	0	1

Видим, что полученные таблицы по операциям сложения и вычитания содержат элементы, не входящие в данное множество *A*. Следовательно, операции сложения и вычитания не являются бинарными алгебраическими на множестве *A*.

Таблица, составленная для операции умножения, содержит только элементы, входящие во множество *A*. Следовательно, результаты операции × не выходят за рамки данного множества, а значит, умножение − бинарная алгебраическая операция на множестве *A*. Для операции деления не выполнимо деление на ноль, поэтому нет смысла говорить о ней как о бинарной алгебраической операции.

Свойства бинарных алгебраических операций

Бинарная алгебраическая операция на множестве *A* называется *коммутативной*, если для любых двух элементов a_1 и a_2 из *A* выполняется условие; $a_1 * a_2 = a_2 * a_1$.

Например, бинарные алгебраические операции сложения и умножения на множестве целых чисел $\boldsymbol{Z}$ коммутативны, а операция вычитания нет.

Операция на множестве *A* называется *ассоциативной,* если для любых трех элементов a_1 , a_2 , a_3 из *A* выполняется условие:

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3).$$

Например, операции сложения и умножения на множестве действительных чисел $\boldsymbol{R}$ ассоциативны, а операция на множестве $\boldsymbol{Z}$, задаваемая формулой $m * n = m^n$, не является ассоциативной.

Если на множестве определена бинарная алгебраическая операция, обладающая свойством ассоциативности, то такое множество с этой операцией называется *полугруппой*.

Пусть на множестве A задана бинарная алгебраическая: операция $*$. Если найдется такой элемент $e \in A$, что для любого элемента $a \in A$ выполняются равенства $e * a = a$ и $a * e = a$, то элемент e называется *нейтральным* относительно данной операции.

Например, число 1 является нейтральным элементом множества действительных чисел $\boldsymbol{R}$ относительно операции умножения, а нулевая матрица второго порядка − нейтральным элементом множества всех матриц второго порядка относительно операции сложения матриц.

Пусть множество A содержит нейтральный элемент e относительно некоторой бинарной операции $*$. Элемент a' называется *обратным* для элемента a, если выполняются равенства; $a * a' = e$ и $a' * a = e$.

Например, обратным для любого отличного от нуля числа $a \in R$ будет число $a^{-1} = \frac{1}{a}$ в случае обычной операции умножения на множестве действительных чисел $\boldsymbol{R}$. Число 0 не имеет обратного элемента, так как $0 * a = 0$ для любого числа $a \in R$. На множестве квадратных матриц второго порядка с операцией матричного умножения для каждой невырожденной матрицы А существует единственный обратный элемент − матрица A^{-1}.

С понятием обратного элемента тесно связано понятие обратимой операции. Операция на множестве A называется *обратимой*, если для любых элементов a, b из A каждое из уравнений $a * x = b$ и $x * a = b$ имеет единственное решение.

Например, операция сложения на множестве $\boldsymbol{R}$ всех действительных чисел (а также на множестве $\boldsymbol{Q}$ всех рациональных чисел или на множестве $\boldsymbol{Z}$ всех целых чисел) обратима, а на множестве целых неотрицательных чисел $\boldsymbol{Z}^+$ необратима (если выполняется условие $a>0$, то уравнение $a+x=0$ не имеет целого неотрицательного решения).

Следующая теорема устанавливает связь между существованием обратных элементов и обратимостью операции.

Теорема. Ассоциативная операция на множестве A обратима тогда и только тогда, когда в A существует нейтральный элемент и для любого элемента из A существует обратный ему элемент.

Задача. Доказать, что на множестве $\boldsymbol{R}^+$ операция $a * b = \sqrt{ab}$ (операция нахождения среднего геометрического) коммутативна, но не ассоциативна.

Решение. Пусть a, b, c - любые действительные положительные числа. В силу коммутативности умножения на $\boldsymbol{R}^+$ получим: $a * b = \sqrt{ab} = \sqrt{ba} = b * a$, т.е. бинарная операция нахождения среднего геометрического на $\boldsymbol{R}^+$ коммутативна. Далее, $(a * b) * c = \sqrt{\sqrt{ab}c} = \sqrt[4]{ab}\sqrt{c}$ и $a * (b * c) = \sqrt{a\sqrt{bc}} = \sqrt[4]{a}\sqrt{bc}$.

Из полученных результатов следует, что при $a \neq c$ равенство $(a * b) * c = a * (b * c)$ не является справедливым. Следовательно, заданная операция $*$ не ассоциативна на множестве $\boldsymbol{R}^+$.

Задача. Доказать, что на некотором непустом множестве M бинарная операция, заданная формулой $a * b = b$, не коммутативна, но ассоциативна.

Решение. Пусть a, b, c - любые элементы множества M. Тогда $a * b = b$, а $b * a = a$. Следовательно, при условии $a \neq b$ равенство $a * b = b * a$ не является справедливым, т.е. операция $*$ на множестве M не коммутативна.

Далее, $(a * b) * c = b * c = c$ и $a * (b * c) = a * c = c$, поэтому равенство $(a * b) * c = a * (b * c)$ справедливо, т.е. операция $*$ на множестве M является ассоциативной.

Задача. Доказать, что на множестве K, содержащем не менее двух элементов, на котором задана бинарная операция $a * b = b$, не существует нейтрального элемента.

Решение. Допустим, что во множестве K существует нейтральный элемент e и пусть a − любой элемент из множества K. По определению нейтрального элемента $a * e = a$ и из условия задачи следует, что справедливо равенство $a=e$. Это означает, что множество K состоит из одного элемента. Полученный результат противоречит условию, а потому допущение ошибочно.

ГРУППА

Группы. Простейшие свойства групп

Непустое множество элементов G называется *группой*, если на множестве G задана бинарная алгебраическая операция $*$, так что выполнены условия:

1) для любых элементов a, b, c из G выполняется соотношение $(a * b) * c = a * (b * c)$ − ассоциативность;

2)в G имеется единица, общая для всех элементов группы, т.е. такой элемент e, что $a * e = e * a = a$ для каждого элемента a из G;

3)для всякого элемента a из G существует обратный элемент, т.е. такой элемент a' что $a' * a = a * a' = e$.

Обратный элемент элемента a в группе G обозначают символом a', a^{-1} или $\frac{1}{a}$

Если для любых элементов a, b из G $a * b = b * a$, то группа называется *коммутативной* или *абелевой*,

В коммутативных (абелевых) группах бинарная операция $*$ часто обозначается символом + и называется сложением элементов из G. В этом

случае нейтральный элемент обозначается символом 0 или 0 («ноль»), а обратный элемент a' к элементу a называется *противоположным* к элементу a и обозначается символом -a. Эта система обозначений для абелевых групп называется *аддитивной.*

Предыдущая система обозначений называется *мультипликативной*; часто умножение обозначается «точкой» $\cdot$ или «крестиком» $\times$ или вообще символ операции умножения опускается.

Группа называется бесконечной или конечной, в зависимости от того, является ли множество G бесконечным или конечным; число элементов $|G|$ конечной группы G называется её *порядком*.

Примеры.

1.Множество всех положительных действительных чисел $\boldsymbol{R}^+$ образует группу относительно операции умножения. В самом деле, умножение ассоциативно, число 1 является нейтральным элементом, т. к. $1 \times a = a \times 1 = a$ для любого $a \in R^+$ и для каждого числа $a>0$ существует обратное число, равное $\frac{1}{a}$, так как $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$. Эта группа $\boldsymbol{R}^+$ называется *мультипликативной* группой положительных действительных чисел.

2.Множество всех действительных чисел $\boldsymbol{R}$ с операцией сложения является группой, так как сложение ассоциативно, число 0 является нейтральным элементом, ибо $a + 0 = 0 + a = a$ для любого $a \in R^+$, и для всякого числа a обратным элементом служит противоположное ему число $– a$, так как $a + (-a) = (-a) + a = 0$. Эта группа называется аддитивной группой действительных чисел.

3. Пусть p - простое число. Рациональное число вида $\frac{m}{p^n}$ где $m, n \in Z$, называется p-адичной дробью. Множество $\boldsymbol{Q_p}$ - всех p-адичных дробей относительно умножения чисел - абелева группа.

4. Арифметическое n-мерное векторное пространство R^n является группой относительно сложения векторов.

5. Множество целых чисел $\boldsymbol{Z}$ с операцией умножения группой не является, так как для любого элемента в $\boldsymbol{Z}$ не существует обратного элемента.

Теорема. Нейтральный элемент e и обратный элемент a' элемента a в группе G единственны.

Доказательство. Пусть e_1, e_2 - единицы группы G. Тогда $e_1 * e_2 = e_1$ и $e_1 * e_2 = e_2$, откуда $e_1 = e_2 = e$ - единственный нейтральный элемент.

Аналогично доказывается единственность обратного элемента в группе.

Теорема. Уравнения $a * x = c$ и $y * b = d$ в группе G имеют единственное решение $x = a^{-1} * c$ и $y = d * b^{-1}$.

Доказательство. Элемент вида $x = a^{-1} * c$ - решение рассматриваемого уравнения, так как $a * (a^{-1} * c) = (a * a^{-1}) * c = e * c = c$.

Покажем единственность решения. Пусть d - другое решение данного уравнения, тогда $a * d = c$. Умножим последнее равенство слева на a^{-1}.

Получаем $a^{-1} * (a * d) = a^{-1} * c$. Но в силу ассоциативности имеем $(a^{-1} * a) * d = e * d = d = a^{-1} * c$. Таким образом $x = d$, и единственность решения x доказана.

Рассмотрим решение примеров.

1. Доказать, что множество $\boldsymbol{Z}$ образует группу относительно операции $\bullet$ заданной формулой:

$$a \bullet b = \begin{cases} a + b, \text{ если } a - \text{ четное число}, b - \text{ любое целое число}, \\ a - b, \text{ если } a - \text{ нечетное число}, b - \text{ любое целое число}. \end{cases}$$

Решение. 1. Рассматриваемая на Z операция сводится к сложению и вычитанию целых чисел, а т.к. сложение и вычитание элементов из Z дают в результате элементы из Z, то на множестве Z рассматриваемая, операция $\bullet$ является бинарной операцией.

2. Рассмотрим возможные случаи:

а) Если a,b - четные числа, а c - любое число из Z, то $a \bullet (b \bullet c) = a + (b + c)$, $(a \bullet b) \bullet c = (a + b) + c = a + (b + c)$, т.е. $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

б) Если a - четное число, b - нечетное, а c - любое число из Z, то $a \bullet (b \bullet c) = a + (b - c)$, $(a \bullet b) \bullet c = (a + b) - c = a + (b - c)$, т. е. $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

в) Если a - нечетное число, b - четное число, а c - любое число из Z, то $a - b$ нечетно и потому $a \bullet (b \bullet c) = a - (b + c) = (a - b) - c$, $(a \bullet b) \bullet c = (a - b) - c$, т.е. $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

г) Если a, b - нечетные числа, а c - любое число из Z, то $a - b$ четно и потому $a \bullet (b \bullet c) = a - (b - c) = (a - b) + c$, $(a \bullet b) \bullet c = (a - b) + c$, т.е. $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

Итак, во всех возможных случаях заданная на множестве Z бинарная операция является ассоциативной.

3. Так как 0 - четное число, то $0 \bullet a = a$. Кроме того, если число a четно, то $a \bullet 0 = a + 0 = a$; если же a нечетно, то $a \bullet 0 = a - 0 = a$. Итак, $0 \bullet a = a \bullet 0 = a$, т. е. 0 является в Z нейтральным элементом относительно заданной операции.

4 .Для любого элемента $a \in Z$ в Z существует обратный элемент: для четного a обратным будет противоположное число $-a$, т.к. $a \bullet (-a) = a + (-a) = 0$; для нечетного a обратным будет само число a, т.к. $a \bullet a = a - a = 0$.

Итак, Z является группой относительно заданной операции. Однако эта группа не является абелевой, поскольку $4 \bullet 5 = 4 + 5 = 9$, $5 \bullet 4 = 5 - 4 = 1$, т.е. $4 \bullet 5 \neq 5 \bullet 4$.

2. Множество всех подстановок n-ой степени относительно алгебраической операции произведения подстановок является группой.

Единицей этой группы служит тождественная подстановка $\begin{pmatrix} 1\,2 \ldots n \\ 1\,2 \ldots n \end{pmatrix}$;

элементом, обратным к подстановке $\begin{pmatrix} 1 & 2 \ldots n \\ i_1 & i_2 \ldots i_n \end{pmatrix}$, является подстановка

$\begin{pmatrix} i_1 & i_2 \ldots i_n \\ 1 & 2 \ldots n \end{pmatrix}$. Эта группа называется *симметрической группой n-ой степени* и

обозначается через S_n, причем она – конечная группа порядка $n!$. При $n \geq 3$ группа S_n некоммутативна. Группа всех четных подстановок n-ой степени называется знакопеременной группой n-ой степени и обозначается A_n.

3. Пусть G – совокупность всех преобразований множества R, задаваемых формулой $f(x) = x + a$, где $a \in R$. Доказать, что G есть группа относительно операции умножения преобразований.

Решение. Проверим, что умножение преобразований есть бинарная операция на множестве G.

По определению операции умножения преобразований φ, h имеем:

$$h(x) = \varphi(f(x)).$$

Обозначим преобразование $x \to x + a$ множества R через f_a. Тогда

$$(f_a f_b)(x) = f_a(f_b(x)) = f_a(x + b) = x + b + a = f_{a+b}(x), \text{ т. е.}$$

$$f_a f_b = f_{a+b}$$

Этим доказано, что $f_a f_b \in G$.

2. Операция умножения преобразований ассоциативна.

3. Тождественное преобразование, играющее роль нейтрального элемента для операции умножения преобразований, принадлежит G. Таким является преобразование f, где $f_0(x) = x$ для любого x из R.

4. Преобразование, обратное любому преобразованию f из G, которое играет роль обратного элемента для f_a, снова принадлежит G. Таким является преобразование $f_{-a}(x) = x - a$.

Итак, G – группа.

ИЗОМОРФИЗМ И ГОМОМОРФИЗМ ГРУПП

Две группы G и H называется изоморфными, если между их элементами можно установить взаимно однозначное соответствие f: $G \to H$, при котором для любых элементов $a, b \in G$ и соответствующих им элементов $a' = f(a), b' = f(b) \in H$ выполняется равенство: $f(ab) = f(a)f(b)$, т.е. элементу

$c=ab$ соответствует элемент $c' = a'b'$, $c' = f(c)$. Само отображение f называется изоморфизмом группы G на группу H.

Изоморфное отображение группы на себя называется автоморфизмом этой группы.

Примеры.

1. Аддитивная группа $\boldsymbol{Z}$ всех целых чисел изоморфна аддитивной группе $2\boldsymbol{Z}$ всех четных чисел (для установления изоморфизма между ними можно каждому числу $z \in Z$ поставить в соответствие число $2z \in 2Z$).

2.Мультипликативная группа всех положительных действительных чисел $\boldsymbol{R}$ изоморфна аддитивной группе всех действительных чисел $\boldsymbol{R}$ (изоморфизм: $a \to \lg a$).

3.Отображение аддитивной группы всех целых чисел $\boldsymbol{Z}$, , при котором каждому целому числу a ставится в соответствие число $-a$, является автоморфизмом.

Заметим, что изоморфное соответствие между группами можно установить многими способами. Изоморфные группы могут отличаться друг от друга только природой своих элементов и названиями операций, определенными в группах. Но все групповые свойства изоморфных между собой групп одинаковы. Например, если группа абелева, то и все изоморфные ей группы абелевы.

Теорема Кэли. Любая конечная группа G порядка n изоморфна некоторой подгруппе G' группы подстановок степени n.

Доказательство. Занумеруем все элементы данной группы G: g_1, g_2, …, g_n, $g_i \neq g_j, i \neq j$. Пусть a - произвольный элемент этой группы. Составим последовательность произведений g_1a, g_2a, …, g_na. Все эти произведения различны, поэтому данная последовательность представляет собой последовательность всех элементов группы. Значит, ее можно записать в виде $g_{i_1}, g_{i_2}, ..., g_{i_n}$, где $i_1, i_2, ..., i_n$ – некоторая перестановка из чисел 1, 2, …, n.

Поставим в соответствие элементу a подстановку $\begin{pmatrix} 1 & 2 \dots n \\ i_1 & i_2 \dots i_n \end{pmatrix}$. Таким образом, каждому элементу a группы G будет соответствовать определенная подстановка степени n. Эта подстановка переводит число k в число i_k, если произведение $g_k a$ равно элементу g_{i_k} с номером i_k.

Разным элементам группы G будут соответствовать разные подстановки. Действительно, если $a \neq b$, то $g_1 a \neq g_1 b$. Поэтому подстановки, соответствующие элементам a и b переводят число 1 в разные числа, т.е. эти подстановки различны.

Обозначим множество из n подстановок, соответствующих элементам $g_1, g_2, \dots, g_n$ группы G через G'. Таким образом, установлено взаимно однозначное отображение группы G на G', сохраняющее операцию.

Действительно, пусть элементам a и b соответствуют подстановки $\begin{pmatrix} 1 & 2 \dots n \\ i_1 & i_2 \dots i_n \end{pmatrix}$ и $\begin{pmatrix} i_1 & i_2 \dots i_n \\ g_1 & g_2 \dots g_n \end{pmatrix}$. Покажем, что для любого l $(1 \le l \le n)$ выполняется условие: $g_l(ab)=gj_l$. Это условие легко проверяется: из подстановок, соответствующих элементам a, b, имеем равенство $g_l a=gi_l$, $gi_l b=gj_l$, откуда $g_l(ab)=(gla)b=gi_l b=gj_l$.

Итак, установлен изоморфизм группы G и множества G' с обычной операцией умножения подстановок. По свойству изоморфного отображения получаем, что G' есть группа относительно операции умножения подстановок степени n. Теорема доказана.

Если каждому элементу группы G соответствует однозначно определенный элемент группы H, причем если элементам $a, b \in G$ соответствуют элементы $a', b' \in H$, то элементу $ab = c$ соответствует элемент $c' = a'b'$, то такое соответствие называется гомоморфизмом. Иначе, гомоморфизм группы G в группу H – это отображение $f: G \to H$, обладающие свойством $f(ab) = f(a)f(b)$ для любых элементов $a, b \in G$. Если

при этом $H = f(G)$, то говорят о гомоморфном отображении f группы G на группу H; такой гомоморфизм называется эпиморфизмом группы G на группу H.

При гомоморфизме единица группы G отображается в единицу группы H, а взаимно обратные элементы из G отображаются во взаимно обратные элементы из H.

Примеры.

1.Если каждому четному числу поставить в соответствие число 1, а каждому нечетному – число -1, то получается гомоморфное отображение аддитивной группы целых чисел в мультипликативную группу всех отличных от нуля рациональных чисел. Это же отображение будет эпиморфизмом аддитивной группы всех целых чисел на мультипликативную группу, состоящую из чисел -1,1.

2.Если каждой невырожденной квадратной матрице n-го порядка с действительными элементами поставить в соответствие определитель этой матрицы, то получится гомоморфное отображение группы (по умножению) всех действительных невырожденных квадратных матриц n-го порядка на мультипликативную группу всех отличных от нуля действительных чисел.

Пример. Покажем, что все группы третьего порядка изоморфны между собой. Привести конкретные примеры групп третьего порядка.

Решение. Пусть G - множество из трех различных элементов e, a, b. Очевидно, что число изоморфных групп третьего порядка равно числу различных (не изоморфных) таблиц умножения, которые можно задать для элементов e, a, b. Заготовим входные строку и столбец таблицы:

	e	a	b
e			
a			
b			

В группе должен быть единичный элемент. Пусть таковым будет e. Тогда первая строка и первый столбец должны будут совпадать со входными строкой и столбцом:

	e	a	b
e	e	a	b
a	a		
b	b		

Осталось заполнить 4 клетки. Учитывая, что в каждой строке и каждом столбце каждый элемент должен встретиться лишь одни раз, то оставшиеся 4 клетки заполняются однозначно:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Это и значит, что существует лишь одна группа из трех элементов, т.е. все группы третьего порядка изоморфны.

Конкретными примерами групп третьего порядка могут служить:

а) группа четных подстановок 3-й степени A_3, т.е. множество подстановок $e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}$, $a = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, b = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}$ относительно умножения подстановок;

б) множество, состоящее из трех комплексных чисел $e = 1$, $a = -1 + i\frac{\sqrt{3}}{2}$, $b = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ относительно умножения чисел.

ПОДГРУППА

§5. Подгруппы

Пусть множество G является группой относительно операции $*$. Подмножество H группы G, являющееся группой относительно той же операции $*$, называется *подгруппой* группы G (обозначение H<G).

Из определения следует, что всякая группа является своей подгруппой и что, множество, состоящее только из единицы группы, так же будет ее подгруппой, Эти подгруппы называются *тривиальными*. Могут существовать и нетривиальные подгруппы, которые называются *собственными подгруппами*.

Например, множество положительных рациональных чисел Q является подгруппой мультипликативной группы положительных действительных чисел R^+, а множество целых чисел Z есть подгруппа аддитивной группы действительных чисел R.

Теорема. Непустое подмножество H группы G является подгруппой этой группы тогда и только тогда, когда H удовлетворяет двум условиям:

1. Для любых двух элементов $h_1 \in H$, $h_2 \in H$ элемент $h = h_1 * h_2 \in H$;
2. Для любого элемента $h \in H$ обратный элемент $h^{-1} \in H$.

Условия 1, 2 можно заменить одним условием: для любых двух элементов $h_1 \in H$, $h_2 \in H$ элемент $h_1 * h_2^{-1} \in H$.

Рассмотрим решение примеров.

1. В группе S_3 всех подстановок третьей степени выделим подмножество H из подстановок

$$e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \qquad a_1 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$$

Легко проверяется, что $ee=e$, $ea_1=a_1e=a_1$, $a_1a_1=e$. Таким образом, попарные произведения элементов из H снова принадлежат H, т.е. условие 1 выполнено, С другой стороны, равенства $ee=e$ и $a_1a_1=e$ показывают, что каждый из элементов e, a_1 является обратным самому себе. Значит, выполнено и условие 2. Следовательно, подмножество H является подгруппой группы S_3.

2. Доказать, что множество М матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in R$ и $a \neq 0$, есть подгруппа мультипликативной группы G всех невырожденных матриц 2-го порядка.

Решение. 1) Пусть $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ - любая матрица из М, тогда $|A| = a^2 \neq 0$, а потому А является невырожденной матрицей. Итак, $M \subset G$.

2) Пусть $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ - любые матрицы из М, $a \neq 0$, $b \neq 0$, тогда $ab \neq 0$, $AB = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}$, т.е. $ab \in M$.

3) Пусть $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Тогда $A^{-1} = \frac{1}{a^2}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$, при этом $\frac{1}{a} \neq 0$, а потому $A^{-1} \in M$.

Из 1),2),3) следует, что М есть подгруппа группы G.

Теорема Кэли. Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_3 всех подстановок *n*-ой степени.

ЦИКЛИЧЕСКИЕ ГРУППЫ

§6. Циклические группы

Если в группе G взять какой-нибудь элемент g и все степени этого элемента (или все его кратные, если операция в группе – сложение), то получится подгруппа группы G. Эта подгруппа называется *циклической подгруппой, порожденной элементом* g, и обозначается {g}. Если подгруппа {g} совпадает со всей группой *G*, то сама группа G называется *циклической*. Элемент *g* группы G называется элементом конечного порядка, если для элемента *g* существует такое натуральное число *k*, что $g^k = e$ (*e* – единица группы *G*). Наименьшее натуральное число n со свойством $g^n = e$ в этом

случае называется *порядком элемента g*. Элемент g называется *элементом бесконечного порядка* (*или свободным элементом*), если для любого натурального числа k $g^k \neq e$ не выполнено; в этом случае все степени элемента g различны между собой.

Циклическая подгруппа $\{g\}$ бесконечна (свободна), если элемент g группы G имеет бесконечный порядок (свободен). Если g – элемент порядка n, то подгруппа $\{g\}$ также имеет порядок n; она состоит из различных между собой элементов $e, g, g^2, \ldots, g^{n-1}$.

Примеры.

1. Аддитивная группа всех целых чисел есть бесконечная циклическая группа, которая состоит из всех кратных числа 1 или числа -1.
2. Все значения корня n-ой степени из 1 образуют относительно операции умножения циклическую группу порядка n порожденную любым из первообразных корней n-ой степени из 1.

Теорема. Все бесконечные циклические группы изоморфны между собой. Изоморфны между собой также все конечные циклические группы одного и того же порядка n.

Всякая подгруппа циклической группы сама является циклической группой.

Рассмотрим решение примера.

Доказать, что в циклической группе порядка n с образующей g элемент g^k тогда и только тогда является образующей, когда k взаимно просто с n.

Решение. Допустим, что числа k и n не являются взаимно простыми. Тогда у них имеется общий делитель $d>1$, т.е. $k=k_1d$, $n=n_1d$. В этом случае $\left(g^k\right)^{n_1} = g^{kn_1} = g^{k_1dn_1} = \left(g^n\right)^{k_1} = e$. Следовательно, среди степеней элемента g^k найдется неболее n различных. Но $n_1<n$, поэтому различные степени элемента g^k не исчерпывают всей группы, состоящей из n различных элементов $g^0, g^1, \ldots, g^{n-1}$. Таким образом, элемент g^k не является образующей группы $\{g\}$.

Пусть теперь числа n и k взаимно просты. Тогда элементы $(g^k)^0$, $(g^k)^1$, …, $(g^k)^{n-1}$ попарно различны. Действительно, допустив, что $g^{kp}=g^{kq}$, где $p<q<n$, получим: $g^{k(q-p)}=e$. Ясно, что k(q-p) делится на n, а раз k взаимно просто с n, то q-p делится на n. Но это невозможно, поскольку $0<q-p<n$. Следовательно, имеется n попарно различных степеней элемента g^k, т.е. различные степени элемента g^k исчерпывают всю группу {g}. Значит g^k служит образующей этой группы.

СМЕЖНЫЕ КЛАССЫ

§7. Смежные классы. Разложение группы по подгруппе

Если H - подгруппа, а g - произвольный элемент группы G, то через gH обозначается множество всех элементов группы G вида gh, где $h \in H$. Это множество называется *левым смежным классом группы* G *по подгруппе* H. Аналогично *правым смежным классом* Hg *группы* G *по подгруппе* H называется множество всех элементов вида hg, где $h \in H$. Если групповая операция сложение, то левые и правые смежные классы соответственно будут иметь вид g+H и H+g. В случае коммутативной группы G левый и правый классы любого элемента g по любой подгруппе H совпадают.

Примеры.

1. В группе всех подстановок третьей степени S_3 возьмем подгруппу H, состоящую из подстановок $e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix} = (1)$ и $h = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} = (23)$, и возьмем элемент $g = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} = (123)$. Тогда левый смежный класс gH будет состоять из подстановок $ge = g = (123)$ и $gh = (123)\cdot(23) = (13)$, а правый смежный класс Hg - из подстановок $eg = g = (123)$ и $hg = (12)$.

2. Пусть G - аддитивная группа целых чисел, а H - ее подгруппа, состоящая из чисел , кратных 4, т.е. $G = \{...,-2,-1,0,1,2,...\}$, $H = \{...,-8,-4,0,4,8,...\}$.

Группа G коммутативна, поэтому правый и левый смежные классы любого элемента по подгруппе H совпадают. Для элемента 0, 1, 2, 3 получаются следующие смежные классы:

$$H + 0 = \{...,-8,-4,0,4,8,...\}$$

$$H + 1 = \{...,-7,-3,1,5,9,...\}$$

$$H + 2 = \{...,-6,-2,2,6,10,...\}$$

$$H + 3 = \{...,-5,-1,3,3,11,...\}$$

Поскольку любое целое число содержится в одном из этих классов H+0, H+1, H+2, H+3, то класс каждого элемента $g \in G$ совпадает с одним из классов.

Каждый левый смежный класс определяется любым входящим в него элементом, т.е. если $g_1 \in gH$, $g_1H = gH$. Два любых ее левых смежных класса группы G по подгруппе H или совпадают или не имеют ни одного общего элемента. Все левые смежные классы по подгруппе H подгруппами группы G не являются, кроме самой подгруппы H ($H = eh$, где e - единица группы G).

Эти же утверждения верны для правых смежных классов.

Число всех различных левых смежных классов группы G по подгруппе H всегда равно числу всех различных правых смежных классов группы G по этой же подгруппе. Это число называется *индексом* подгруппы H группы G.

Индекс часто обозначают символом [G:H]. В случае бесконечного множества смежных классов индексом называется мощность этого множества.

Если в произвольной группе G выбрана подгруппа H, то все элементы группы G можно разбить на попарно непересекающиеся классы элементов группы G, которыми служат смежные классы группы G по

подгруппе H. Такое разбиение называется *левосторонним разложением группы по подгруппе* H. Если вместо левых смежных классов взять правые смежные классы по подгруппе H, то получится *правостороннее разложение группы* G *по подгруппе* H.

Рассмотрим решение примера.

Найти левые и правые разложения симметрической группы

$$S_3 = \{e = (1), a_1 = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} = (23), a_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} = (12), a_3 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} = (123),$$

$$a_4 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} = (132), a_5 = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} = (13)\}$$

по ее подгруппе H=$\{e, a_1\}$.

Решение 1) Найдем левое разложение группы S_3. В качестве первого смежного класса возьмем саму подгруппу H=eH=$\{e, a_1\}$. Рассмотрим любой элемент из S_3, не вошедший в первый класс, например a_2, и умножим на него слева элементы подгруппы H: $a_2e=a_2$, $a_2a_1=(12)*(23)=(132)a_4$. Получим второй смежный класс a_2H=$\{a_2, a_4\}$. Далее возьмем элемент a_5 непринадлежащий предыдущим двум классам. Получим третий класс a_5H=$\{a_3, a_5\}$. В построенные классы вошли все элементы S_3; т.е. $H \cup a_2H \cup a_5H = \{e, a_1\} \cup \{a_2, a_4\} \cup \{a_2, a_5\} = S_3$. Эти классы попарно не пересекаются. Следовательно, классы H, a_2H, a_5H составляет левое разложение группы S_3 по ее подгруппе H.

2) Найдем правое разложение группы S_3 по подгруппе H. Первый правый класс - сама подгруппа H=$\{e, a_1\}$, второй правый класс – Ha_2=$\{a_2, a_3\}$, третий - Ha_5=$\{a_4, a_5\}$. Так как эта классы не пересекаются и $H \cup Ha_2 \cup Ha_5 = S_3$, то классы: H, H$a_2$, H$a_5$, составляют правое разложение группы S_3 по ее подгруппе H. Так как $a_5H \neq Ha_5$, то левое и правое разложение группы S_3 по подгруппе H не совпадают.

Теорема Лагранжа. Порядок конечной группы делится на порядок любой подгруппы.

Доказательство. Пусть конечная группа имеет подгруппу H порядка m, состоящую из элементов h_1, h_2, ..., h_n. Для любого $g \in G$, правый класс Hg состоит из элементов h_1g, h_2g, ..., h_mg, которые все попарно различны (из $h_ig=h_jg$ следовало бы $h_i = h_j$). Таким образом, всякий правый класс содержит ровно m элементов. Пусть имеется всего $k \leq n$ различных правых классов.

Обозначив их через Hg_1, Hg_2,…, Hg_k получаем: $G = Hg_1 \cup Hg_2 \cup ... \cup Hg_k$ т.е. группа G, состоящая из n элементов, разбивается на k непересекающихся классов по m элементам в каждом. Отсюда n=mk, значит n делится на m.

Теорема Коши. Порядок любого элемента конечной группы является делителем порядка этой группы.

Обратно, если порядок конечной группы G делится на простое число p, то G обладает элементами порядка p.

НОРМАЛЬНЫЕ ДЕЛИТЕЛИ

§8. Нормальный делитель группы. Фактор-группы

Если при левостороннем и при правостороннем разложении группы G по некоторой ее подгруппе H классы, на которые распадаются элементы группы G, получаются одинаковыми, то подгруппа H называется *нормальным делителем* группы G (*нормальной* или *инвариантной подгруппой*),

Примеры.

1. Пусть G - группа всех невырожденных квадратных матриц n-ого порядка с действительными элементами, H - ее подгруппа, состоящая из всех матриц, определитель которых равен 1. И является нормальным делителем группы G.

2. Подгруппа H=$\{e, (13)\}$ группы S_3 не является нормальным делителем этой группы.

Теорема. Подгруппа H тогда и только тогда является нормальным делителем группы G, когда для любого элемента g группы G gH=Hg.

Это равенство означает, что для всякого элемента h из H можно найти такие элементы h', h'', что $gh = h'g$, $hg = gh''$.

Пример.

Если группа G абелева, то всякая ее подгруппа H является нормальным делителем (достаточно взять $h' = h'' = h$). Существуют и некоммутативные группы с таким свойством. Например, группа кватернионов.

Элементы g_1 и g_2 группы G называются *сопряженными* в этой группе, если в G существует такой элемент g, что $g_2 = g^{-1}g_1g$ (говорят также, что элемент g_2 получен из g_1 *трансформированием* элементом g).

Если A - подгруппа, g - фиксированный элемент некоторой группы G, то совокупность всех элементов вида $g^{-1}ag$, где *a* пробегает всю подгруппу A, есть снова подгруппа группы G. Эта подгруппа называется подгруппой, *сопряженной* с A в группе G.

Пример.

Подгруппа $H_1 = \{e,(23)\}$ группы S_3 сопряжена с подгруппой $H = \{e,(13)\} : H_1 = (12)^{-1}H(12)$.

Подгруппа H группы G тогда и только тогда является нормальным делителем этой группы, когда вместе с каждым элементом h она содержит и все элементы, сопряженные с h в группе G.

В любой группе единичная подгруппа и сама группа являются нормальными делителями. Если других нормальных делителей в группе нет, она называется *простой* группой. Примером простой группы служит знакопеременная группа n-ой степени при n>5. Существуют и бесконечные простые группы.

Если в группе G все подгруппы являются нормальными делителями, причем группа G не абелева, то она называется *гамильтоновой* группой.

Если в множестве всех смежных классов группы G по нормальному делителю H ввести операцию по правилу $(g_1H)(g_2H) = (g_1g_2)H$ (при аддитивной записи $(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H$), то это будет алгебраическая операция, относительно которой множество всех смежных классов группы G по нормальному делителю H само является группой. Эта группа называется *фактор-группой группы G по нормальному делителю H* и

обозначается G/H. Единицей фактор-группы G/H является смежный класс H. Элементом, обратным элементу фактор-группы gH, является смежный класс $g^{-1}H$. Порядок фактор-группы G/H равен индексу H в G.

Примеры.

1. Фактор-группа аддитивной группы; всех целых чисел Z по подгруппе всех чисел, делящихся на 3, состоит из трех элементов - классов 0+Z, 1+Z, 2+Z. Это – циклическая группа 3-го порядка, порожденная элементом 1+Z.

2.В мультипликативной группе Q^* всех отличных от нуля рациональных чисел числа 1, -1 образуют нормальный делитель H. Смежные классы по этому нормальному делителю являются парами чисел c, $-c$, где c – некоторое положительное рациональное число. Произведением смежных классов c_1, $-c_1$ и c_2, $-c_2$ является смежный класс группы Q^* по нормальному делителю H, состоящий из чисел c_1c_2 , $-c_1c_2$ ($c_1Hc_2H=(c_1c_2)H$). Фактор-группа Q^*/H изоморфна мультипликативной группе всех положительных рациональных чисел.

3.Если в мультипликативной группе G всех невырожденных квадратных матриц n-го порядка с действительными элементами взять множество H, состоящее из всех матриц, определитель которых равен 1, то H будет нормальным делителем. Смежные классы по H будут состоять из всех матриц с одинаковым определителем. Если каждому смежному классу поставить в соответствие действительное число, равное определителю матриц, входящих в этот смежный класс, то получится изоморфизм между фактор-группой G/H и мультипликативной группой всех отличных от нуля действительных чисел R^+.

Рассмотрим решение примеров.

1. Построить фактор-группу аддитивной группы Z по ее подгруппе $H = \{x / x = 5k, k \in Z\}$. Найти сумму смежных классов 3+H, 4+H и элемент фактор-группы Z/H, противоположный элементу 2+H.

Решение. Аддитивная группа Z коммутативна, а потому любая ее подгруппа, в том числе и данная циклическая подгруппа H, является нормальным делителем группы Z. Следовательно, левые и правые классы группы Z по подгруппе H совпадут и из них составится одна фактор-группа. Разбиваем группу Z с помощью ее подгруппы H на попарно непересекающиеся классы: $0+H=\{x/x=5k,k\in Z\}$, $1+H=\{x/x=1+5k,k\in Z\}$, $2+H=\{x/x=2+5k,k\in Z\}$, $3+H=\{x/x=3+5k,k\in Z\}$, $4+H=\{x/x=4+5k,k\in Z\}$. Построенные смежные классы полностью исчерпывают элементы данной группы Z, т.е. $(0+H)\cup(1+H)\cup(2+H)\cup(3+H)\cup(4+H)=Z$. Полученные классы, очевидно, попарно не пересекаются. Следовательно, они составляют разложение группы Z по нормальному делителю H. Итак, множество $Z/H=\{0+H,1+H,2+H,3+H,4+H\}$ будет аддитивной фактор-группой со сложением элементов (классов): $(3+H)+(4+H)=(3+4)+H=7+H=\{x:x=7+5k=2+(5+5k)=2+5t,t\in Z\}=2+H$; $(3+H)+(0+H)=(3+0)+H=3+H$; Аналогично, $(0+H)+(3+H)=(3+H)$, поэтому элемент 0+H в группе Z/H играет роль нуля.

Поскольку

$(2+H)+(3+H)=(2+3)+H=5+H=\{x:x=5+5k=5(1+k)=5s,s\in Z\}=0+H$, то элемент 3+H является противоположным элементу 2+H.

2. Охарактеризовать все нормальные делители в группе Z_p вычетов по mod p и фактор-группы по ним.

Решение. Т. к. аддитивная группа $Z_p=\{0,1,2,...,n-1\}$ является циклической, а циклические группы коммутативны, то все ее подгруппы являются нормальными делителями. Но любая подгруппа группы Z_p имеет вид $\{0,d,2d,...,(n-d)\}$, где d - любой натуральный делитель числа n, n=dk или $n-d=dk-d=(k-1)d$. Таким образом, нормальный делитель будет состоять из k элементов и иметь следующий вид: $H=\{0,d,2d,...,(k-1)d\}$. Фактор-группа группы Z_p по нормальному делителю H будет состоять из d смежных классов:

$H+0=H=\{0=0d,1d,2d,...,(k-1)d\}=\{x:x=ds\}$,

$H+1=\{1,d+1,2d+1,...,(k-1)d+1\}=\{x:x=ds+1\}$,

$H+2=\{2,d+2,2d+2,...,(k-1)d+2\}=\{x:x=ds+2\}$,

$H+d-1=\{x:x=ds+d-1\}$, где s пробегает все целые числа от 0 до k-1. Следовательно, $\mathbf{Z_P/H=\{H, H+1, H+2,..., H+d-1\}}$.

ТЕОРЕМА О ГОМОМОРФИЗМЕ ГРУПП

§9. Гомоморфные образы группы

Пусть $f:G\to G'$ – гомоморфизм группы G в группу G'. Рассмотрим множество $Kerf=\{g\in G:f(g)=e'\}$, где e' – единица группы G'. Нетрудно показать, что Kerf является нормальным делителем группы G. Он называется *ядром гомоморфизма f.*

Теорема о гомоморфизме. Если $f:G\to G'$ – гомоморфизм группы G в группу G', то группа G' изоморфна фактор-группе G/H, где H=Kerf.

Доказательство. Пусть f – гомоморфное отображение G на G'. По каждому элементу $g'\in G'$ составим класс $f^{-1}(g')=f(g)Kerf$ тех элементов нз G, которые отображением переводятся в g'. Множество всевозможных таких классов образует разбиение группы G, которые обозначим G/H, где H=Kerf. Зададим отображение F группы G' на множество G/H классов, полагая, что для каждого элемента $g'\in G'$ класс $F(g')=f^{-1}(g')$. Отображение F взаимно однозначно, поскольку разным элементам группы G' отвечают разные классы прообразов.

Покажем теперь, что для любых элементов g'_1, g'_2 группы G' выполняется равенство $F(g'_1)F(g'_2)=F(g'_1g'_2)$. Тогда это равенство определяет умножение классов, превращающее это множество классов G/H в группу.

Следовательно, умножение классов есть операция на данном множестве классов и отображение F изоморфно. Убедимся, что каждый элемент

произведения классов $F(g'_1)$ и $F(g'_2)$ принадлежит классу $F(g'_1 g'_2)$ и обратно.

Пусть $g \in F(g'_1)F(g'_2)$. Тогда $g = g_1 g_2$, причем $g_1 \in F(g'_1)$, $g_2 = F(g'_2)$ и поэтому $f(g) = g'_1$ и $f(g) = g'_2$. Отсюда получаем: $f(g) = f(g_1 g_2) = f(g_1)f(g_2) = g'_1 g'_2$. Значит, $g \in F(g'_1 g'_2)$. Обратно, пусть $g \in F(g'_1 g'_2)$. Возьмем произвольный элемент $g_2 \in \Phi(g'_2)$ и представим элемент g в виде произведения элементов $g = \bar{g} g_2^{-1}$, $\bar{g} = g g_2^{-1}$. Имеем одновременно: $f(g)g'_1 g'_2$ и $f(g) = f(\bar{g})f(g_2) = f(\bar{g})g'_2$. Отсюда следует, что $f(\bar{g}) = g'_1$, т.е. $\bar{g} \in F(g'_1)$. Значит, $g \in F(g'_1)F(g'_2)$.

Таким образом, группа G' изоморфна фактор-группе G/H группы G. Теорема доказана.

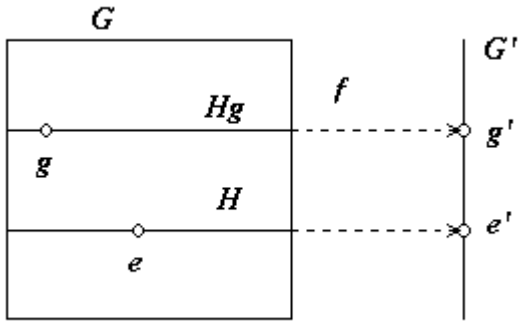


Рисунок иллюстрирует соответствие между G' и G/H. Отображение G на G' представлено как проектирование. Различные классы группы G по подгруппе H изображаются горизонтальными отрезками; все элементы каждого такого класса отображаются в один элемент из G'. Сопоставляя каждому элементу $g' \in G'$ соответствующий горизонтальный отрезок, получаем изоморфное отображение группы G' на группу G.

Пусть G – группа и H - ее нормальный делитель. Отображение $\pi : G \to G/H$, $\pi(g) = \bar{g} = gH$ является гомоморфизмом группы G на фактор-группу G/H который называется *естественным гомоморфизмом* группы G на факторгруппу G/H.

Если $f : G \to G'$ – гомоморфизм группы G на группу G' и]H=Kerf – ядро этого гомоморфизма, то согласно теореме о гомоморфизме группа G' изоморфна фактор-группе G/H. Поэтому, если группу G' отождествить с

фактор-группой G/H, то отображение f можно рассматривать как проекцию G на G'.

Рассмотрим решение примеров.

1. Доказать, что мультипликативную группу M невырожденных матриц порядка n ($n \geq 1$) можно гомоморфно отобразить на группу $R^* = R \setminus \{0\}$ действительных чисел, отличных от нуля.

Решение. Отобразим группу M в группу R^* по правилу f, которое каждой матрице A из M ставит в соответствие ее определитель $|A|$ – элемент из R^*, т.е. $f(A) = |A|$. Т.к. при этом отображении для любого заданного элемента из R^* полный прообраз есть непустое множество, то f является отображением M на R^*. Это отображение сохраняет операцию. Действительно, если A, B - любые элементы из группы M, то и $AB \in M$, и по теореме об определителе произведения матриц получим: $f(AB) = |AB| = |A| \circ |B| = f(A) f(B)$.

Итак, f есть отображение группы M на группу R^*, сохраняющее операцию, т.е. f - гомоморфное отображение.

2. Построить фактор-группу мультипликативной группы $Q^* = Q \setminus \{0\}$ рациональных чисел, отличных от нуля, по ее нормальному делителю H={1, -1} и гомоморфно отобразить группу Q^* на фактор-группу Q^* / H.

Решение. Пусть x - любое положительное рациональное число. Тогда $xH = \{x, -x\}$, $(-x)H = \{x, -x\}$, значит, смежные классы xH и $(-x)H$ совпадают. Отсюда следует, что при разложении группы Q^* по нормальному делителю H смежные классы можно порождать лишь при помощи положительных рациональных чисел. Итак, $Q^* / H = \{\{x, -x\} : x \in Q^+\}$, Q^+ - положительные рациональные числа.

Отобразим Q^* в Q^* / H по правилу $f : f(x) = xH = \{x, -x\}$.

Т.к. любой смежный класс не пуст, то при отображении f полный прообраз любого элемента из Q^* / H также не пуст, а потому f является

отображением группы Q^* на группу Q^*/H, сохраняющим операцию: если x и y - любые элементы из группы Q^*, то $f(xy) = (xy)H = xHyH = f(x)f(y)$.

Следовательно, f - гомоморфное отображение группы Q^* на группу Q^*/H.

МНОГОЧЛЕНЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

§1. Понятие многочлена.

п. 1. Алгебраическое определение кольца многочленов.

Пусть K – произвольное кольцо.

Определение. Многочленом от x с коэффициентами из K называется формальное выражение вида:

$$a_0+a_1\cdot x+a_2\cdot x^2+\ldots+a_n\cdot x^n, \quad (1)$$

где n – любое неотрицательное целое число, a_k – элементы кольца K, $k = \overline{0,n}$.

Замечание. Выражение (1) рассматривается как единый символ, никаких операций сложения или умножения над отдельными его частями не подразумевается.

Элемент $a_k \in K$ называется коэффициентом многочлена (1) при x^k. Для $k>n$ условимся считать, что коэффициент при x^k равен нулю.

Обозначение многочленов: $f(x)$, $g(x)$, $f_1(x), f_2(x)$ и т. п.

Определение. Многочлены $f_1(x)$ и $f_2(x)$ равны, если для любого $k=0,1,\ldots,n$ коэффициент многочлена $f_1(x)$ при x^k равен коэффициенту многочлена $f_2(x)$ при x^k. Равенство записывают обычным образом: $f_1(x)=f_2(x)$.

Рассмотрим два многочлена:

$$f(x)=a_0+a_1\cdot x+a_2\cdot x^2+\ldots+a_n\cdot x^n \quad (2)$$

и

$$g(x)=b_0+b_1\cdot x+b_2\cdot x^2+\ldots+b_m\cdot x^m, \quad (3)$$

где a_i и $b_j \in K$, $i = \overline{0,n}$, $j = \overline{0,m}$.

Определение. Суммой двух многочленов $f(x)$и $g(x)$ называется многочлен вида:

$$f(x)+g(x)=(a_0+b_0)+ (a_1+b_1)\cdot x+(a_2+b_2)\cdot x^2+\ldots+(a_p+b_p)\cdot x^p \ , \quad (4)$$

где $p=max\{n,m\}$.

Определение. Произведением многочленов (2) и (3) называется многочлен вида:

$$f(x)\cdot g(x)=c_0+c_1\cdot x+c_2\cdot x^2+\ldots+c_{n+m}\cdot x^{n+m}, \quad (5)$$

где $c_k\cdot x^k=a_0\cdot b_k\cdot x^k+ a_1\cdot x\cdot b_{k-1}\cdot x^{k-1}+ a_1\cdot x^2\cdot b_{k-2}\cdot x^{k-2}+\ldots+ a_k\cdot x^k\cdot b_0=$

$= (a_0\cdot b_k + a_1\cdot b_{k-1}+ a_2\cdot b_{k-2}+\ldots+ a_k\cdot b_0)\cdot x^\kappa$, (6)

Свойства операций сложения и умножения многочленов.

1. *Коммутативность сложения*.

Пусть многочлены $f(x)$ и $g(x)$ заданы формулами (2) и (3). Тогда, согласно определению, многочлен $f(x)+g(x)$ по формуле (4) равен многочлену

$$g(x)+f(x)=(b_0+a_0)+ (b_1+a_1)\cdot x+(b_2+a_2)\cdot x^2+\ldots+(b_p+a_p)\cdot x^p, \qquad p=max\{n,m\}.$$

Так как в кольце K сложение коммутативно, то $a_k+b_k=b_k+a_k$, $(k=0,\ldots,p)$ и, значит, $f(x)+g(x)= g(x)+f(x)$.

2. *Ассоциативность сложения*.

Доказательство аналогично 1, исходя из ассоциативности сложения в кольце K.

3. Существование нулевого элемента.

Определение. Нулевым элементом, обозначаемым θ , называется многочлен, все коэффициенты которого равны нулю, т.е.:

$$\theta (x)=0+0\cdot x+0\cdot x^2+\ldots+0\cdot x^n$$

Свойство: Для любого $f(x)$существует $\theta (x)$ такой, что: $f(x)+\theta (x)=\theta (x)+f(x)=f(x)$.

4. Существование противоположного элемента.

Определение: Противоположным многочленом называется многочлен, все коэффициенты которого противоположны соответствующим коэффициентам многочлена $f(x)$. Обозначение: $-f(x)$.

Ясно, что для любого $f(x)$ существует $-f(x)$ такой, что: $f(x)+(-f(x))=\theta(x)$.

5. Дистрибутивность умножения относительно сложения.

Пусть даны три многочлена:

$f(x)$ вида (2), $g(x)$ вида (3) и многочлен $h(x)=c_0+c_1\cdot x+c_2\cdot x^2+\ldots+c_l\cdot x^l$, где $c_k \in K,\ k=\overline{0,l}$.

Докажем, что

$$(f(x)+g(x))\cdot h(x)=f(x)\cdot h(x)+g(x)\cdot h(x). \quad (7)$$

Многочлен $f(x)+g(x)$ задается формулой (4). Согласно определению умножения многочленов, имеем:

$(f(x)+g(x))\cdot h(x)=d_0+d_1\cdot x+d_2\cdot x^2+\ldots+d_{p+l}\cdot x^{p+l}$, где

$d_k=(a_0+b_0)\cdot c_k+(a_1+b_1)\cdot c_{k-1}+(a_2+b_2)\cdot c_{k-2}+\ldots+(a_k+b_k)\cdot c_0$

Воспользовавшись дистрибутивностью в K, мы можем представить d_k в виде суммы: $d_k'+d_k''$, где

$d_k'=a_0\cdot c_k+a_1\cdot c_{k-1}+a_2\cdot c_{k-2}+\ldots+a_k\cdot c_0$

$d_k''=b_0\cdot c_k+b_1\cdot c_{k-1}+b_2\cdot c_{k-2}+\ldots+b_k\cdot c_0$

Ясно, что d_k' - коэффициент при x^k многочлена $f(x)\cdot h(x)$, а d_k'' - коэффициент при x^k многочлена $g(x)\cdot h(x)$, отсюда следует равенство (7).

Аналогично доказывается, что $h(x)\cdot(f(x)+g(x))=h(x)\cdot f(x)+h(x)\cdot g(x)$.

Свойства 1-5 означают, что многочлены с коэффициентами из кольца K сами образуют кольцо относительно определенных операций сложения и умножения. Это кольцо называется кольцом многочленов над K и обозначается через $K[x]$.

В $K[x]$ определима операция вычитания, обратная операции сложения (как и во всяком кольце).

Кольцо K, элементами которого являются многочлены, не содержащие x, т.е. выражение (1), в котором $n=0$ – это подкольцо кольца $K[x]$.

Многочлен вида $a \cdot x^k$ называется одночленом.

Определение. Степенью ненулевого многочлена $f(x)=a_0+a_1 \cdot x+a_2 \cdot x^2+\ldots+a_n \cdot x^n$ называется наибольшее из таких чисел k, что $a_k \neq 0$. Обозначение: $deg(f(x))=n$.

Замечание: $deg(\theta(x))=\infty$.

Всякий многочлен степени $n \geq 0$ может быть записан в виде (1), где $a_n \neq 0$. При этом $a_n \cdot x^n$ называется его старшим членом, а a_n – старшим коэффициентом многочлена.

Определение. Многочлен, старший коэффициент которого равен единице (если в кольце K есть единица), называется нормированным (или приведенным).

Из определения суммы и произведения следует, что

$$deg(f(x)+g(x)) \leq max\{deg(f(x),deg(g(x))\}, \quad (8)$$

$$deg(f(x) \cdot g(x)) \leq deg(f(x))+deg(g(x)). \quad (9)$$

п. 2. *Кольцо многочленов над областью целостности.*

Пусть K – область целостности, т.е. коммутативное, ассоциативное кольцо с единицей и без делителей нуля. Установим некоторые дополнительные свойства умножения многочленов, которые выполняются при условии, что K – область целостности.

6. *Коммутативность умножения:* $f(x) \cdot g(x)=g(x) \cdot f(x)$

Доказательство. Докажем сначала коммутативность умножения одночленов.

Для любых одночленов $a \cdot x^n$ и $b \cdot x^m$, где a и $b \in K$, выполняются равенства $a \cdot x^n \cdot b \cdot x^m=a \cdot b \cdot x^{n+m}$ и $b \cdot x^m \cdot a \cdot x^n=b \cdot a \cdot x^{n+m}$. Так как в кольце K умножение коммутативно, то $a \cdot b=b \cdot a$ и, значит $a \cdot x^n \cdot b \cdot x^m= b \cdot x^m \cdot a \cdot x^n$.

Пусть теперь $f(x)$ и $g(x)$ – произвольные многочлены.

Многочлен $f(x)\cdot g(x)$ по определению равен сумме всевозможных произведений вида $u\cdot v$, где u – член многочлена $f(x)$, v – член многочлена $g(x)$. Аналогично многочлен $g(x)\cdot f(x)$ равен сумме всевозможных произведений вида $v\cdot u$. А так как умножение одночленов $u\cdot v=v\cdot u$ – коммутативно, то отсюда следует, что для любого $v\in g(x)$, $u\in f(x)$: $f(x)\cdot g(x)= g(x)\cdot f(x)$.

7. *Ассоциативность умножения:* $(f(x)\cdot g(x))\cdot h(x)=f(x)\cdot(g(x)\cdot h(x))$.

Доказательство аналогично доказательству свойства 6.

Достаточно показать, что $(u\cdot v)\cdot w=u\cdot(v\cdot w)$, где u – член многочлена $f(x)$, v – член многочлена $g(x)$, c – член многочлена $h(x)$.

Для любых одночленов $u= a\cdot x^n$, v= $b\cdot x^m$, w= $c\cdot x^p$ имеем:

$(a\cdot x^n\cdot b\cdot x^m)\cdot c\cdot x^p= a\cdot b\cdot x^{n+m}\cdot c\cdot x^p=(a\cdot b)\cdot c\cdot x^{n+m+p}$,

$a\cdot x^n\cdot(b\cdot x^m\cdot c\cdot x^p)=a\cdot x^n\cdot b\cdot c\cdot x^{m+p}=a\cdot(b\cdot c)\cdot x^{n+m+p}$.

Следовательно, так как в кольце K умножение ассоциативно: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, то $(u\cdot v)\cdot w=u\cdot(v\cdot w)$.

8. Существование единицы.

Единицей в $K[x]$ является единица кольца K.

В самом деле, из определения умножения многочленов ясно, что $1\cdot f(x)=f(x)$, для любого $f(x)\in K[x]$. В частности, $1\cdot x^k= x^k$.

9. *Отсутствие делителей нуля*.

Пусть даны $f(x)\neq\theta$ (x), $g(x)\neq\theta$ (x). Докажем, что $f(x)\cdot g(x)\neq\theta$ (x).

Поскольку $f(x)\cdot g(x)=a_0\cdot b_0+(a_0\cdot b_1+a_1\cdot b_0)\cdot x+\ldots+(a_{n-1}\cdot b_m+a_n\cdot b_{m-1})\cdot x^{n+m-1}+a_n\cdot b_m\cdot x^{n+m}$, то коэффициент многочлена $f(x)\cdot g(x)$ при x^{n+m} равен $a_n\cdot b_m$. Так как в кольце K нет делителей нуля, то $a_n\cdot b_m\neq 0$, отсюда следует, что $f(x)\cdot g(x)\neq\theta$ (x).

Отсюда следует, также, что $deg(f(x)\cdot g(x))=deg(f(x))+deg(g(x))$ –

(10)

уточнение неравенства (9) для случая, когда в K нет делителей нуля.

Таким образом, свойства 6 – 9 означают, что кольцо $K[x]$ является областью целостности.

п. 3. Деление с остатком на двучлен $x-x_0$. Теорема Безу.

В кольце многочленов деление в обычном смысле слова, как правило, невозможно (например в кольце $K[x]$ многочлен x^2 нельзя разделить на $x+1$, т.е. не существует такого многочлена $g(x)$, что $x^2=g(x)\cdot(x+1))$, однако во многих случаях выполнимо так называемое «деление с остатком».

Существует частный случай, когда делитель является двучленом вида $x-x_0$.

Теорема 1. Пусть $f(x)$ – многочлен с коэффициентами из кольца K. Для любого $x_0 \in K$ многочлен $f(x)$ можно представить в виде: $f(x)=g(x)\cdot(x-x_0)+c$, (11)

где $g(x) \in K[x]$, $c \in K$, при этом $c=f(x_0)$.

Доказательство:

Если $f(x)=a \in K$, то можно взять $g(x)=0$, $c=a$.

Пусть теперь $\deg f(x)=n>0$.

Расположим многочлен f(x) по убывающим степеням x:

$$f(x)=a_0\cdot x^n + a_1\cdot x^{n-1} + a_2\cdot x^{n-2} + \ldots + a_{n-1}\cdot x + a_n$$

Ясно, что если представление $f(x)$ в виде (11) возможно, то $\deg g(x)=n-1$. Запишем $g(x)$ с неопределёнными коэффициентами:

$$g(x)=b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}\ .$$

Подставляя выражения для $f(x)$ и $g(x)$ в (11), получаем:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = (b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1})(x - x_0)+c$$

или

$$\boxed{a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n} = =$$

$$b_0x^n + (b_1 - b_0x_0)x^{n-1} + (b_2 - b_1x_0)x^{n-2} + \ldots + (b_{n-1} - b_{n-2}x_0)x + (c - b_{n-1}x_0)\,.$$

Откуда в силу определения равенства двух многочленов, получаем:

$$
\begin{aligned}
b_0 &= a_0,\\
b_1 &= a_1 + x_0 b_0,\\
b_2 &= a_2 + x_0 b_1,\\
&\cdots\cdots\cdots\cdots\\
b_{n-1} &= a_{n-1} + x_0 b_{n-2},\\
c &= a_n + x_0 b_{n-1}
\end{aligned}
$$

(12)

Эти формулы позволяют последовательно находить $b_0, b_1, \ldots, b_{n-1}$, c.

Проведённое рассуждение доказывает, что многочлен $g(x)$ и элемент c, удовлетворяют соотношению (11).

Для доказательства того, что $c = f(x_0)$, вычислим по (11) значение $f(x)$ в точке x_0 : $f(x_0) = g(x_0)(x_0 - x_0) + c$. Откуда $f(x_0) = c$.

Определение: Элемент x_0 кольца K называется корнем многочлена $f(x) \in K[x]$, если $f(x_0) = 0$.

Следствие (*Теорема Безу):*

Многочлен $f(x)$ делится на $x - x_0$ в кольце $K[x]$ $\Leftrightarrow$ x_0-его единственный корень.

Доказательство:

В силу доказанного, ясно, что $f(x) \vdots (x - x_0)$ $\Leftrightarrow$, когда в (11) $c = 0$, но т.к. $c = f(x_0)$, то условие $c = 0$ равносильно тому, что x_0-корень многочлена $f(x)$.

Нахождение многочлена $g(x)$ и элемента c, удовлетворяющих (11), называется делением с остатком многочлена $f(x)$ на двучлен $(x - x_0)$. При этом $g(x)$ называется неполным частным , а c – остатком.

Формулы (12) дают практический способ деления с остатком $f(x)$ на $(x - x_0)$. Но вычисления (12) удобно располагать по *схеме Горнера:*

–

	a_0	a_1	a_2	.....	a_{n-1}	a_n
x_0	b_0	b_1	b_2	.....	b_{n-1}	c

Пример 1:

В кольце K[x] разделить с остатком x^4-3x^2+x+5 на $(x-2)$.

Решение:

$\square=2$.

Расположим коэффициенты делимого многочлена по строке, а коэффициенты неполного частного и остатка найдём по формулам (12).

	1	0	-3	1	5
2	1	1·2+0=2	2·2-3=1	2·1+1=3	3·2+5=11= c

Ответ: $g(x)=x^3+2x^2+x+3$ *и* $c=11=f(2)$.

Пример2:

Вычислить значение многочлена $f(x)= i\cdot x^3+(1-2i)\cdot x^2-2\cdot(1-i)\cdot x+2$ в точке $\square=1+i$.

Решение:

	i	1-2i	-2+2i	2
1+i	i	-i	-1+i	0=f(1+i)

Ответ: f(1+i)=0.

п.4. Алгебраическое и функциональное равенство многочленов.

Теорема Безу позволяет указать верхнюю границу числа корней многочлена.

Теорем2:

Число корней ненулевого многочлена не превосходит его степени.

Доказательство.

Докажем с помощью индукции по степеням многочлена.

Многочлен нулевой степени вообще не имеет корней. Докажем утверждение теоремы для многочлена $deg=n-1$ и $\forall$ $f(x)$, $deg\, f(x)=n$.

От противного.

Пусть $x_1,x_2,\ldots,x_m$ – корни $f(x)$, причем $m>n$. По Теореме Безу $f(x) \vdots (x-x_1)$, т.е. $f(x)= (x-x_1)\cdot g(x)$, где $deg\ g(x)=n-1$. Элементы $x_1,x_2,\ldots,x_m \in K$ являются корнями многочлена $g(x)$.

В силу доказанного при $i=2,\ldots,m$ имеем:

$f(x_i)= (x_i-x_1)\cdot g(x_i)=0.$

Так как $x_i-x_1 \neq 0$, а кольцо K не имеет делителей нуля, то $g(x_i)=0$.

Таким образом, многочлен $g(x)$ имеет не менее чем $m-1$ корней, что противоречит предположению индукции, поскольку $deg\ g(x)=n-1<m-1$.

Следствие: Многочлен степени не выше n однозначно определяется своими значениями в $n+1$ точках. Иначе говоря, существует не более одного многочлена степени не выше, принимающего в данных точках $x_1,x_2,\ldots,x_{n+1}$ данные значения $y_1,y_2,\ldots,y_{n+1}$.

Теорема 3:

Если K – бесконечно, то равенство функций определяемых двумя многочленами из $K[x]$, влечёт за собой равенство самих многочленов.

Доказательство.

Пусть $f(x), g(x) \in K[x]$ определяют одинаковые функции , т.е. $f(x)=g(x)$ $\forall\ x \in K$. Обозначим через n наивысшую из степеней многочленов $f(x), g(x)$.

Так как K - бесконечно, то в нём найдутся $n+1$ различных элементов $x_1,x_2,\ldots,x_{n+1}$. Согласно предположению, $f(x)$ и $g(x)$ принимают одинаковые значения в каждой из точек $x_1,x_2,\ldots,x_{n+1}$. Отсюда и из следствия т.2 можно сделать вывод, что $f(x)=g(x)$.

Замечание.

Для конечного кольца K утверждение т.3 в общем случае неверно. Но при некотором дополнительном предположении утверждение т.3 оказывается возможным.

Например,

Теорема 4.

Если многочлены $f(x), g(x) \in Z_p[x]$, имеющие степень не выше чем $p-1$, эквивалентны (т.е. они определяют одну и ту же функцию над Z_p, $f(x) \sim g(x)$), то они равны.

§2. Корни многочлена.

Разработка методов решения алгебраических уравнений $f(x)=0$ породила развитие многих разделов алгебры, в том числе и алгебры многочленов, и теории групп.

Рассмотрим только многочлены над полем, т.е. $f(x) \in P[x]$.

О точном числе корней многочлена и, в частности, о существовании хотя бы одного корня однозначно говорить нельзя.

Пусть $f(x) \in P[x]$, и x_0 - его корень, т.е. $f(x_0)=0$. Согласно теореме Безу $f(x) \vdots (x-x_0)$.

Определение. Кратностью корня $x_0 \in f(x)$ называется наибольшее целое число r такое, что $f(x) \vdots (x-x_0)^r$. Если $r=1$, то x_0 - простой корень $f(x)$.

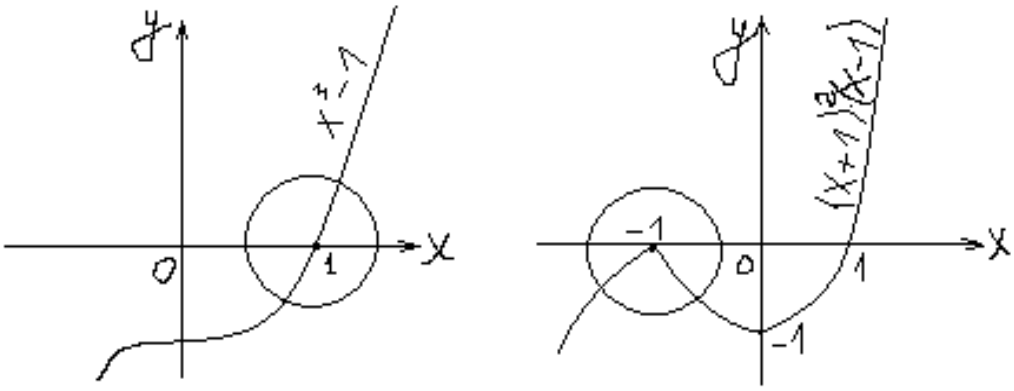
Утверждение. Элемент $x_0 \in P$ - корень кратности r многочлена $f(x) \in P[x]$<=>, когда $f(x)= (x-x_0)^r \cdot g(x)$, где $g(x) \in P[x]$, причем $g(x_0) \neq 0$.

Например, $f(x)=(x-2)^2 \cdot (x^5-10x+1) \in R[x]$ имеет число 2 корнем кратности 2, поскольку $g(x)$ в точке $2 \neq \theta(x)$.

Для любого $f(x) \in R[x]$ понятие простого и кратного корня имеют геометрический смысл.

Если $x_0 \in f(x)$ - простой корень, то график $f(x)$ пересекает ось абсцисс.

Если x_0 - кратный корень $f(x)$, то график $f(x)$ при $x=x_0$ касается оси абсцисс, причем порядок касания равен $(r1)$.



Теорема1.

Сумма кратностей всех корней ненулевого многочлена *f(x)* не превосходит его степени, причем равенство имеет место <=>, когда *f(x)* разлагается на линейные множители.

Доказательство основано на следующих двух леммах:

Лемма1.

Всякий ненулевой многочлен $f(x) \in P(x)$ может быть представлен в виде:

$$f(x)= (x-x_1)^{r1}\cdot(x-x_2)^{r2}\cdot\ldots\cdot(x-x_s)^{rs}\cdot g(x), \quad (1)$$

где $x_1,\ldots, x_s$- различные элементы поля *P, g(x)* - многочлен, не имеющий корней.

Лемма2.

Если многочлен *f(x)* представлен в виде (1), то $x_1, x_2, \ldots, x_s$ - это все его корни, причем кратность корня x_i равна r_i.

Например: $f(x)=(x+1)^3\cdot(x-2)\cdot(5\cdot x^4+1) \in R[x]$ имеет *(-1)* - трехкратный корень, 2- простой.

Доказательство Теоремы1.

Представим многочлен *f(x)* в виде (1). Тогда

$$\deg f(x)=r_1+r_2+\ldots+r_s+\deg g(x)\geq r_1+r_2+\ldots+r_s \quad (2),$$

а по Лемме2 $r_1+r_2+\ldots+r_s$ и есть сумма кратностей всех корней многочлена f(x). Тем самым доказано первое утверждение Теоремы.

Если в (2) имеет место равенство, то *deg g(x)=0*, т.е. $g(x)=a\neq\theta\ \epsilon\ P$ и

$f(x)=a\ (x-x_1)^{r1}(x-x_2)^{r2}\dots(x-x_s)^s$

(3),

т.е. получаем разложение многочлена *f(x)* на линейные множители.

Формулы Виетта.

Пусть $f(x)= a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n$, причем $a_0\neq0$, и пусть $x_1, x_2, \dots x_n$ - корни многочлена, каждый из которых повторен столько раз, какова его кратность.

Тогда коэффициент a_r *(r=1,2,…n)* равен произведению $(-1)^r a_0$ на сумму всевозможных произведений по r элементов из $x_1, x_2, \dots x_n$, т.е.

$a_1=-a_0(x_1+x_2+\dots+x_n)$,

$a_2=a_0(x_1x_2+x_1x_3+\dots+x_{n-1}x_n)$,

(4)

……

$a_n=(-1)^n a_0x_1x_2\dots x_n$.

- формулы Виета.

Выражение для a_r содержит C_n^r слагаемых.

Алгебраические сравнения по простому модулю.

Пусть p- простое число.

Определение: Алгебраическим сравнением по модулю p называется сравнение вида $a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n\equiv0\ (mod\ p)$,

(5)

где $a_0, a_1, \dots, a_{n-1}, a_n$ - целые числа, *x*- неизвестное, допустимые значения которого также целые числа.

Следствия:

1) если a_i, $i=0,\dots n$ из (5) заменить любыми целыми числами, сравнимыми с ними по модулю p, то полученное сравнение будет эквивалентно формуле (5).

2) если x_0 - решение сравнения (5), то и любое целое число сравнимое с x_0 по модулю *p*, будет решением этого сравнение.

Определение: Классом решений сравнения (5) называется совокупность его решений, составляющих один класс вычетов по модулю *p*.

Такой класс соответствует одному решению уравнения:

$$\bar{a}_0 x^n + \bar{a}_1 x^{n-1} + \ldots + \bar{a}_{n-1} x + \bar{a}_n = \bar{0}$$

(6)

где $\bar{a}$ - класс вычетов по модулю *p*, содержащий *a*.

Замечание: deg уравнения (6) равна *deg* сравнения (5).

Теорема2.

Число классов решений нетривиального алгебраического сравнения по простому модулю не превосходит его степени.

Отсюда можно любое алгебраическое сравнение по модулю *p* можно заменить эквивалентным ему сравнением степени не выше *p-1* . Например, сравнение $x^7-x^5+x^4-x^3-x-1\equiv 0 \pmod 3$ эквивалентно сравнению $x^2+x+1\equiv 0 \pmod 3$.

ТЕОРЕМА О СУЩЕСТВОВАНИИ КОРНЯ В ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Теорема (основная теорема алгебры). Всякое алгебраическое уравнение положительной степени с числовыми коэффициентами имеет корень в поле комплексных чисел.

Данная теорема впервые была доказана Гауссом в 1799 году.

Существует несколько способов доказательства этой теоремы. Рассмотрим доказательство, основанное на применении леммы о минимуме функции и леммы Даламбера.

Рассмотрим нормированный многочлен $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$ степени $n\geq 0$ с комплексными коэффициентами и уравнение $f(x) = 0$.

Лемма 1. Существует такое положительное число *A*, что при всех $x_0 \in \boldsymbol{C}$, удовлетворяющих условию $|x_0| > A$, выполняется неравенство $|f(x_0)| > |f(0)|$.

Доказательство. Для всякого комплексного числа x_0 имеем:

$$f(x_0) = x_0^{\,n} + a_1 x_0^{\,n-1} + a_2 x_0^{\,n-2} + \ldots a_{n-1} x_0 + a_n = x_0^n \left(1 + \frac{a_1}{x_0} + \frac{a_2}{x_0^2} + \ldots + \frac{a_n}{x_0^n} \right),$$

так что

$$| f(x_0) | = \left| x_0^n \right| \left| 1 + \frac{a_1}{x_0} + \ldots + \frac{a_n}{x_0^n} \right| \geq \left| x_0^n \right| \left(1 - \left| \frac{a_1}{x_0} + \ldots + \frac{a_n}{x_0^n} \right| \right) \geq |x_0|^n \left(1 - \left| \frac{a_1}{x_0} \right| - \ldots - \left| \frac{a_n}{x_0^n} \right| \right) =$$

$$= |x_0|^n \left(1 - \frac{|a_1|}{|x_0|} - \ldots - \frac{|a_n|}{|x_0^n|} \right).$$

Рассмотрим функцию $\varphi(t) = t^n \left(1 - \frac{|a_1|}{t} - \frac{|a_2|}{t^2} - \ldots - \frac{|a_n|}{t^n} \right)$ действительного переменного *t.* Очевидно, что $\lim\limits_{t \to +\infty} \varphi(t) = +\infty$. Следовательно, для любого *C* существует такое $A>0$, что $\varphi(t)>C$ при всех $t>A$. В частности, можно взять $C = |f(0)| = |a_n|$. Соответствующее *A* будет удовлетворять условию леммы. В самом деле, при $|x_0|>A$ имеем:

$$|f(x_0)| \geq \varphi(|x_0|) > C = |f(0)|.$$

Лемма доказана.

Лемма 2 (лемма Даламбера). Если многочлен $f(x)$ не обращается в нуль в точке $x_0 \in C$, то для любого $\varepsilon > 0$ существует такое $u \in C$, что $|u| < \varepsilon$ и $|f(x_0 + u)| < |f(x_0)|$.

Доказательство. Сделаем замену $x = x_0 + y$, где *y* – новая переменная и представим многочлен $f(x)$ в виде многочлена от *y*:

$$f(x) = (x_0 + y)^n + a_1 (x_0 + y)^{n-1} + \ldots + a_{n-1}(x_0 + y) + a_n = c_0 + c_1 y + \ldots + c_{n-1} y^{n-1} + c_n y^n. \qquad (1)$$

Так как $y = x - x_0$, то при подстановке в это равенство $x = x_0$ получаем $f(x_0) = c_0$. По условию $f(x_0) \neq 0$.Следовательно, $c_0 \neq 0$. Кроме того, $c_n = 1 \neq 0$, поскольку член y^n, появляется только при раскрытии скобок в выражении $(x_0 + y)^n$. Пусть *k* – наименьшее положительное число такое, что $c_k \neq 0$. Тогда

$$f(x) = c_0 + c_k y^k + c_{k+1} y^{k+1} + \ldots + c_n y^n \quad (c_0 \neq 0,\ c_k \neq 0). \qquad (2)$$

Идея доказательства леммы Даламбера заключается в том, что поведение функции $f(x)$ в малой окрестности точки x_0 в основном определяется первыми двумя членами разложения (2). Если бы остальных членов разложения не было, то можно было бы рассуждать так. Обозначим через y_0 какое – либо решение уравнения $c_0 + c_k y^k = 0$, т.е. одно из значений корня k-ой степени из $-\frac{c_0}{c_k}$.

Пусть t – действительное число, лежащее в интервале (0;1). Тогда

$$f(x_0 + ty_0) = c_0 + c_k t^k y_0^k = c_0(1 - t^k),$$

откуда видно, что

$$|f(x_0 + ty_0)| < |c_0|.$$

Выбирая t достаточно малым, можно добиться того, чтобы $|ty_0| < \varepsilon$ и тогда комплексное число $u = ty_0$ будет удовлетворять требованиям леммы. В общем случае доказательство будет отличаться тем, что оценивается модуль суммы остальных членов разложения (2).

Доказательство основной теоремы алгебры. Пусть число A – число, определенное по лемме 1. Рассмотрим на комплексной плоскости круг K радиуса A с центром в начале координат. По лемме вне круга K многочлен $f(x)$ принимает значения по модулю большие, чем $f(0)$.

Рассмотрим функцию $\psi(u;v) = |f(u + iv)|$ двух действительных переменных u и v. Покажем, что она непрерывна на всей плоскости. Пусть $a_k = b_k + ic_k$, где $b_k,\ c_k \in R$; тогда $f(u + iv) = (u + iv)^n + (b_1 + ic_i)(u + iv)^{n-1} + \ldots + (b_n + ic_n) = \psi_1(u,v) + i\psi_2(u,v)$, где $\psi_1(u,v)$ и $\psi_2(u,v)$ – некоторые многочлены с действительными коэффициентами. Очевидно, что $\psi(u,v) = \sqrt{\psi_1^2(u,v) + \psi_2^2(u,v)}$. Так как многочлены $\psi_1(u,v)$ и $\psi_2(u,v)$ – непрерывные функции, то и функция $\psi(u,v)$ непрерывна. Область определения функции $\psi(u,v)$, т.е. плоскость переменных u и v можно отождествить с комплексной плоскостью.

Из курса анализа известно, что всякая функция двух действительных переменных, определенная и непрерывная во всех точках замкнутого ограниченного множества достигает минимума в некоторой точке этого множества. Применяя эту теорему к функции $\psi(u,v)$ в круге K, можно заключить, что существует точка $x_0 = u_0 + iv_0$ этого круга, в которой функция $\psi(u,v)$ достигает минимума. Это означает, что $|f(x_0)| \le |f(x_1)|$ для всех $x_1 \in K$. В частности, $|f(x_0)| \le |f(0)|$, так как $0 \in K$. Согласно построения круга K, значение многочлена $f(x)$ вне этого круга по модулю больше, чем $f(0)$, и тем более, чем $f(x_0)$. Следовательно, неравенство $|f(x_0)| \le |f(x_1)|$ выполняется для всех $x_1 \in \boldsymbol{C}$.

Смысл же леммы Даламбера заключается в следующем: на комплексной плоскости найдутся точки, в которых значение многочлена $f(x)$ по модулю меньше, чем $f(x_0)$. Поэтому если $|f(x)|$ достигает минимума в какой-то точке комплексной плоскости, то этот минимум равен нулю.

С другой стороны, выше было доказано, что $|f(x)|$ достигает минимума в некоторой точке x_0. По лемме Даламбера заключаем, что $|f(x_0)| = 0$ и значит, $f(x_0) = 0$, т.е. x_0 – корень уравнения $f(x) = 0$.

Следствие. Всякое алгебраическое уравнение степени ≥1 с числовыми коэффициентами имеет в поле комплексных чисел $\boldsymbol{C}$ ровно n корней (с учетом кратностей).

УРАВНЕНИЯ 3 СТЕПЕНИ

Если дано кубическое уравнение с любыми комплексными коэффициентами

$$y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$

то с помощью замены $y - \frac{a_1}{3} = x$ можно добиться того, чтобы оно не содержало слагаемое второй степени.

Рассмотрим полученное неполное кубическое уравнение с произвольными комплексными коэффициентами

$$x^2 + px + q = 0.$$

Это уравнение по основной теореме алгебры обладает тремя комплексными корнями. Пусть x_0 – один из этих корней имеет вид $x_0 = u + v$, тогда левая часть уравнения примет вид

$$(u+v)^3 + p(u+v) + q = u^3 + v^3 + (3uv + p)(u+v) + q.$$

Отсюда следует, что u и v являются решениями системы уравнений

$$\begin{cases} u^3 + v^3 + q = 0 \\ 3uv + p = 0 \end{cases}.$$

Для решения этой системы представим второе уравнение в виде $u^3v^3 = -\frac{p^3}{27}$, тогда система примет вид $\begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -\frac{p^3}{27} \end{cases}$.

Следуя теореме Виета выражения u^3 и v^3 можно рассматривать как корни некоторого квадратного уравнения

$$z^2 + qz - \frac{p^3}{27} = 0,$$

дискриминант которого равен $D = q^2 - 4\left(-\frac{p^3}{27}\right) = q^2 + \frac{4p^3}{27}$.

Тогда решения квадратного уравнения имеют вид

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}; \; v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Тогда u и v соответственно равны

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \; v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Из этих формул получаем формулу решения неполного кубического называемую формулой Кардано

$$x_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Значение кубических корней в этой формуле не могут выбираться произвольно, так как в системе уравнений относительно u и v имеется условие $uv = -\frac{p}{3}$. Значение кубических корней в формуле Кардано следует выбирать таким образом, чтобы их произведение равнялось $-\frac{p}{3}$.

Пусть u_1 будет одно из трех значений радикала u. Тогда два других можно получить умножением u_1 на кубические корни $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $\varepsilon^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ из единицы:

$$u_2 = u_1\varepsilon\ ,\ \ u_3 = u_1\varepsilon^2.$$

Обозначим через v_1 одно из трех значений радикала v, которое соответствует значению u_1 радикала u на основании равенства $uv = -\frac{p}{3}$. Два других значения v будут

$$v_2 = v_1\varepsilon^2,\ \ v_3 = v_1\varepsilon\ .$$

Так как, ввиду $\varepsilon^3 = 1$,

$$u_2v_2 = u_1\varepsilon \cdot v_1\varepsilon^2 = u_1v_1\varepsilon^3 = u_1v_1 = -\frac{p}{3} \text{ и } u_3v_3 = u_1\varepsilon^2 \cdot v_1\varepsilon = u_1v_1\varepsilon^3 = u_1v_1 = -\frac{p}{3},$$

то значению u_2 радикала u соответствует значение v_2 радикала v; аналогично значению u_3 соответствует значение v_3. Таким образом, все корни три корня неполного кубического уравнения могут быть записаны следующим образом:

$$x_1 = u_1 + v_1,$$
$$x_2 = u_2 + v_2 = u_1\varepsilon + v_1\varepsilon^2,$$
$$x_3 = u_3 + v_3 = u_1\varepsilon^2 + v_1\varepsilon.$$

Теперь, возвращаясь к обратной замене, можно получить корни исходного кубического уравнения.

Пример. Решить уравнение в поле комплексных чисел $\boldsymbol{C}$

$$x^3 - 6x^2 + 57x - 196 = 0.$$

Решение. Делая замену $x = y + 2$ в данном уравнении, получаем неполное кубическое уравнение:

$$y^3 + 6y^2 + 12y + 8 - 6(y^2 + 4y + 4) + 57y + 114 - 196 = 0$$

$$y^3 + 6y^2 + 12y + 8 - 6y^2 - 24y - 24 + 57y - 82 = 0$$

$$y^3 + 45y - 98 = 0$$

$$p = 45,\ q = -98$$

$$y = \alpha + \beta = \sqrt[3]{-\frac{-98}{2} + \sqrt{\frac{(-98)^2}{4} + \frac{45^3}{27}}} + \sqrt[3]{-\frac{-98}{2} - \sqrt{\frac{(-98)^2}{4} + \frac{45^3}{27}}} =$$

$$= \sqrt[3]{49 + \sqrt{5776}} + \sqrt[3]{49 - \sqrt{5776}} = \sqrt[3]{125} + \sqrt[3]{-27}$$

Пусть $\alpha_1 = 5$, тогда $\beta_1 = -3$, так как $\alpha_1\beta_1 = -\frac{p}{3} = -15$. Следовательно,

$$y_1 = \alpha_1 + \beta_1 = 5 + (-3) = 2.$$

Найдем y_2 и y_3:

$$y_2 = \alpha_2 + \beta_3 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = 5(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) = -1 + 4\sqrt{3}i,$$

$$y_3 = \alpha_3 + \beta_2 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = 5(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = -1 - 4\sqrt{3}i.$$

Делая обратную замену, получим корни исходного уравнения

$$x_1 = 4,\ x_2 = 1 + 4\sqrt{3}i,\ x_3 = 1 - 4\sqrt{3}i.$$

Пример. Решить уравнение $y^3 + 3iy^2 - (3 + 6i)y + 10 - 5i = 0$.

Решение. Сделаем замену в данном уравнении $y = x - i$:

$$(x - i)^3 + 3i(x - i)^2 - (3 + 6i)(x - i) + 10 - 5i = 0$$

$$x^3 - 3ix^2 - 3x + i + 3i(x^2 - 2ix - 1) - (3x - 3i + 6ix + 6) + 10 - 5i = 0$$

$$x^3 - 3ix^2 - 3x + i + 3ix^2 + 6x - 3i - 3x + 3i - 6ix - 6 + 10 - 5i = 0$$

и получим неполное кубическое уравнение

$$x^3 - 6ix + 4 - 4i = 0,$$

где $p = -6i,\ q = 4 - 4i$.

Найдем корни полученного уравнения по формулам Кардано

$$x = \alpha + \beta = \sqrt[3]{-\frac{4-4i}{2}+\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}}+\sqrt[3]{-\frac{(4-4i)}{2}-\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}}$$

,

$$\alpha = \sqrt[3]{-\frac{4-4i}{2}+\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}} = \sqrt[3]{-2+2i+\sqrt{(2-2i)^2+8i}} =$$

$$= \sqrt[3]{-2+2i+\sqrt{4-8i-4+8i}} = \sqrt[3]{-2+2i}$$

$$\beta = \sqrt[3]{-\frac{(4-4i)}{2}-\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}} = \sqrt[3]{-2+2i}\,.$$

$$\sqrt[3]{-2+2i} = \sqrt{2}\left(\cos\frac{\frac{3\pi}{4}+2\pi k}{3}+i\sin\frac{\frac{3\pi}{4}+2\pi k}{3}\right),\ k = 0,\ 1,\ 2$$

Укажем значение корня при k=0 , тогда

$$\alpha_1 = \sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right) = 1+i$$

Найдем β_1 из условия $\alpha_1\beta_1 = -\frac{p}{3}$

$\alpha_1\beta_1 = (1+i)\beta_1 = -\frac{-6i}{3} = 2i$, отсюда $\beta_1 = 1+i$.

Тогда $x_1 = \alpha_1 + \beta_1 = 2+2i$,

$$x_2 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = (1+i)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)+(1+i)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) =$$

$$= -1-i,$$

$$x_3 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = (1+i)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)+(1+i)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) =$$

$$= -1-i.$$

Выполним обратную замену и получим корни исходного уравнения

$$y_1 = 2+i,\ y_2 = -1-2i,\ y_3 = -1-2i.$$

Кубические уравнения с действительными коэффициентами

Рассмотрим неполное кубическое уравнение с действительными коэффициентами

$$x^2 + px + q = 0.$$

Выражение $D = -4p^3 - 27q^2 = -108(\frac{q^2}{4} + \frac{p^3}{27})$ называется дискриминантом кубического уравнения. В зависимости от знака выражения $\frac{q^2}{4} + \frac{p^3}{27}$, стоящего в формуле Кардано под знаком квадратного корня и имеющего противоположный знак дискриминанту, кубическое уравнение может иметь три различных действительных корня, один действительный и два комплексно-сопряженных корня и три действительных корня, из которых два корня равны между собой.

1. При $D<0$ выражение $\frac{q^2}{4} + \frac{p^3}{27}$ положительно, поэтому в формуле Кардано под знаком каждого из кубических радикалов оказываются различные действительные числа. Тогда

$$x_1 = u_1 + v_1,$$
$$x_2 = u_1\varepsilon + v_1\varepsilon^2,$$
$$x_3 = u_1\varepsilon^2 + v_1\varepsilon = \bar{x}_2.$$

Так как $x_2 \neq x_3$, то x_2 и x_3 – сопряженные мнимые числа. Число x_1, очевидно, действительное.

Итак, если $D<0$, то уравнение $x^2 + px + q = 0$ имеет один действительный и два сопряженных мнимых корня.

2. При $D>0$ выражение $\frac{q^2}{4} + \frac{p^3}{27}$ отрицательно, поэтому в формуле Кардано под знаком квадратного корня находится отрицательное число и кубические корни извлекаются из двух сопряженных комплексных чисел. Тогда, учитывая $\varepsilon^2 = \bar{\varepsilon}$,

$$x_1 = u_1 + \bar{u}_1,$$
$$x_2 = u_1\varepsilon + \bar{u}_1\varepsilon^2 = u_1\varepsilon + \overline{u_1\varepsilon},$$
$$x_3 = u_1\varepsilon^2 + \bar{u}_1\varepsilon = u_1\varepsilon^2 + \overline{u_1\varepsilon^2}.$$

Итак, если $D>0$, то уравнение $x^2 + px + q = 0$ имеет

3. При $D=0$ имеем $u_1 = v_1$ и тогда, используя очевидное равенство, получим:

$$x_1 = 2u_1,$$
$$x_2 = u_1(\varepsilon + \varepsilon^2) = -u_1,$$
$$x_3 = u_1(\varepsilon^2 + \varepsilon) = -u_1.$$

Итак, если $D=0$, то все корни уравнения $x^2 + px + q = 0$ действительны, причем два из них равны между собой.

РЕШЕНИЕ УРАВНЕНИЯ 4 СТЕПЕНИ МЕТОДОМ ФЕРРАРИ

Рассмотрим приведенное уравнение 4-й степени

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Сделав замену переменной $x = y - \frac{a}{4}$, приведем данное уравнение к виду

$$. \; y^4 + py^2 + qy + r = 0.$$

Будем решать это уравнение методом, который носит название метода Феррари.

Преобразуем левую часть уравнения так:

$$\left(y^2 + \frac{p}{2}\right)^2 + qy + \left(r - \frac{p^2}{4}\right) = 0.$$

Затем введем новую переменную z следующим образом:

$$\left(y^2 + \frac{p}{2} + z\right)^2 - \left[2z\left(y^2 + \frac{p}{2}\right) + z^2 - qy + \frac{p^2}{4} - r\right] = 0.$$

Подберем значение z так, чтобы многочлен 2-й степени стоящий в квадратных скобках, стал полным квадратом. Для того чтобы многочлен $2zy^2 - qy + \left(zp + z^2 + \frac{p^2}{4} - r\right)$ был полным квадратом необходимо и достаточно, чтобы его дискриминант равнялся нулю, т.е.

$$D = q^2 - 4 \cdot 2z\left(zp + z^2 + \frac{p^2}{4} - r \right) = 0,$$

$$8z^3 + 8pz^2 - 8rz + (2p^2 - q^2) = 0.$$

Получили уравнение 3-й степени относительно неизвестного z, которое можно решить по формулам Кардано и найти хотя бы один действительный корень z_0. Подставляя это значение в уравнение $\left(y^2 + \frac{p}{2} + z \right)^2 - \left[2z\left(y^2 + \frac{p}{2} \right) + z^2 - qy + \frac{p^2}{4} - r \right] = 0$, получим в левой части разность квадратов. Тогда полученную разность квадратов можно разложить в произведение двух многочленов второй степени относительно y. После этого останется решить два получившихся уравнения 2-й степени.

Таким образом, уравнение 4-й степени всегда может быть решено и, более того, можно, аналогично случаю уравнения 3-й степени, получить формулу, выражающую корни общего уравнения 4-й степени через коэффициенты уравнения с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени.

Однако, общее уравнение с одним неизвестным степени выше 4-й неразрешимо в радикалах, т.е. не существует формулы, выражающей корни общего уравнения степени выше 4-й через коэффициенты уравнения с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени. Это положение известно как теорема Абеля.

Пример. Решить уравнение методом Феррари

$$x^4 - 2x^3 + 2x^2 + 4x - 8 = 0.$$

Решение.

$$x^4 - 2x^3 = -2x^2 - 4x + 8$$

$$(x^2)^4 - 2x^2x + x^2 = -x^2 - 4x + 8$$

$$(x^2 - x)^2 = -x^2 - 4x + 8$$

$$(x^2 - x + y)^2 = -x^2 - 4x + 8 + 2(x^2 - x)y + y^2$$

$$(x^2 - x + y)^2 = (2y - 1)x^2 + (-2y - 4)x + y^2 + 8$$

$$D = (-2y - 4)^2 - 4(2y - 1)(y^2 + 8) = 4y^2 + 16y + 16 - 8y^3 + 4y^2 - 64y + 32 =$$

$$= -8y^3 + 8y^2 - 48y + 48$$

$$-8y^3 + 8y^2 - 48y + 48 = 0$$

$$y^3 - y^2 + 6y - 6 = 0$$

$$y^2(y - 1) + 6(y - 1) = 0$$

$$(y - 1)(y^2 + 6) = 0$$

$$y - 1 = 0$$

$$y = 1$$

$$(x^2 - x + 1)^2 = x^2 - 6x + 9$$

$$(x^2 - x + 1)^2 = (x - 3)^2$$

$$x^2 - x + 1 = x - 3 \text{ или } x^2 - x + 1 = -x + 3$$

$$x^2 - 2x + 4 = 0 \text{ или } x^2 - 2 = 0$$

$$x^2 - 2x + 4 = 0$$

$$D = 2^2 - 4 \cdot 4 = -12$$

$$x_{1,2} = \frac{2 \pm 2\sqrt{3}i}{2} = 1 \pm \sqrt{3}i;$$

$$x^2 - 2 = 0$$

$$x_{3,4} = \pm\sqrt{2}.$$

КОЛЬЦА И ИДЕАЛЫ

§ 1. Кольца

Прежде чем давать определение кольца, рассмотрим, какими общими свойствами обладают множество целых чисел Z и множество многочленов с действительными коэффициентами $R[x]$.

Во-первых, сумма целых чисел — целое число; аналогично сумма многочленов с действительными коэффициентами — многочлен с действительными коэффициентами. Во-вторых, как в Z, так и в $R[x]$, операция сложения коммутативна и ассоциативна. В третьих, как в Z, так и в $R[x]$, имеется нулевой элемент 0, такой, что для всех a имеем $a + 0 = a$, и для всех a есть противоположный элемент $-a$: $a + (-a) = 0$.

Все эти свойства можно кратко сформулировать так: и Z и $R[x]$ являются коммутативными группами относительно операции сложения.

Кроме операции сложения, и в Z, и в $R[x]$ есть операция умножения, причем эта операция дистрибутивна относительно операции сложения:

$a(b + c) = ab + ac$.

Определим в общем виде понятие дистрибутивности одной бинарной операции относительно другой. Пусть в множестве M заданы две бинарные операции, одна из которых обозначена $\circ$,а вторая*.

Определение 1. Операция $*$ в M дистрибутивна слева относительно операции $\circ$, если для любых трех элементов a, b, c. из M имеем:

$$a * (b \circ c) = (a * b) \circ (a * c).$$

Операция $*$ дистрибутивна справа относительно $\circ$, если для любых трех элементов a, b, c из M имеем:

$(b \circ c) - a = (b * a) \circ (c * a)$.

В дальнейшем, как правило, мы будем иметь дело с коммутативными операциями. Для таких операций понятия дистрибутивности слева и справа

совпадают, а потому говорят просто, что операция $*$ дистрибутивна относительно.

Примеры.

1. Умножение в множестве Z дистрибутивно как относительно сложения, так и относительно вычитания:

$a(b+c)=ab+ac$, $a(b-c)=ab-ac$.

То же справедливо и для множества многочленов $R[x]$.

2. Пусть $*$ — операция возведения в степень в множестве N натуральных чисел, а $\circ$ — операция умножения в том же множестве, т. е.

$a*b=a^b$, $a\circ b=ab$, a, $b\in N$

Операция $*$ дистрибутивна справа относительно операции $\circ$, поскольку

$(b\circ c)*a=(bc)^a=b^a c^a=(b*a)\circ(c*a)$.

Но $*$ не дистрибутивна слева относительно $\circ$, так как

$a*(b\circ c)=a^{bc}$, но $(a*b)\circ(a*c)=a^b a^c\neq a^{bc}$,

Определение 2. Кольцом называется непустое множество R, в котором определены две бинарные операции: сложение $a+b$ и умножение $a\cdot b$, причем:

1) R является коммутативной группой относительно сложения;

2) умножение дистрибутивно слева и справа относительно сложения.

В развернутом виде определение кольца таково:

Определение 2'. Кольцом называется непустое множество R, в котором определены две бинарные операции: сложение $a+b$ и умножение $a\cdot b$, причем:

1) сложение ассоциативно и коммутативно:

$(a+b)+c=a+(b+c)$ для любых $a, b, c\in R$;

2) существует нулевой элемент кольца 0, такой, что для любого $a\in R$ имеем: $a+0=a$ (поскольку сложение коммутативно, то и $0+a=a$);

3) для любого $a \in R$ существует противоположный элемент кольца $-a$, такой, что $a + (-a) = 0$ (и тем самым $-a + a = 0$);

умножение дистрибутивно относительно сложения, т. е. для любых трех элементов a, b, c из R

$$a(b + c) = ab + ac$$

и

$$(b + c)a = ba + ca.$$

Мы уже отмечали, что все требования 1) — 4) выполняются и в множестве Z целых чисел, и в множестве $R[x]$ многочленов с действительными коэффициентами. Поэтому как Z, так и $R[x]$ являются кольцами. Эти кольца обладают дополнительными свойствами, которые, вообще говоря, могут не иметь места в произвольных кольцах: умножение и в Z, и в $R[x]$ коммутативно и ассоциативно. Кольца, в которых умножение ассоциативно, называются ассоциативными, а кольца, в которых умножение коммутативно, — коммутативными. Таким образом, Z и $R[x]$ — коммутативные ассоциативные кольца. Кроме того, в Z и $R[x]$ есть единица, т. е. такой элемент 1, что для всех a имеем: $a \cdot 1 = a$. Любое кольцо R в котором есть такой нейтральный элемент e, что для всех $a \in R$ имеем $ae = ea = a$, называют кольцом с единицей.

Сравнивая определение кольца с определением поля, видим, что всякое поле является кольцом (обратное, вообще говоря, неверно— кольцо Z целых чисел не является полем). Поле — это ассоциативное и коммутативное кольцо с отличной от нуля единицей, в котором каждый отличный от нуля элемент имеет обратный. Иными словами, если a — отличный от нуля элемент поля P, то в P есть такой элемент a^{-1} что $a \cdot a^{-1} = a^{-1} \cdot a = e$.

3. Примеры колец.

1) Простейшим кольцом является множество, состоящее лишь из нуля: $R = \{0\}$. В самом деле, равенства $0 + 0 = 0$ и $0 \cdot 0 = 0$ показывают, что сложение и

умножение — бинарные операции в $\square$. Очевидна и ассоциативность, и коммутативность сложения, а также ассоциативность и коммутативность умножения. Умножение дистрибутивно относительно сложения. В этом кольце элемент 0 сам себе является противоположным. Он же выполняет и роль единицы, и роль нуля кольца.

Множество $Ч$ всех четных чисел образует кольцо. Это видно из того, что сумма и произведение четных чисел — четные числа, а число, противоположное четному — четно. Ассоциативность, коммутативность сложения и умножения, а также дистрибутивность умножения относительно сложения вытекают из того, что все эти свойства имеют место для операций в кольце $\square$ целых чисел. Кольцо $Ч$ не содержит единицы.

3) Множество $Z[i]$ всех комплексных чисел вида $a + bi$, где $\square$ и $\square$ — целые числа, является кольцом относительно обычных операций сложения и умножения комплексных чисел. В самом деле, пусть $z_1 = a_1 + b_1 i \in Z[i]$ и $z_2 = a_2 + b_2 i \in Z[i]$. Тогда имеем:

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$

$$z_1 \cdot z_2 = (a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.$$

Так как $a_1 + a_2$, $b_1 + b_2$, $a_1 a_2 - b_1 b_2$, $a_1 b_2 + a_2 b_1$ — целые числа, то $z_1 + z_2 \in Z[i]$ и $z_1 \cdot z_2 \in Z[i]$. Иными словами, сложение и умножение — бинарные операции в $Z[i]$. Число $-z = -a - bi$, противоположное числу $z = a + bi$, тоже принадлежит $\square$ (так как $-a$ и $-b$ — целые числа). Проверка условий коммутативности и ассоциативности сложения, дистрибутивности умножения относительно сложения излишня, поскольку эти свойства действий имеют место для любых комплексных чисел.

Кольцо $\square$ впервые изучал великий немецкий математик Карл Фридрих Гаусс. Поэтому $\square$ называют кольцом целых гауссовых чисел.

Множество нечетных чисел не является кольцом, так как сумма нечетных чисел четна, а потому сложение не является бинарной операцией в этом множестве.

Не является кольцом и множество N натуральных чисел, поскольку $\square$ не содержит нуля. Множество Z_0 неотрицательных целых чисел тоже не является кольцом, так как, например, $4 \in Z_0$, но $-4 \notin Z_0$.

Элементами колец из примеров 1—3 являлись числа.

Определение 3. Кольцо, элементами которого являются некоторые комплексные числа с обычными операциями сложения и умножения, называется числовым кольцом. Таким образом, 0, $\square$, $Ч$, $\square$ — числовые кольца.

Рассмотрим теперь несколько примеров колец, не являющихся числовыми кольцами.

6) С каждым числовым кольцом R связано кольцо $R[x]$, состоящее из многочленов от x, коэффициенты которых принадлежат $\square$. Например, $Z[x]$ — кольцо многочленов с целыми коэффициентами, $R[x]$ — кольцо многочленов с действительными коэффициентами, $C[x]$ — кольцо многочленов с комплексными коэффициентами. Эти кольца будут изучены в четвертой части курса.

7) Множество всех квадратных матриц n-го порядка с действительными элементами образует кольцо относительно операций сложения и умножения матриц. В самом деле, сумма (и произведение) двух квадратных матриц n-го порядка с действительными элементами является матрицей n-го порядка с действительными элементами. Роль нуля играет матрица с нулевыми элементами, а роль противоиоложного элемента для матрицы A — матрица $-A$, получаемая из A изменением знаков элементов.

Это кольцо ассоциативно, но некоммутативно. Оно имеет единицу — единичную матрицу E.

8) Множество $C[a,b]$ всех действительных функций, непрерывных на отрезке $[a,b]$, образует кольцо относительно обычных операций сложения и умножения функций (сумма и произведение непрерывных функций — непрерывные функции, а вместе с $f(x)$ функция $-f(x)$ непрерывна). Кольцо $C[a,b]$ коммутативно, ассоциативно и имеет единичный элемент — функцию, тождественно равную 1.

9) Пусть $\square$ — любое кольцо. Обозначим через R_n множество кортежей $(a_1,...,a_n)$, где все $a_k \in R$. Операции сложения и умножения в R_n введем «покоординатно»:

$(a_1,...,a_n)+(b_1,...,b_n)=(a_1+b_1,...,a_n+b_n)$ **и** $(a_1,...,a_n)\cdot(b_1,...,b_n)=(a_1\cdot b_1,...,a_n\cdot b_n)$.

Легко проверить, что $\square$ тоже является кольцом. Если кольцо $\square$ ассоциативно (соответственно коммутативно), то и $\square$ — ассоциативное (соответственно коммутативное) кольцо. Если $\square$ — кольцо с единицей e, то единицей в $\square$ является кортеж $(e,...,e)$.

10) Наконец, приведем пример кольца, которое неассоциативно и некоммутативно. Пусть R^3 — множество векторов трехмерного прострaнства. В качестве бинарных операций в $\square$ возьмем сложение векторов и векторное произведение. Из курса геометрии известно, что векторное произведение некоммутативно и неассоциативно, и значит, и кольцо $\square$ некоммутативно и неассоциативно. В кольце $\square$ вместо этих свойств выполняются соотношения;

$$[a,b]=-[b,a] \quad (1)$$

(антикоммутативность) и

$$[[a,b],c]+[[b,c],a]+[[c,a],b]=0 \quad (2)$$

(тождество Якоби). Кольца, обладающие свойствами (1) и (2), напеваются кольцами Ли.

Простейшие свойства колец.

Рассмотрим некоторые свойства конец. По определению каждое кольцо является коммутативной группой относительно сложения. Эту группу называют аддитивной группой кольца R (иными словами, аддитивная группа кольца R — это то же самое множество элементов, в котором рассматривают не две, а лишь одну операцию — сложение).

Из свойств бинарных операций вытекают следующие утверждения об аддитивной группе кольца R:

1) нуль кольца R является единственным элементом, нейтральным относительно сложения;

2) для любого $a \in R$ элемент $-a$ является единственным элементом в R, симметричным с а относительно сложения, причем $-(-a) = a$;

3) уравнение $b + x = a$ для любых, $a, b \in R$ имеет одно и только одно решение: $x = a + (-b)$, называемое разностью элементов a и b и обозначаемое $a - b$.

Итак, $a - b = a + (-b)$;

4) если $a + b = a + c$, то $b = c$;

для любого кортежа $(a_1, ..., a_n)$ элементов кольца R определена сумма $a_1 + ... + a_n$, значение которой не зависит ни от расстановки скобок, ни от порядка слагаемых.

Пусть a – любой элемент кольца R. Обозначим сумму n слагаемых, каждое из которых равно a, через na, а сумму n слагаемых, равных $-a$, через $-na$.

Элемент na нельзя, вообще говоря, рассматривать как произведение n и a, поскольку кольцо R не всегда содержит кольцо Z целых чисел. Лишь в случае, когда R содержит единицу e, можно отожествить n с $(ne)a$, т. е. с произведением элементов ne и a кольца R. В самом деле, в этом случае мы имеем при натуральном n

$$(ne)a = \underbrace{(e + ... + e)}_{n\ раз}a = \underbrace{ea + ... + ea}_{n\ раз} = \underbrace{a + ... + a}_{n\ раз} = na$$

В любом кольце R выполняются следующие равенства (где a и b — любые элементы из R, а m и n — любые целые числа):

$$a - (-b) = a + b, \quad (1)$$

$$-(a + b) = -a - b, \quad (2)$$

$$\sum_{k=1}^{m} a_k + \sum_{k=m+1}^{m+n} a_k = \sum_{k=1}^{m+n} a_k, \quad (3)$$

$$ma + na = (m + n)a, \quad (4)$$

$$m(na) = mn(a), \quad (5)$$

$$na + nb = n(a + b). \quad (6)$$

Равенство (1) следует из того, что $-(-b) = b$, и потому

$$a - (-b) = a + [-(-b)] = a + b.$$

Чтобы доказать равенство (2), достаточно заметить, что в силу ассоциативности и коммутативности сложения в кольце R имеем:

$$a + b + [(-a) + (-b)] = [a + (-a)] + [b + (-b)] = 0.$$

Это и означает, что элемент $(-a) + (-b)$ противоположен $a + b$, т. е. равен $-(a + b)$ (напомним, что в кольце каждый элемент имеет единственный противоположный элемент).

Далее, равенство (3) справедливо в любом множестве с ассоциативной бинарной операцией сложения. При натуральных m и n равенство (4) следует из (3), если положить $a_k = a$. Если m и n — отрицательные целые числа, $m = -|m|$, $n = -|n|$, то по определению имеем:

$$ma = |m|(-a), \quad na = |n|(-a),$$

а тогда

$$ma + na = |m|(-a) + |n|(-a) = (|m| + |n|)(-a) = -(|m| + |n|)a = (-|m| - |n|)a = (m + n)a.$$

Рассмотрим, наконец, случай, когда $m > 0$, $n = -|n|$, причем $m \geq |n|$. Тогда по определению

$$ma + na = \underbrace{a + \ldots + a}_{m\ раз} + \underbrace{(-a) + \ldots + (-a)}_{|n|\ раз}.$$

Эту сумму можно переписать следующим образом:

$$ma + na = \underbrace{[a + (-a)]}_{|n|\ раз} + \underbrace{a + \ldots + a}_{m-|n|\ раз}$$

Так как $a + (-a) = 0$, то получим, что

$$ma + na = (m - |n|)a = (m + n)a.$$

Аналогично рассматривается случай, когда $m > 0$, $n = -|n|$, $m < |n|$. Так как при $m = 0$ или $n = 0$ равенство (4) очевидно, то мы доказали справедливость этого равенства при любых целых $\square$ и $\square$.

Справедливость равенства (5) при натуральных $\square$ и $\square$ видна того, что

$$m(na) = \underbrace{na + \ldots + na}_{m\ раз} = \underbrace{\underbrace{a + \ldots + a}_{n\ раз} + \ldots + \underbrace{a + \ldots + a}_{n\ раз}}_{m\ раз} = \underbrace{a + \ldots + a}_{mn\ раз} = (mn)a$$

случае, когда $n < 0$, имеем:

$$na = \underbrace{(-a) + \ldots + (-a)}_{|n|\ раз}$$

после чего доказательство заканчивается аналогично. Если же и $n < 0$ и $m < 0$, то надо еще воспользоваться равенством $-(-a) = a$.

Равенство (6) при натуральном $\square$ следует из того, что сложение в R коммутативно и ассоциативно, а потому

$$na + nb = \underbrace{a + \ldots + a}_{n\ раз} + \underbrace{b + \ldots + b}_{n\ раз} = \underbrace{(a + b) + \ldots + (a + b)}_{n\ раз} = n(a + b)$$

Случай $n < 0$ рассматривается аналогично, а при $n = 0$ обе части равенства равны нулю,

Перейдем теперь к изучению свойств умножения в кольцах. Сначала докажем, что для любого элемента a кольца R выполняются равенства:

$$a \cdot 0 = 0 \qquad (7)$$

и

$$0 \cdot a = 0. \qquad (8)$$

В самом деле, пусть $b \in R$. Тогда имеем:

$$ab + a \cdot 0 = a(b + 0) = ab,$$

Значит, $a \cdot 0 = ab - ab = 0$. Равенство $0 \cdot a = 0$ доказывается точно так же.

Теперь докажем правило знаков:

$$a(-b) = -ab, \quad (9)$$

$$(-a)b = -ab, \quad (10)$$

$$(-a)(-b) = ab. \quad (11)$$

В самом деле, в силу дистрибутивности умножения относительно сложения имеем:

$$ab + a(-b) = a[b + (-b)] = a \cdot 0 = 0.$$

Значит, элемент $a(-b)$ противоположен ab, т. е. $a(-b) = -ab$ Равенство (10) доказывается точно так же. Из (9) и (10) следует, что

$$(-a)(-b) = -a(-b) = -(-ab) = ab.$$

Наконец, докажем, что умножение в любом кольце дистрибутивно не только относительно сложения, но и относительно вычитания, т. е. что для любых трех элементов кольца $\boxed{\ }$ выполняются равенства:

$$a(b - c) = ab - ac \quad (12)$$

и

$$(b - c)a = ba - ca. \quad (13)$$

Так как $b - c = b + (-c)$, то

$$a(b - c) = a[b + (-c)] = ab + a(-c) = ab - ac,$$

Точно так же получаем, что

$$(b - c)a = [b + (-c)]a = ba + (-c)a = ba - ca.$$

Доказанные выше свойства умножения имеют место в любых кольцах. Если умножение в кольце $\boxed{\ }$ ассоциативно, то в силу общих свойств ассоциативных бинарных операций (см. п. приложения к главе II) для любого кортежа $(a_1, \ldots, a_n)$ элементов из $\boxed{\ }$ определено произведение $a_1, \ldots, a_n$, значение которого не зависит от расстановки скобок. В частности,

$$\prod_{k=1}^{m} a_k \cdot \prod_{k=m+1}^{m+n} a_k = \prod_{k=1}^{m+n} a_k . \qquad (14)$$

В ассоциативном кольце произведение n множителей, каждый из которых равен a, обозначают a^n. Справедливы формулы:

$$a^m \cdot a^n = a^{m+n} \qquad (15)$$

и

$$\left(a^m\right)^n = a^{mn}, \quad (16)$$

доказываемые, как в обычной алгебре.

Если кольцо K не только ассоциативно, но и коммутативно, то справедлива формула:

$$(ab)^n = a^n b^n . (17)$$

В коммутативном и ассоциативном кольце верна формула бинома Ньютона:

$$(a+b)^n = a^n C_n^1 a^{n-1} b + \ldots + C_n^k a^{n-k} b^k + \ldots + b^n . \qquad (18)$$

Подкольца.

Определение 4. Подмножество S кольца K называется подкольцом в K, если оно само является кольцом относительно тех же операций сложения и умножения, что и кольцо K. Чтобы проверить, является ли подмножество S кольца K подкольцом, достаточно убедиться в том, что:

а) сумма двух элементов a и b из S принадлежит S;

б) элемент $-a$, противоположный любому элементу a из S,принадлежит S;

в) произведение любых двух элементов из S принадлежит S.

В самом деле, условия а) и в) показывают, что сложение и умножие являются бинарными операциями в S. При этом сложение в S обладает свойствами ассоциативности и коммутативности, поскольку оно обладает этими свойствами и во всем кольце K. Поскольку в силу условия б) вместе с каждым элементом a в S входит и противоположный ему элемент $-a$ то S является группой относительно сложения. Наконец, умножение в S

дистрибутивно относительно сложения, поскольку это имеет место и во всем кольце . Тем самым доказано, что — кольцо, т. е. подкольцо в .

Заметим, что условия а) и б) можно заменить одним условием а') разность любых двух элементов из принадлежит .

В самом деле, из условия а') вытекает, что $0 \in S$, поскольку $0 = a - a$. Кроме того, если $a \in S$, то и $-a = 0 - 0 \in S$. Наконец, если $a \in S$, $b \in S$, то $a + b = a - (-b) \in S$. Значит, из условия а') вытекают и условие а), и условие б).

Числовые кольца — это подкольца поля C комплексных чисел. Поэтому, чтобы проверить, что множество комплексных чисел является числовым кольцом, достаточно убедиться, что:

а) разность любых двух элементов из принадлежит ;

б) произведение любых двух элементов из принадлежит .

Если кольцо ассоциативно, то любое его подкольцо тоже ассоциативно, а если коммутативно, то и любое его подкольцо коммутативно. Но из того, что содержит единицу, не следует, что любое подкольцо в содержит единицу. Например, кольцо Z содержит единицу, а его подкольцо, состоящее из четных чисел, не содержит единицы.

Примеры.

1. Покажем, что множество $Z[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, где и — целые числа, является кольцом. Для этого достаточно убедиться, что разность и произведение чисел такого вида имеют тот же самый вид. А это следует из равенств:

$$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2}$$

и

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1b_1 - 2a_2b_2) + (a_1b_2 - a_2b_1)\sqrt{2}.$$

2. Множество M чисел вида $a + b\sqrt[3]{2}$, где $a \in Z$, $b \in Z$, не является кольцом. В самом деле, $\sqrt[3]{2} \in M$, но $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \notin M$. Проверьте, что множество $Z[\sqrt[3]{2}]$ чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ где $a, b, c \in Z$ — кольцо.

3. Множество $Z[x]$ многочленов с целыми коэффициентами является подкольцом в $R[x]$ — кольце многочленов с действительными коэффициентами. Чтобы убедиться в этом, достаточно заметить, что разность и произведение многочленов с целыми коэффициентами имеют целые коэффициенты.

4. Множество M чисел вида $a + b\sqrt{2} + c\sqrt{3}$, где a,b,c целые числа, не является числовым кольцом, так как $\sqrt{2}\cdot\sqrt{3} = \sqrt{6} \in M$. Проверьте, что множество $Z\left[\sqrt{2},\sqrt{3}\right]$ чисел вида $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, где $a,b,c,d \in Z$, является кольцом

5. Матрицы n-го порядка с целыми элементами образуют подкольцо в кольце всех матриц n-го порядка с действительными элементами. Это вытекает из того, что разность и произведение матриц с целыми элементами имеют целые элементы.

6. Диагональные матрицы n-го порядка, т, е. матрицы вида

$$\begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & .. \\ 0 & \ldots & 0 & \lambda_n \end{pmatrix}$$

образуют подкольцо в кольце всех матриц n-го порядка. Это следует из того, что разность и произведение диагональных матриц – диагональные матрицы.

6. Характеристика кольца с единицей. Пусть $\boxed{\ }$ — кольцо с единицей e. Найдем в этом кольце наименьшее подкольцо, содержащее единицу. Из определения подкольца вытекает, что вместе с единицей e это подкольцо должно содержать и противоположный элемент $-e$, а также все суммы

$$ne = \underbrace{e + \ldots + e}_{n\ раз} \quad \text{и} \quad -ne = \underbrace{(-e) + \ldots + (-e)}_{n\ раз}.$$

11ными словами, искомое подкольцо должно содержать все элементы вида ne, где $n \in Z$. Но разность двух таких элементов, а также их произведение являются элементами того же вида:

$ne - me = (n - m)e$, $(ne)(me) = nmee = nme$.

Тем самым доказано, что множество элементов вида ne является подкольцом в $\boxed{}$, причем это— наименьшее подкольцо в $\boxed{}$, содержащее единицу e.

Возможны два случая:

а) ни один из элементов ne, где $n \neq 0$, не равен нулю:

$n \neq 0 \rightarrow ne \neq 0$;

б) существует такое $\boxed{n \neq 0}$, что $ne = 0$. В этом случае и $-ne = 0$, а потому, не теряя общности, можно считать, что $n > 0$. В множестве A натуральных чисел m, таких, что $me = 0$, существует наименьшее число.

Определение 5. Характеристикой кольца с единицей R называется нуль, если при $\boxed{n \neq 0}$ имеем $ne \neq 0$, и наименьшее натуральное число, для которого $ne = 0$, в противном случае.

Характеристика любого числового кольца равна нулю. Примеры колец с ненулевой характеристикой будут приведены ниже.

Теорема 1. Если $\boxed{}$ — кольцо характеристики n, то для нового элемента $a \in R$ имеем $na = 0$.

Доказательство. Теорема вытекает из того, что

$na = n(ea) = (ne)a = 0$.

7. Отношение делимости в кольцах. Мы уже говорили выше, что кольца являются естественной областью для построения теории делимости. При этом мы будем рассматривать лишь ассоциативные и коммутативные кольца с единицей. Таким образом, до конца параграфа слово «кольцо» будет обозначать ассоциативное и коммутативное кольцо с единицей.

Определение 6. Элемент a кольца $\boxed{}$ делится на элемент $b \neq 0$ того же кольца, если существует такой элемент $q \in R$, что $a = bq$. В этом случае пишут $a \vdots b$. Элемент b называется делителем пемента $\boxed{}$.

Примеры.

1. В кольце $R[x]$ многочленов с действительными коэффициентами отношение делимости совпадает с обычным отношением делимости для многочленов: многочлен $f(x)$ делится на многочлен $\varphi(x)$, если существует

такой многочлен $q(x)$, что $f(x) = \varphi(x) \cdot q(x)$.Например, $x^4 - 16$ делится на $x^2 - 4$, так как $x^4 - 16 = (x^2 - 4) \times (x^2 - 4)$,

2. В кольце Zi целых гауссовых чисел $23 + 2i$ делится на $2 + 3i$. В самом деле,

$\frac{23 + 2i}{2 + 3i} = \frac{(23 + 2i)(2 - 3i)}{(2 + 3i)(2 - 3i)} = \frac{52 + 65i}{13} = 4 - 5i$, а $4 - 5i \in Z[i]$.

3. Точно так же доказывается, что в кольце $Z[\sqrt{3}]$ число $-7 + 18\sqrt{3}$ делится на $4 + \sqrt{3}$:

$\frac{-7 + 18\sqrt{3}}{4 - \sqrt{3}} = \frac{(-7 + 18\sqrt{3})(4 + \sqrt{3})}{(4 - \sqrt{3})(4 + \sqrt{3})} = \frac{26 + 65\sqrt{3}}{13} = 2 + 5\sqrt{3} \in Z[\sqrt{3}]$.

4. Докажем, что в кольце $Z[\sqrt[3]{2}]$, состоящем из чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — целые числа, $-19 + 10\sqrt[3]{2} + 20\sqrt[3]{4}$ делится на $1 - 3\sqrt[3]{2} + 5\sqrt[3]{4}$. Для этого надо найти число $x + y\sqrt[3]{2} + z\sqrt[3]{2}$ из $Z[\sqrt[3]{2}]$, такое, что $(1 - 3\sqrt[3]{2} + 5\sqrt[3]{4})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = -19 + 10\sqrt[3]{2} + 20\sqrt[3]{4}$

Раскрывая скобки, получаем, что

$x + 10y - 6z + (3x + y + 10z)\sqrt[3]{2} + (5x - 3y + z)\sqrt[2]{4} = -19 + 10\sqrt[3]{2} + 20\sqrt[3]{4}$

Это равенство может иметь место лишь при условии, что x, y, z удовлетворяют системе уравнений:

$$\begin{cases} x + 10y - 6z = -19 \\ -3x + y + 10z = 10 \\ 5x - 3y + z = 20 \end{cases}$$

Решая эту систему, получаем, что $x = 3$, $y = -1$, $z = 2$. Значит, $-19 + 10\sqrt[3]{2} + 20\sqrt[3]{4} = (1 - 3\sqrt[3]{2} + 5\sqrt[3]{4})(3 - \sqrt[3]{2} + 2\sqrt[3]{4})$. А число $-18 + 10\sqrt[3]{2} + 20\sqrt[3]{4}$ не делится на $1 - 3\sqrt[3]{2} + 5\sqrt[3]{4}$. В этом случае мы получили бы систему уравнений:

$$\begin{cases} x + 10y - 6z = -18 \\ -3x + y + 10z = 10 \\ 5x - 3y + z = 20 \end{cases},$$

имеющую дробные решения.

5. В поле P любой элемент $\square$ делится на любой отличный от нуля элемент $\square$. В самом деле, если $b \neq 0$, то существует элемент b^{-1}, обратный $\square$, т. е. такой, что $b \cdot b^{-1} = e$. А тогда имеем: $a = b(ab^{-1})$. Так как $ab^{-1} \in P$ то $a \vdots b$.

Многие свойства отношения делимости в кольце целых чисел Z сохраняются для любых колец (напомним еще раз, что мы рассматриваем лишь ассоциативные и коммутативные кольца с единицей). Именно, справедливы следующие утверждения:

1) Отношение делимости рефлексивно, т. е. для любого $a \in R$, $a \neq 0$ имеем $a \vdots a$.

В самом деле, $a = ae$ (по условию $e \in R$).

2) Отношение делимости транзитивно: если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.

В самом деле, если $a \vdots b$, то существует такое $q \in R$, что $a = bq$. А так как $b \vdots c$, то существует такое $s \in R$, что $b = cs$. Но тогда мы имеем:

$a = bq = (cs)q$.

В силу ассоциативности кольца $\square$ получаем, что $a = c(sq)$. А это и означает, что $a \vdots c$.

3) Если $a \vdots c$ и $b \in R$, то $ab \vdots c$,

В самом деле, так как $a \vdots c$, то существует такое $q \in R$, что $a = cq$. А тогда имеем: $ab = (cq)b$. В силу ассоциативности кольца $\square$ получаем, что $ab = c(qb)$. Так как $qb \in R$, то $ab \vdots c$.

4) Если $a \vdots c$ и $b \vdots c$, то $(a \pm b) \vdots c$.

В самом деле, $a = cq$, $b = cs$, где $q \in R$ и $s \in R$. А тогда имеем:

$a \pm b = cq \pm cs = c(q \pm s)$.

Так как $(q \pm s) \in R$, то $(a \pm b) \vdots c$

Если $a \vdots c$, а $\square$ не делится на c, то $a \pm b$ не делится на c.

Нуль делится на любой отличный от нуля элемент $\square$ кольца $\square$.

В самом деле, $0 = 0 \cdot b$.

7) Любой элемент a кольца R делится на единицу e. В самом деле, $a = e \cdot a$.

8. Обратимые элементы. Чтобы сформулировать дальнейшие свойства отношения делимости в кольцах, введем понятие обратимого элемента.

Определение 7. Элемент ε кольца R называется обратимым, если в R существует такой элемент ε_1 что $\varepsilon\varepsilon_1 = e$.

Примеры.

В кольце Z целых чисел обратимыми являются числа 1 и -1. Других обратимых чисел в Z нет, так как единственными делителями числа 1 являются 1 и -1.

В кольце $Z[i]$ целых гауссовых чисел 4 обратимых элемента: 1, -1, i и $-i$. Других обратимых элементов в $Z[i]$ нет. В самом деле, если элемент $(a+bi) \in Z[i]$ обратим, то найдется число $(c+di) \in Z[i]$, такое, что $(a+bi)(c+di) = 1$.

Но тогда и $|a+bi|^2|c+di|^2 = 1$, т. е.

$(a^2+b^2)(c^2+d^2) = 1$.(1)

Так как a,b,c,d — целые числа и $(a^2+b^2) > 0$, то равенство (1) может иметь место лишь при условии, что $a^2+b^2 = 1$, т. е. в одном из четырех случаев: $a = 1$, $b = 0$; $a = -1$, $b = 0$; $a = 0$, $b = 1$; $a = 0$, $b = -1$. Это и означает, что $a+bi$ может иметь лишь четыре значения: 1, -1, i и $-i$.

3. Аналогичным образом ищут обратимые элементы в кольце $Z[\sqrt{3}]$ чисел вида $a+b\sqrt{3}$ где a и b — целые числа. Если число $a+b\sqrt{3}$ обратимо, то

$(a+b\sqrt{3})(c+d\sqrt{3}) = 1$. (2)

Раскрывая скобки, получаем, что $ac+3d^2 = 1$ и $ad+bc = 0$. Но тогда и

$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3d^2) - (ad+bc)\sqrt{3} = 1$. (3)

Перемножая равенства (2) и (3), получаем, что $(a^2-3b^2)(c^2-3d^2) = 1$.

Значит, a^2-3b^2 является целым делителем единицы, и потому $a^2-3b^2 = \pm 1$. Четыре решения этого уравнения находятся сразу: $a = 2$, $b = 1$; $a = 2$, $b = -1$;

$a=-2$, $b=1$; $a=-2$, $b=-1$. Значит, числа $\pm(2+\sqrt{3})$, $\pm(2-\sqrt{3})$ обратимы в $Z[\sqrt{3}]$. Но числа $(2+\sqrt{3})^n$ и $(2-\sqrt{3})^n$ при любом натуральном значении n тоже обратимы в $Z[\sqrt{3}]$, так как

$(2+\sqrt{3})^n(2-\sqrt{3})^n=(4-3)^n=1$.

Можно показать, что множество всех обратимых чисел кольца $Z[\sqrt{3}]$ состоит из элементов вида $\pm(2+\sqrt{3})^n$ где n — целое число (в частности, при $n=0$ получаем число 1, а при $n=-1$ число $2-\sqrt{3}$).

4. В кольце $R[x]$ многочленов с действительными коэффициентами обратимыми являются многочлены нулевой степени, т. е. отличные от нуля действительные числа.

Выясним теперь роль обратимых элементов при делении элементов кольца. В кольце Z целых чисел отношение делимости не нарушилось при умножении делителя на -1, т. е. на обратимый элемент. Аналогичное утверждение верно в любом кольце.

Если $a \vdots b$ и элемент ε обратим в R, то $a \vdots b\,\varepsilon$.

В самом деле, так как $a \vdots b$, то существует такой элемент q, что $a=bq$. А так как ε обратим в R, то существует такой элемент $\varepsilon_1 \in R$, что $\varepsilon\cdot\varepsilon_1=e$. А тогда имеем:

$a=(b\varepsilon\varepsilon_1)q=(b\varepsilon)(\varepsilon_1 q)$.

Это равенство показывает, что $a \vdots b\varepsilon$. Утверждение доказано.

Заметим, что (в силу свойства 3 отношения делимости в кольцах) если $a \vdots b$, то и $a\varepsilon \vdots b$.

Докажем следующую теорему об обратимых элементах любого кольца.

Теорема 2. Множество $\widetilde{R}$ обратимых элементов кольца R образует коммутативную группу относительно умножения.

Доказательство. Так как по условию кольцо R коммутативно, ассоциативно и обладает единицей, то для доказательства теоремы нам достаточно показать справедливость двух утверждений:

а) произведение двух обратимых элементов обратимо в R;

б) если ε — обратимый элемент в R, то и ε^{-1} обратимо в R.

Пусть δ и ε обратимы в R. Тогда существуют такие элементы δ_1 и ε_1 в R, что $\delta\delta_1 = e$ и $\varepsilon\varepsilon_1 = e$. Но тогда имеем:

$$(\delta\varepsilon)(\delta_1\varepsilon_1) = (\delta\delta_1)(\varepsilon\varepsilon_1) = e \cdot e = e.$$

Значит, $\delta\varepsilon$ тоже обратимо в R. Этим доказано утверждение а) Утверждение же б) сразу следует из того, что если $\varepsilon\varepsilon_1 = e$, то не только ε, но и $\varepsilon_1 = \varepsilon^{-1}$ обратимо в R.

Группу J называют группой обратимых элементов кольца R. Единичным элементом группы J является единица e кольца R. Предоставляем читателю проверить, что во всех разобранных выше примерах множество обратимых элементов действительно является коммутативной группой относительно операции умножения.

9. Области целостности. Мы видели, что многие свойства отношения делимости в кольце целых чисел сохраняются и для отношения делимости в любом кольце. Но в произвольном кольце нельзя говорить о частном двух элементов даже в случае, когда a делится на b. Дело в том, что в некоторых кольцах деление неоднозначно, т. е. для некоторых элементов $a \in R$, $b \in R$ можно найти несколько элементов q, таких, что $a = bq$. Мы хотим выделить класс колец, в которых имеет смысл говорить и о частном двух элементов. Определение 8. Отличный от нуля элемент a кольца R называется делителем нуля в R, если в R существует отличный от нуля элемент b, такой, что $ab = 0$ (разумеется, в этом случае и элемент b является делителем нуля в R).

Определение 9. Кольцо $\square$ называется областью целостности, если в нем нет делителей нуля.

Иными словами, кольцо $\square$ является областью целостности, если из $ab = 0$ следует, что $a = 0$ или $b = 0$:

$ab = 0 \to a = 0 \vee b = 0$.

Примеры.

1. Пусть R^2 — кольцо, состоящее из пар (a,b) действительных чисел, в котором сложение и умножение определяются «покоординатно»:

$(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$ и $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2)$.

Элементы $(1,0)$ и $(0,1)$ кольца $\square$ отличны от нулевого элемента $(0,0)$, но $(1,0)(0,1) = (0,0)$. Значит, эти элементы-делители нуля в $\square$, и потому $\square$ не является областью целостности.

Любое поле является областью целостности. В самом деле, если P — поле и $a \in P$, $a \neq 0$, то существует элемент a^{-1}, обратный $\square$. Если $ab = 0$, то $a^{-1}(ab) = 0$, т. е. $b = 0$. Значит, равенство $ab = 0$ может выполняться лишь при условии, что $a = 0$ или $b = 0$. Это и значит, что P — область целостности.

Так как множество C комплексных чисел является полем, то в C нет делителей нуля. А тогда их нет и ни в каком числовом кольце. Значит, любое числовое кольцо является областью целостности. В частности, областями целостности являются кольцо $Z[i]$ целых гауссовых чисел, кольцо $Z[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, $a,b \in Z$ и т. д. Разумеется, областью целостности является и кольцо Z целых чисел.

Кольцо многочленов $P[x]$ с коэффициентами из числового поля P является областью целостности. Это вытекает из того, что при умножении многочленов их степени складываются, а потому произведение двух отличных от нуля многочленов не может равняться нулю.

Кольцо $C[a,b]$ функций, непрерывных на отрезке $[a,b]$ не является областью целостности. В самом деле, если функция $f(x)$ отлична от нуля лишь на промежутке (a,c), а функция $\varphi(x)$ — лишь на промежутке (b,c), то их произведение $f(x)\varphi(x)$ равно нулю на всем отрезке $[a,b]$. Например, можно положить

$$f(x) = \begin{cases} (x-a)(c-x), & a \le x \le c \\ 0, & c < x \le b \end{cases}$$

$$\varphi(x) = \begin{cases} 0, & a \le x \le c \\ (x-a)(c-x), & c < x \le b \end{cases}.$$

Свойства отношения делимости в областях целостности.

Теорема 3. Если $\square$ — отличный от нуля элемент области целостности $\square$, то из равенства $ab = ac$, где $b,c \in R$, следует, что $b = c$.

Иными словами, в областях целостности можно сокращать обе части равенства на отличный от нуля элемент.

Доказательство. Из равенства $ab = ac$ следует, что $a(b-c) = 0$, Поскольку по условию $a \neq 0$, а $\square$ не содержит делителей нуля, то равенство $a(b-c) = 0$ может иметь место лишь при условии, что $b-c = 0$, т. е. что $b = c$. Теорема доказана.

Из теоремы 3 вытекает, что если $\square$ и $b \neq 0$ — элементы области целостности $\square$, причем $a \vdots b$, то в $\square$ существует единственный элемент q, такой, что $a = bq$. В самом деле, если $a = bq$ и $a = bs$, то $bq = bs$, и поскольку $b \neq 0$, то $q = s$

.

Определение 10. Если $\square$ — область целостности и $a \vdots b$, то единственный элемент $q \in R$, такой, что $a = bq$, называют частным от деления $\square$ на $\square$.

В кольце целых чисел Z из отношений $a \vdots b$, $b \vdots a$ следует, что $a = b$ или $a = -b$, т. е. $\square$ и $\square$ отличаются друг от друга лишь обратимым множителем. По аналогии введем следующее определение:

Определение 11. Элементы a и b области целостности R называются ассоциированными в R, если существует обратимый элемент $\varepsilon \in R$, такой, что $a = b\varepsilon$.

Например, числа 5 и -5 ассоциированы в кольце Z целых чисел. А числа $5+2\sqrt{3}$ и $4-\sqrt{3}$ ассоциированы в кольце $Z[\sqrt{3}]$ мсел вида $a+b\sqrt{3}$, a, $b \in Z$. В самом деле, мы видели (см. стр. 76), что $2-\sqrt{3}$ обратимо в $Z[\sqrt{3}]$, а $4-\sqrt{3} = (5+2\sqrt{3})(2-\sqrt{3})$.

Бинарное отношение «элемент a ассоциирован с элементом b в кольце целостности R» является отношением эквивалентности — оно рефлексивно, симметрично и транзитивно. В самом деле, a ассоциировано с a, так как $a = ae$, а e обратимо в R. Далее, пусть a ассоциировано с b. Тогда есть такой обратимый элемент ε, что $a = bs$. Но в R есть такой обратимый элемент ε_1, что $\varepsilon\varepsilon_1 = e$. Умножая обе части равенства $a = b\varepsilon$ на ε_1 получаем, что $a\varepsilon_1 = b$. Это показывает, что b ассоциировано с a. Значит, отношение ассоциированности симметрично. Наконец, если a ассоциировано с b, а b ассоциировано с c, то $a = b\delta$, $b = c\varepsilon$, где δ и ε — обратимые в R. А тогда

$$a = b\delta = (c\varepsilon)\delta = c(\varepsilon\delta).$$

Но элемент $\varepsilon\delta$ обратим в силу теоремы 2 п. 8. Значит, a ассоциировано с c. Этим доказана транзитивность отношения ассоциированности.

В п. 8 было доказано, что если $a \vdots b$ и элемент ε обратим в R, то $a \vdots b\varepsilon$ и $a\varepsilon \vdots b$. Отсюда вытекает следующее утверждение:

Если a ассоциировано с a_1, а b – с b_1 и $a \vdots b$, то $a_1 \vdots b_1$.

В самом деле, $a_1 = a\delta$, $b_1 = b\varepsilon$, где δ и ε — обратимые элементы, а из $a \vdots b$ следует, что $a\delta \vdots b\varepsilon$, т. е. что $a_1 \vdots b_1$.

Теорема 4. Для того чтобы в области целостности [1] выполнялись отношения $a \vdots b$ и $b \vdots a$, необходимо и достаточно, чтобы элементы [2] и [3] были ассоциированы в [4].

Доказательство. Сначала докажем достаточность условия. Пусть элементы [5] и [6] ассоциированы. Так как $a \vdots a$, то из ассоциированности [7] и [8] следует в силу доказанного выше, что $a \vdots b$. Точно так же из $a \vdots a$ и ассоциированности [9] и [10] следует, что $b \vdots a$.

Значит, из ассоциированности [11] и [12] вытекают оба отношения делимости: $a \vdots b$ и $b \vdots a$.

Теперь докажем необходимость этого условия, т. е. докажем, что из [13] и [14] вытекает ассоциированность элементов [15] и [16] в [17]. Так как [18], то в [19] найдется такой элемент δ, что $a = b\delta$, а так как [20], то в [21] найдется такой элемент ε, что $b = a\varepsilon$. Для доказательства ассоциированности [22] и [23] осталось показать, что элементы δ и ε обратимы в [24]. Для этого перемножим почленно равенства $a = b\delta$ и $b = a\varepsilon$. Мы получим $ab = ab\delta\varepsilon$, откуда следует, что $ab(e - \delta\varepsilon) = 0$. Так как по условию [25] — область целостности и $a \neq 0$, $b \neq 0$, то $ab \neq 0$, а тогда из $ab(e - \delta\varepsilon) = 0$ следует, что $(e - \delta\varepsilon) = 0$, т. е. $\delta\varepsilon = e$. Это и показывает, что δ и [26] обратимы в [27]. Теорема доказана.

Простые и составные элементы области целостности.

Определение 12. Элемент [28] области целостности [29] называется простым в [30], если он не обратим в [31], а любой делитель [32] элемента [33] либо обратим в [34], либо ассоциирован с [35].

Это определение можно сформулировать так: элемент [36] области целостности [37] является простым, если он не обратим в [38], а любое разложение [39] на два множителя имеет вид $a = bc$, где один из элементов [40], с обратим в [41], а второй ассоциирован с [42].

Определение 13. Элемент a области целостности R называется составным, если он допускает разложение на множители $a = bc$, причем ни b, ни c не обратимы в R.

Таким образом, все элементы области целостности R распадаются на четыре класса: нуль, обратимые элементы, простые элементы и составные элементы.

Ясно, что элемент, ассоциированный с простым элементом a, является простым, а ассоциированный с составным элементом — составным (напомним, что умножение на обратимые элементы не изменяет отношения делимости).

Одно и то же число может оказаться простым в одном кольце и составным в другом кольце. Например, число 5 просто в кольце Z целых чисел. А в кольце $Z[i]$ целых гауссовых чисел оно является составным, так как $5 = (1+2i)(1-2i)$.

Одной из задач, вызвавших построение теории колец, была задача о разложении на простые множители в числовых кольцах. Оказалось, что в некоторых числовых кольцах дело обстоит примерно так же, как в кольце целых чисел, т. е. любое составное число разлагается на простые множители, причем это разложение по сути дела однозначно определено (смысл этих слов будет уточнен ниже), в других числовых кольцах разложение на простые множители существует, но некоторые числа могут иметь несколько существенно различных разложений, а в третьих кольцах есть числа, не имеющие разложений на простые множители.

Уточним, что мы будем понимать под словами «разложение элемента a области целостности R на простые множители однозначно определено». Во-первых, мы знаем, что эти множители можно переставлять друг с другом. Но, кроме того, можно умножить один из простых множителей на какой-нибудь обратимый элемент ε, а другой — на такой обратимый элемент ε_1, что $\varepsilon\varepsilon_1 = e$. Тогда оба множителя останутся простыми, произведение же не

изменится. Ясно, что полученное разложение не следует считать отличающимся от исходного. Итак, введем следующее определение:

Определение 14. Два разложения

$$a = p_1 \dots p_n \quad \text{и} \quad a = s_1 \dots s_m$$

элемента $\square$ области целостности $\square$ на простые множители по существу одинаковы, если они содержат одинаковое число множителей и могут быть переведены друг в друга перестановкой множителей и умножением их на обратимые элементы.

Примеры.

1. В кольце $Z[i]$ целых гауссовых чисел существуют такие разложения для 5 на простые множители:

$\boxed{5 = (1+2i)(1-2i)}$ и $5 = (-1+2i)(-1-2i)$

Эти разложения по существу одинаковы, так как второе разложение получается из первого умножением первого множителя на обратимый элемент i, а второго на обратимый элемент $-i$.

2. В кольце $Z[\sqrt{3}]$ чисел вида $a+b\sqrt{3}$, $\square$, $b \in Z$ разложения

$13 = (4-\sqrt{3})(4+\sqrt{3})$ и $5 = (5-2\sqrt{3})(5+2\sqrt{3})$

по существу одинаковы, так как второе разложение получается из первого следующим образом: первый множитель умножается на обратимый элемент $2+\sqrt{3}$, второй — на обратимый элемент $2-\sqrt{3}$, после чего множители переставляются.

3. В кольце $Z[\sqrt{-3}]$ чисел вид $a+b\sqrt{-3}$, $\square$, $b \in Z$ число 4 разлагается на множители следующими способами:

$4 = 2 \cdot 2$ и $4 = (1+\sqrt{-3})(1-\sqrt{-3})$.

Можно доказать (мы опускаем здесь это доказательство), что числа 2, $1+\sqrt{-3}$, $1-\sqrt{-3}$ просты в $Z[\sqrt{-3}]$, причем 2 и $1+\sqrt{-3}$ не являются ассоциированными.

Значит, в кольце $Z[\sqrt{-3}]$ число 4 допускает два существенно различных разложения на простые множители.

4. Обозначим через $\square$ числовое кольцо, состоящее из конечных сумм вида $\sum a_r 2^r$, где a_r — целые числа и r неотрицательные рациональные числа (при этом, например, $3\cdot 2^{\frac{3}{2}} - 4\cdot 2^{\frac{1}{2}}$ и $2\cdot 2^{\frac{1}{2}}$ – один и тот же элемент кольца, поскольку $2^{\frac{3}{2}} = 2\cdot 2^{\frac{1}{2}}$, и потому $3\cdot 2^{\frac{3}{2}} - 4\cdot 2^{\frac{1}{2}} = 2\cdot 2^{\frac{1}{2}}$). Так как $\square$ — числовое кольцо, оно является областью целостности. В этом кольце для числа 2 имеем бесконечную последовательность разложений:

$$2 = 2^{\frac{1}{2}}\cdot 2^{\frac{1}{2}} = 2^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot 2^{\frac{1}{4}} = 2^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot 2^{\frac{1}{8}}\cdot 2^{\frac{1}{8}} = \ldots$$

Значит, число 2 не имеет в $\square$ разложения на простые множители.

Разобранные примеры показывают, что вопрос о разложении на простые множители в произвольных числовых кольцах сложнее, чем в кольце Z целых чисел. Причиной этого является то, что в произвольных числовых кольцах два элемента $\square$ и $\square$ могут не иметь наибольшего общего делителя, т. е. такого общего делителя $\square$ и $\square$, который бы делился на все общие делители этих чисел. Чтобы найти выход из создавшегося положения, обобщили понятие делимости элементов. Это привело к созданию теории идеалов, которая и будет рассмотрена в следующем параграфе. С помощью теории идеалов удалось выяснить, в каких кольцах имеет место теорема о существовании и однозначности разложения на простые множители.

ПОСТРОЕНИЕ ПОЛЯ КОМПЛЕКСНЫХ ЧИСЕЛ

Известно, что уравнение $x^2 + 1 = 0$ не имеет корней в поле действительных чисел $\boldsymbol{R}$. Расширим поле $\boldsymbol{R}$ до такого поля, в котором это уравнение разрешимо.

Рассмотрим множество упорядоченных пар действительных чисел

$$\boldsymbol{C} = \{(a,b)/a,b \in R\}.$$

Будем считать две пары (a,b) и (c,d) равными, если $a = c$ и $b = d$.

Введем на множестве $\boldsymbol{C}$ операции сложения + и умножения $\cdot$ так, чтобы они были бинарными алгебраическими операциями

$$(a,b)+(c,d)=(a+c,b+d)\in \boldsymbol{C},$$

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)\in \boldsymbol{C}.$$

Покажем обратимость сложения и умножения. Для этого необходимо рассмотреть уравнения

$$(a,b)+(x,y)=(c,d),\ (a+x,b+y)=(c,d)$$

и показать, что они имеют решения во множестве $\boldsymbol{C}$.

Из уравнения $(a,b)+(x,y)=(c,d)$ следует, что $a+x=c$ и $b+y=d$, а данные уравнения в поле $\boldsymbol{R}$ имеют единственные решения $x=c-a\in \boldsymbol{R}$ и $y=d-b\in \boldsymbol{R}$. Значит, $(x,y)=(c-a,d-b)\in \boldsymbol{C}$.

Из уравнения $(a,b)\cdot(x,y)=(c,d)$ следует, что $(ax-by,ay+bx)=(c,d)$, а значит, $ax-by=c$ и $ay+bx=d$. Решая систему

$$\begin{cases} ax-by=c \\ bx+ay=d \end{cases}$$

по формулам Крамера, получим

$$x=\frac{\begin{vmatrix} c & -b \\ d & a \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}}=\frac{ac+bd}{a^2+b^2}\in R \text{ и } y=\frac{\begin{vmatrix} a & c \\ b & d \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}}=\frac{ad-cb}{a^2+b^2}\in R \text{ при } a,b\neq 0,$$

$$(x,y)=\left(\frac{ac+bd}{a^2+b^2};\frac{ad-cb}{a^2+b^2}\right)\in C.$$

Убедившись в обратимости операций + и $\cdot$, можно сделать вывод о замкнутости множества $\boldsymbol{C}$ относительно основных арифметических операций. Следовательно, множество $\boldsymbol{C}$ является числовым полем. Элементы этого поля можно изобразить в виде точек декартовой плоскости с координатами (*a,b*).

Рассмотрим подмножество $\bar{R}=\{(a,0)/a\in R\}$ с заданными операциями + и $\cdot$:

$$(a,0)+(b,0)=(a+b,0),$$

$$(a,0)-(b,0)=(a-b,0),$$

$$(a,0)\cdot(b,0)=(ab,0),$$

$$\frac{(a,0)}{(b,0)}=\left(\frac{a}{b},0\right).$$

Данное подмножество само является числовым полем.

Построим отображение $\varphi: \bar{R} \to R$ по правилу $\varphi(a,0)=a$. Оно является взаимно – однозначным (если $(a,0)=(b,0)$, то $\varphi(a,0)=\varphi(b,0)$) и сохраняющим операции + и ·

($\varphi\boxed{(a,0)+(b,0)=\varphi(a+b,0)=a+b=\varphi(a,0)+\varphi(b,0)}$ и

$\varphi((a,0)(b,0))=\varphi(ab,0)=a\cdot b=\varphi(a,0)\cdot\varphi(b,0)$).

Следовательно, данное отображение φ является изоморфным и можно отождествить множества R и $\bar{R}$, т.е. $\boxed{(a,0)=a}$. Тогда любую пару (a,b) из множества $\boldsymbol{C}$ представим в виде суммы пар

$$(a,b)=(a,0)+(0,b)=(a,0)+(b,0)(0,1)=a+bi,$$

где пара $(0,1)=i$ не является элементом множества $\bar{R}$, значит, его нельзя отождествить ни с одним из действительных чисел. Это число нового качества, для которого верно равенство

$$(0,1)\cdot(0,1)=i\cdot i=(0\cdot 0-1\cdot 1,0\cdot 1+1\cdot 0)=(-1,0)=-1.$$

Назовем число i *мнимой единицей*, а числа вида $a+bi$ – *алгебраической формой комплексного числа*.

Таким образом, рассмотренное множество $\boldsymbol{C}=\{(a,b)/a,b\in R\}=$ $=\{a+bi/a,b\in R\}$ – *множество комплексных чисел* содержит число i, являющееся корнем квадратного уравнения $x^2+1=0$.

§7. ДЕЙСТВИЯ НАД КОМПЛЕКСНЫМИ ЧИСЛАМИ

В АЛГЕБРАИЧЕСКОЙ ФОРМЕ

Пусть $z=\boxed{a+bi}$ – алгебраическая форма комплексного числа, где a – действительная часть $a=\operatorname{Re} z$, а bi – мнимая часть комплексного числа $b=\operatorname{Im} z$. Величина равная $\sqrt{a^2+b^2}$ называется *модулем комплексного числа* и обозначается $|a+bi|$ или $|z|$.

Два комплексных числа $a+bi$ и $c+di$ равны, если равны их действительные и мнимые части, т.е. $a=b$ и $c=d$.

При сложении комплексных чисел складывают отдельно их действительные и мнимые части

$$(a+bi)+(c+di)=(a+c)+(b+d)i.$$

Аналогичное правило существует и для вычитания

$$(a+bi)-(c+di)=(a-c)+(b-d)i.$$

Для умножения комплексных чисел в алгебраической форме необходимо выполнить следующие действия

$$(a+bi)(c+di)=ac+adi+cbi+bdi^2=(ac-bd)+(ad+cb)i.$$

Число, *сопряженное* числу $z=a+bi$ – это число $\bar{z}=a-bi$, для которого верны соотношения $z+\bar{z}=2a$ и

$z\bar{z}=(a+bi)(a-bi)=a^2-(bi)^2=a^2+b^2=|z|$.

Пример. Доказать, что $\overline{z_1+z_2}=\overline{z_1}+\overline{z_2}$.

Решение. Пусть $z_1=x_1+y_1i$ и $z_2=x_2+y_2i$ – данные комплексные числа, а

$\overline{z_1}=x_1-y_1i$ и $\overline{z_2}=x_2-y_2i$ – им сопряженные комплексные числа. Тогда

$\overline{z_1+z_2}=\overline{(x_1+y_1i)+(x_2+y_2i)}=\overline{(x_1+x_2)+(y_1+y_2)i}=(x_1+x_2)-(y_1+y_2)i=$

$=(x_1-y_1i)+(x_2-y_2i)=\overline{z_1}+\overline{z_2}$.

Кроме этого свойства комплексно – сопряженные числа удовлетворяют следующим свойствам:

1) $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$;

2) $z^{-1} = \dfrac{\overline{z}}{|z|^2}$;

3) $\overline{\overline{z}} = z$;

4) $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$;

5) $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z_1}}{\overline{z_2}}$.

При делении комплексных чисел числитель и знаменатель данной дроби умножают на число, сопряженное знаменателю:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

Извлечение квадратного корня

из алгебраической формы комплексного числа

$\sqrt{a+bi} = x+yi$

$a+bi = (x+yi)^2$

$a+bi = x^2+2xyi+(yi)^2 = (x^2-y^2)+2xyi$, отсюда справедлива система уравнений:

$$\begin{cases} x^2-y^2=a \\ 2xy=b \end{cases} \Rightarrow \begin{cases} (x^2-y^2)^2=a^2 \\ 4x^2y^2=b^2 \end{cases} \Rightarrow \begin{cases} x^2-y^2=a \\ x^4-2x^2y^2+y^4+4x^2y^2=a^2+b^2 \end{cases} \Rightarrow$$

$$\begin{cases} x^2-y^2=a \\ x^4+2x^2y^2+y^4=a^2+b^2 \end{cases} \Rightarrow \begin{cases} x^2-y^2=a \\ (x^2+y^2)^2=a^2+b^2 \end{cases} \Rightarrow (\text{т.к. } x^2+y^2>0)$$

$$\begin{cases} x^2-y^2=a \\ x^2+y^2=\sqrt{a^2+b^2} \end{cases}.$$

При сложении уравнений последней системы получаем

$$2x^2 = a+\sqrt{a^2+b^2},\ x_{1,2} = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}},$$

а при вычитании уравнений последней системы получаем

$$2y^2 = -a + \sqrt{a^2 + b^2}\ ,\ y_{1,2} = \pm\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\ .$$

Так как $2xy = b$, то при $b>0$ x и y имеют одинаковые знаки, а при $b<0$ x и y имеют различные знаки.

Итак, $\sqrt{a + bi} = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \pm i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$ – формула извлечения квадратного корня из алгебраической формы комплексного числа при $b>0$;

$\sqrt{a + bi} = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \mp i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$ – формула извлечения квадратного корня из алгебраической формы комплексного числа при $b<0$;

ТРИГОНОМЕТРИЧЕСКАЯ ФОРМА КОМПЛЕКСНОГО ЧИСЛА

Любое комплексное число $z = a + bi$ можно изобразить точкой $M(a,b)$ на плоскости OXY.

Плоскость, на которой изображаются комплексные числа, называются комплексной плоскостью. Ось абсцисс называют действительной осью, а ось ординат – мнимой.

Комплексное число $\boxed{z = a + bi}$ можно изобразить и с помощью радиус–вектора $\vec{OM} = (a,b)$. Длина радиус–вектора, изображающего комплексное число z, называется модулем этого числа, обозначается $|z|$ или ρ и однозначно определяется по формуле $|z| = \rho = \sqrt{a^2 + b^2}$.

Величина угла φ между положительным направлением действительной оси и вектором $\vec{OM}$, изображающим комплексное число, называется аргументом этого числа и обозначается $\arg z$.

Аргумент φ определяется из формул $\cos\varphi = \frac{a}{\rho}$, $\sin\varphi = \frac{b}{\rho}$, где $\rho = \sqrt{a^2 + b^2}$. И так как аргумент комплексного числа $z \neq 0$ величина

многозначная: $\arg z = \varphi + 2\pi k,\ k = 0,\pm 1,\pm 2,...,$ то в качестве аргумента можно брать величину из промежутка $[0;2\pi)$.

Запись числа z в виде $z = a + bi = \rho\cos\varphi + \rho\sin\varphi \cdot i = \rho(\cos\varphi + i\sin\varphi)$ называется тригонометрической формой комплексного числа.

А запись числа z в виде $z = |z|e^{i\varphi}$ называется показательной формой комплексного числа.

ДЕЙСТВИЯ НАД КОМПЛЕКСНЫМИ ЧИСЛАМИ В ТРИГОНОМЕТРИЧЕСКОЙ ФОРМЕ

Даны два комплексных числа в тригонометрической форме $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1),\ z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2)$

$$z_1 z_2 = \rho_1(\cos\varphi_1 + i\sin\varphi_1)\rho_2(\cos\varphi_2 + i\sin\varphi_2) =$$
$$= \rho_1\rho_2[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)] =$$
$$= \rho_1\rho_2[\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)]$$

$$|z_1 z_2| = \rho_1\rho_2 = |z_1||z_2|,\ \arg z_1 z_2 = \varphi_1 + \varphi_2 = \arg z_1 + \arg z_2.$$

$$\frac{z_1}{z_2} = \frac{\rho_1(\cos\varphi_1 + i\sin\varphi_1)}{\rho_2(\cos\varphi_2 + i\sin\varphi_2)} = \frac{\rho_1}{\rho_2}\cdot\frac{(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 - i\sin\varphi_2)}{(\cos\varphi_2 + i\sin\varphi_2)(\cos\varphi_2 - i\sin\varphi_2)} =$$
$$= \frac{\rho_1}{\rho_2}\cdot\frac{(\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 - \cos\varphi_1\sin\varphi_2)}{(\cos\varphi_2)^2 - (i\sin\varphi_2)^2} =$$
$$= \frac{\rho_1}{\rho_2}\cdot\frac{\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)}{\cos^2\varphi_2 + \sin^2\varphi_2} = \frac{\rho_1}{\rho_2}\cdot\frac{\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)}{1} =$$
$$= \frac{\rho_1}{\rho_2}\cdot[\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)]$$

$$\left|\frac{z_1}{z_2}\right| = \frac{\rho_1}{\rho_2} = \frac{|z_1|}{|z_2|},\ \arg\frac{z_1}{z_2} = \varphi_1 - \varphi_2 = \arg z_1 - \arg z_2$$

$z^n = [\rho(\cos\varphi + i\sin\varphi)]^n = \rho^n[\cos n\varphi + i\sin n\varphi]$ – формула Муавра для возведения комплексных чисел в натуральную степень.

Эта формула позволяет выразить $\cos n\varphi$ и $\sin n\varphi$ через $\cos\varphi$ и $\sin\varphi$. Для этого нужно вычислить $[\rho(\cos\varphi + i\sin\varphi)]^n$ другим способом, пользуясь формулой бинома Ньютона. В результате получим

$$\cos n\varphi = \cos^n\varphi - C_n^2\cos^{n-2}\varphi\sin^2\varphi + C_n^4\cos^{n-4}\varphi\sin^4\varphi - \ldots$$

и

$$\sin n\varphi = n\cos^{n-1}\varphi\sin n\varphi - C_n^3\cos^{n-3}\varphi\sin^3\varphi + C_n^5\cos^{n-5}\varphi\sin^5\varphi - \ldots$$

$$\sqrt[n]{z} = \sqrt[n]{\rho(\cos\varphi + i\sin\varphi} = r(\cos\theta + i\sin\theta)$$

$$\rho(\cos\varphi + i\sin\varphi) = r^n(\cos n\theta + i\sin n\theta)$$

$$\rho = r^n$$

$$\varphi + 2\pi k = n\theta \quad \theta = \frac{\varphi + 2\pi k}{n},\ k = 0,1,\ldots,n-1.$$

$$\sqrt[n]{z} = \sqrt[n]{\rho(\cos\varphi + i\sin\varphi} = \sqrt[n]{\rho}\,(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}).$$

ТЕОРЕМА О СУЩЕСТВОВАНИИ КОРНЯ В ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Теорема (основная теорема алгебры). Всякое алгебраическое уравнение положительной степени с числовыми коэффициентами имеет корень в поле комплексных чисел.

Данная теорема впервые была доказана Гауссом в 1799 году.

Существует несколько способов доказательства этой теоремы. Рассмотрим доказательство, основанное на применении леммы о минимуме функции и леммы Даламбера.

Рассмотрим нормированный многочлен $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ степени $n \geq 0$ с комплексными коэффициентами и уравнение $f(x) = 0$.

Лемма 1. Существует такое положительное число A, что при всех $x_0 \in \boldsymbol{C}$, удовлетворяющих условию $|x_0| > A$, выполняется неравенство $|f(x_0)| > |f(0)|$.

Доказательство. Для всякого комплексного числа x_0 имеем:

$$f(x_0) = {x_0}^n + a_1{x_0}^{n-1} + a_2{x_0}^{n-2} + \ldots a_{n-1}x_0 + a_n = x_0^n\left(1 + \frac{a_1}{x_0} + \frac{a_2}{x_0^2} + \ldots + \frac{a_n}{x_0^n}\right),$$

так что

$$\left| f(x_0) \right| = \left|x_0^n\right|\left|1 + \frac{a_1}{x_0} + \ldots + \frac{a_n}{x_0^n}\right| \geq \left|x_0^n\right|\left(1 - \left|\frac{a_1}{x_0} + \ldots + \frac{a_n}{x_0^n}\right|\right) \geq \left|x_0\right|^n\left(1 - \left|\frac{a_1}{x_0}\right| - \ldots - \left|\frac{a_n}{x_0^n}\right|\right) =$$

$$= \left|x_0\right|^n\left(1 - \frac{|a_1|}{|x_0|} - \ldots - \frac{|a_n|}{|x_0^n|}\right).$$

Рассмотрим функцию $\varphi(t) = t^n\left(1 - \frac{|a_1|}{t} - \frac{|a_2|}{t^2} - \ldots - \frac{|a_n|}{t^n}\right)$ действительного переменного *t.* Очевидно, что $\lim\limits_{t \to +\infty} \varphi(t) = +\infty$. Следовательно, для любого C существует такое $A>0$, что $\varphi(t)>C$ при всех $t>A$. В частности, можно взять $C = |f(0)| = |a_n|$. Соответствующее A будет удовлетворять условию леммы. В самом деле, при $|x_0|>A$ имеем:

$$|f(x_0)| \geq \varphi(|x_0|) > C = |f(0)|.$$

Лемма доказана.

Лемма 2 (лемма Даламбера). Если многочлен $f(x)$ не обращается в нуль в точке $x_0 \in C$, то для любого $\varepsilon > 0$ существует такое $u \in C$, что $|u| < \varepsilon$ и $|f(x_0 + u)| < |f(x_0)|$.

Доказательство. Сделаем замену $x = x_0 + y$, где y – новая переменная и представим многочлен $f(x)$ в виде многочлена от y:

$$f(x) = (x_0 + y)^n + a_1(x_0 + y)^{n-1} + \ldots + a_{n-1}(x_0 + y) + a_n = c_0 + c_1 y + \ldots + c_{n-1}y^{n-1} + c_n y^n. \qquad (1)$$

Так как $y = x - x_0$, то при подстановке в это равенство $x = x_0$ получаем $f(x_0) = c_0$. По условию $f(x_0) \neq 0$.Следовательно, $c_0 \neq 0$. Кроме того, $c_n = 1 \neq 0$, поскольку член y^n, появляется только при раскрытии скобок в выражении $(x_0 + y)^n$. Пусть k – наименьшее положительное число такое, что $c_k \neq 0$. Тогда

$$f(x) = c_0 + c_k y^k + c_{k+1}y^{k+1} + \ldots + c_n y^n \quad (c_0 \neq 0,\ c_k \neq 0). \qquad (2)$$

Идея доказательства леммы Даламбера заключается в том, что поведение функции $f(x)$ в малой окрестности точки x_0 в основном определяется первыми двумя членами разложения (2). Если бы остальных членов разложения не было, то можно было бы рассуждать так. Обозначим через y_0 какое – либо решение уравнения $c_0 + c_k y^k = 0$, т.е. одно из значений корня k-ой степени из $-\frac{c_0}{c_k}$.

Пусть t – действительное число, лежащее в интервале (0;1). Тогда

$$f(x_0 + ty_0) = c_0 + c_k t^k y_0^k = c_0(1 - t^k),$$

откуда видно, что

$$|f(x_0 + ty_0)| < |c_0|.$$

Выбирая t достаточно малым, можно добиться того, чтобы $|ty_0| < \varepsilon$ и тогда комплексное число $u = ty_0$ будет удовлетворять требованиям леммы. В общем случае доказательство будет отличаться тем, что оценивается модуль суммы остальных членов разложения (2).

Доказательство основной теоремы алгебры. Пусть число A – число, определенное по лемме 1. Рассмотрим на комплексной плоскости круг K радиуса A с центром в начале координат. По лемме вне круга K многочлен $f(x)$ принимает значения по модулю большие, чем $f(0)$.

Рассмотрим функцию $\psi(u;v) = |f(u + iv)|$ двух действительных переменных u и v. Покажем, что она непрерывна на всей плоскости. Пусть $a_k = b_k + ic_k$, где $b_k,\ c_k \in R$; тогда $f(u + iv) = (u + iv)^n + (b_1 + ic_i)(u + iv)^{n-1} + \ldots + (b_n + ic_n) = \psi_1(u,v) + i\psi_2(u,v)$, где $\psi_1(u,v)$ и $\psi_2(u,v)$ – некоторые многочлены с действительными коэффициентами. Очевидно, что $\psi(u,v) = \sqrt{\psi_1^2(u,v) + \psi_2^2(u,v)}$. Так как многочлены $\psi_1(u,v)$ и $\psi_2(u,v)$ – непрерывные функции, то и функция $\psi(u,v)$ непрерывна. Область определения функции $\psi(u,v)$, т.е. плоскость переменных u и v можно отождествить с комплексной плоскостью.

Из курса анализа известно, что всякая функция двух действительных переменных, определенная и непрерывная во всех точках замкнутого ограниченного множества достигает минимума в некоторой точке этого множества. Применяя эту теорему к функции $\psi(u,v)$ в круге K, можно заключить, что существует точка $x_0 = u_0 + iv_0$ этого круга, в которой функция $\psi(u,v)$ достигает минимума. Это означает, что $|f(x_0)| \le |f(x_1)|$ для всех $x_1 \in K$. В частности, $|f(x_0)| \le |f(0)|$, так как $0 \in K$. Согласно построения круга K, значение многочлена $f(x)$ вне этого круга по модулю больше, чем $f(0)$, и тем более, чем $f(x_0)$. Следовательно, неравенство $|f(x_0)| \le |f(x_1)|$ выполняется для всех $x_1 \in \boldsymbol{C}$.

Смысл же леммы Даламбера заключается в следующем: на комплексной плоскости найдутся точки, в которых значение многочлена $f(x)$ по модулю меньше, чем $f(x_0)$. Поэтому если $|f(x)|$ достигает минимума в какой-то точке комплексной плоскости, то этот минимум равен нулю.

С другой стороны, выше было доказано, что $|f(x)|$ достигает минимума в некоторой точке x_0. По лемме Даламбера заключаем, что $|f(x_0)| = 0$ и значит, $f(x_0) = 0$, т.е. x_0 – корень уравнения $f(x) = 0$.

Следствие. Всякое алгебраическое уравнение степени ≥1 с числовыми коэффициентами имеет в поле комплексных чисел $\boldsymbol{C}$ ровно n корней (с учетом кратностей).

УРАВНЕНИЯ 3 СТЕПЕНИ

Если дано кубическое уравнение с любыми комплексными коэффициентами

$$y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$

то с помощью замены $y - \frac{a_1}{3} = x$ можно добиться того, чтобы оно не содержало слагаемое второй степени.

Рассмотрим полученное неполное кубическое уравнение с произвольными комплексными коэффициентами

$$x^2 + px + q = 0.$$

Это уравнение по основной теореме алгебры обладает тремя комплексными корнями. Пусть x_0 – один из этих корней имеет вид $x_0 = u + v$, тогда левая часть уравнения примет вид

$$(u+v)^3 + p(u+v) + q = u^3 + v^3 + (3uv + p)(u+v) + q.$$

Отсюда следует, что u и v являются решениями системы уравнений

$$\begin{cases} u^3 + v^3 + q = 0 \\ 3uv + p = 0 \end{cases}.$$

Для решения этой системы представим второе уравнение в виде $u^3v^3 = -\frac{p^3}{27}$, тогда система примет вид $\begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -\frac{p^3}{27} \end{cases}$.

Следуя теореме Виета выражения u^3 и v^3 можно рассматривать как корни некоторого квадратного уравнения

$$z^2 + qz - \frac{p^3}{27} = 0,$$

дискриминант которого равен $D = q^2 - 4\left(-\frac{p^3}{27}\right) = q^2 + \frac{4p^3}{27}$.

Тогда решения квадратного уравнения имеют вид

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}};\ v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Тогда u и v соответственно равны

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},\ v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Из этих формул получаем формулу решения неполного кубического называемую формулой Кардано

$$x_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Значение кубических корней в этой формуле не могут выбираться произвольно, так как в системе уравнений относительно u и v имеется условие $uv = -\frac{p}{3}$. Значение кубических корней в формуле Кардано следует выбирать таким образом, чтобы их произведение равнялось $-\frac{p}{3}$.

Пусть u_1 будет одно из трех значений радикала u. Тогда два других можно получить умножением u_1 на кубические корни $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $\varepsilon^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ из единицы:

$$u_2 = u_1\varepsilon\ ,\ \ u_3 = u_1\varepsilon^2.$$

Обозначим через v_1 одно из трех значений радикала v, которое соответствует значению u_1 радикала u на основании равенства $uv = -\frac{p}{3}$. Два других значения v будут

$$v_2 = v_1\varepsilon^2,\ \ v_3 = v_1\varepsilon\ .$$

Так как, ввиду $\varepsilon^3 = 1$,

$$u_2v_2 = u_1\varepsilon \cdot v_1\varepsilon^2 = u_1v_1\varepsilon^3 = u_1v_1 = -\frac{p}{3} \text{ и } u_3v_3 = u_1\varepsilon^2 \cdot v_1\varepsilon = u_1v_1\varepsilon^3 = u_1v_1 = -\frac{p}{3},$$

то значению u_2 радикала u соответствует значение v_2 радикала v; аналогично значению u_3 соответствует значение v_3. Таким образом, все корни три корня неполного кубического уравнения могут быть записаны следующим образом:

$$x_1 = u_1 + v_1,$$
$$x_2 = u_2 + v_2 = u_1\varepsilon + v_1\varepsilon^2,$$
$$x_3 = u_3 + v_3 = u_1\varepsilon^2 + v_1\varepsilon.$$

Теперь, возвращаясь к обратной замене, можно получить корни исходного кубического уравнения.

Пример. Решить уравнение в поле комплексных чисел $\boldsymbol{C}$

$$x^3 - 6x^2 + 57x - 196 = 0.$$

Решение. Делая замену $x = y + 2$ в данном уравнении, получаем неполное кубическое уравнение:

$$y^3 + 6y^2 + 12y + 8 - 6(y^2 + 4y + 4) + 57y + 114 - 196 = 0$$

$$y^3 + 6y^2 + 12y + 8 - 6y^2 - 24y - 24 + 57y - 82 = 0$$

$$y^3 + 45y - 98 = 0$$

$$p = 45,\ q = -98$$

$$y = \alpha + \beta = \sqrt[3]{-\frac{-98}{2} + \sqrt{\frac{(-98)^2}{4} + \frac{45^3}{27}}} + \sqrt[3]{-\frac{-98}{2} - \sqrt{\frac{(-98)^2}{4} + \frac{45^3}{27}}} =$$

$$= \sqrt[3]{49 + \sqrt{5776}} + \sqrt[3]{49 - \sqrt{5776}} = \sqrt[3]{125} + \sqrt[3]{-27}$$

Пусть $\alpha_1 = 5$, тогда $\beta_1 = -3$, так как $\alpha_1\beta_1 = -\frac{p}{3} = -15$. Следовательно,

$$y_1 = \alpha_1 + \beta_1 = 5 + (-3) = 2.$$

Найдем y_2 и y_3:

$$y_2 = \alpha_2 + \beta_3 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = 5(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) = -1 + 4\sqrt{3}i,$$

$$y_3 = \alpha_3 + \beta_2 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = 5(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) - 3(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = -1 - 4\sqrt{3}i.$$

Делая обратную замену, получим корни исходного уравнения

$$x_1 = 4,\ x_2 = 1 + 4\sqrt{3}i,\ x_3 = 1 - 4\sqrt{3}i.$$

Пример. Решить уравнение $y^3 + 3iy^2 - (3 + 6i)y + 10 - 5i = 0$.

Решение. Сделаем замену в данном уравнении $y = x - i$:

$$(x - i)^3 + 3i(x - i)^2 - (3 + 6i)(x - i) + 10 - 5i = 0$$

$$x^3 - 3ix^2 - 3x + i + 3i(x^2 - 2ix - 1) - (3x - 3i + 6ix + 6) + 10 - 5i = 0$$

$$x^3 - 3ix^2 - 3x + i + 3ix^2 + 6x - 3i - 3x + 3i - 6ix - 6 + 10 - 5i = 0$$

и получим неполное кубическое уравнение

$$x^3 - 6ix + 4 - 4i = 0,$$

где $p = -6i,\ q = 4 - 4i$.

Найдем корни полученного уравнения по формулам Кардано

$$x = \alpha + \beta = \sqrt[3]{-\frac{4-4i}{2}+\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}}+\sqrt[3]{-\frac{(4-4i)}{2}-\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}}$$

,

$$\alpha = \sqrt[3]{-\frac{4-4i}{2}+\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}} = \sqrt[3]{-2+2i+\sqrt{(2-2i)^2+8i}} =$$

$$= \sqrt[3]{-2+2i+\sqrt{4-8i-4+8i}} = \sqrt[3]{-2+2i}$$

$$\beta = \sqrt[3]{-\frac{(4-4i)}{2}-\sqrt{\frac{(4-4i)^2}{4}-\frac{(6i)^3}{27}}} = \sqrt[3]{-2+2i}\,.$$

$$\sqrt[3]{-2+2i} = \sqrt{2}\left(\cos\frac{\frac{3\pi}{4}+2\pi k}{3}+i\sin\frac{\frac{3\pi}{4}+2\pi k}{3}\right),\ k = 0,\ 1,\ 2$$

Укажем значение корня при k=0 , тогда

$$\alpha_1 = \sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right) = 1+i$$

Найдем β_1 из условия $\alpha_1\beta_1 = -\frac{p}{3}$

$\alpha_1\beta_1 = (1+i)\beta_1 = -\frac{-6i}{3} = 2i$, отсюда $\beta_1 = 1+i$.

Тогда $x_1 = \alpha_1 + \beta_1 = 2+2i$,

$$x_2 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = (1+i)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)+(1+i)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) =$$

$$= -1-i,$$

$$x_3 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = (1+i)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)+(1+i)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) =$$

$$= -1-i.$$

Выполним обратную замену и получим корни исходного уравнения

$$y_1 = 2+i,\ y_2 = -1-2i,\ y_3 = -1-2i.$$

Кубические уравнения с действительными коэффициентами

Рассмотрим неполное кубическое уравнение с действительными коэффициентами

$$x^2 + px + q = 0.$$

Выражение $D = -4p^3 - 27q^2 = -108(\frac{q^2}{4} + \frac{p^3}{27})$ называется дискриминантом кубического уравнения. В зависимости от знака выражения $\frac{q^2}{4} + \frac{p^3}{27}$, стоящего в формуле Кардано под знаком квадратного корня и имеющего противоположный знак дискриминанту, кубическое уравнение может иметь три различных действительных корня, один действительный и два комплексно-сопряженных корня и три действительных корня, из которых два корня равны между собой.

1. При $D<0$ выражение $\frac{q^2}{4} + \frac{p^3}{27}$ положительно, поэтому в формуле Кардано под знаком каждого из кубических радикалов оказываются различные действительные числа. Тогда

$$x_1 = u_1 + v_1,$$
$$x_2 = u_1\varepsilon + v_1\varepsilon^2,$$
$$x_3 = u_1\varepsilon^2 + v_1\varepsilon = \overline{x}_2.$$

Так как $x_2 \neq x_3$, то x_2 и x_3 – сопряженные мнимые числа. Число x_1, очевидно, действительное.

Итак, если $D<0$, то уравнение $x^2 + px + q = 0$ имеет один действительный и два сопряженных мнимых корня.

2. При $D>0$ выражение $\frac{q^2}{4} + \frac{p^3}{27}$ отрицательно, поэтому в формуле Кардано под знаком квадратного корня находится отрицательное число и кубические корни извлекаются из двух сопряженных комплексных чисел. Тогда, учитывая $\varepsilon^2 = \overline{\varepsilon}$,

$$x_1 = u_1 + \overline{u}_1,$$
$$x_2 = u_1\varepsilon + \overline{u}_1\varepsilon^2 = u_1\varepsilon + \overline{u_1\varepsilon},$$
$$x_3 = u_1\varepsilon^2 + \overline{u}_1\varepsilon = u_1\varepsilon^2 + \overline{u_1\varepsilon^2}.$$

Итак, если $D>0$, то уравнение $x^2 + px + q = 0$ имеет

3. При D=0 имеем $u_1 = v_1$ и тогда, используя очевидное равенство, получим:

$$x_1 = 2u_1,$$
$$x_2 = u_1(\varepsilon + \varepsilon^2) = -u_1,$$
$$x_3 = u_1(\varepsilon^2 + \varepsilon) = -u_1.$$

Итак, если D=0, то все корни уравнения $x^2 + px + q = 0$ действительны, причем два из них равны между собой.

РЕШЕНИЕ УРАВНЕНИЯ 4 СТЕПЕНИ МЕТОДОМ ФЕРРАРИ

Рассмотрим приведенное уравнение 4-й степени

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Сделав замену переменной $x = y - \frac{a}{4}$, приведем данное уравнение к виду

$$. \; y^4 + py^2 + qy + r = 0.$$

Будем решать это уравнение методом, который носит название метода Феррари.

Преобразуем левую часть уравнения так:

$$\left(y^2 + \frac{p}{2}\right)^2 + qy + \left(r - \frac{p^2}{4}\right) = 0.$$

Затем введем новую переменную z следующим образом:

$$\left(y^2 + \frac{p}{2} + z\right)^2 - \left[2z\left(y^2 + \frac{p}{2}\right) + z^2 - qy + \frac{p^2}{4} - r\right] = 0.$$

Подберем значение z так, чтобы многочлен 2-й степени стоящий в квадратных скобках, стал полным квадратом. Для того чтобы многочлен $2zy^2 - qy + \left(zp + z^2 + \frac{p^2}{4} - r\right)$ был полным квадратом необходимо и достаточно, чтобы его дискриминант равнялся нулю, т.е.

$$D = q^2 - 4 \cdot 2z\left(zp + z^2 + \frac{p^2}{4} - r \right) = 0,$$

$$8z^3 + 8pz^2 - 8rz + (2p^2 - q^2) = 0.$$

Получили уравнение 3-й степени относительно неизвестного z, которое можно решить по формулам Кардано и найти хотя бы один действительный корень z_0. Подставляя это значение в уравнение $\left(y^2 + \frac{p}{2} + z \right)^2 - \left[2z\left(y^2 + \frac{p}{2} \right) + z^2 - qy + \frac{p^2}{4} - r \right] = 0$, получим в левой части разность квадратов. Тогда полученную разность квадратов можно разложить в произведение двух многочленов второй степени относительно y. После этого останется решить два получившихся уравнения 2-й степени.

Таким образом, уравнение 4-й степени всегда может быть решено и, более того, можно, аналогично случаю уравнения 3-й степени, получить формулу, выражающую корни общего уравнения 4-й степени через коэффициенты уравнения с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени.

Однако, общее уравнение с одним неизвестным степени выше 4-й неразрешимо в радикалах, т.е. не существует формулы, выражающей корни общего уравнения степени выше 4-й через коэффициенты уравнения с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени. Это положение известно как теорема Абеля.

Пример. Решить уравнение методом Феррари

$$x^4 - 2x^3 + 2x^2 + 4x - 8 = 0.$$

Решение.

$x^4 - 2x^3 = -2x^2 - 4x + 8$

$(x^2)^4 - 2x^2x + x^2 = -x^2 - 4x + 8$

$(x^2 - x)^2 = -x^2 - 4x + 8$

$(x^2 - x + y)^2 = -x^2 - 4x + 8 + 2(x^2 - x)y + y^2$

$(x^2 - x + y)^2 = (2y - 1)x^2 + (-2y - 4)x + y^2 + 8$

$D = (-2y - 4)^2 - 4(2y - 1)(y^2 + 8) = 4y^2 + 16y + 16 - 8y^3 + 4y^2 - 64y + 32 =$

$= -8y^3 + 8y^2 - 48y + 48$

$-8y^3 + 8y^2 - 48y + 48 = 0$

$y^3 - y^2 + 6y - 6 = 0$

$y^2(y - 1) + 6(y - 1) = 0$

$(y - 1)(y^2 + 6) = 0$

$y - 1 = 0$

$y = 1$

$(x^2 - x + 1)^2 = x^2 - 6x + 9$

$(x^2 - x + 1)^2 = (x - 3)^2$

$x^2 - x + 1 = x - 3$ или $x^2 - x + 1 = -x + 3$

$x^2 - 2x + 4 = 0$ или $x^2 - 2 = 0$

$x^2 - 2x + 4 = 0$

$D = 2^2 - 4 \cdot 4 = -12$

$x_{1,2} = \frac{2 \pm 2\sqrt{3}i}{2} = 1 \pm \sqrt{3}i$

$x^2 - 2 = 0$

$x_{3,4} = \pm\sqrt{2}$.

5. МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И ИТОГОВОГО КОНТРОЛЯ

Индивидуальное задание № 1 по теме «Б. А.О. Группа»

Вариант	1. Определить, являются ли бинарными алгебраическими операциями действия +, -, ×, ÷ на указанном множестве	2. Определить, какими свойствами обладает указанная бинарная операция $*$ на множестве действительных чисел	3. Определить, является ли указанное множество группой относительно заданной бинарной алгебраической операции $*$.

		R	
1	а) $\{x : x \in N\}$; б) $\{0\}$	$a * b = b$	$R^* = R \setminus \{0\}$; $a * b = 4ab$
2	а) $\{-x : x \in N\}$; б) $\{1\}$	$a * b = a + b + 2$	$R^* = R \setminus \{0\}$; $a * b = \frac{ab}{4}$
3	а) $\{x : x \in Z \setminus \{0\}\}$; б) $\{-1, +1\}$	$a * b = a + b - 2$	$R \setminus \left\{-\frac{1}{2}\right\}$; $a * b = a + b + 2ab$
4	а) $\{x : x \in Z^+\}$; б) $\{0,1,2\}$	$a * b = 2a\lvert b\rvert$	$R^* = R \setminus \{0\}$; $a * b = \frac{ab}{3}$
5	а) $\{x : x \in Z^-\}$; б) $\{0, +1\}$	$a * b = 2\lvert a\rvert b$	$R^* = R \setminus \{0\}$; $a * b = 3ab$
6	а) $\{2x : x \in Z\}$; б) $\{0, -1\}$	$a * b = \frac{1}{2}a\lvert b\rvert$	$R \setminus \{-1\}$; $a * b = a + b + ab$
7	а) $\{2x + 1 : x \in Z\}$; б) $\{-1\}$	$a * b = \frac{1}{2}\lvert a\rvert b$	$\{a + b\sqrt{2} : a, b \in Q\}$; $a * b = a + b$
8	а) $\{nx : x \in Z, n \in N\}$; б) $\{i, -i, 1, -1\}$ $(i^2 = -1)$	$a * b = 5ab$	$\{a + b\sqrt{3} : a, b \in Q\}$; $a * b = a + b$
9	а) $\{x : x \in Q\}$; б) $\{0\}$	$a * b = \sqrt[4]{a}$	$\{a + b + ab\sqrt{2} : a, b \in Q\}$; $a * b = a + b$
10	а) $\{x : x \in Q \setminus \{0\}\}$; б) $\{1\}$	$a * b = a + b - 1$	$\{a + 2b\sqrt{2} : a, b \in Q\}$; $a * b = a + b$
11	а) $\{x : x \in Q^+\}$; б) $\{-1, +1\}$	$a * b = a + b + 1$	$\{a + b\sqrt[3]{2} : a, b \in Q\}$; $a * b = a + b$
12	а) $\{x : x \in Q^-\}$; б) $\{-1, 0, +1\}$	$a * b = (a + b)^2$	$\{a - b\sqrt{2} : a, b \in Q\}$; $a * b = a + b$
13	а) $\{x : x \in R\}$; б) $\{0, +1\}$	$a * b = (a + b)^3$	$\{-1, +1\}$; $a * b = a + b$
14	а) $\{x : x \in R \setminus \{0\}\}$;	$a * b = \frac{a + b}{3}$	$\{a + b\sqrt[3]{5} : a, b \in Z\}$;

	б) $\{0,-1\}$		$a * b = a + b$
15	а) $\{x : x \in R^-\}$; б) $\{-1\}$	$a * b = \frac{a-b}{3}$	$\{2a+2b\sqrt{2} : a,b \in Z\}$; $a * b = a + b$

ЗАДАЧИ ПО ТЕОРИИ ГРУПП

1. Доказать, что если порядок конечной группы G делится на простое число p, то G содержит элемент порядка p. (Теорема Коши)

Доказательство**.**

Доказывается индукцией по порядку n групп G.

Для n=2 группа G циклическая второго порядка. Предположим, что утверждение верно для всех групп, порядок которых меньше n, и G группа порядка n и $n \vdots p$, p - простое.

Пусть сначала G - коммутативна. Возьмем $\forall a \in G, a \neq e$. Порядок a - $k > 1$, если $k \vdots p, k = pq$, то элемент a^q имеет порядок p, так как $n \vdots k \quad n = km \vdots p$. Если же k не $\vdots p$, то, так как группа G абелева, фактор группа $G/\{a\} = G'$ имеет порядок $\frac{n}{k} = m < n$ и $m \vdots p$.

По предположению G'содержит элемент b' порядка p. Пусть b - элемент группы G, входящий в смежный класс b'. Из того, что $b'^p = e'$, где e' - единица группы G', следует, что $b^p \in e' = \{a\}$, то есть $b^p = a^l$. Тогда $b^{pk} = a^{kl} = e$. Если $b^k = e$, то $b'^k = e'$ и тогда $k \vdots p$ что невозможно. Значит, $b^{kp} = e$ и $b^k \neq e$, а это значит, этот элемент b^k имеет порядок p.

Теперь пусть группа G - некоммутативная. Если существует подгруппа H, отличая от G индекс которой не $\vdots p$, то порядок H меньше n и $\vdots p$. По предположению H содержит элементы порядка p. Если же индексы всех подгрупп, отличны от G, делятся на β, то число элементов, сопряженных любому элементу группы G, не входящему в её центр Z делится на p (число элементов, сопряженных с a равно индексу нормализатора a $(N(a))$). Каждый же элемент центра Z сопряжен лишь только самому себе.

Следовательно, порядок Z делится на p и меньше n. По предположению Z содержит элементы порядка p.

2. Доказать, что если $G = A + B_1 = A + B_2$ - прямые разложения абелевой группы G и если B_1 содержит B_2, то $B_1 = B_2$.

Доказательство

Так как $G = A + B_1 = A + B_2$ - прямые разложения, то $A \bigcap B_1 = \emptyset$ $A \bigcap B_2 = \emptyset$. Кроме того $B_2 \subset B_1$, то есть $B_1 = B' + B_2$ $B' \bigcap B_2 = \emptyset$. Получаем $A + B_2 = A + B' + B_2 \Rightarrow B' = \emptyset$, то есть $B_1 = B_2$.

3. Доказать, что подгруппа H абелевой группы G тогда и только тогда будет слагаемым в прямом разложении $G = H + K$, когда существует гомоморфное отображение G на H, сохраняющие на месте все элементы из H.

Доказательство.

Покажем, что существует $\varphi : G \to H$ гомоморфизм $\forall h \in H \quad h\varphi \in H$.

$\forall x \in G \quad x = h + k$ - единственно.

$\varphi : G \to H \quad x\varphi = h$, ясно что $\forall h \in H \quad h\varphi = h$.

$x_1 = h_1 + k_1$, $x_2 = h_2 + k_2 \quad x_1 + x_2 = (h_1 + h_2) + (k_1 + k_2)$

$(x_1 + x_2)\varphi = h_1 + h_2 = x_1\varphi + x_2\varphi$

Обратно $\exists \varphi : G \to H \quad \forall x, y \in G \quad (x + y)\varphi = x\varphi + y\varphi \quad \forall h \in H \quad h\varphi = h$

$K = \ker\varphi \quad \forall x \in G \quad x\varphi = h = h\varphi$

$x\varphi - h\varphi = 0 = k\varphi \quad (x - h)\varphi = 0 \quad x - h \in K \quad x - h = k \quad x \neq k + h$

4. Пусть $G = A_1 + A_2 + \ldots + A_s$ разложение абелевой группы G в прямую сумму подгрупп и $x = a_1 + a_2 + \ldots + a_s, a_i \in A_i, i = 1,2,\ldots,s$ соответствующие разложение элемента x в сумму компонент. Доказать, что группа G тогда и только тогда конечный порядок n,когда каждая его подгруппа A_i имеет конечный порядок $n_i, i = 1,2,\ldots,s$, причем $n = n_1 n_2 \ldots n_s$

Доказательство:

Пусть G имеет конечный порядок n. Покажем, что подгруппа A_i имеет порядок $n_i, i = 1,2,\ldots,s$, причем $n = n_1 n_2 \ldots n_s$. Для этого рассмотрим группу

$G_1 = A_1 + A_2$, где $|G_1| = n$. Так как A_1 и A_2 подгруппы группы G, то $|A_1| < |G|$ и $|A_2| < |G_1|$, то есть A_1 и A_2 - конечны. Пусть $|A_1| = n_1$ и $|A_2| = n_2$, то по теореме Лагранжа $|A_1| \mid |G_1|$ и $|A_2| \mid |G_1|$, то есть $n = n_1 q_1$ и $n = n_2 q_2$.

Рассмотрим G_1 / A_1, тогда $G_1 = A_1 + G_1 / A_1$, так как $G_1 / A_1 \cong A_2$. Действительно, если $A_1 + g$ есть смежный класс группы G по подгруппе A_1 и $g = a_1 + a_2$, то , то есть всякий смежный класс по A_1 содержит один и только один элемент из A_2.

Кроме того $|G_1 / A_1| = |A_2|$, а по теореме Лагранжа $G_1 = |A_1| \cdot |G_1 / A_1|$, следовательно $n = n_1 n_2$.

Применяя метод математической индукции, получаем доказательство для случая s слагаемых в разложении группы G.

5. Пусть G - абелева группа, T - её периодическая часть. Доказать что ранг G равен рангу G/T.

Доказательство:

Это утверждение вытекает из предположения, что всякая подгруппа A и фактор-группа G/A абелевой группы G конечного ранга сами имеют конечный ранг, причем сумма их рангов равна рангу самой группы G.

Возьмем в подгруппе A максимальную линейно не зависимую систему элементов $a_1, a_2, ..., a_k$, а в фактор-группе G/A максимальную линейно не зависимую систему смежных классов $b_1 + A, b_2 + A, ..., b_l + A$. Тогда систему элементов $a_1, a_2, ...a_k, b_1, b_2, ..., b_l$ - линейно независима в G.

$$\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k + \beta_1 b_1 + \beta_2 b_2 + ... + \beta_l b_l = 0$$

Переходя к фактор-группе по A,

$$\beta_1 (b_1 + A) + \beta_2 (b_2 + A) + ... + \beta_l (b_l + A) = 0$$

имеем, что $\beta_1 = \beta_2 = ... = \beta_l = 0$

Тогда

$$\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k = 0$$

$$a_1 = a_2 = ... = a_k = 0$$

Покажем что $a_1, a_2, ... a_k, b_1, b_2, ..., b_l$ - максимальная линейно независимая система группы G.

Если g - произвольный элемент G, то $g + A$ будет линейно зависеть от $b_1 + A, b_2 + A, ..., b_l + A$, то есть

$$\alpha (g + A) = \gamma_1 (b_1 + A) + \gamma_2 (b_2 + A) + ... + \gamma_l (b_l + A)$$

$$\alpha g = a + \gamma_1 b_1 + \gamma_2 b_2 + ... + \gamma_l b_l, a \in A, \alpha \neq 0$$

Но a линейно зависит от $a_1, a_2, ..., a_k$

$$\beta a = \delta_1 a_1 + \delta_k a_k + ... + \delta_k a_k, \beta \neq 0$$

Следовательно

$$(\alpha \beta) g = \delta_1 a_1 + \delta_k a_k + ... + \delta_k a_k + (\beta \gamma_1) b_1 + (\beta \gamma_2) b_2 + ... + (\beta \gamma_l) b_l$$

То есть ранг G равен сумме рангов подгруппы A и фактор-группы G / A

.

6. Доказать, что всякая примарная компонента группы G образует вполне характеристическую подгруппу G.

Доказательство

Пусть A - примарная компонента группы G, то есть порядки элементов подгруппы A группы G есть степени одного и того же числа ρ

$a \in A, \rho^{\alpha} a = e$, ρ^{α} - порядок элемента a.

$$e = (\rho^{\alpha} a)\varphi = (a + ... + a)\varphi = a\varphi + ... + a\varphi = \rho^{\alpha} (a\varphi) = e$$

7. Всякая периодическая группа может быть разложена в прямые произведения примарных групп, относящихся к различным простым числам. Доказать.

8. Найти все подгруппы группы G порядка 8, все элементы которой, кроме единицы e, имеют порядок 2.

$G, |G| = 8, \forall a \in G, a^2 = e \Rightarrow G$ - абелева группа(№1636)

$G = \{e, a, b, c, ab, ac, cb, abc\}$

G имеет 16 подгрупп:

$< e >, < e, a >, < e, b >, < e, c >, < e, ab >, < e, ac >, < e, bc >, < e, abc >,$
$< e, a, b, ab >, < e, a, c, ac >, < e, b, c, bc >, < e, a, bc, abc >, < e, b, ac, abc >,$
$< e, c, ab, abc >, < e, ab, ac, cb >, G$

9. Пусть $G = \{a\}$ - конечная циклическая группа порядка n. Доказать:

а) порядок любой подгруппы группы G делит порядок n этой группы $|G| = n$

Доказательство

$H < G$. Подгруппа циклической группы циклическая и её порядок делит порядок группы G.

$H < \{a\}$ $|H| = k$ $|\{a\}| = n$

$H = \{b\}$ $n = kq + r$, $0 \le r \le n$

$b^{kq+r} = b^r = e$ $r = 0$, $n \vdots k$

б) для любого делителя d числа n существует единственная подгруппа H группы G, имеющая порядок d.

Доказательство

$n = du$ $a \ne e$ $a^n = a^{du} = (a^u)^d = b^d = e$ $a^u = b$

Итак, $b^d = e$

Если $b^l = e$, $l < d$, то $a^{lu} = e$ и $lu < du = n$

d - порядок b, $\{b\}$ - циклическая подгруппа порядка d

$\{c\}$ - циклическая подгруппа группы G порядка d.

Докажем, что $c \in \{b\}$

$c = a^v$ $c^d = a^{vd} = e$ $vd \vdots n = ud$ $v \vdots u$ $v = uq$

$c = a^v = a^{uq} = (a^u)^q = b^q \in \{b\}$, ясно что $\{b\} = \{c\}$

Подгруппа H порядка d содержит в качестве образующих все элементы порядка d группы G. В частности, $H = \{a^{\frac{n}{d}}\}$

Доказательство

$H = \{a\}$, $|H| = d$ $\forall b \in \{a\}$ и имеющего $|b| = d$ $b^d = e$ $\{b\}$ имеет порядок d. В силу пункта б) $H = \{b\}$.

10. Найти все подгруппы примарной циклической группы, то есть $G = \{a\}$ $|G| = p^k$, где p - простое.

Решение

В силу пункта б) номера 1656 $G = \{a\}, \{a^p\}, \{a^{p^2}\}, ..., \{a^{p^k}\}$, так как $p, p^2, ..., p^k$ являются делителями порядка группы.

11. Доказать утверждения

а) симметричная группа S_n при $n > 1$, порождается множеством транспозиций (i, j).

Доказательство

$\forall\, a \in S_n \quad a = (i_1, i_2, ..., i_k)$ или $a = (i_1 i_2)(i_1 i_3)...(i_1 i_k)$, то любая подстановка из S_n представляет собой произвольную транспозицию.

б) симметричная группа S_n при $n > 1$, порождается множеством транспозициями $(12), (13), ..., (1n)$.

Доказательство

Так как $(1i)(1j)(1i) = (ij)$, то любая подстановка (по пункту а)) из S_n может быть представлена в произведения транспозиций $(12), (13), ..., (1n)$.

в) знакопеременная группа A_n при $n > 2$ порождается множеством всех тройных циклов.

Доказательство

Любая подстановка из A_n разлагается в четное число транспозиций.

1) две транспозиции содержат общее число $(ab)(ac) = (abc)$

2) $(ab)(cd) = (ab)(ca)(ac)(cd) = (abc)(cad)$

г) знакопеременная группа A_n при $n > 2$ порождается тройными циклами $(123), (124), ..., (12n)$

Доказательство

При $n = 3$ получим $A_3 = \{(123)\}$.

$n = 4 \quad G = \{(123), (124)\}$;

G содержит вместе с $(12i)$ и $(i21)$.

$(12j)(12i)(j21) = (1ij)$

$(j21)(i21)(12j) = (2ij)$

Таким образом G содержит все тройные циклы и $G = A_n$ (в силу в))

$n > 4$

$(12k)(1ij)(k21) = (ijk) \in G \quad G = A_n$

18. Найти смежные классы:

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному числу n.

Решение

Z - аддитивная группа целых чисел

$H < Z \quad H = \{nz \mid z \in Z\}$

$\{\bar{0},\bar{1},...,\overline{n-1}\} \quad \bar{m} = m + H$

б) аддитивной группы действительных чисел по подгруппе целых чисел.

Решение

R^+ - аддитивная группа действительных чисел.

Z - аддитивная подгруппа целых чисел.

$\forall \alpha \in R \quad \alpha + Z = \bar{\alpha}$.

Все числа этого класса имеют одинаковые мантиссы и равные $\mu(\alpha)$.

в) аддитивной группы комплексных чисел по подгруппе целых гауссовых чисел.

Решение

C - аддитивная группа комплексных чисел.

H - подгруппа целых гауссовых чисел.

$\forall (\alpha + \beta i) \in C \quad (\alpha + \beta i) + H = \{(\alpha + a) + (\beta + b)i \mid \alpha, \beta \in R\}$

Любому числу $\alpha + \beta i$, $0 \le \alpha \le 1$ и $0 \le \beta \le 1$ соответствует смежный класс. Разность между любыми двумя числами одного смежного класса есть число (гауссово).

19. Доказать что:

а) подгруппа H порядка k конечной группы G порядка 2 содержит квадраты всех элементов группы G.

Доказательство

$G, \mid G \mid = 2k \quad H < G \quad \mid H \mid = k$. Покажем $\forall a \in G a^2 \in H \quad [G;H] = 2 \Rightarrow G = H + aH$

Если $a \in H$, то $a^2 \in H$.

Если $a \notin H$, то $a \in aH$ и $a^2 \notin aH$, то есть $a^2 \in H$.

б) подгруппа H индекса 2 любой группы G содержит квадраты всех элементов группы G.

Доказательство

Аналогично пункту а).

20. Доказать, что при $n > 1$ знакопеременная группа A_n является единственной подгруппой индекса 2 в симметричной группе S_n. Привести пример конечной группы, содержащих несколько подгрупп индекса 2.

Доказательство

Пусть H_n подгруппа группы S_n индекса 2. Тогда в силу №1660 $\forall a \in S_n$ $a^2 \in H_n$. А так как квадрат тройного цикла снова тройной цикл, то H_n содержит все тройные циклы и следовательно в силу №1658 $H_n = A_n$.

Пример:

$G = \{1,(12)(34),(13)(24),(14)(23)\}$ содержит три подгруппы индекса 2.

21. Доказать, что любая подгруппа индекса 2 является нормальным делителем.

Доказательство

$H < G \ [G;H] = 2 \ G = H + aH = H + Ha \Rightarrow \ Ha = aH$

22. Доказать, что множество Z всех элементов группы G, каждый из которых перестановочен со всеми элементами этой группы, является нормальным делителем.

Доказательство

$\forall z \in Z \ \forall g \in G \ gz = zg$

1) $\forall z_1 z_2 \in Z \ \forall g \in G \ (z_1 z_1)g = z_1(z_2 g) = z_1(gz_2) = .. = g(z_1 z_2) \Rightarrow \ z_1 z_2 \in Z$

2) $\forall z \in Z \ \forall g \in G \ gz = zg \Rightarrow \ z^{-1}g = gz^{-1} \Rightarrow \ z^{-1} \in Z$

3) $\forall z \in Z \ \forall g \in G \ g^{-1}zg = z \ \Rightarrow \ gz = zg \ \Rightarrow \ g^{-1}zg = z \in Z$

23. Доказать, что подстановка $x^{-1}ax$, сопряженная в группе подстановок подстановке a, полученная путем трансформирующей подстановки x ко всем числам в разложении подстановки a на независимые циклы.

Дано $a = (a_{1,1}...a_{1,r})(a_{2,1}...a_{2,s})...(a_{m,1}...a_{m,t})$ и $x = \begin{pmatrix} a_{1,1}...a_{1,r} & a_{2,1}...a_{2,s} & ... & a_{m,1}...a_{m,t} \\ b_{1,1}...b_{1,r} & b_{2,1}...b_{2,s} & ... & b_{m,1}...b_{m,t} \end{pmatrix}$.

Покажем, что $x^{-1}ax = (b_{1,1}...b_{1,r})(b_{2,1}...b_{2,s})...(b_{m,1}...b_{m,t})$

Доказательство

$\forall b_{j,k} \quad b_{j,k} \xrightarrow{x^{-1}} a_{j,k} \xrightarrow{a} a_{j,kh} \xrightarrow{x} b_{j,kh}$, то есть подстановка $x^{-1}ax$ любой элемент $b_{j,k}$ переводит в $b_{j,kh}$.

24. Доказать, что

а) четверная группа V является нормальным делителем симметрической группы S_4.

Доказательство

$V = \{1,(12)(34),(13)(24),(13)(24),(14)(23)\}$.

В силу задачи №1667 $\forall a \in V \quad \forall g \in S_4 \quad g^{-1}ag \in V$, так как представляет собой произведение двух циклов.

б) фактор группа S_4/V изоморфно группа S_3

Доказательство

$S_4/V = \{V,(12)V,(13)V,(23)V,(123)V,(132)V\}$.

$\varphi : S_4/V \to S_3 \quad (aV)\varphi = a \quad \big((aV)(bV)\big)\varphi = \big((ab)V\big)\varphi = ab = (aV)\varphi\,(bV)\varphi$

25. Пользуясь №1667, найти число подстановок симметрической группы S_n, перестановочных с данной подстановкой S.

Решение

$s \in S_n \quad s = (a_{11}...a_{1k})(b_{12}...b_{1r})...(e_{11}...e_{1m})$

Нужно найти такие подстановки $x \in S_n$, которые удовлетворяют условию $xs = sx$, или $s = x^{-1}sx$, или $x = sxs^{-1}$

$x = \begin{pmatrix} a_{11}...a_{1k} & b_{11}...b_{1r} & ... & e_{11}...e_{1m} \\ \alpha_{11}...\alpha_{1k} & \beta_{11}...\beta_{1r} & ... & \gamma_{11}...\gamma_{1m} \end{pmatrix}$

$x^{-1}sx = (\alpha_{11}...\alpha_{1k})(\beta_{11}...\beta_{1r})...(\gamma_{11}...\gamma_{1m})$

Таким образом $x^{-1}sx$ состоит из тех же циклов, что и S, и от S отличается только порядком. При этом первое число любого цикла S переходит в любое число любого цикла той же длины.

26. Доказать, что если пересечение двух нормальных делителей H_1 и H_2 группы G содержит лишь границу e, то $\forall h_1 \in H_1$ перестановочен с $\forall h_2 \in H_2$.

Доказательство

$\forall h_1 \in H_1$ и $\forall h_2 \in H_2$ покажем $h_1 h_2 = h_2 h_1$.

$[h_1 h_2] = h_1 h_2 h_1^{-1} h_2^{-1} = h_1 \left(h_2 h_1^{-1} h_2^{-1}\right) = \left(h_1 h_2 h_1^{-1}\right) h_2^{-1} \in H_1 \bigcap H_2$

$h_1 h_2 h_1^{-1} h_2^{-1} = e \quad h_1 h_2 = h_2 h_1$

27. Доказать, что

а) элементы группы G, перестановочные с данным элементом a, образуют подгруппу $N(a)$ группы G (нормализатор a в G), содержит циклическую подгруппу $\{a\}$ в качестве нормального делителя.

Доказательство

$\forall x, y \in N(a) \quad xa = ax \quad ya - ay \quad a \in G$

$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, то есть $(xy)a = a(xy) \quad xy \in N(a)$

$\forall x \in N(a) \quad xa = ax \Rightarrow \quad ax^{-1} = x^{-1}a$, то есть $x^{-1} \in N(a)$

Итак, $N(a) < G \quad \{a\} = H < N(a)$, так как $a \in N(a)$

Ясно, что $\forall x \in N(a) \quad xH = Hx$ (если x перестановочен с a, то он перестановочен с любой степенью a).

б) число элементов группы G, сопряженных с a, равно индексу нормализатора $N(a)$ в G

Доказательство

$[G : N(a)] = k$. Пусть $x \neq y$, такие что $x^{-1}ax = y^{-1}ay \to (yx^{-1})a = a(yx^{-1}) \to yx^{-1} \in N(a)$, то есть $yx^{-1} = n \in N(a) \quad y = nx$ или $y = N \cdot x$, таким образом x и y принадлежат одному смежному классу по N.

Обратно, пусть x и $y \in Nx_i = Nx = Ny \quad y = nx \quad yx^{-1} = n \in N(a) \to (yx^{-1})a = a(yx^{-1})$ или $x^{-1}ax = y^{-1}ay$.

Ясно, что сопряженных элементов с a столько, сколько различных смежных классов по $N(a)$, то есть $[G : N(a)]$.

28. Доказать, что аддитивную группу рациональных чисел нельзя гомоморфно отобразить на аддитивную группу Z.

Доказательство

От противного

$\varphi : Q \to Z \quad (a+b)\varphi = a\varphi + b\varphi$

$\exists a \in Q \quad a\varphi = 3 \quad a/2 + a/2 = a$

$(a/2)\varphi = x \quad x + x = 3 \quad 2x = 3$, где x целое, получили противоречие, то есть не существует $\varphi : Q \to Z$.

29. Доказать, что нормальный делитель H группы G, имеющий конечный индекс j, содержит все элементы группы G, порядки которых взаимно просты с j. Показать на примере, что для подгруппы H, не являющихся нормальным делителем, утверждение может быть неверным.

Доказательство

$[G:H] = j \quad G/H = \{H, Hx_2, Hx_3, ..., Hx_j\} \quad |G/H| = j$. Значит порядок всякого её элемента равен j или делит j

Пусть $|a| = m$ и $a \notin H$

КОНТРОЛЬНАЯ РАБОТА ПО ТЕМЕ «ТЕОРИЯ ГРУПП»

1. Выяснить, образуют ли группу:

а) положительные действительные числа, если операция определена так $a*b = a^2b^2$;

б) невырожденные матрицы порядка n с действительными элементами относительно умножения.

2. Найти смежные классы аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу n.

,3. Доказать, что ядро гомоморфизма группы является нормальным делителем.

4.Доказать, что фактор-группа группы действительных матриц по подгруппе матриц с определителем равным ±1, изоморфна

мультипликативной группе положительных действительных.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ ПО ТЕМЕ «УРАВНЕНИЯ 3 И 4 СТЕПЕНИ»

1 вариант

1. Решить уравнения 3 –ей степени по формулам Кардано

а) $x^3 + x^2 - 10x + 8 = 0$; б) $x^3 + 6x + 2 = 0$; в) $x^3 + (1 - i)x^2 + (1 - i)x - i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 + 2x^3 + 8x^2 + 2x + 7 = 0$.

2 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 - 5x^2 + 2x + 8 = 0$; б) $x^3 + 18x + 15 = 0$; в) $4x^3 - 2(10 - i)x^2 + 10(3 - i)x + 15i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 6x^3 + 10x^2 - 2x - 3 = 0$.

3 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 - 6x^2 + 5x + 12 = 0$; б) $x^3 - 3x^2 - 3x + 11 = 0$; в) $x^3 - 6x + 4(1 - i) = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 2x^3 + 4x^2 + 2x - 5 = 0$.

4 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 - 4x^2 + x + 6 = 0$; б) $x^3 + 3x^2 - 6x + 4 = 0$; в) $x^3 - 3x^2 + 3(1 - 2i)x + 3 + 2i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - x^3 - 3x^2 + x + 1 = 0$.

5 вариант

1. Решить уравнения по формулам Кардано

а) $3x^3 - 10x^2 + 13x + 14 = 0$; б) $x^3 + 9x - 26 = 0$; в) $x^3 - 3x^2 + 9x - 7 + 6i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - x^3 - 4x^2 + 4x + 1 = 0$.

6 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 + 6x^2 + 30x + 25 = 0$; б) $x^3 + 24x - 56 = 0$; в) $x^3 + 3ix^2 - 3(1+2i)x + 10 - 5i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 4x^3 - 20x^2 - 8x + 4 = 0$.

7 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 - 5x^2 + 20x - 16 = 0$; б) $x^3 + 45x - 98 = 0$; в) $x^3 - (4-i)x^2 + 4(1-i)x + 4i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 2x^3 + 3x^2 - 2x - 2 = 0$.

8 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 + 6x + 2 = 0$; б) $x^3 + 6x^2 + 30x + 25 = 0$; в) $x^3 + (1-i)x^2 + (1-i)x - i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 6x^3 + 6x^2 + 27x - 56 = 0$.

9 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 + 18x + 15 = 0$; б) $x^3 + 9x^2 + 18x + 28 = 0$; в) $4x^3 - 2(10-i)x^2 + 10(3-i)x + 15i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - x^3 - 3x^2 + 5x - 10 = 0$.

10 вариант

1. Решить уравнения по формулам Кардано

а) $x^3 - 3x^2 - 3x + 11 = 0$; б) $x^3 + 12x + 63 = 0$; в) $x^3 - (4-i)x^2 + 4(1-i)x + 4i = 0$.

2. Решить уравнение 4 – ой степени методом Феррари

$x^4 - 3x^3 + x^2 + 4x + 6 = 0$.

ИНДИВИДУАЛЬНОЕПО ЗАДАНИЕ ПО ТЕМЕ «АЛГЕБРАИЧЕСКИЕ ЧИСЛА»

1 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = 1 - \sqrt{5 - \sqrt{3}}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\omega}{\omega - 1}, \text{ где } \omega^3 - 2\omega - 2 = 0.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$y = \frac{1}{2}x^3, \quad y = x^2 + x + 1.$$

2 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = \sqrt{3 - \sqrt{2}}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\omega}{\omega^3 + 5}, \text{ где } \omega^3 - 8\omega + 2 = 0.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$\frac{x^2}{9} + \frac{y^2}{16} = 1, \quad y = x3x + 1.$$

3 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = \sqrt{17} - \sqrt{19}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\omega}{\omega + 1}, \text{ где } \omega^3 - 2\omega - 3 = 0.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$y = x^3 + 1, \quad y = 6x - 3.$$

4 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = \sqrt{2} - \sqrt[3]{5}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\omega}{\omega^2 + 1}, \text{ где } \omega^3 + 3\omega^2 - 3\omega + 6 = 0.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$y = x^2, \quad y^2 + 5xy + 9y + 5x - 4 = 0.$$

5 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = \sqrt[3]{2 + \sqrt{7}}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\omega^2 - 3\omega - 1}{\omega^2 + 2\omega + 1}, \text{ где } \omega^3 + \omega^2 + 3\omega + 4 = 0.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$y = 2x^2 - 3x + 2, \quad yx = \frac{1}{2}.$$

6 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = 1 - \sqrt[3]{3}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{2}{\sqrt[3]{49} - \sqrt[3]{7} + 3}.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$yx = 1,\ \frac{x^2}{4} + \frac{y^2}{9} = 1.$$

7 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = 1 + \sqrt{\sqrt[3]{5} - 1}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{2}{\sqrt[4]{27} - 2\sqrt[4]{9} + \sqrt[4]{3} - 1}$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$y = 3x^3,\ y = 3x^2 - x - 2.$$

8 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = 2 + i\sqrt{3}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{3\sqrt{2} + 1}{\sqrt[4]{8} + \sqrt[4]{2} + 1}.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$x^2 - \frac{y^2}{3} = 1,\ y = \frac{1}{2}x.$$

9 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = 3 - i\sqrt{5}.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\sqrt{7} + 1}{\sqrt{7} + \sqrt[4]{7} - 1}.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$x^2 + y^2 - 2y - 5 = 0,\ \ y = 2x - 1.$$

10 вариант

1. Доказать, что число α является алгебраическим, найти его минимальный многочлен

$$\alpha = \sqrt{3} + 2i.$$

2. Освободиться от иррациональности в знаменателе дроби

$$\frac{\sqrt[3]{25} + \sqrt[3]{5} - 2}{\sqrt[3]{25} + 2\sqrt[3]{5} - 1}.$$

3. Можно ли с помощью циркуля и линейки построить линии пересечения следующих линий

$$2y^2 + 3xy + y + x - 3 = 0,\ \ y = x^2 + x + 1.$$

Самостоятельная работа по теме

«Результант двух многочленов. Дискриминант»

Вариант 1

1. Вычислить результант многочленов

$$2x^3-3x^2-x+1 \text{ и } 2x^4-2x^2-3x+4.$$

2. Вычислить дискриминант многочлена

$$2x^4 - x^3 - 4x^2 + x + 1.$$

Вариант 2

1. Вычислить результант многочленов

$$3x^3+2x^2+x+1 \text{ и } 2x^4+x^2-x-1,$$

2. Вычислить дискриминант многочлена

$$x^4 - x^3 - 3x^2 + x + 1.$$

Вариант 3

1. Вычислить результант многочленов

$$2x^4-x^3+3 \text{ и } 3x^3-x^2+4.$$

2. Вычислить дискриминант многочлена

$$2x^4-x^3-4x^2+x+1.$$

Вариант 4

1. Вычислить результант многочленов

$$x^3-3x+6 \text{ и } x^4+x^2-x-1.$$

2. Вычислить дискриминант многочлена

$$x^4-x^3-3x^2+x+1.$$

Индивидуальное задание по теме: "Симметрические многочлены"

1 вариант

1. Следующие многочлен представить в виде суммы однородных многочленов,
   каждый из которых упорядочить лексикографически:

$$f(x,y)=(5-i)x^2y+(3ixy-4i)(7y+6)+(8+i)(x+y) \qquad в\ C[x,y]$$

2. Найти симметрический многочлен $f(x_1,x_2,x_3)$, выраженный через основные (элементарные) $\sigma_1,\sigma_2,\sigma_3$:

$$3\sigma_1^2\sigma_2 - 6\sigma_2^2 - 3\sigma_1\sigma_3 - 5\sigma_1^2 + 10\sigma_2$$

3. Доказать, что следующие многочлены являются симметрическими, каждый
   из них выразить через основные (Элементарные) и вычислить их значения от
   корней многочлена $g(x)$

$$f(X_1,X_2,X_3) =(x_1X_2+X_3)(x_1X_3+X_2)\ (X_3\ X_2+X_1)$$

$$g(x)=9x^3-18x^2+x-9$$

4. Используя симметрические многочлены, решить уравнения или системы
   уравнений:

$$\begin{cases} x - y = 3 \\ x^5 - y^5 = 3093 \end{cases}$$

5. При помощи результанта решить над C системы уравнений:

$$\begin{cases} x^2 - x + y^2 - y - 2 = 0 \\ x^2 + (6y - 5) + (-y^2 - 5y + 6) = 0 \end{cases}$$

2 вариант

1. Следующие многочлен представить в виде суммы однородных многочленов, каждый из которых упорядочить лексикографически:

$f(x,y)=(\sqrt{3}\,x-\sqrt{2}\,y)(\sqrt{2}\,x-2xy+\sqrt{3}\,y)(2+y)$ *в* $\mathbf{R}[x,y]$

2. Найти симметрический многочлен $f(x_1,x_2,x_3)$, выраженный через основные (элементарные) σ_1, σ_2, σ_3:

$$\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_1^2$$

3. Доказать, что следующие многочлены являются симметрическими, каждый из них выразить через основные (Элементарные) и вычислить их значения от корней многочлена $g(x)$

$$f(x_1,x_2,x_3)=(x_1+x_2-5x_3)(x_2+x_3-x_1)(x_1+x_3-5x_2)^2$$

$$g(x)=2x^3-9x^2+3x-1$$

4. Используя симметрические многочлены, решить уравнения или системы уравнений:

$$\sqrt[3]{10-x}-\sqrt[3]{3-x}=1$$

5. При помощи результанта решить над **C** системы уравнений:

$$\begin{cases} x^2 + 2y^2 = 17 \\ 6x^2 - xy - 12y^2 = 0 \end{cases}$$

3 вариант

1. Следующие многочлен представить в виде суммы однородных многочленов, каждый из которых упорядочить лексикографически:

$f(x,y)=5xy(x+y)(2+y)$ *в* $\mathbf{Q}[x,y]$

2. Найти симметрический многочлен $f(x_1,x_2,x_3)$, выраженный через основные (элементарные) σ_1, σ_2, σ_3:

$$\sigma_1^2+2\sigma_2\sigma_3-3\sigma_3^2$$

3. Доказать, что следующие многочлены являются симметрическими, каждый из них выразить через основные (Элементарные) и вычислить их значения от корней многочлена $g(x)$

$$f(x_1,x_2,x_3)=(x_1^2-x_2x_3)(x_2^2-x_1x_3)\ (x_3^2-x_1x_2)$$

$$g(x)=6x^3+3x^2-3$$

4. Используя симметрические многочлены, решить уравнения или системы уравнений:

$$\sqrt[4]{8-x}+\sqrt[4]{89+x}=5$$

5.При помощи результанта решить над **C** системы уравнений:

$$\begin{cases} x^2-y^2-3=0 \\ x^2+xy-y-3=0 \end{cases}$$

Контрольная работа №1

по теме «Многочлены от одной переменной».

Вариант 1.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p=5,$
$f(x)=\overline{4}x^3+\overline{2}x^2-x+\overline{1},$
$g(x)=\overline{2}x+\overline{3}.$

Задание №2.

Найти a и b, если $f(x)=2x^4+3x^3-ax^2+bx-3$ делится без остатка на $(x+3)$, а при делении на $(x+2)$ даёт остаток, равный 5.

Задание №3.

Применяя алгоритм Евклида в $Q[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$:

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

Задание №4.

Найти кратность k корня $a = 3$ многочлена $f(x) \in Q(x)$:

$f(x) = x^4 - 6x^3 + 10x^2 - 6x + 9.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^4 + 16.$

Вариант 2.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 7,$
$f(x) = \overline{3}x^7 + \overline{6}x^3 + \overline{3}x^2 + \overline{6},$
$g(x) = x^2 + \overline{6}x + \overline{5}.$

Задание №2.

Найти a и b, если $f(x) = x^3 + ax + b$ делится без остатка на $g(x) = x^2 + 3x + 10$.

Задание №3.

Применяя алгоритм Евклида в $Q[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$:

$g(x) = x^5 + x^2 - x + 1,$
$f(x) = x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5.$

Задание №4.

Найти кратность k корня $a = 2$ многочлена $f(x) \in Q(x)$:

$f(x) = x^5 + 4x^4 - 7x^3 - 11x^2 + 4.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^3 - 8.$

Вариант 3.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 7,$
$f(x) = \overline{5}x^6 + \overline{5}x^5 - \overline{2}x^3 + \overline{3}x^2 - \overline{2}x + \overline{5},$
$g(x) = \overline{6}x^3 + \overline{4}.$

Задание №2.

Найти a и b, если $f(x) = ax^4 + bx^3 + 1$ делится без остатка на $(x-1)^2$ в кольце $R[x]$.

Задание №3.

Применяя алгоритм Евклида в $R[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$, если :

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

Задание №4.

С помощью схемы Горнера разложите по степеням x многочлен $f(x+2)$, если $f(x) = 2x^4 - 3x^3 + 5x^2 + 6x - 1.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^3 + 8.$

Вариант 4.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 5,$
$f(x) = x^5 + x^2 - x - \overline{1},$
$g(x) = x^3 - \overline{2}x + \overline{1}.$

Задание №2.

Найти a так, чтобы $f(x) = x^5 - ax^2 - ax + 1$ имел число -1 корнем не ниже второй кратности.

Задание №3.

Применяя алгоритм Евклида в $R[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$, если :

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

Задание №4.

С помощью схемы Горнера разложите по степеням x многочлен

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

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^4 - 16.$

Вариант 5.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 5,$
$f(x) = \bar{2}x^4 + x^2 + \bar{2}x,$
$g(x) = x^2 - \bar{2}.$

Задание №2.

Найти a и b, если $f(x) = x^4 - 21x + b$ делится без остатка на $(x^2 + ax + 1)$ в кольце Q[x]

Задание №3.

Применяя алгоритм Евклида в $R[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$:

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

Задание №4.

Найти кратность k корня $a = 2$ многочлена $f(x) \in Q(x)$:

$f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^6 - 27.$

Вариант 6.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 3,$
$f(x) = \overline{2}x^4 + x^2 + \overline{2}x,$
$g(x) = x^2 - \overline{2}.$

Задание №2.

Найти a и b, если $f(x) = x^4 + b$ делится без остатка на $g(x) = x^2 + ax + 1$.

Задание №3.

Применяя алгоритм Евклида в $R[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$:

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

Задание №4.

Найти кратность k корня $a = -2$ многочлена $f(x) \in Q(x)$:

$f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R:

$f(x) = x^6 + 27.$

Вариант 7.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 3,$
$f(x) = x^3 + x^2 + \overline{2}x + \overline{2},$
$g(x) = x^2 + x + \overline{1}.$

Задание №2.

Найти a и b, если $f(x) = x^4 - 7x^2 + b$ делится без остатка на $x^2 + ax + 1$ в кольце $Q[x]$.

Задание №3.

Применяя алгоритм Евклида в $R[x]$, найти НОД и НОК многочленов $f(x)$ и $g(x)$, если:

$g(x) = x^4 + 2x^3 + 2x + 2,$
$f(x) = x^3 + 3x + 2.$

Задание №4.

С помощью схемы Горнера разложите по степеням x многочлен $f(x+3)$, если $f(x) = x^4 - x^3 + 1$.

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^8 - 6x^4 + 9$.

Вариант 8.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 3$,
$f(x) = x^5 + x^2 - x - \overline{1}$,
$g(x) = x^3 - \overline{2}x + \overline{1}$.

Задание №2.

Найти a так, чтобы один из корней многочлена $f(x) = x^3 - 21x + a$ был равен удвоенному другому.

Задание №3.

Применяя алгоритм Евклида в $Q[x]$, найти линейное представление НОД многочленов $f(x)$ и $g(x)$, если :

$g(x) = x^4 + 2x^3 - x^2 - 4x - 2$,
$f(x) = x^4 + x^3 - x^2 - 2x - 2$.

Задание №4.

С помощью схемы Горнера разложите по степеням x многочлен

$f(x) = (x+3)^5 - 2(x+3)^3 + 3(x+3)^2 + 7(x+3) - 8$.

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^4 - 1$.

Вариант 9.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 5,$

$f(x) = x^3 + x^2 + \overline{2}x + \overline{2},$

$g(x) = x^2 + x + \overline{1}.$

Задание №2.

При каких значениях *a* многочлен $f(x) = x^3 + ax^2 + 3x - 1$ имеет кратный корень 1 и какова кратность этого корня.

Задание №3.

Применяя алгоритм Евклида в $Q[x]$, найти линейное представление НОД многочленов $f(x)$ и $g(x)$, если :

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

$f(x) = x^2 - x - 1.$

Задание №4.

С помощью схемы Горнера разложите по степеням $(x-1)$ многочлен $f(x)$, если

$f(x) = x^5.$

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^4 + x^2 + 1$

Вариант 10.

Задание№1.

Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$ в $Z_p[x]$.

$p = 3,$

$f(x) = x^4 + x^3 - x^2 + \overline{1},$

$g(x) = x^3 - \overline{2}x - \overline{1}.$

Задание №2.

При каких значениях *a* многочлен $f(x) = 2x^3 - x^2 + ax + 3$ имеет кратный корень 1 и какова кратность этого корня.

Задание №3.

Применяя алгоритм Евклида в $Q[x]$, найти линейное представление НОД многочленов $f(x)$ и $g(x)$, если :

$g(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1,$

$f(x) = x^4 + 2x^3 + x + 2.$

Задание №4.

С помощью схемы Горнера разложите по степеням $(x+1)$ многочлен

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

Задание №5.

Разложить многочлен $f(x)$ на неприводимые множители над полем C и R :

$f(x) = x^4 + 1.$

Контрольная работа №2

по теме «Многочлены от нескольких переменных.»

Вариант 1.

Задание№1.

Данный симметрический многочлен выразить через основные симметрические многочлены $\sigma_1, \sigma_2, \sigma_3$:

$f = (2x_1 - x_2 - x_3)(2x_2 - x_1 - x_3)(2x_3 - x_1 - x_2)$.

Задание №2.

Разложить на множители, неприводимые над полем R, симметрический однородный многочлен 4-й степени:

$f(x, y) = 2x^4 + 7x^3y + 9x^2y^2 + 7xy^3 + 2y^4$.

Задание №3.

Решить систему уравнений над полем С, исключив переменную у (двумя способами):

$$\begin{cases} y^2 + (x-4)y + x^2 - 2x + 3 = 0 \\ y^3 - 5y^2 + (x+7)y + x^3 - x^2 - 5x - 3 = 0. \end{cases}$$

Задание №4.

Решить систему уравнений, сведя их с помощью вспомогательных переменных к симметрическим:

$$\begin{cases} \sqrt[3]{x} + \sqrt[3]{y} = 3, \\ x \cdot y = 8. \end{cases}$$

Вариант 2.

Задание№1.

Данный симметрический многочлен выразить через основные симметрические многочлены $\sigma_1, \sigma_2, \sigma_3$:

$$f = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2.$$

Задание №2.

Разложить на множители, неприводимые над полем R, симметрический однородный многочлен 4-й степени:

$$f(x, y) = 2x^4 - x^3 y + x^2 y^2 - xy^3 + 2y^4.$$

Задание №3.

Решить систему уравнений над полем C, исключив переменную x (двумя способами):

$$\begin{cases} 5x^2 - 6xy + 5y^2 - 16 = 0 \\ 2x^2 - (y + 1)x + y^2 - y - 4 = 0. \end{cases}$$

Задание №4.

Решить иррациональное уравнение:

$$\sqrt[4]{8 - x} + \sqrt[4]{89 + x} = 5.$$

Вариант 3.

Задание№1.

Данный симметрический многочлен выразить через основные симметрические многочлены $\sigma_1, \sigma_2, \sigma_3$:

$$f = (x_1 x_2 + x_3 x_4)(x_1 x_3 + x_2 x_4)(x_1 x_4 + x_2 x_3).$$

Задание №2.

Разложить на множители, неприводимые над полем R, симметрический однородный многочлен 4-й степени:

$$f(x, y) = 3x^4 - 8x^3 y + 14x^2 y^3 - 8xy^3 + 3y^4.$$

Задание №3.

Решить систему уравнений над полем C, исключив переменную x (двумя способами):

$$\begin{cases} x^2 - 5y^3 + 2 = 0 \\ 2x^2 + y^2 - 7 = 0. \end{cases}$$

Задание №4.

Решить иррациональное уравнение:

$$x + \sqrt{17 - x^2} + x\sqrt{17 - x^2} = 9.$$

Вариант 4.

Задание№1.

Данный симметрический многочлен выразить через основные симметрические многочлены $\sigma_1, \sigma_2, \sigma_3$:

$$f = x_1^4 + x_2^4 + x_3^4 - x_2^2 x_1^2 - x_3^2 x_1^2 - x_3^2 x_2^2.$$

Задание №2.

Разложить на множители, неприводимые над полем R, симметрический однородный многочлен 4-й степени:

$$f(x, y) = 18x^4 - 21x^3 y - 94x^2 y^2 - 21xy^3 + 18y^4.$$

Задание №3.

Решить систему уравнений над полем C, исключив переменную x (двумя способами):

$$\begin{cases} x^3 - xy - y^3 + y = 0 \\ x^2 + x - y^2 = 1. \end{cases}$$

Задание №4.

Решить иррациональное уравнение:

$$\sqrt[4]{629 - x} + \sqrt[4]{77 + x} = 8.$$

ТЕСТ ДЛЯ АТТЕСТАЦИИ ПО АЛГЕБРЕ

I вариант.

1. Укажите номера алгебраических структур, являющихся группами:

1) <2Z+1; +>;

2) <Z; +>;

3) Матрицы порядка n с целыми элементами относительно умножения;

4) Нечётные подстановки чисел *1,2,….,n* относительно умножения;

5) Действительные многочлены любой степени (включая ноль) от неизвестного *x* относительно сложения.

Ответы:

1. 1), 4), 5);

2. 2), 5);

3. 2), 3), 4);

4. 3), 5).

2. Укажите номера алгебраических структур, являющихся кольцами:

1) <2Z; +, ·>;

2) <N; +, ·>;

3) Числа вида $a + b\sqrt{2}$ с целыми *a,b*;

4) Множество вещественных симметрических матриц порядка *n* относительно матричного сложения и умножения;

5) Множество многочленов степени *n* с действительными коэффициентами относительно сложения и умножения.

Ответы:

1. 2), 3), 5);

2. 1), 4);

3. 1), 4), 5);

4. 1), 3).

3. Какое из перечисленных утверждений является неверным:

1) Множество целых степеней числа 3 есть подгруппа мультипликативной группы Q\{0};

2) Множество {-1; 1} является подгруппой мультипликативной группы кватернионов;

3) Множество подстановок {(123), (132)} является подгруппой группы S_3;

4) Множество нечётных целых чисел относительно сложения не является подгруппой группы <Z; +>.

Ответы:

1. 4);

2. 3);

3. 2);

4. 1).

4. Порядок элемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ равен:

1) $p(a)=1$;

2) $p(a)=2$;

3) $p(a)=3$;

4) $p(a)=4$;

Ответы:

1. 2);

2. 3);

3. 1);

4. 4).

5. Какие из отображений групп $f : C^* \to R^*$ являются гомоморфизмами:

1) $f(z) = |z|$;

2) $f(z) = 2|z|$;

3) $f(z) = \frac{1}{|z|}$;

4) $f(z) = 1$.

Ответы:

1. 2), 4);

2. 1), 3);

3. 1), 4);

4. 2), 3).

6. Остаток при делении многочлена $f(x) = 3x^4 - 5x^3 + 2x^2 + 4x - 7$ на многочлен $g(x) = 3x^2 + x + 4$ равен:

1) $5\frac{1}{3}x + \frac{16}{3}$;

2) $2\frac{2}{3}x - \frac{16}{3}$;

3) $12x$;

4) $9\frac{2}{3}x + \frac{32}{3}$.

Ответы:

1. 2);

2. 4);

3. 1);

4. 3).

7. Кубическое уравнение $x^3 - 9x + 28 = 0$ имеет:

1) Три действительных корня;

2) Три комплексных корня;

3) Один действительный и два комплексно-сопряжённых корня;

4) Три действительных корня, два из которых равны.

Ответы:

1. 3);

2. 2);

3. 1);

4. 4).

8. Старший член многочлена $2x_1^2x_2^3x_4 + 4x_2^5x_3^2x_4^2 - 5x_1^3x_2^2x_4^6 + 7x_3^4x_4^7 - x_1x_2^3x_3^5$ в лексикографическом упорядочении равен:

1) $-5x_1^3x_2^2x_4^6$;

2) $2x_1^2x_2^3x_4$;

3) $4x_2^5x_3^2x_4^2$;

4) $7x_3^4x_4^7$.

Ответы:

1. 2);

2. 1);

3. 4);

4. 3).

9. Рациональными корнями многочлена $f(x) = 5x^3 + 7x^2 - 8x - 4$ являются числа:

1) -1; 2; $\frac{2}{5}$;

2) 1; -2; $\frac{1}{5}$;

3) -1; 2; $-\frac{2}{5}$;

4) 1; -2; $-\frac{2}{5}$.

Ответы:

1. 3);

2. 1);

3. 2);

4. 4).

10. Зная корни x_1=1, x_2=3, x_3= -2 кубического уравнения $x^3 + ax^2 + bx + c = 0$ с помощью теоремы Виета найти $a+b+c$:

II вариант.

1. Укажите номера алгебраических структур, являющихся группами:

1) Положительные действительные числа, если операция определяется так $a * b = a^2b^2$;

2) <N; +>;

3) <2Z; +>;

4) Действительные многочлены степени n от неизвестного x относительно сложения;

5) Степени данного действительного числа a, $a \neq 0, \pm 1$ с целыми показателями относительно сложения.

Ответы:

1. 3), 5);

2. 2), 3), 4);

3. 1), 5);

4. 2), 3), 5).

2. Укажите номера алгебраических структур, являющихся кольцами:

1) <C; +, ·>;

2) Матрицы порядка n с целыми элементами относительно сложения и умножения матриц;

3) <2Z+1; +, ·>;

4) <N; +, ·>;

5) Множество вещественных чисел вида $a + b\sqrt[5]{2}$, где $a, b \in$ Q.

Ответы:

1. 2), 3);

2. 2), 4), 5);

3. 1), 2);

4. 1), 3).

3. Какое из перечисленных утверждений является неверным:

1) Натуральные числа не являются подгруппой группы целых чисел относительно сложения;

2) Множество матриц $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ является подгруппой мультипликативной группы невырожденных матриц;

3) Действительные многочлены степени n от неизвестного x не являются подгруппой действительных многочленов степени $\leq n$ от неизвестного x относительно сложения;

4) Множество {i, -i} является подгруппой группы кватернионов.

Ответы:

1. 4);

2. 3);

3. 2);

4. 1).

4. Порядок элемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ равен:

1) $p(a)=1$;

2) $p(a)=2$;

3) $p(a)=3$;

4) $p(a)=4$;

Ответы:

1. 2);

2. 3);

3. 1);

4. 4).

5. Какие из отображений групп $f : C^* \to R^*$ являются гомоморфизмами:

1) $f(z) = 1 + |z|$;

2) $f(z) = |z|$;

3) $f(z) = 2|z|$;

4) $f(z) = (|z|)^2$.

Ответы:

1. 1), 4);

2. 3), 4);

3. 1), 3);

4. 2), 4).

6. Остаток при делении многочлена $f(x) = 9x^4 + 2x^2 - 7x + 8$ на многочлен $g(x) = 3x^2 - 5x + 3$ равен:

1) $22x - 10$;

2) $8x - 10$;

3) $-52x+26$;

4) $16x+15$.

Ответы:

1. 2);

2. 4);

3. 1);

4. 3).

7. Кубическое уравнение $y^3-\frac{25}{3}y+\frac{250}{27}=0$ имеет:

1) Три действительных корня;

2) Три комплексных корня;

3) Один действительный и два комплексно-сопряжённых корня;

4) Три действительных корня, два из которых равны.

Ответы:

1. 3);

2. 2);

3. 4);

4. 1).

8. Старший член многочлена $4x_1^3x_2-3x_1^2x_3^6+5x_2x_4-7x_1^3x_3^3x_4^4+10x_1^2x_2^5$ в лексикографическом упорядочении равен:

1) $4x_1^3x_2$;

2) $-3x_1^2x_3^6$;

3) $10x_1^2x_2^5$;

4) $-7x_1^3x_3^3x_4^4$.

Ответы:

1. 2);

2. 4);

3. 1);

4. 3).

9. Рациональными корнями многочлена $f(x) = 2x^3 + 3x^2 - 3x - 2$ являются числа:

1) 2; $-\frac{1}{4}$; 1;

2) 2; $-\frac{1}{2}$; 1;

3) -2; $\frac{1}{4}$; $-\frac{1}{4}$;

4) 2; $\frac{1}{2}$; -1.

Ответы:

1. 3);

2. 1);

3. 2);

4. 4).

10. Зная корни x_1=2, x_2= -4, x_3= 3 кубического уравнения $x^3 + ax^2 + bx + c = 0$ с помощью теоремы Виета найти $a+b+c$:

III вариант.

1. Укажите номера алгебраических структур, являющихся группами:

1) $<Z^+ \cup \{0\}; +>$;

2) $<nZ, n \in N; +>$;

3) Положительные действительные числа, если операция определяется так: $a * b = a^b$;

4) $<Q; \cdot >$;

5) Невырожденные матрицы порядка n с действительными элементами относительно умножения.

Ответы:

1. 1), 5);

2. 2), 3), 4);

3. 4), 5);

4. 2), 5).

2. Укажите номера алгебраических структур, являющихся кольцами:

1) Матрицы порядка *n* с целыми элементами относительно сложения и умножения матриц;

2) Множество вещественных чисел вида $x + y\sqrt[3]{2}$, где $x, y \in$ Q, относительно сложения и умножения;

3) <R; +, ·>;

4) Множество вещественных ортогональных матриц порядка *n* относительно сложения и умножения;

5) Множество многочленов третьей степени относительно сложения и умножения.

Ответы:

1. 2), 5);

2. 4), 5);

3. 1), 3);

4. 1), 2).

3. Какое из перечисленных утверждений является неверным:

1) Множество <2Z; +> является подгруппой группы <Z; +>;

2) Множество подстановок {1, (12), (13), (23)} является подгруппой группы S_3;

3) Множество подстановок {(123), (132)} является подгруппой группы S_3;

4) Повороты трёхмерного пространства R_3 относительно данной точки *O* являются подгруппой движений трёхмерного пространства R_3 относительно композиции движений.

Ответы:

1. 2);

2. 4);

3. 1);

4. 3).

4. Порядок элемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ равен:

1) $p(a)=1$;

2) $p(a)=2$;

3) $p(a)=3$;

4) $p(a)=4$;

Ответы:

1. 1);

2. 3);

3. 2);

4. 4).

5. Какие из отображений групп $f : C^* \to R^*$ являются гомоморфизмами:

1) $f(z) = 1$;

2) $f(z) = 2$;

3) $f(z) = (|z|)^2$;

4) $f(z) = \frac{1}{|z|}$.

Ответы:

1. 2), 3);

2. 1), 2);

3. 3), 4);

4. 1), 3).

6. Остаток при делении многочлена $f(x) = 6x^4 + 4x^3 - 4x^2 + 1$ на многочлен $g(x) = 2x^2 - 1$ равен:

1) $2x + \frac{3}{2}$;

2) $2x + \frac{1}{2}$;

3) $-2x^2 + 2x + \frac{3}{2}$;

4) $-2x+\frac{3}{2}$.

Ответы:

1. 2);

2. 4);

3. 3);

4. 1).

7. Кубическое уравнение $x^3-6x+4=0$ имеет:

1) Три комплексных корня;

2) Три действительных корня;

3) Один действительный и два комплексно-сопряжённых корня;

4) Три действительных корня, два из которых равны.

Ответы:

1. 2);

2. 3);

3. 4);

4. 1).

8. Старший член многочлена $f(x)=5x_1^4x_3^3+10x_2^3x_1+7x_1^4x_2^2x_3^3+8x_1^2x_2x_3+2x_1^3x_2^5x_3^2$ в лексикографическом упорядочении равен:

1) $10x_2^3x_1$;

2) $5x_1^4x_3^3$;

3) $7x_1^4x_2^2x_3^3$;

4) $2x_1^3x_2^5x_3^2$.

Ответы:

1. 2);

2. 4);

3. 3);

4. 1).

9. Рациональными корнями многочлена $f(x)=8x^3-6x^2-6x+1$ являются числа:

1) $\frac{1}{2}; -\frac{1}{8};$

2) $-\frac{1}{2}; \frac{1}{4};$

3) $\frac{1}{4}; \frac{1}{8};$

4) $-\frac{1}{2}; -\frac{1}{4}.$

Ответы:

1. 3);

2. 1);

3. 4);

4. 2).

10. Зная корни x_1=1, x_2= 3, x_3= 6 кубического уравнения $x^3 + ax^2 + bx + c = 0$ с помощью теоремы Виета найти $a+b+c$:

IV вариант.

1. Укажите номера алгебраических структур, являющихся группами:

1) Матрицы порядка n с действительными элементами относительно умножения;

2) $<Q^+; \div>$;

3) $<Q; +>$;

4) $<Z; - >$;

5) Чётные подстановки чисел $1,2,\ldots,n$ относительно умножения.

Ответы:

1. 1), 3);

2. 4);

3. 3), 5);

4. 2), 4).

2. Укажите номера алгебраических структур, являющихся кольцами:

1) Функции с действительными значениями, непрерывные на [-1;1], относительно обычных сложения и умножения функций;

2) $<N; +, \cdot>$;

3) $<Z^+; +, \cdot>$;

4) Числа вида $a + b\sqrt{3}$ с рациональными a и b;

5) Множество вещественных симметрических матриц порядка n относительно матричного сложения и умножения.

Ответы:

1. 2), 5);

2. 1), 4);

3. 1), 2), 5);

4. 1), 3).

3. Какое из перечисленных утверждений является неверным:

1) Множество {-1, 1, -j, j} является подгруппой группы кватернионов;

2) Множество подстановок нечётной степени является подгруппой симметрической группы S_n относительно умножения;

3) Матрицы порядка n с действительными элементами и определителями, равными ±1, являются подгруппой группы невырожденных матриц порядка n с действительными элементами относительно умножения;

4) Параллельные переносы трёхмерного пространства R_3 относительно композиции движений.

Ответы:

1. 1);

2. 3);

3. 2);

4. 4).

4. Порядок элемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$ равен:

1) $p(a)=1$;

2) $p(a)=2$;

3) $p(a)=3$;

4) $p(a)=4$;

Ответы:

1. 2);

2. 3);

3. 1);

4. 4).

5. Какие из отображений групп $f : C^* \to R^*$ являются гомоморфизмами:

1) $f(z) = |z|$;

2) $f(z) = 1$;

3) $f(z) = 1 + |z|$;

4) $f(z) = 2$.

Ответы:

1. 1), 3);

2. 1), 2);

3. 3), 4);

4. 2), 4).

6. Остаток при делении многочлена $f(x) = x^4 + 2x^3 + 6x^2 - 6x + 10$ на многочлен $g(x) = x^2 + 2x - 6$ равен:

1) $-26x - 2$;

2) $28x + 2$;

3) $-14x - 38$;

4) $-46x + 58$.

Ответы:

1. 3);

2. 4);

3. 1);

4. 2).

7. Кубическое уравнение $x^3 - 6x + 9 = 0$ имеет:

1) Три действительных корня;

2) Три комплексных корня;

3) Один действительный и два комплексно-сопряжённых корня;

4) Три действительных корня, два из которых равны.

Ответы:

1. 2);

2. 4);

3. 3);

4. 1).

8. Старший член многочлена $6x_1^3 + 10x_1x_2x_3 + 13x_2^2x_4^6 + 3x_1^3x_2^2x_3x_4^3 + 8x_1^3x_2x_3^5x_4^3 + 9x_1^3x_2x_5^3$ в лексикографическом упорядочении равен:

1) $6x_1^3$;

2) $13x_2^2x_4^6$;

3) $3x_1^3x_2^2x_3x_4^3$;

4) $8x_1^3x_2x_3^5x_4^3$.

Ответы:

1. 2);

2. 4);

3. 1);

4. 3).

9. Рациональными корнями многочлена $f(x) = 9x^3 - 3x^2 - 24x + 4$ являются числа:

1) $-\frac{2}{3}; -\frac{2}{3}; 1;$

2) $-\frac{4}{3}; \frac{2}{3}; 1;$

3) $-\frac{2}{3}; \frac{2}{3}; -1;$

4) $\frac{4}{3}; -\frac{2}{3}; -1.$

Ответы:

1. 1);

2. 3);

3. 2);

4. 4).

10. Зная корни x_1=1, x_2= 2, x_3= -2 кубического уравнения $x^3 + ax^2 + bx + c = 0$ с помощью теоремы Виета найти $a+b+c$:

6. КАРТА КАДРОВОЙ ОБЕСПЕЧЕННОСТИ ДИСЦИПЛИНЫ

Лектор – старший преподаватель кафедры МАиМ Кван Наталья Владимировна (стаж работы в вузе 14 лет); ассистент Грек Надежда Анатольевна (стаж работы в вузе 4 года).

ведущий практические занятия – старший преподаватель кафедры МАиМ Кван Наталья Владимировна (стаж работы в вузе 14 лет); ассистент Грек Надежда Анатольевна (стаж работы в вузе 4 года).

.

ОГЛАВЛЕНИЕ