Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»

УТВЕРЖДЕНО
Проректор по учебной работе
А.А. Воронов
19 октября 2021 г.

ПРОГРАММА

по дисциплине: **Основы высшей алгебры и теории кодирования**
по направлению подготовки: 03.03.01 «Прикладные математика и физика»
школа: **ФПМИ**
кафедра: **математических основ управления**
курс: 1
семестр: 2
Трудоёмкость:
вариативная часть – 4 зач. ед.
лекции – 30 часов Экзамен – 2 семестр
практические (семинарские)
занятия – нет
лабораторные занятия – 30 часов

ВСЕГО АУДИТОРНЫХ ЧАСОВ – 60 Самостоятельная работа –120 часов

Программу и задание составили:
академик РАН, проф. Ю.И. Журавлёв, чл.-корр. РАН, проф. Ю.А. Флёров, к.ф.-м.н., доцент М.Н. Вялый, к.т.н. К.В. Чувилин, к.ф.-м.н. А.А. Рубцов, к.ф.-м.н. С.А. Шестаков, к.ф.-м.н. А.В. Зухба, к.ф.-м.н. Е.Г. Молчанов

Программа принята на заседании
кафедры математических основ управления
25 июня 2021 года

Заведующий кафедрой С. А. Гуз

Основы теории полугрупп, групп, колец и полей

1. Элементарная теория чисел: делимость, деление с остатком, вычеты. Свойства арифметических действий с вычетами. Наибольший общий делитель. Взаимно простые числа. Обратимость вычетов.
2. Алгебраические структуры. Бинарные операции. Группы. Примеры групп. Циклические группы. Аддитивная группа вычетов по модулю n. Мультипликативная группа вычетов по модулю n. Группа перестановок (симметрическая группа). Цикловое разложение перестановки. Группы геометрических преобразований.
3. Подгруппы. Порождающие или образующие элементы группы. Прямые произведения групп.
4. Левые и правые смежные классы группы по подгруппе. Индекс подгруппы. Порядок элемента группы. Теорема Лагранжа. Малая теорема Ферма, теорема Эйлера.
5. Изоморфизмы, автоморфизмы и гомоморфизмы групп. Четные и нечетные перестановки.
6. Фактор-группы. Ядро гомоморфизма. Теорема о гомоморфизме групп.
7. Сопряженные элементы и сопряженные подгруппы. Нормальные подгруппы. Внутренние автоморфизмы групп.
8. Действия групп. Теорема Кэли. Лемма Бернсайда.
9.
10. Кольца, поля. Примеры колец. Кольцо целых чисел. Кольца классов вычетов в кольце целых чисел и кольце многочленов. Прямые суммы колец. Подкольцо. Обратимые элементы кольца, группа обратимых элементов кольца, делители нуля. Нильпотентные элементы.
11. Поля. Примеры полей. Характеристика поля. Простое подполе.
12. Кольцо многочленов над кольцом (полем). Лемма о количестве корней многочлена с коэффициентами в поле. Приложения: критерий квадратичного вычета по простому модулю, цикличность мультипликативной группы конечного поля. Первообразные корни.
13. Левые, правые и двусторонние идеалы. Главные идеалы. Максимальные и простые идеалы. Кольца классов вычетов. Идеалы в кольцах многочленов. Факторкольцо. Теорема о гомоморфизме колец.
14. Деление с остатком в кольцах целых чисел и многочленов над кольцом целых чисел. Евклидовы кольца. Идеалы в евклидовых кольцах. Факториальность евклидовых колец. Китайская теорема об остатках.
15. Алгоритм Евклида в евклидовых кольцах. Решение линейных диофантовых уравнений.
16. Неприводимые многочлены и максимальные идеалы в кольце многочленов. Алгебраические расширения полей. Поле разложения. Конечные поля: существование и единственность.
17. Корректирующие коды. Код Хэмминга, коды БЧХ. Оценка размерности и кодового расстояния для кодов БЧХ.

Литература

Основная

1. *Журавлёв Ю.И., Флёров Ю.А., Вялый М.Н.* Дискретный анализ. Основы высшей алгебры. Москва : МЗ Пресс, 2006.
2. *Кострикин А.И.* Введение в алгебру. Москва : Физматлит, 2004.
3. *Винберг Э.Б.* Курс алгебры. 2-е изд., испр. и доп. — Москва : Факториал Пресс, 2001. — 544 с.
4. *Курош А.Г.* Курс высшей алгебры. 17-е изд., стереотипное. — Санкт-Петербург : Лань, 2008. — 544 с.
5. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. 5-е изд., стереотипное — Санкт-Петербург: Лань, 2009. — 288 с.

Дополнительная литература

1. *Ван-дер-Варден Б.Л.* Алгебра. Москва : Наука, 1976.
2. *Ленг С.* Алгебра. Москва : Мир, 1971.
3. *Виноградов И.М.* Основы теории чисел. Москва : Наука, 1972.

ЗАДАНИЯ

Обязательные задачи

1. Корни уравнения $x^n = 1$ как действительные, так и комплексные называются корнями n-й степени из единицы. Проверить, что корни n-й степени образуют группу по умножению. (а) Верно ли, что всякий корень 35-й степени из единицы является кубом некоторого корня 35-й степени из единицы? (б) Тот же вопрос про корни 36-й степени из единицы.
2. C_{360} – циклическая группа порядка 360. Найти число решений уравнения $x^k=e$ и количество элементов порядка k в группе C_{360} при а) $k = 7$; б) $k = 12$; в) $k = 48$. Сколько в C_{360} порождающих элементов?
3. Уравнение $x^{12} = e$ имеет 14 решений в группе G. Доказать, что группа G не является циклической.
4. Доказать, что в группе S_8 нет элементов порядка 56.
5. Найти порядок перестановки (123)(4567)(89) и количество сопряженных ей перестановок в группе S_9. Является ли эта перестановка четной?
6. Доказать, что все элементы порядка 11 сопряжены в S_{11}.
7. Порождают ли перестановки порядка 11 группу S_{11}?
8. Построить некоммутативную группу минимального порядка.
9. Вычислить (а) $12^{257} \bmod 17$; (б) $10^{111} \bmod 121$.

10. Найти порядок элемента (2,5) в прямом произведении циклических групп $C_{16} \times C_{12}$.

11. Доказать, что группа вращений трехмерного куба изоморфна группе S_4.

12. Пусть G – группа вращений трехмерного куба, а H_v – ее подгруппа, состоящая из тех вращений, которые оставляют вершину v на месте. Указать повороты на 90º и на 180º из одного левого смежного класса по подгруппе H_v.

13. Существует ли сюръективный гомоморфизм а) $C_{24} \times C_{18}$ на C_{16}; б) $C_{25} \times C_{18}$ на C_{15}?

14. Доказать, что подгруппа, порожденная некоторым классом сопряженных элементов группы G, является нормальным делителем группы G.

15. Найти число различных раскрасок ребер трехмерного куба в два цвета. Две раскраски считаются различными, если нельзя добиться совпадения цветов ребер вращениями куба.

16. (а) Построить гомоморфизм φ аддитивной группы рациональных чисел $(Q,+)$, ядром которого является подгруппа целых чисел $(Z,+)$. (б) Проверить, что $(Q,+)$ / Ker φ бесконечна, но все ее элементы имеют конечный порядок.

17. Доказать, что если элемент a кольца R не является делителем нуля, то из $ax = ay$ следует $x = y$. И наоборот: если элемент a кольца R является делителем нуля, то для некоторых $x \neq y$ выполняется $ax = ay$.

18. Ненулевой элемент кольца K называется нильпотентным, если $x^n = 0$ при некотором n. Показать, что:
а) нильпотентность x влечет обратимость $1\text{-}x$, если K – кольцо с единицей;

б) кольцо $Z_m = Z / m\ Z$ содержит нильпотентные элементы в том и только том случае, если m делится на квадрат натурального числа, большего единицы;

в) множество нильпотентных элементов коммутативного кольца вместе с нулевым элементом образует подкольцо. Привести опровергающий пример в некоммутативном случае.

19. Является ли кольцом главных идеалов кольцо Z_{72}?

20. Решить линейное диофантово уравнение $33x + 23y = 4$.

21. Решить сравнения: $21x \equiv 13 \bmod 34$, $7x \equiv 2 \bmod 73$.

22. Решить систему сравнений

a. $x \equiv 1 \bmod 33$,

b. $x \equiv -1 \bmod 23$.

23. Найти наибольший общий делитель многочленов $x^{48} - 1$ и $x^{20} - 1$.

24. Найти порядок группы обратимых элементов кольца Z_{72}.

25. Сумма идеалов $I_1 + I_2$ – это идеал, порожденный всеми суммами элементов из идеалов I_1 , I_2 . Аналогично, произведение идеалов $I_1 I_2$ – это идеал, порожденный всеми произведениями элементов из I_1 , I_2 . Пусть I_1 порожден в $Q[x]$ многочленом x^2-x, а I_2 порожден многочленом x^2+x. Найти I_1+I_2 , $I_1 I_2$, $I_1 \cap I_2$.

26. Являются ли полями следующие кольца вычетов:

а) $Q[x]/(x^3+1)$; б) $F_3[x]/(x^3+2)$; в) $F_7[x]/(x^3+3)$;

г) $Q[x]/(x^4+1)$; д) $F_3[x]/(x^4+1)$; е) $F_{17}[x]/(x^4+1)$?

27. Многочлен $f(x)$ над полем F_5 степени 2 принимает значение 1 в точке 1, значение 2 в точке 3 и значение 3 в точке 4. Найти $f(x)$.

28. Ненулевой элемент a поля $Z_p = Z / p\ Z$ называется квадратичным вычетом по модулю p, если уравнение $x^2 = a$ имеет решение в поле Z_p. В противном случае a называется квадратичным невычетом. а) Найти сумму всех квадратичных вычетов по модулю 73. б) Найти произведение всех квадратичных невычетов по модулю 103.

29. Найти все первообразные корни по модулю 29.

30. Решить уравнение

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \bmod 29.$$

31. а) Доказать, что в любом поле характеристики 2 уравнение $x^2 + x + 1$ либо имеет ровно 2 различных корня, либо не имеет корней вовсе. б) Сколько решений имеет уравнение $x^2 + x + 1$ в поле из 512 элементов?

Дополнительные задачи

Д1. Построить группу G, в которой уравнение $x^{12} = e$ имеет ровно 14 решений.

Д2. Пусть G – группа, порожденная элементами a и b, для которых выполняются соотношения $ab = ba$, $a^2 = b^2$, $a^4 b^4 = e$. Найти порядок группы G. Является ли эта группа циклической?

Д3. Построить подгруппу порядка 56 группы S_8. (*указание*: используйте поле из 8 элементов.)

Д4. Указать две несопряженные изоморфные подгруппы порядка 12 в S_{11}.

Д5. Доказать, что если H – собственная подгруппа конечной группы G, то объединение сопряженных с H подгрупп не содержит всех элементов группы.

Д6. Пусть G – абелева группа и H – подгруппа всех ее элементов конечного порядка. Тогда в фактор-группе G/H все неединичные элементы имеют бесконечный порядок.

Д7. Укажите такую абелеву группу G и две такие ее изоморфные подгруппы H_1, H_2, что фактор-группы G/H_1 и G/H_2 неизоморфны.

Д8. Доказать, что группа автоморфизмов циклической группы абелева. Найти порядок группы автоморфизмов циклической группы порядка 12. Является ли эта группа циклической?

Д9. Доказать, что нормальная подгруппа индекса k содержит все элементы, порядки которых взаимно просты с k.

Д10. Построить некоммутативную группу порядка 8, все подгруппы которой нормальны.

Д11. Доказать, число элементов, сопряженных с элементом a в группе G, равно индексу $N(a)$ в группе G, т.е. числу смежных классов по подгруппе $N(a)$ – нормализатору элемента a:

$$N(a) = (g \mid ga = ag \quad \forall g \in G).$$

Д12. Коммутант группы – это подгруппа, порожденная коммутаторами, то есть элементами вида $xyx^{-1}y^{-1}$. Доказать, что коммутант является нормальной подгруппой.

Д13. Доказать, что фактор-группа G/H абелева тогда и только тогда, когда H содержит коммутант K группы G.

Д14. Доказать, что если порядок абелевой группы G равен nm, где $(n,m) = 1$, то G изоморфна прямому произведению групп порядков n и m.

Д15. Группа называется p-группой, если ее порядок является степенью простого числа p. Центром группы называется множество элементов, коммутирующих со всеми элементами группы. Доказать, что центр p-группы состоит не только из единичного элемента.

Д16. Доказать, что всякая группа порядка p^2, где p – простое число, абелева.

Д17. Пусть порядок группы G равен $p^n m$, где p – простое число и $(p,m) = 1$. (а) Доказать, что в группе G есть подгруппа порядка p^n (силовская p-подгруппа). (б) Доказать, что любая p-подгруппа группы G содержится в силовской p-подгруппе. (в) Доказать, что все силовские p-подгруппы сопряжены. (г) Доказать, что количество силовских p-подгрупп равно 1 по модулю p.

Д18. Пусть n делит порядок группы G. Доказать, что число решений уравнения $x^n = e$ делится на n (а) для абелевой группы; (б) для p-группы; (в) для произвольной группы.

Д19. Указать пример коммутативного кольца с единицей R и его подкольца R_1 таких, что R_1 также является кольцом с единицей u, но $1 \neq u$.

Д20. Построить кольцо из 21 элемента, в котором произведения принимают ровно три различных значения.

Д21. В коммутативном кольце R с $0 \neq 1$ уравнение $x^2 = 2$ имеет три различных решения. Доказать, что в R есть делители нуля.

Д22. Доказать, что кольцо гауссовых целых чисел

$$Z(i) = \{a + bi : a, b - \text{целые}\},\ i^2 = -1,$$

евклидово.

Д23. Проверить простоту элементов 17, 11, $2 + 3i$ в кольце $Z(i)$.

Д24. Является ли кольцо $Z(j) = \{a + bj : a, b - \text{целые}\}$, $j^2 = -6$, евклидовым кольцом?

Д25. Доказать, что любой элемент кольца $Z/143Z$ является суммой двух делителей нуля. Найти представление в виде суммы двух делителей нуля для элемента 17.

Д26. Найти все идеалы в кольце $F_2{}^n$ (n-я прямая степень поля F_2).

Д27. Доказать, что идеал (x) в кольце многочленов $Z[x]$ над кольцом целых чисел Z имеет в качестве собственного делителя идеал $(2, x)$. Показать, что оба идеала при этом являются простыми.

Д28. Доказать, что кольцо многочленов $Z[x]$ над кольцом целых чисел Z не является евклидовым.

Д29. (а) Привести пример коммутативного кольца с единицей, в котором некоторый простой элемент порождает идеал, не являющийся простым. (б) Привести пример коммутативного кольца с единицей, в котором некоторый простой идеал не является идеалом, порожденным простым элементом.

Д30. Построить пример коммутативного кольца с единицей, в котором разложение на простые множители неоднозначно.

Д31. Найти наибольший порядок элемента мультипликативной группы кольца Z_{72}.

Д32. Найти количество нильпотентных элементов в кольце

$$F_7[x]/(x^{14} + x^7 + 2).$$

Д33. Найти порядок группы обратимых элементов колец

(а) $F_7[x]/(x^2 + 3x - 5)$; (б) $F_3[x]/(x^2 + x + 1)$.

Д34. Построить изоморфизм полей $F_5[x]/(x^2-2)$ и $F_5[x]/(x^2-3)$.
Д35. Найти наименьшее конечное поле характеристики 2, в котором многочлен $x^{14}+1$ раскладывается на линейные множители.
Д36. Сколько различных решений имеет уравнение $1+x^2+x^8++x^{26}=0$ в поле F_{81} из 81 элемента?
Д37. Элемент a порождает мультипликативную группу поля F из 343 элементов. Является ли многочлен $x^2+ax-a+2a^2$ неприводимым в кольце многочленов $F[x]$?
Д38. Указать степени неприводимых делителей многочленов (а) x^5-2 из кольца $F_{67}[x]$; (б) $x^{28}-1$ из кольца $F_3[x]$.
Д39. Найти порядок группы GL(2,4) обратимых линейных отображений векторного пространства $F_2{}^4$ в себя. Существует ли в этой группе элемент порядка 5?

Подписано в печать 19.10.2021. Формат $60\times84\,{}^{1}\!/_{16}$. Усл. печ. л. 0,5.
Тираж 160 экз. Заказ № 169.

Федеральное государственное автономное образовательное учреждение
высшего образования «Московский физико-технический институт
(национальный исследовательский университет)»
141700, Московская обл., г. Долгопрудный, Институтский пер., 9
Тел. (495) 408-58-22. E-mail: rio@mipt.ru

Отдел оперативной полиграфии «Физтех-полиграф»
141700, Московская обл., г. Долгопрудный, Институтский пер., 9
Тел. (495) 408-84-30. E-mail: polygraph@mipt.ru