Алгебра. ИТМО. 1 курс, 2022-23

Глава 0. Основные понятия

1. Кольцо, поле, типы колец.
2. Свойства 0, 1 и обратных элементов. Вычитание и деление.
3. Подкольцо и подполе.
4. Гомоморфизмы колец. Ядро и образ гомоморфизма.
5. Типы гомоморфизмов. Мономорфизм и ядро.
6. Отображение, обратное к изоморфизму — изоморфизм.
7. Изоморфные кольца.
8. Идеал. Ядро гомоморфизма является идеалом.
9. Идеал и обратимые элементы. Идеалы в поле. Гомоморфизм из поля — инъекция.
10. Идеал, порожденный множеством элементов. Главный идеал.
11. Сравнения по модулю идеала. Вычеты.
12. Факторкольцо
13. Теорема о гомоморфизме колец.
14. Дроби: эквивалентность, простейшие свойства. Сложение и умножение дробей.
15. Поле частных.
16. Вложение кольца в поле частных.
17. Характеристика поля.
18. Теорема о подполе.

1. Комплексные числа

1. Вещественная и мнимая часть, умножение, сложением, норма, модуль.
2. Поле комплексных чисел.
3. Тригонометрическая форма записи комплексного числа. Изменение модуля и аргумента при перемножении комплексных чисел. Формула Муавра.
4. Вложение вещественных чисел в комплексные.
5. Извлечение корня из комплексного числа. Корни из 1.

2. Целые числа

1. Делимость. Свойства. Теорема о делении с остатком
2. НОД. Свойства.
3. Алгоритм Евклида. Следствия из алгоритма Евклида.
4. Линейное представление НОД.
5. НОД нескольких чисел через НОД двух чисел. Линейное представление НОД нескольких чисел.
6. Взаимно простые числа. Свойства.
7. Простые числа, свойства. Бесконечность количества простых.
8. Основная теорема арифметики в $\mathbb{Z}$.
9. Каноническое разложение. Количество натуральных делителей числа.
10. Представление НОД чисел через их канонические разложения.
11. Линейные диофантовы уравнения с двумя неизвестными.
12. Идеалы в $\mathbb{Z}$
13. Линейное представление НОД: доказательство существования с помощью идеала.
14. Сравнения по модулю натурального числа, свойства. Вычеты.
15. Полная система вычетов, свойства.
16. Приведенная система вычетов, свойства.
17. Теорема Эйлера.
18. Мультипликативность функции Эйлера.
19. Функция Эйлера: значение на степени простого числа, явный вид.

20. Сумма функции Эйлера по делителям числа.
21. Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю.
22. Алгоритм поиска обратного вычета. Решение сравнения с одним неизвестным.
23. Делимость на попарно взаимно простые числа.
24. Китайская теорема об остатках.
25. Алгоритмы поиска решения для КТО.
26. Функция Мёбиуса. Сумма функции Мёбиуса по промежуточным делителям.
27. Формула обращения Мёбиуса, аддитивный вариант.
28. Вывод формулы для функции Эйлера из формулы обращения Мёбиуса.
29. Формула обращения Мёбиуса, мультипликативнй вариант.
30. Сумма мультипликативной функции по делителям числа мультипликкативна.
31. Сумма натуральных делителей числа.
32. Первообразные корни из 1 в $\mathbb{C}$.

3. Многочлены над полем

1. Сложение и умножение многочленов. Степень многочлена. Свойства.
2. Кольцо многочленов.
3. Вложение K в $K[t]$. Константы. Ассоциированные многочлены.
4. Теорема о делении с остатком в кольце многочленов над полем.
5. Делимость многочленов. Свойства.
6. Идеалы в кольце многочленов над полем.
7. НОД в кольце многочленов над полем: теорема о линейном представлении.
8. Свойства НОДа в кольце многочленов над полем.
9. Вычисление НОДа нескольких многочленов через НОДы двух.
10. Взаимно простые многочлены. Свойства.
11. Неприводимые многочлены. Свойства.
12. Основная теорема арифметики в кольце многочленов над полем. Каноническое разложение.
13. Значение многочлена в точке. Корень многочлена. Теорема Безу.
14. Кратность корня. Теорема о сумме кратностей корней.
15. Производная многочлена. Производная суммы и произведения.
16. Производная многочлена, раскладываемого на линейные множители.
17. Определение кратности корня многочлена с помощью производной.
18. Основная теорема алгебры (формулировка). Неприводимые многочлены в $\mathbb{C}[t]$, разложение на линейные множители многочлена в $\mathbb{C}[t]$.
19. Сопряженные корни. Теорема о корнях многочлена с вещественными коэффициентами.
20. Неприводимые многочлены в $\mathbb{R}[t]$, разложение на неприводимые множители многочлена в $\mathbb{R}[t]$.
21. Теорема Виета.
22. Интерполяция: формула Лагранжа.
23. Метод интерполяции по Ньютону.
24. Рациональные функции над полем. Правильные дроби и их свойства.
25. Разложение правильной дроби в сумму правильных дробей, знаменатели которых — степени неприводимых многочленов.
26. Разложение правильной дроби в сумму простейших.
27. Связь задачи разложения правильной дроби в сумму простейших с интерполяцией. Критерий отсутствия кратных корней.
28. Поле $\mathbb{C}$, как факторкольцо $\mathbb{R}[x]$.
29. Многочлен деления круга. Представление $t^n - 1$ в виде произведение многочленов деления круга.
30. Многочлен деления круга: формула, целые коэфициенты.

4. Многочлены и теория чисел

1. Показатель, к которому принадлежит вычет. Свойства.

2. Количество корней многочлена $t^d - 1$ в $\mathbb{Z}_p$, где $p - 1 \vdots d$.

3. Количество вычетов, принадлежащих к показателю d.

4. Первообразный корень по простому модулю и их количество. Структура приведенной системы вычетов.

5. Квадратичные вычеты и невычеты в $\mathbb{Z}_p$, их количества.

6. Умножение квадратичных вычетов и невычетов на квадратичные вычеты и невычеты.

7. Решение квадратных уравнений в $\mathbb{Z}_p$.

8. Символ Лежандра. Свойства. ($\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Вычисление $\left(\frac{-1}{p}\right)$.)

9. Формула $(\frac{a}{p}) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$.

10. Формула $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$ при нечетном a и вычисление $\left(\frac{2}{p}\right)$.

11. Квадратичный закон взаимности Гаусса.

12. Лемма Гаусса и следствие о содержании произведения многочленов.

13. Лемма о связи разложений многочлена с целыми коэффициентами на множители в $\mathbb{Q}[x]$ и в $\mathbb{Z}[x]$. Эквивалентность неприводимости в $\mathbb{Z}[x]$ и в $\mathbb{Q}[x]$.

14. ОТА в $\mathbb{Z}[x]$.

15. Критерий Эйзенштейна.

16. Свойства рациональных корней и значений в целых точках многочленов с целыми коэффициентами.

17. Разностный многочлен.

5. Линейные пространства

1. Линейное пространство. Свойства.

2. Линейное подпространство.

3. Линейная комбинация, линейная оболочка. Порождающая система векторов.

4. Линейно зависимые и линейно независимые системы векторов и их свойства.

5. Однородные системы линейных уравнений: приведение к ступенчатому виду, нетривиальное решение.

6. Лемма о линейной зависимости линейных комбинаций.

7. Базис, размерность. Корректность определения размерности. Разложение по базису.

8. Существование базиса в конечно порожденном пространстве. Выделение базиса из конечной порождающей системы.

9. Дополнение до базиса линейно независимой системы. в конечномерном пространстве.

10. Три эквивалентных определения базиса.

11. Сумма и пересечение линейных пространств.

12. Размерность суммы двух линейных пространств.

13. Прямая сумма. Свойство прямой суммы.

14. Критерий прямой суммы.

15. Размерность и базис прямой суммы конечного числа пространств.

16. Аффинные подпространства. Свойства.

17. Факторпространство и его размерность.

6. Теория групп

1. Группа, подгруппа. Простейшие свойства.

2. Подгруппа, порожденная множеством элементов.

3. Степени элементов и их свойства.

4. Циклическая группа.

5. Смежные классы.

6. Теорема Лагранжа.

7. Симметрическая группа. Разложение подстановки на независимые циклы и определение ее порядка.

8. Транспозиции.

9. Четные и нечетные подстановки. Транспозиция меняет четность.

10. Свойства четных и нечетных подстановок.

11. Группа A_n.

12. Гомоморфизм групп, ядро и образ. Свойства.

13. Типы гомоморфизмов. Свойства.

14. Отображение, обратное к изоморфизму. Изоморфные группы.

15. Автоморфизмы и сопряжения группы.

16. Нормальные подгруппы. Критерий нормальности.

17. Нормальность пересечения нормальных подгрупп. Нормальность ядра гомоморфизма.

18. Факторгруппа. Лемма о подгруппе факторгруппы.

19. Теорема о гомоморфизме групп.

20. Теорема о сокращении.

21. Коммутаторы и коммутант. Свойства.

22. Теорема об абелевой факторгруппе.

23. Действие группы на множестве. Примеры действий.

24. Стабилизатор: определение и свойства.

25. Орбита: определение и свойства. Связь мощностей орбиты и стабилизатора элемента.

26. Теорема Кэли.

27. Центр группы. Свойства.

28. Связь центра с группой сопряжений.

29. Центр p-группы.

30. Элемент порядка p в абелевой группе.

31. Первая теорема Силова и теорема Коши об элементе порядка p.

32. Вторая теорема Силова

7. Матрицы, определители и системы линейных уравнений

1. Матрицы. Сложение, умножение. Свойства. Кольцо квадратных матриц $M_n(K)$.

2. Определитель. Определение и свойства (1 элементарное преобразование, определитель с двумя одинаковыми строками).

3. Свойства определителя: умножение строки на число, разложение по строке, 2 элементарное преобразование.

4. Определитель транспонированной матрицы.

5. Минор, алгебраическое дополнение. Сумма произведений элементов строки матрицы на алгебраические дополнения этой (другой) строки (без доказательства теоремы Лапласа).

6. Теорема Лапласа.

7. Определитель ступенчатой матрицы.

8. Определитель произведения матриц.

9. Невырожденные (обратимые) матрицы. Матрица A обратима тогда и только тогда, когда определитель не равен 0. Обратимость матрицы, имеющей левую (правую) обратную.

10. Строчный и столбцовый ранг матрицы. Сохранение строчного ранга при элементарных преобразованиях строк.

11. Сохранение столбцового ранга при элементарных преобразованиях строк.

12. Равенство строчного и столбцового ранга матрицы.

13. Сохранение наибольшего порядка ненулевого минора матрицы при элементарных преобразованиях.

14. Равенство ранга матрицы и наибольшего порядка ненулевого минора. Ранг невырожденной матрицы.

15. Матрицы элементарных преобразований. Представление матрицы в виде произведения элементарных матриц.

16. Алгоритм поиска обратной матрицы с помощью элементарных преобразований строк.

17. Совместность системы линейных уравнений. Теорема Кронекера-Капелли.

18. Пространство решений однородной системы линейных уравнений.

19. Размерность пространства решений однородной системы линейных уравнений.

20. Решения неоднородной системы линейных уравнений.

8. Линейные отображения

1. Линейные отображения. Ядро и образ линейного отображения.

2. Соответствие линейных отображений и матриц.

3. Композиция линейных отображений и умножение матриц.

4. Сумма размерностей ядра и образа линейного отображения.

5. Размерности ядра и образа линейного отображения: связь с рангом матрицы отображения.

6. Ранг произведения матриц не превосходит рангов сомножиетелей.

7. Кольцо линейных операторов $\mathrm{End}(V)$, связь с кольцом матриц.

8. Обратимые линейные операторы и их свойства.

9. Координаты вектора в разных базисах. Матрицы перехода и их свойства.

10. Матрицы оператора в разных базисах. Свойства подобных матриц.

11. Многочлен от оператора и от матрицы, соответствие между ними.

12. Инвариантные подпространства.

13. Характеристический многочлен оператора. Корректность определения, свойства.

14. Теорема Гамильтона-Кэли.

15. Минимальный многочлен оператора.

16. Собственные числа, векторы и подпространства. Связь с характеристическим многочленом.

17. Линейная независимость собственных векторов разных собственных чисел. Сумма собственных пространств — прямая.

18. Диагонализируемые операторы и матрицы.

19. Корневые подпространства. Свойства.

20. Лемма о двух взаимно простых операторных многочленах.

21. Сумма корневых пространств — прямая.

22. Разложении пространства в прямую сумму корневых. Инвариантность корневых подпространств.

23. Размерность корневого подпространства.

24. Относительный базис.

25. Разбиение корневого пространства на ядра. Лемма о ЛНЗ векторов над W_{t-2}.

26. Лемма о дополнении до относительного базиса.

27. Жорданова нормальная форма оператора и жорданов базис: алгоритм построения.

9. Квадратичные формы и скалярное произведение

1. Квадратичные формы. Матрицы квадратичной формы в разных базисах.

2. Приведение квадратичной формы к диагональному виду.

3. Закон инерции квадратичных форм.
4. Положительно определенные квадратичные формы.
5. Вещественное и комплексное скалярное произведение. Свойства. Матрица Грама.
6. Неравенство Коши-Буняковского-Шварца.
7. Длина вектора.
8. Ортогональный и ортонормированный базис. Вычисление скалярного произведения.
9. Ортогонализация набора векторов.
10. Ортогональное дополнение: теорема о размерности и прямой сумме.
11. Свойства ортогонального дополнения: сумма и пересечение.
12. Теорема об изоморфизме, сохраняющем скалярное произведение.

10. Поля

1. Расширение полей. Степень расширения. Теорема о произведении степеней расширения.
2. Расширение поля, в которым многочлен имеет корень.
3. Алгебраические и трансцедентные элементы. Минимальный многочлен алгебраического элемента. Конечное расширение — алгебраическое.
4. Присоединение элементов к полю: определение и простейшие свойства.
5. Присоединение алгебраического элемента к полю.
6. Множество всех алгебраических над K элементов — поле.
7. Существование поля разложения многочлена, оценка степени расширения.
8. Единственность с точностью до изоморфизма поля разложения многочлена.
9. Количество элементов конечного поля — степень простого.
10. Существование и единственность с точностью до изоморфизма поля $\mathbb{F}_{p^n}$.
11. Подполя $\mathbb{F}_{p^n}$.
12. Мультипликативная группа конечного поля — циклическая.
13. Возведения в степень — автоморфизм конечного поля.
14. Теорема о минимальном многочлене примитивного элемента конечного поля. Существование неприводимого многочлена любой степени над $\mathbb{F}_q$.
15. Теорема о поле разложения неприводимого над $\mathbb{F}_q$ многочлена.
16. Разложение $x^{q^m} - x$ на множители в $\mathbb{F}_q[x]$.
17. Формула обращения Мёбиуса и количество неприводимых многочленов степени d в $\mathbb{F}_q[x]$.
18. Теорема о минимальном мноочлене элемента конечного поля.

11. Теория чисел и криптография

1. Криптосистема RSA.
2. Вероятностные тесты для проверки простоты. Тест Ферма. Числа Кармайкла.
3. Символ Якоби. Закон взаимности.
4. Первообразные корни.
5. Существование первообразного корня по модулю p^2.
6. Эйлеровы псевдопростые.
7. Тест Соловея-Штрассена.
8. Тест Миллера-Рабина.

12. Основы теории кодирования

1. Кодовое расстояние.
2. Линейные коды. Параметры. КОдовое расстояние линейного кода.
3. Скалярное произведение и ортогональное дополнение в $\mathbb{F}_q^n$.
4. Порождающая и проверочная матрицы линейного кода.
5. Теорема о столбцах проверочной матрицы. Граница Синглтона.
6. Граница Хэмминга и код Хэмминга.

7. Циклические коды. Теорема об идеале.
8. Порождающий многочлен циклического кода.
9. Теорема о размерности циклического кода. Порождающая матрица циклического кода.
10. Проверочный многочлен и проверочная матрица циклического кода.
11. Методы кодирования и декодирования циклического кода.
12. Нули циклического кода.
13. Граница БЧХ.
14. Коды БЧХ и коды Рида-Соломона.