Алгебра. ИТМО. Наслаждение. 1 курс, 2 сем, 2025

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. Кривые второго порядка на плоскости.
6. Вещественное и комплексное скалярное произведение. Свойства. Матрица Грама.
7. Неравенство Коши-Буняковского-Шварца.
8. Длина вектора.
9. Ортогональный и ортонормированный базис. Вычисление скалярного произведения.
10. Ортогонализация набора векторов.
11. Ортогональное дополнение: теорема о размерности и прямой сумме.
12. Свойства ортогонального дополнения: сумма и пересечение.
13. 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 многочлене 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.