

ПРОГРАММА КУРСА «ПРИКЛАДНАЯ АЛГЕБРА»  
2017 год.

**1. Группы (повторение), конечные группы**

Алгебраические операции, алгебраические системы, полугруппы, моноиды.

Единичный элемент (левый/правый), обратный элемент (левый/правый).

Группа.

Конечные группы малых порядков.

Циклические группы (+ факты о циклических группах).

Подгруппы. Критерии «подгрупповости».

Симметрические группы. Перестановки (определение, свойства, быстрое перемножение). Группа перестановок. Нормальные подгруппы группы перестановок. Чётность перестановки. Группа чётных перестановок.

Теорема Кэли.

Смежные классы.

Отношение эквивалентности в группе (через принадлежность смежным классам).

Сопряжённые элементы. Порядок элемента. Порядок группы.

Теорема Лагранжа (доказательство со вспомогательными леммами), ее следствия и невозможность обращения.

Нормальные делители. Факторгруппы.

Критерий нормальности делителя через сопряженные элементы.

Гомоморфизм, эпиморфизм, мономорфизм, группа автоморфизмов.

Внутренний автоморфизм, группа внутренних автоморфизмов.

Ядро и образ гомоморфизма.

Естественный (канонический) гомоморфизм. Свойства гомоморфизмов групп.

Теорема о гомоморфизмах групп.

Теорема Коши.

Прямое произведение групп.

Группы поворотов.

**Порождение групп, свободные группы.**

Центр группы.

Коммутант, коммутатор.

Циклические структуры, связь с сопряжённостью.

**Пример теоретического вопроса:** сформулировать и доказать теорему Коши.

**Пример задачи:** найти  $|\text{Aut}(\mathbb{Z}_2)| + |\text{Aut}(\mathbb{Z}_6)|$ .

**2. Кольца, евклидовы кольца, кольца многочленов**

Кольца (ассоциативные).

Целостные, коммутативные, нетривиальные кольца, кольца с 1.

Делители нуля.

Тело.

Кольцо классов вычетов.

Свойства сравнений. Корректность операций в кольце классов вычетов.

Гомоморфизмы колец. Теорема о гомоморфизмах колец.

Идеалы. Главные идеалы. Кольца главных идеалов.

Максимальные идеалы.

Простые идеалы.

Необходимое и достаточное условие для кольца классов вычетов быть полем (Теорема о максимальном идеале).

Евклидовы кольца. Свойства евклидовых колец (теоремы с доказательствами).

Наибольший общий делитель.

Собственные делители, ассоциированные элементы. Теорема о собственном делителе.

Разложение элементов в евклидовых кольцах.

Кольцо многочленов над полем (напоминание о нулях многочленов, теореме Безу).

Неприводимые (простые) многочлены (определение, построение, примеры).

Гомоморфизмы, изоморфизмы, автоморфизмы колец.

Идемпотенты. Нильпотенты.

Прямое произведение колец.

**Пример теоретического вопроса:** перечислить все известные Вам факты об евклидовых кольцах.

**Пример задачи:** найти все неприводимые многочлены второй степени над  $GF(3)$ .

### 3. Конечные поля

Поле. Характеристика поля.

Теорема о том, что конечное поле является векторным пространством.

Теорема о размерности кольца классов вычетов.

Теорема о минимальной функции элемента  $\bar{x}$  (элемента  $\{x\}$  в  $F[x]/(g(x))$ ).

Число элементов в конечном поле характеристики  $p$ .

Существование полей порядка  $p^m$  для всех простых  $p$  и целых положительных  $m$ .

Существование в конечном поле примитивного элемента (с доказательством вспомогательной леммы).

Уравнение, которому удовлетворяют все элементы конечного поля.

Минимальный многочлен (минимальная функция над подполем) элемента поля.

Теорема о разложении многочлена  $X^{p^m}-X$  на множители (со всеми вспомогательными леммами, формулировки, доказательства).

Критерий делимости многочленов вида  $X^n+1$ .

Теорема о делимости многочлена  $X^{p^n}+1$  на неприводимый многочлен.

Корни уравнения  $f(x)=a_0+\dots+a_nx^n=0$  с неприводимым многочленом  $f(x)$  в  $GF(p^m)$ ,  $n \leq m$  (Теоремы о корнях).

Трансцендентные и алгебраические элементы.

Поле рациональных дробей.

Решение систем и уравнений в полях.

**Пример теоретического вопроса:** доказать, что любое конечное поле является векторным пространством над любым своим подполем.

**Пример задачи:** разложить  $X^7+1$  на множители (над  $GF(2)$ ).

#### **4. Теория кодирования, коды БЧХ**

Кодирование.

Коды Боуза-Чоудхури-Хоквингема (БЧХ).

Оценка расстояния между кодовыми вершинами БЧХ.

Теорема о линейной независимости в проверочной матрице.

Теорема об идеалах в  $GF(p)[x]/(g(x))$ .

Теорема о размерности и базисах идеалов в  $GF(p)[x]/(g(x))$ .

Циклические линейные подпространства.

Теорема о циклических линейных подпространствах кольца классов вычетов по  $(X^n+1)$ .

Примеры кодов Хэмминга и Боуза-Чоудхури-Хоквингема (БЧХ).

Матрица Адамара (определение, примеры).

**Пример теоретического вопроса:** сформулировать и доказать теорему об идеалах в  $GF(p)[x]/(g(x))$ .

**Пример задачи:** привести пример кода БЧХ, который совпадает с кодом Хэмминга, построить его проверочную матрицу (булеву).

Не было в этом году:

Теорема Шеннона (только формулировка).

Префиксное кодирование, код Хаффмана (примеры).