

ЭКЗАМЕНАЦИОННАЯ ПРОГРАММА
ПО КУРСУ «ОБЩАЯ АЛГЕБРА»,
НАПРАВЛЕНИЕ ПОДГОТОВКИ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»,
2 КУРС, 1 СЕМЕСТР 2010-2011 УЧЕБНОГО ГОДА

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. Теорема о делении с остатком. Отношение делимости. Наибольший общий делитель, теорема существования и единственности. Взаимно простые числа, теорема о свойствах, равносильных взаимной простоте. Алгоритм Евклида. Простые числа. Определение и элементарные свойства простых чисел. Основная теорема арифметики. Каноническое разложение числа. Мультипликативные функции. Суммы, распространенные на все делители числа. Функция Мебиуса. Произведение Дирихле, преобразование Дирихле. Мультипликативность преобразования Дирихле мультипликативной функции. Функция Эйлера, мультипликативность функции Эйлера, вычисление функции Эйлера.

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ С ОДНОЙ ОПЕРАЦИЕЙ. Бинарная операция. Моноид. Единственность единичного элемента. Целые неотрицательные степени элемента.

Группа, аксиоматика, единственность обратного элемента, свойства обратного элемента, уравнение, определяющее единичный элемент. Конечные и бесконечные группы, порядок группы. Примеры групп. Строки и столбцы таблицы Кэли в случае групп, обоснование. Подгруппы, примеры собственные и несобственные подгруппы. Критерии, того, что подмножество является подгруппой. Порядок элемента группы, свойства порядка.

Циклическая группа, примеры циклических групп. Примеры нециклических групп. Подгруппа $\langle a \rangle$, связь ее порядка с порядком элемента a , определение цикличности в терминах $\langle a \rangle$. Критерий цикличности группы, следствия об образующих циклической группы. Теорема о подгруппах циклической группы, следствие о подгруппах \mathbb{Z} . Теорема о подгруппах конечной циклической группы.

Гомоморфизм, свойства гомоморфизмов. Ядро и образ гомоморфизма. Критерий инъективности и сюръективности гомоморфизма. Изоморфизм. Теоремы о реализации циклических групп. Смежные классы, свойства смежных классов. Теорема Лагранжа; следствия. Критерий существования собственных подгрупп. Нормальные делители; критерий того, что подгруппа является нормальным делителем. Примеры нормальных делителей. Факторгруппа, теорема о гомоморфизмах. Примеры реализации факторгрупп.

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ С ДВУМЯ ОПЕРАЦИЯМИ. Определение кольца, примеры колец. Обратимые элементы, делители нуля. Поле, примеры. Теорема о конечном кольце без делителей нуля.

Идеалы, определение, собственные, несобственные, главные, порожденные несколькими элементами. Идеалы кольца \mathbb{Z} . Факторкольцо. Гомо-

морфизм колец, ядро и образ гомоморфизма. Теорема о гомоморфизмах в случае колец. Максимальные идеалы, теорема о факторкольце по максимальному идеалу. Кольцо многочленов, теорема об идеалах кольца $\mathbb{F}[x]$.

Евклидовы кольца. Примеры евклидовых колец. Ассоциированные элементы. Теорема об идеалах евклидова кольца. Неприводимые элементы. Наибольший общий делитель в евклидовом кольце. Свойства неприводимых элементов. Разложение на неприводимые множители в евклидовом кольце (вспомогательные утверждения и теорема). Критерий максимальности идеала в евклидовом кольце. Теорема существования неприводимых многочленов с коэффициентами в конечном поле. Построение поля, содержащего p^n элементов.

Подполе, критерий. Характеристика поля, свойства характеристики. Конечные расширения, степень расширения. Теорема о числе элементов конечного поля.

Цикличность конечной подгруппы мультипликативной группы конечного поля. Лемма о числе корней многочлена. Экспонента группы, теорема существования элемента, порядок которого равен экспоненте группы. Критерий цикличности конечной коммутативной группы в терминах экспоненты. Доказательство теоремы о цикличности подгруппы мультипликативной группы. Следствие для группы \mathbb{Z}_p^* . Критерий цикличности мультипликативной группы кольца \mathbb{Z}_n^* (б/д).

Сравнения. Полная система вычетов, приведенная система вычетов. Основные свойства сравнений. Теоремы Эйлера и Ферма. Сравнения первой степени (теория разрешимости, алгоритм решения). Китайская теорема об остатках.