Экзаменационная программа по курсу «Общая алгебра и теория чисел», направление подготовки «Информационные технологии», 2 курс, 1 семестр 2011-2012 учебного года

Элементы теории чисел. Аксиома вполне упорядоченности. Теорема о делении с остатком. Отношение делимости. Наибольший общий делитель, теорема существования и единственности. Алгоритм Евклида. Взаимно простые числа, теорема о свойствах, равносильных взаимной простоте, свойства взаимно простых чисел. Наименьшее общее кратное (определение, свойства наименьшего общего кратного). Простые числа. Определение и элементарные свойства простых чисел. Основная теорема арифметики. Каноническое разложение числа. Функция Эйлера (определение, формула для вычисления функции Эйлера).

Алгебраические системы с одной операцией. Бинарная операция, коммутативность и ассоциативность. Моноид. Единственность единичного элемента. Мультипликативная и аддитивная запись. Примеры моноидов. Целые неотрицательные степени элемента моноида.

Группа, аксиоматика, единственность обратного элемента, свойства обратного элемента. Примеры групп. Биективность отображений $x \mapsto ax$ и $x \mapsto xa$ в группе. Уравнение, определяющее единичный элемент группы. Конечные и бесконечные группы, порядок группы. Порядок элемента группы, свойства порядка. Подгруппы, примеры подгрупп. Критерии того, что подмножество является подгруппой.

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

Гомоморфизм и изоморфизм групп, свойства гомоморфизмов. Ядро и образ гомоморфизма. Критерий инъективности и сюръективности гомоморфизма. Критерий того, что гомоморфизм является изоморфизмом. Изоморфные группы, свойства отношения изоморфности. Теоремы о реализации циклических групп ($G \cong U_n$ или $G \cong \mathbb{Z}$).

Операции с подмножествами элементов группы, свойства этих операций. Отношение эквивалентности, определяемое подгруппой, левый смежный класс, теорема о том, что левые смежные классы имеют вид xH. Равномощность двух левых смежных классов. Равномощность множества

всех левых смежных классов и множества всех правых смежных классов. Индекс подгруппы. Теорема Лагранжа, следствия. Критерий того, что группа не имеет собственных подгрупп. Нормальные делители; критерий того, что подгруппа является нормальным делителем. Примеры нормальных делителей. Факторгруппа, теорема о гомоморфизмах. Примеры реализации факторгрупп. Прямое произведение групп, элементарные свойства. Критерий цикличности прямого произведения конечных групп.

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

Идеалы, определение, собственные, несобственные, главные, порожденные несколькими элементами. Идеалы кольца $\mathbb{Z}$, критерий максимальности идеала кольца $\mathbb{Z}$. Кольцо многочленов с коэффициентами из кольца, лемма о делении с остатком, теорема об идеалах кольца $\mathbb{F}[x]$. Приводимые и неприводимые многочлены. Факторкольцо. Критерий того, что факторкольцо является полем. Критерий максимальности идеала кольца $\mathbb{F}[x]$. Реализация факторкольца $\mathbb{F}[x]/(m(x))$. Разложение многочлена на неприводимые множители. Теорема о числе корней многочлена, следствие о цикличности конечной подгруппы мультипликативной группы произвольного поля. Кольцо $\mathbb{Z}[i\sqrt{5}]$.

Характеристика кольца. Простота характеристики в случае кольца без делителей нуля, случай поля. Подполе. Теорема о соотношении $n \mid C_n^k$, следствие о вычислении $(a+b)^{p^k}$. Теорема о числе элементов конечного поля. Теорема о присоединении корня неприводимого многочлена. Следствие о существовании расширения, в котором полином разлагается на линейные множители. Доказательство существования поля $GF(p^n)$.

Сравнения. Основные свойства сравнений. Полная и приведенная системы вычетов. Сравнения первой степени. Система сравнений первой степени; китайская теорема об остатках.