Академический университет
Программа курса "Алгебра"

1 семестр

Глава 1. Введение.

§1. Логическая терминология. Множества, операции над ними.

Высказывания, основные логические связки, кванторы. Множества, объединение, пересечение, дополнение. Упорядоченные наборы, декартовы произведения множеств. Множество подмножеств. Принцип математической индукции.

§2. Отображения.

График отображения. Образ, полный прообраз. Тождественное отображение. Композиция отображений, ассоциативность композиции. Обратимые отображения, обратимые слева и справа отображения. Обратное отображение. Инъективные, сюръективные и биективные отображения, связь с обратимостью. Конечные множества. Принцип Дирихле.

§3. Отношения на множествах.

Бинарные отношения. Основные типы бинарных отношений. Примеры. Отношения частичного порядка. Отношение эквивалентности. Классы эквивалентности. Разбиение на классы эквивалентности.

Глава 2. Группы.

§1. Понятие группы.

Аксиомы группы. Примеры, группы перетановок. Простейшие свойства аксиом группы.

§2. Гомоморфизмы и изоморфизмы..

Гомоморфизмы групп. Простейшие свойисва. Изоморфизм групп. Примеры.

§3. Подгруппы.

Подгруппы. Подгруппы, порожденные семейством. Образующие. Циклические группы. Лемма о делении с остатком в множестве целых чисел. Классификация циклических групп с точностью до изоморфности. Порядок группы, порядок элемента.

§4. Смежные классы.

Левые и правые классы смежности по подгруппе. Индекс подгруппы. Теорема Лагранжа.

§5. Симметрическая группа.

Перестановки конечных множеств. Симметрическая группа. Циклы, транспозиции. Непересекающиеся циклы. Разложение перестановки в произведение непересекающихся циклов. Цикловый тип перестановки. Симметрическая группа порождается транспозициями. Число инверсий, четные и нечетные перестановки. Теорема об изменении четности при умножении на транспозицию и следствия из нее. Знакопеременная группа.

Глава 3. Кольца, тела, поля.

§1. Понятия кольца, тела, поля.

Аксиомы ассоциативных колец, тел, полей. Простейшие свойства. Примеры. Явное построение полей из 2, 3 и 4 элементов. Подкольца. Гомоморфизмы колец и их простейшие свойства. Изоморфизмы колец. Делители нуля и область целостности. Мультипликативная группа кольца.

§2. Кольцо многочленов

Кольцо многочленов от одной переменной. Биномиальная формула. Степень многочлена и ее свойства. Теорема о делении с остатком в кольце многочленов от одной переменной над полем. Корни многочлена. Теорема Безу. Формальная производная многочлена, ее свойства. Кратные корни. Теорема о числе корней многочлена. Алгебраически замкнутые поля. Интерполяционная задача, метод Ньютона и метод Лагранжа. Кольцо многочленов от нескольких переменных.

§3. Поле комплексных чисел.

Поле комплексных чисел как множество пар вещественных. Алгебраическая форма записи комплексного числа. Комплексное сопряжение. Геометрическое представление, модуль, аргумент, тригонометрическая и показательная формы записи комплексных чисел, неравенство треугольника. Мультипликативность модуля. Формула Муавра. Примеры вычисления тригонометрических сумм. Многочлены Чебышева. Корни из 1. Первообразные корни из 1. Примеры применения комплексных чисел для доказательства теорем планиметрии.

§4. Кольцо матриц.

Умножение матриц и его свойства. Кольцо квадратных матриц размера n. Отсутствие коммутативности умножения. Матричная конструкция поля комплексных чисел. Матричная конструкция тела кватернионов. Кватернионы: сопряженный кватернион, модуль, мультипликативность модуля, тождество Эйлера.

Глава 4. Теория делимости в коммутативных кольцах.

§1. Делимость в кольце

Отношение делимости, его свойства. Обратимые, простые и неприводимые элементы в кольце. Наибольший общий делитель и его свойства. Взаимно простые элементы.

§2. Идеалы в кольце.

Идеалы, их свойства. Пересечение, сумма и произведение идеалов. Идеалы, порожденные семейством. Главные идеалы. Область главных идеалов.

§3. Евклидовы кольца.

Евклидовы кольца. Примеры ($\mathbb{Z}$, $K[x]$). Евклидовость кольца гауссовых чисел $\mathbb{Z}[i]$. Алгоритм Евклида и линейное представление наибольшего общего делителя. Линейные уравнения в евклидовых кольцах. Евклидово кольцо является областью главных идеалов.

§4. Теорема об однозначном разложении на множители.

Существование наибольшего общего делителя и его линейного представления в кольце главных идеалов. Теорема об однозначном разложении на множители в кольце главных идеалов. Приложения: разложение на множители в $\mathbb{Z}$, $K[x]$, $\mathbb{C}[x]$, $\mathbb{R}[x]$.

§5. Сравнения и кольца вычетов.

Сравнимость по модулю идеала. Свойства. Решение линейных сравнений в кольцах главных идеалов. Китайская теорема об остатках. Классы вычетов. Построение кольца классов вычетов по модулю идеала. Кольцо классов вычетов по максимальному идеалу — поле. Примеры построения конечных полей как колец классов вычетов. Простые конечные поля. Конструкция поля комплексных чисел как кольца классов вычетов.

§6. Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$.

Обратимые классы вычетов. Функция Эйлера. Функция Мебиуса, формула обращения Мебиуса. Явная формула для функции Эйлера. Теорема Эйлера, малая теорема Ферма, теорема Вильсона. Алгоритм RSA. Квадратичные сравнения. Символ Лежандра, символ Якоби. Квадратичный закон взаимности.

§7. Поле частных.

Построение поля частных области целостности. Поле рациональных функций. Теорема о разложении на простейшие дроби.

§8. Конечные поля.

Расширения полей. Присоединение корней многочлена. Поле разложения. Построение конечных полей мощности p^k, единственность с точностью до изоморфности.