Лектор Гуров Сергей Исаевич

На одной из лекции будет КР. Допуск к экзамену <- зачёт по КР.

Группа - тройка $< G, \circ, e >$, где G - непустое множество, е - единичный(нейтральный) элемент, причём выполнены следующие аксиомы:

1. Замкнутость(устойчивость) G относительно операции.
2. Ассоциативность операции.
3. $(x \circ e) = (e \circ x) = x$
4. $\forall x \in G \exists y \in G x \circ y = e$

Таблица Кэли - аналог таблицы умножения.

$V_4 = \{e, a, b, c\}$

∘	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Примеры групп: $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ относительно сложения. $n\mathbb{Z}, B^n, S_n$.

В случае, если операция коммутативна, группа называется **коммутативной** или **абелевой**.

Пусть $a \in G$. Наименьшее n такое, что $a^n = e$ называется **порядком** элемента $a(\operatorname{ord} a)$.

Подгруппой G называется $H \subset G$ являющееся подгруппой: $H \leq G$. Каждый элемент порождает группу $\{a, a^2, \dots, a^{\operatorname{ord} a}\}$.

Пусть $H \leq G, x \in G$. **Правым(левым) смежным классом** x называют множество:

$$xH = \{x \circ n | n \in H\}, Hx = \{n \circ x | n \in H\}$$

Подгруппа, для которой левые и правые классы с одинаковым представителем совпадают, называется **нормальной**.

Теорема 1. *Правые(левые) смежные классы разных элементов либо совпадают, либо не пересекаются.*

Изоморфизм - биекция, сохраняющая операцию. Группы, между которыми существуют изоморфизмы, называются **изоморфными**.

Теорема 2. *Любая конечная группа порядка n изоморфна некоторой подгруппе S_n.*

Гомоморфизм - отображение меджу группами, сохраняющее операцию.

Теорема 3. *Пусть H - нормальная подгруппа G. Тогда*

$$|G| = |H| \cdot [G : H]$$

Число $[G : H]$ называется индексом группы G относительно нормальной подгруппы H.

Циклическими называют группы, порождённые одним элементом. Бесконечные циклические группы изоморфны группе целых чисел по сложению. Циклические группы порядка n изоморфны группе вычетов порядка n.

Все порождающие элементы $\mathbb{Z}_n$ это числа, взаимно простые с n.

Функция Эйлера - количество чисел, взаимно простых с p, меньших p. Свойства функции Эйлера:

1. $\varphi(p^k) = p^{k-1}\varphi(p)$.
2. Если $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Абелева группа называется **кольцом**, если на ней определена операция умножения, связанная с операцией сложения дистрибутивностью.

Если умножение ассоциативно(коммутативно), кольцо называется **ассоциативным(коммутативным)**. Если у умножения существует нейтральный элемент, кольцо называется **кольцом с единицей**. Если $\forall a \neq 0, b \neq 0 ab \neq 0$, кольцо называется **кольцом без делителей нуля**. Ассоциативное коммутативное кольцо с единицей без делителей нуля называется **целостным**.

Пусть R - кольцо. Множество обратимых элементов R обозначаем R^*.

Элемент кольца называется **неразложимым**, если он не может быть представлен в виде произведения двух других.

Факториальным называется кольцо, каждый ненулевой элемент которого либо обратим, либо однозначно с точностью до порядка сомножителей и умножения на обратимые элементы раскладывается на неразложимые множители. Такое разложение числа называется **примарным**.

Рассмотрим $S \subset R$, являющееся кольцом. Такое множество называется **подкольцом**. Условия:

1. S - подгруппа по сложению

2. S замкнуто по умножению.

(Двухсторонним)*Идеалом* называется подкольцо коммутативного кольца, замкнутое относительно и умножения на элементы кольца.

Идеал I коммутативного кольца R называется **главным** с представителем $a \in R$(идеалом, порождённым a), если

$$I = \{r \cdot a | r \in R\} = (a)$$

Кольца, в которых все идеалы являются главными, называются **кольцами главных идеалов**. **Максимальным** называется идеал, такой что $I_{max} \subset I \Rightarrow I = R$.

Утверждение: В коммутативном кольце всегда существует максимальный идеал.

Классом вычетов по модулю идеала I коммутативного кольца R с представителем $r \in R$ называется множество $r + I = \{r + i | i \in I\} = \overline{r_I}$.

Фактор-кольцом R/I называется кольцо классов вычетов $\overline{r_I}$.

Утверждение: Фактор-кольцо по максимальному идеалу является полем.

Целостное кольцо R называется **евклидовым**, если $\forall a \in R, a \neq 0 \exists N(a) \in \mathbb{N}$, такая, что $\forall b \neq 0 a = bq + r$, причём $r = 0$ или $N(r) < N(b)$.

Целостное кольцо, в котором каждый ненулевой элемент обратим, называется **полем**. У поля есть мультипликативная группа(абелева группа по умножению).

Будем обозначать R^* множество обратимых элементов кольца R.

У поля существуют только тривиальные идеалы.

Структура, аналогичная полю, в которой умножение некоммутативно, называется **телом**.

Теорема 4. *В теле нет нетривиальных идеалов.*

Линейным векторным пространством V над полем P называется аддитивная группа по сложению, для элементов которой определено умножение на элементы поля, обладающая свойствами:

$$a(v_1 + v_2) = av_1 + av_2 \forall a \in P, v_1, v_2 \in V$$

$$(a + b)v = av + bv \forall a, b \in P, v \in V$$

$$a(bv) = (ab)v \forall a, b \in P, v \in V$$

$$1v = v \forall v \in V$$

и замкнутая относительно линейной комбинации с коэффициентами из P.

Поля вычетов по модулю p, где p - простое, называются **простыми полями Галуа**. Минимальное число p такое, что $\underbrace{1+1+\ldots+1}_{p}=0$, называется **характеристикой** поля. Если $p=\infty$, считается, что $p=0$. Поле дробей-многочленов имеет конечную характеристику, но является бесконечным.

Утверждение(тождество Фробениуса): $\forall a,b \in GF(p)(a+b)^p = a^p + b^p$

Пусть $F_p^* = F_p \ \{0\}$.

Утверждение: $|F_q^*| = q-1$.

Рассмотрим $K[x]$ - кольцо многочленов над полем K от переменной x. Будем считать, что $a_n = 1$. Рассмотрим $\mathbb{F}_p[x]$. В $\mathbb{F}_2[x]$ неприводимыми являются многочлены $x^2+x+1, x^3+x^2+1, x^3+x+1$. В $\mathbb{F}_5[x]$ неприводимыми являются 6 многочленов.

Теорема 5. *В $\mathbb{F}_p \forall n < p$ существует неприводимый многочлен степени n.*

Пусть $a(x) \in \mathbb{F}_p[x]$ - неприводимый многочлени степени n. Рассмотрим $(a(x)) = \{q(x)a(x) | q(x) \in \mathbb{F}_p[x]\}$. Тогда $\mathbb{F}_p[x]/(a(x))$ - множество остатков от деления многочленов на a(x) - является полем. Если $a(x)$ - многочлен степени n, то все остатки - многочлены степени до $n-1$. Получили **расширение** поля Галуа $\mathbb{F}_p^n$, $GF(p^n)$.

Пример:
$\mathrm{F}_3^2 -?$

$$\mathbb{F}_3^2[x] = \mathbb{F}_3^2[x]/(x^2+1) = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\} \tag{1}$$

Пример 2:
Рассмотрим $\mathbb{R}[x]$, a(x) $= \mathrm{x}^2 + 1 . \mathbb{R}[x]/(x^2+1) = \{ax+b | a, b \in \mathbb{R}\}$ - поле комплексных чисел(2)

Теорема 6. *Поля расширения по разным многочленам изоморфны.*

Теорема 7 (Соотношение Безу)**.** $\forall a, b \in \mathbb{N} \exists d \in \mathbb{N}, x, y \in \mathbb{Z} : ax + by = d, d = (a, b)$.

Расширенный алгоритм Евклида:

$$E = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, r = 0.$$

Если $r=0$, то второй столбец E даёт x и y.

Иначе

$$E \to E \cdot \begin{Vmatrix} 0 & 1 \\ 1 & -q \end{Vmatrix} \tag{3}$$

и $(a,b) \to (b,r)$.

Алгоритм Евклида позволяет искать обратный элемент в $\mathbb{Z}_m$:

1. Пусть $(c,m)=1$.
2. Рассмотрим матрицу

$$\begin{Vmatrix} m & 0 \\ c & 1. \end{Vmatrix} \tag{4}$$

3. Поделим m на c с остатком: $m = qc + r$.
4. Вторую строку домножаем на q и вычитаем из первой.
5. Когда первый элемент последней строки становится равным нулю, второй элемент даёт c^{-1}.

Обобщённый алгоритм Евклида для нахождения в $\mathbb{F}_p/(a(x))y(x)$, обратного к $b(x)$: Шаг 0: $r_{-2}(x) = a(x), r_{-1}(x) = b(x), y_{-2}(x) = 0, y_{-1}(x) = 1$.
Шаг 1:

$$r_{-2}/r_{-1} \Rightarrow q_0, r_0$$

$$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$$

$$y_0(x) = -q_0(x)$$

Если $\deg r_0(x) \geq 1$ - к следующему шагу, иначе к $(n+1)$-му шагу.
Шаг 2:

$$r_{i-3}(x) = r_{i-2}(x)q_{i-1}(x) + r_{i-1}(x)$$

$$y_{i-1}(x) = y_{i-3}(x) - y_{i-2}(x)q_{i-1}(x)$$

Если $\deg r_{i-1} > 0$, продолжаем итерации.