Практическое занятие 9
Построение алгебраических структур

- Модулярная арифметика.
- Группа подстановок. Теорема о представлении групп.

© I.Krivtsova
ITMO University

Нахождение остатков от деления отрицательных целых чисел

$-2 : 3$

- находим целую часть $|-2| : |3| = 0$
- берем $0-1= -1$
- тогда $-2 = 3 \cdot (-1)+1$, т.е. остаток от деления равен 1

$-7 : 3$

- находим целую часть $|-7| : |3| = 2$
- берем $-2-1= -3$
- тогда $-7 = 3 \cdot (-3)+2$, т.е. остаток от деления равен 2

1. Модулярная арифметика

Пусть $x, y \in \boldsymbol{Z}$, $n \in \boldsymbol{N}$.

- **Определение**

Числа x и y называются сравнимыми (равными) по модулю n, если разность $(x - y)$ делится на n.

Обозначение: $x \equiv y \ (mod \ n)$

или $x = y \ (mod \ n)$.

Число n называется *модулем*, каждое из чисел x и y – *вычетом по модулю* n.

$$x = y \ (mod\ n) \Leftrightarrow x - y = tn, \text{ где } t \in \mathbf{Z}.$$

Остатки от деления целых чисел на n порождают попарно различные классы эквивалентности

$$[0],\ [1], \ldots,\ [n-1],$$

которые называются *классами вычетов по модулю n*.

Множество

$$\boldsymbol{Z}_{[\boldsymbol{n}]} = \{\, [0], [1], \ldots, [n - 1] \}$$

– *множество классов вычетов по модулю n*.

Класс эквивалентности элемента a :

$$[a] = \{a + t \cdot n,\ \ t \in \boldsymbol{Z}\}$$

Операции на $Z_{[n]}$

- *Сложение по модулю* n :

$$[a] \oplus [b] = [a+b]$$

- *Умножение по модулю* n :

$$[a] \otimes [b] = [a \cdot b]$$

Определим класс:

$$-[a] = [n - a]$$

Арифметика целых чисел по модулю n рассматривается как арифметика остатков или модулярная арифметика.

$A = < \boldsymbol{Z}_{[\boldsymbol{n}]}, \oplus, \otimes >$

Ненулевые элементы $[a]$ и $[b]$ множества $\boldsymbol{Z}_{[\boldsymbol{n}]}$ называются делителями нуля, если

$$[a]\otimes[b] = [0] \text{ или } [b]\otimes[a] = [0]$$

Группа называется циклической, если существует такой элемент x_0, что любой элемент группы является некоторой целой степенью элемента x_0:

- в мультипликативной форме

$$\exists x_0 \in X: \ \forall x \in X \quad x = x_0^k, \ k \in \mathbf{Z}$$

- в аддитивной форме

$$\exists x_0 \in X: \ \forall x \in X \quad x = kx_0, \ k \in \mathbf{Z}$$

x_0 – *образующий элемент* группы.

$< X, \cdot, \mathbf{1} >$ – циклическая группа.

Порядок образующего элемента циклической группы – это наименьшее число $k > 0$, такое, что

$$x_0^k = \mathbf{1}.$$

2. Группа подстановок

$X \neq \varnothing$

$f : X \to X$ – биекция X на себя

f_X – множество всех биекций X на себя

$\circ$ – композиция биекций:

$$\forall x \in X \quad (g \circ f)(x) = g(f(x)) \in f_X$$

$A = < f_X, \circ >$

(1) $\forall\ g,f,h \in f_X$ выполняется $(g\circ f)\circ h = g\circ(f\circ h)$
$\Rightarrow (\circ)$ – ассоциативная

(2) $\forall x \in X \quad e_X(x) = x$ – тождественное отображение на X:

$e_X \in f_X$ и $\forall f \in f_X \quad f \circ e_X = e_X \circ f = f$

$\Rightarrow e_X$ – нейтральный элемент по $(\circ)$

(3) $\forall\, f \in f_X$ определено отображение $f^{-1} \in f_X$:

$$f \circ f^{-1} = f^{-1} \circ f = e$$

$\Rightarrow f^{-1}$ – элемент, обратный биекции f по $(\circ)$

$G = \langle f_X, \circ \rangle$ – симметрическая группа множества X.

Пусть $X = \{1, 2, \ldots, n\}$ *конечно*.

Произвольную биекцию f обычно записывают в виде:

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

Биекцию X на себя называют *подстановкой* этого множества.

Тогда $G = < f_X, \circ >$ – группа подстановок множества X.

Группа подстановок конечного множества X с числом элементов n называется симметрической группой степени n.

Обозначение: S_n

- **Теорема Лагранжа**

Число элементов всякой подгруппы *конечной* группы является делителем порядка группы.

Следствие 1

Любая группа *простого* порядка является циклической.

Следствие 2

В *конечной* группе G $\forall a \in G$ имеет место равенство:

$$a^{|G|} = \mathbf{1}$$

- **Теорема Кэли** (о представлении групп)

Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.