§3. Примеры основных алгебраических структур

1. ($\mathbf{N}$, +)

1. (**N**, +) – полугруппа, коммутативная;

(**N**, ·) – полугруппа, коммутативная, с нейтральным элементом (моноид).

2. ($\mathbf{Z}$, +) – группа, абелева;

($\mathbf{Q}$, +) – группа, абелева.

3. (**Z**, +, ·) – кольцо, коммутативно-ассоциативное с 1;

(**Q**, +, ·) – поле;

(**R**, +, ·) – поле;

(**C**, +, ·) – поле.

4. Группа вычетов по модулю n.

$A = \{0, 1, \ldots, n - 1\}$;

$x \oplus y = (x + y) \bmod n$	Наименьший положительный остаток от деления $(x + y)$ на n

Тогда $(A, \oplus)$ абелева группа.

1) A замкнуто относительно $\oplus$;
2) $\oplus$ коммутативна;

3) $\oplus$ ассоциативна:

$$x \oplus y = (x + y) - k \cdot n$$

$$\Rightarrow (x \oplus y) \oplus z = ((x + y) - k \cdot n) + z - m \cdot n = (x + y + z) - (k + m) \cdot n =$$

$$= x \oplus (y \oplus z).$$

4) Нейтральный элемент 0.

5) Существование обратного элемента: $x \oplus (-x) = 0$.

Если $x = 0$, то $(-x) = 0$.

Если $x \neq 0$, то $(-x) = n - x$.

Обозначение: Z_n .

5. Кольцо вычетов по модулю n.

$A = \{0, 1, \ldots, n-1\}$;

$x \oplus y = (x + y) \bmod n$ $x \otimes y = (x \cdot y) \bmod n$	Наименьший положительный остаток от деления $(x \cdot y)$ на n

Тогда $(A, \oplus, \otimes)$ – кольцо, коммутативно-ассоциативное; с 1, если $n > 1$.

1) A замкнуто относительно $\otimes$;
2) $\otimes$ коммутативна;
3) $\otimes$ ассоциативна:

$$x \otimes y = (x \cdot y) - k \cdot n$$

$$\Rightarrow (x \otimes y) \otimes z = ((x \cdot y) - k \cdot n) \cdot z - m \cdot n = (x \cdot y \cdot z) - (k \cdot z + m) \cdot n =$$

$$= x \otimes (y \otimes z) .$$

4) нейтральным элементом относительно $\otimes$ является число 1.

5) $\otimes$ дистрибутивна относительно $\oplus$:

$$x \otimes (y \oplus z) = x \cdot ((y + z) - k \cdot n) - m \cdot n = (x \cdot y + x \cdot z) - (k \cdot x + m) \cdot n =$$

$$= (x \otimes y) \oplus (x \otimes z) .$$

Теорема (без доказательства).
Кольцо вычетов по модулю n является полем $\Leftrightarrow$ n простое число.

Опр. Поле Галуа – конечное поле.

Теорема.

Кольцо вычетов по модулю n является полем $\Leftrightarrow$ n простое число.

Примеры. Рассмотрим кольцо вычетов по модулю 5.

$\otimes$	0	1	2	3	4
0					
1					
2					
3					
4					

Теорема.
Кольцо вычетов по модулю *n* является полем $\Leftrightarrow$ *n* простое число.

Пример 1. Рассмотрим кольцо вычетов по модулю 5.

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1^{-1} = 1;\ \ 2^{-1} = 3;\ \ 3^{-1} = 2;\ \ 4^{-1} = 4.$

Поле вычетов по модулю 5.

Пример 2. Рассмотрим кольцо вычетов по модулю 6.

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$1^{-1} = 1;\ \ 5^{-1} = 5;$

$2^{-1},\ 3^{-1},\ 4^{-1}$ – не существуют.

Кольцо вычетов по модулю 6 не является полем.

§4. Симметрические полугруппа и группа

1. Симметрическая полугруппа над M.

Пусть $M \neq \varnothing$.
$A = \{f \mid f$ – всюду определенное отображение $M \to M\}$;
$*$ – операция суперпозиции двух отображений.

Тогда $(A, *)$ – полугруппа с нейтральным элементом e, где e тождественное отображение $M \to M$.

1) A замкнуто относительно $*$;

2) $*$ ассоциативна, т.е.
$(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$.

Покажем, что для каждого $x \in M$ значения функций совпадают:
$((f_1 * f_2) * f_3)(x) = f_3((f_1 * f_2)(x)) = f_3(f_2(f_1(x)))$;

$(f_1 * (f_2 * f_3))(x) = (f_2 * f_3)(f_1(x)) = f_3(f_2(f_1(x)))$.

3) Нейтральный элемент – тождественное отображение e, т.е.
$f * e = e * f = f$.

Покажем, что для каждого $x \in M$ значения функций совпадают:

$(f * e)(x) = e(f(x)) = f(x)$;

$(e * f)(x) = f(e(x)) = f(x)$.

4) $*$ не коммутативна.

Замечание: если M конечна, в частности для $M = \{1, 2, \ldots, k\}$, каждое отображение f можно задать таблицей («подстановкой»), имеющей вид матрицы $\begin{pmatrix} 1 & 2 & \ldots & k \\ f(1) & f(2) & \ldots & f(k) \end{pmatrix}$.

Тогда говорят о симметрической полугруппе подстановок.

2. Симметрическая группа над M.

Пусть $M \neq \varnothing$.
$A = \{f \mid f$ – биекция $M \to M\}$;
$*$ – операция суперпозиции двух биекций.

Тогда $(A, *)$ – группа (не абелева).

1) A замкнуто относительно $*$.

2) $*$ ассоциативна.

3) Нейтральный элемент – тождественное отображение e.

4) $*$ не коммутативна.

5) Для каждой биекции f существует обратный элемент относительно $*$ – это обратное отображение f^{-1}, являющееся тоже биекцией, и $f * f^{-1} = f^{-1} * f = e$.

Замечание: если M конечна, в частности для $M = \{1, 2, \ldots, k\}$, каждая биекция f является перестановкой M , и ее можно задать подстановкой $\begin{pmatrix} 1 & 2 & \ldots & k \\ f(1) & f(2) & \ldots & f(k) \end{pmatrix}$, или строкой $(f(1), f(2), \ldots, f(k))$.

Тогда говорят о симметрической группе перестановок.

§5. Свободные полугруппа и группа

1. Свободная полугруппа (полугруппа слов над алфавитом M).

Опр. Алфавит M – конечное непустое множество.
Буква – каждый элемент множества M.

Слово над алфавитом M – конечная последовательность $a_1 \dots a_n$, где каждая $a_k \in M$.
(цепочка, string)

A = {множество всех слов над алфавитом M}.

Опр. (Умножение слов)
Произведением слова $u = a_1 \ldots a_n$ на слово $v = b_1 \ldots b_m$ называется слово $u \cdot v = a_1 \ldots a_n b_1 \ldots b_m$.

(конкатенация)

Тогда (A, $\cdot$) – полугруппа (не коммутативная).

Опр. Пустое слово ε – слово, не содержащее ни одной буквы.

Тогда $u \cdot \varepsilon = \varepsilon \cdot u = u$, т.е. ε – нейтральный элемент.

Тогда $(A \cup \{\varepsilon\}, \cdot)$ – полугруппа с нейтральным элементом (моноид).

Обозначение: M^* – множество всех слов над алфавитом M, включая пустое слово ε.

2. Свободная группа (над M).

Пусть M – конечное непустое множество.

Для каждой буквы $a \in M$ определим обратную букву («антибукву») a^{-1}, такую, что $a \cdot a^{-1} = a^{-1} \cdot a = \varepsilon$.

Обозначим M^{-1} = {все «антибуквы» к M }

A = {множество всех слов над алфавитом $(M \cup M^{-1})\} \cup \{\varepsilon\}$.

Тогда $(A, \cdot)$ – группа (не абелева).