Математические основы защиты информации

Лекция 3

Пилиди Владимир Ставрович

7 апреля 2020 года

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.
Элемент e находится единственным образом.

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.
Элемент e находится единственным образом.

$$\forall a \in S \quad ae = ea = a, \tag{1}$$

$$\forall a \in S \quad ae' = e'a = a. \tag{2}$$

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.

Элемент e находится единственным образом.

$$\forall a \in S \quad ae = ea = a, \tag{1}$$

$$\forall a \in S \quad ae' = e'a = a. \tag{2}$$

$$ee' \overset{(1)}{=} e'$$

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.

Элемент e находится единственным образом.

$$\forall a \in S \quad ae = ea = a, \tag{1}$$

$$\forall a \in S \quad ae' = e'a = a. \tag{2}$$

$$ee' \overset{(1)}{=} e', \; ee' \overset{(2)}{=} e$$

Моноиды

Непустое множество S называется моноидом, если в нем определена бинарная операция $(a, b) \mapsto ab$, удовлетворяющая следующим условиям:

- для любых элементов a, b, $c \in S$ имеет место равенство $(ab)c = a(bc)$;
- существует элемент $e \in S$ такой, что для любого $a \in S$ $ae = ea = a$.

Моноид S называется коммутативным, если для любых a, $b \in S$ выполняется равенство $ab = ba$.
Элемент e находится единственным образом.

$$\forall a \in S \quad ae = ea = a, \tag{1}$$

$$\forall a \in S \quad ae' = e'a = a. \tag{2}$$

$$ee' \overset{(1)}{=} e',\ ee' \overset{(2)}{=} e \ \Rightarrow e = e'.$$

Этот единственный элемент e называется единичным. В случае аддитивной записи операции он называется нулевым и обозначается через 0.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Примеры моноидов.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Примеры моноидов.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cap B$. Это коммутативный моноид.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Примеры моноидов.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cap B$. Это коммутативный моноид.
Единичный элемент — множество X.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Примеры моноидов.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cap B$. Это коммутативный моноид.
Единичный элемент — множество X.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cup B$. Это коммутативный моноид.

Моноиды

Аддитивная запись, как правило, используется только для коммутативных бинарных операций. В этом случае определение моноида выглядит так:

- для любых элементов a, b, $c \in S$ $(a + b) + c = a + (b + c)$;
- для любых элементов a, $b \in S$ имеет место равенство $a + b = b + a$;
- существует элемент $0 \in S$ такой, что для любого $a \in S$ $a + 0 = a$.

Примеры моноидов.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cap B$. Это коммутативный моноид.
Единичный элемент — множество X.
Множество 2^X с бинарной операцией $(A, B) \mapsto A \cup B$. Это коммутативный моноид.
Единичный элемент — множество $\varnothing$.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$, $\{0, 1, \ldots, n\}$

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$, $\{0, 1, \ldots, n\}$, $(a, b) \mapsto \max\{a, b\}$.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$, $\{0, 1, \ldots, n\}$, $(a, b) \mapsto \max\{a, b\}$.
Это коммутативный моноид с нулевым элементом 0.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$, $\{0, 1, \ldots, n\}$, $(a, b) \mapsto \max\{a, b\}$.
Это коммутативный моноид с нулевым элементом 0.
Бинарная операция $(a, b) \mapsto \min\{a, b\}$.

Моноиды

$\mathcal{A}$ — непустое множество, алфавит.
$\mathcal{A}^*$ множество всех строк конечной длины, составленных из элементов алфавита $\mathcal{A}$.
Бинарная операцию в $\mathcal{A}^*$ — конкатенация этих строк.
$\mathcal{A}^*$ становится моноидом, некоммутативным, если $|\mathcal{A}| > 1$.
$n \in \mathbb{N}$, $\{0, 1, \ldots, n\}$, $(a, b) \mapsto \max\{a, b\}$.
Это коммутативный моноид с нулевым элементом 0.
Бинарная операция $(a, b) \mapsto \min\{a, b\}$.
Это коммутативный моноид с нулевым элементом n.

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Неотрицательные целые степени элемента $a \in S$:
$a^0 = e$, $a^n = a^{n-1} a$, $n \geq 1$.

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Неотрицательные целые степени элемента $a \in S$:
$a^0 = e$, $a^n = a^{n-1} a$, $n \geq 1$.
Свойства степеней.

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Неотрицательные целые степени элемента $a \in S$:
$a^0 = e$, $a^n = a^{n-1} a$, $n \geq 1$.
Свойства степеней.

- $a^m a^n = a^{m+n}$, $m, n \geq 0$;

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Неотрицательные целые степени элемента $a \in S$:
$a^0 = e$, $a^n = a^{n-1} a$, $n \geq 1$.
Свойства степеней.

- $a^m a^n = a^{m+n}$, $m, n \geq 0$;
- $(a^m)^n = a^{mn}$, $m, n \geq 0$;

Моноиды

S — моноид, $a_1, a_2, \ldots, a_n \in S$.
Произведение $a_1 a_2 \ldots a_n$, $n > 2$ определяется по индукции:

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n.$$

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+2} \ldots a_n).$$

$$((ab)c)d, \qquad a(b(cd)), \qquad (ab)(cd).$$

Неотрицательные целые степени элемента $a \in S$:
$a^0 = e$, $a^n = a^{n-1} a$, $n \geq 1$.
Свойства степеней.

- $a^m a^n = a^{m+n}$, $m, n \geq 0$;
- $(a^m)^n = a^{mn}$, $m, n \geq 0$;
- если $a, b \in S$ и $ab = ba$, то $(ab)^n = a^n b^n$, $n \geq 0$.

Моноиды

Аддитивная запись операции: вводятся кратные элемента.

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$, $0a = 0$, $na = (n-1)a + a$, $n \geq 1$.

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$, $0a = 0$, $na = (n-1)a + a$, $n \geq 1$.
Свойства кратных элементов.

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$, $0a = 0$, $na = (n-1)a + a$, $n \geq 1$.
Свойства кратных элементов.

- $ma + na = (m+n)a, \quad m, n \geq 0;$

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$, $0a = 0$, $na = (n-1)a + a$, $n \geq 1$.
Свойства кратных элементов.

- $ma + na = (m+n)a, \quad m, n \geq 0;$
- $n(ma) = (mn)a, \quad m, n \geq 0;$

Моноиды

Аддитивная запись операции: вводятся кратные элемента.
$a \in S$, ma, $m \geq 0$, $0a = 0$, $na = (n-1)a + a$, $n \geq 1$.
Свойства кратных элементов.

- $ma + na = (m+n)a, \quad m, n \geq 0;$
- $n(ma) = (mn)a, \quad m, n \geq 0;$
- $n(a+b) = na + nb, \; n \geq 0.$

Определение

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:

1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:

1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;

2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$, $ab = ba = e$, $ab' = b'a = e$.

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$, $ab = ba = e$, $ab' = b'a = e$.
$(ba)b' = b(ab')$

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$, $ab = ba = e$, $ab' = b'a = e$.
$(ba)b' = b(ab')$, $eb' = be$

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$, $ab = ba = e$, $ab' = b'a = e$.
$(ba)b' = b(ab')$, $eb' = be \quad \Rightarrow \quad b' = b$,

Определение

Множество G с определенной на нем бинарной операцией $(a, b) \mapsto ab$ называется группой, если выполняются следующие свойства:
1) операция является ассоциативной: для любых элементов a, b, $c \in G$ выполняется соотношение $(ab)c = a(bc)$;
2) существует такой элемент $e \in G$, что для всех $a \in G$ выполняется равенство $ea = ae = a$;
3) для каждого $a \in G$ найдется такой элемент $b \in G$, что выполняется равенство $ab = ba = e$.
Если для любых a, $b \in G$ выполняется равенство $ab = ba$, то группа называется коммутативной, или абелевой.

$a \in G$, b, $b' \in G$, $ab = ba = e$, $ab' = b'a = e$.
$(ba)b' = b(ab')$, $eb' = be \quad \Rightarrow \quad b' = b$,
$b = a^{-1}$ — элемент, обратный к a.

Аддитивная запись:

Аддитивная запись:

$$(a, b) \mapsto a + b$$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$;

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $\qquad a + b = b + a$;

$0 + a = a + 0 = a$;

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

$ac = bc$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

$ac = bc$, $(ac)c^{-1} = (bc)c^{-1}$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

$ac = bc$, $(ac)c^{-1} = (bc)c^{-1}$, $a(cc^{-1}) = b(cc^{-1})$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $a + b = b + a$;

$0 + a = a + 0 = a$; $a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

$ac = bc$, $(ac)c^{-1} = (bc)c^{-1}$, $a(cc^{-1}) = b(cc^{-1})$, $ae = be$

Аддитивная запись:

$(a, b) \mapsto a + b$

$e \Rightarrow 0$ — нулевой элемент

$a^{-1} \Rightarrow -a$ — противоположный элемент.

Соотношения из определения группы принимают вид:

$(a + b) + c = a + (b + c)$; $\quad a + b = b + a$;

$0 + a = a + 0 = a$; $\quad a + (-a) = (-a) + a = 0$.

Разность двух элементов группы: $a - b = a + (-b)$.

Элементарные свойства групп.

1) $e^{-1} = e$, так как $ee = e$.

2) $(a^{-1})^{-1} = a$, так как $aa^{-1} = a^{-1}a = e$

3) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

4) a, b, $c \in G$ $ac = bc \Rightarrow a = b$, аналогично для $ca = cb$.

$ac = bc$, $(ac)c^{-1} = (bc)c^{-1}$, $a(cc^{-1}) = b(cc^{-1})$, $ae = be$, $a = b$.

В случае аддитивной записи:

Группы

В случае аддитивной записи:

$$-0 = 0, \quad -(-a) = a, \quad -(a-b) = b-a, \quad a+c = b+c \Rightarrow a = b.$$

В случае аддитивной записи:

$$-0 = 0, \quad -(-a) = a, \quad -(a-b) = b-a, \quad a+c = b+c \Rightarrow a = b.$$

Замечание

В случае моноидов свойство о возможности сокращения может оказаться неверным:

В случае аддитивной записи:

$$-0 = 0, \quad -(-a) = a, \quad -(a-b) = b-a, \quad a+c = b+c \Rightarrow a = b.$$

Замечание

В случае моноидов свойство о возможности сокращения может оказаться неверным:
2^X, операция $(A, B) \mapsto A \cup B$,

В случае аддитивной записи:

$$-0 = 0, \quad -(-a) = a, \quad -(a-b) = b-a, \quad a+c = b+c \Rightarrow a = b.$$

Замечание

В случае моноидов свойство о возможности сокращения может оказаться неверным:
2^X, операция $(A, B) \mapsto A \cup B$,
A, $B \subset X$, $A \neq B$, но $A \cup X = B \cup X$.

В случае аддитивной записи:

$$-0 = 0, \quad -(-a) = a, \quad -(a-b) = b-a, \quad a+c = b+c \Rightarrow a = b.$$

Замечание

В случае моноидов свойство о возможности сокращения может оказаться неверным:
2^X, операция $(A, B) \mapsto A \cup B$,
A, $B \subset X$, $A \neq B$, но $A \cup X = B \cup X$.

Определение

Группа G называется конечной, если число ее элементов конечно, и бесконечной в противном случае. Число элементов конечной группы называется ее порядком и обозначается через $|G|$. В случае бесконечной группы используется запись $|G| = \infty$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.

Группы

Примеры групп

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
z_1, $z_2 \in \mathbb{U}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
z_1, $z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
z_1, $z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1, z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in \mathbb{U}_n$.
$|\mathbb{U}_n| = n$.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in \mathbb{U}_n$.
$|\mathbb{U}_n| = n$.
6) $n \in \mathbb{N}$

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in \mathbb{U}_n$.
$|\mathbb{U}_n| = n$.
6) $n \in \mathbb{N}$, $\mathbb{S}_n$ — множество всех подстановок степени n с операцией суперпозиции.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in \mathbb{U}_n$.
$|\mathbb{U}_n| = n$.
6) $n \in \mathbb{N}$, $\mathbb{S}_n$ — множество всех подстановок степени n с операцией суперпозиции.
Группа $\mathbb{S}_n$ называется симметрической, в этом случае говорят не о суперпозиции, а о произведении подстановок.

1) Множество $G = \{e\}$, с операцией $(e, e) \mapsto e$. Единичная группа.
2) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, сложение.
3) Множество $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, умножение.
Аналогично $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
4) $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}$, $|z_1 z_2| = |z_1| \cdot |z_2| = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}$, $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$, $\frac{1}{z} \in \mathbb{U}$.
5) $n \in \mathbb{N}$, $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, $(z_1, z_2) \mapsto z_1 z_2$.
$z_1,\ z_2 \in \mathbb{U}_n$, $(z_1 z_2)^n = z_1^n \cdot z_2^n = 1 \ \Rightarrow z_1 z_2 \in \mathbb{U}_n$.
$1 \in \mathbb{U}$, $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in \mathbb{U}_n$.
$|\mathbb{U}_n| = n$.
6) $n \in \mathbb{N}$, $\mathbb{S}_n$ — множество всех подстановок степени n с операцией суперпозиции.
Группа $\mathbb{S}_n$ называется симметрической, в этом случае говорят не о суперпозиции, а о произведении подстановок.
$n = 1,\ 2$ — группы $\mathbb{S}_n$ коммутативные.

$n \geq 3$ — группы $\mathbb{S}_n$ некоммутативные.

$n \geq 3$ — группы $\mathbb{S}_n$ некоммутативные.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$n \geq 3$ — группы $\mathbb{S}_n$ некоммутативные.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$n \geq 3$ — группы $\mathbb{S}_n$ некоммутативные.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix},$$

$n \geq 3$ — группы $\mathbb{S}_n$ некоммутативные.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}.$$

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n. $\mathbb{A}_n$ с операцией умножения подстановок образует группу.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.
8) $n \geq 2$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.
8) $n \geq 2$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
$a \oplus b = (a + b) \bmod n$.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.
8) $n \geq 2$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
$a \oplus b = (a + b) \bmod n$.
$\mathbb{Z}_n$ с введенной бинарной операцией является абелевой группой.

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.
8) $n \geq 2$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
$a \oplus b = (a + b) \bmod n$.
$\mathbb{Z}_n$ с введенной бинарной операцией является абелевой группой.
Таблица Кэли для $\mathbb{Z}_5$:

7) $\mathbb{A}_n$ $(n \geq 2)$ — множество всех четных подстановок степени n.
$\mathbb{A}_n$ с операцией умножения подстановок образует группу.
$|\mathbb{A}_n| = n!/2$.
$\mathbb{A}_n$ коммутативная при $n = 2, 3$ и некоммутативная при $n \geq 4$.
$\mathbb{A}_n$ называется знакопеременной группой.
8) $n \geq 2$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
$a \oplus b = (a + b) \bmod n$.
$\mathbb{Z}_n$ с введенной бинарной операцией является абелевой группой.
Таблица Кэли для $\mathbb{Z}_5$:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

9) $n \geq 2$

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.
Множество $\mathbb{Z}_n^*$ с введенной бинарной операцией является абелевой группой, $|\mathbb{Z}_n^*| = \varphi(n)$.

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.
Множество $\mathbb{Z}_n^*$ с введенной бинарной операцией является абелевой группой, $|\mathbb{Z}_n^*| = \varphi(n)$.

Таблица Кэли для $\mathbb{Z}_{18}^*$

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.
Множество $\mathbb{Z}_n^*$ с введенной бинарной операцией является абелевой группой, $|\mathbb{Z}_n^*| = \varphi(n)$.

Таблица Кэли для $\mathbb{Z}_{18}^*$

$\otimes$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.
Множество $\mathbb{Z}_n^*$ с введенной бинарной операцией является абелевой группой, $|\mathbb{Z}_n^*| = \varphi(n)$.

Таблица Кэли для $\mathbb{Z}_{18}^*$

$\otimes$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Обратимость: $7 \otimes x = 1$

9) $n \geq 2$, $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n-1, (k,n) = 1\}$
Бинарная операция $a \otimes b = (ab) \bmod n$.
Множество $\mathbb{Z}_n^*$ с введенной бинарной операцией является абелевой группой, $|\mathbb{Z}_n^*| = \varphi(n)$.

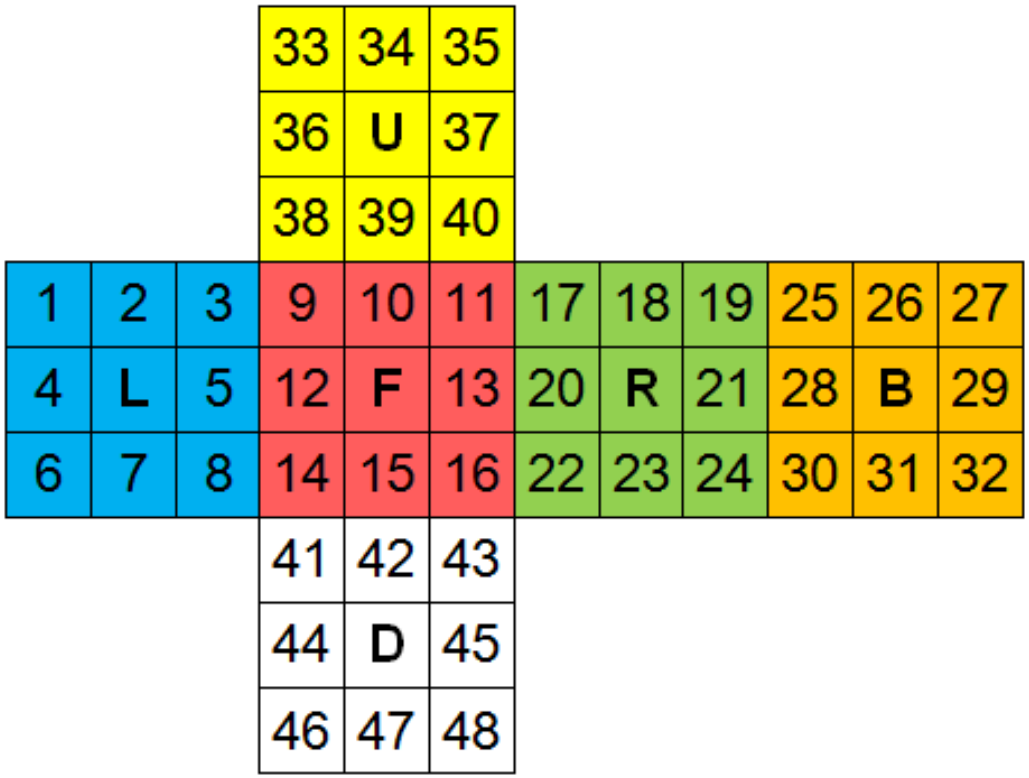
Таблица Кэли для $\mathbb{Z}_{18}^*$

$\otimes$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Обратимость: $7 \otimes x = 1$
$7x \equiv 1 \pmod{18}$, имеет единственное решение $x \in \mathbb{Z}_{18}^*$.

Группа преобразований кубика Рубика

Группа преобразований кубика Рубика



Группа преобразований кубика Рубика некоммутативная.

Группа преобразований кубика Рубика некоммутативная.

Сначала повернули правую грань на 90° против часовой стрелки, потом левую грань на 90° по часовой стрелке.

Группа преобразований кубика Рубика некоммутативная.

Сначала повернули правую грань на 90° против часовой стрелки, потом левую грань на 90° по часовой стрелке.

В обратном порядке.

Группы

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

Группы

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G,\ f : x \mapsto ax$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2\,, \quad \not{a}x_1 = \not{a}x_2\,, \quad x_1 = x_2.$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2\,, \quad \not{a}x_1 = \not{a}x_2\,, \quad x_1 = x_2.$

2) Сюръективность: $\forall y \in G\ \exists x \in G$: $f(x) = y$.

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2\,, \quad \not{a}x_1 = \not{a}x_2\,, \quad x_1 = x_2.$

2) Сюръективность: $\forall y \in G\ \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \ \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \; \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax = a(a^{-1}y)$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \ \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax = a(a^{-1}y) = a(a^{-1}y)$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \; \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax = a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \ \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax = a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = ey$

Теорема

Для произвольного фиксированного элемента a группы G отображения $G \to G$, действующие по правилам $x \mapsto ax$ и $x \mapsto xa$, являются биективными.

$f : G \to G$, $f : x \mapsto ax$

1) Инъективность: $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

$ax_1 = ax_2$, $\quad \not{a}x_1 = \not{a}x_2$, $\quad x_1 = x_2$.

2) Сюръективность: $\forall y \in G \; \exists x \in G$: $f(x) = y$.

$x = a^{-1}y$, $f(x) = ax = a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = ey = y$. $\square$