Математические основы защиты информации

Лекция 5

Пилиди Владимир Ставрович

21 апреля 2020 года

Подгруппы

Критерии, случай аддитивной записи

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняются условия:

1) если $a, b \in H$, то $a + b \in H$;
2) если $a \in H$, то $-a \in H$.

Подгруппы

Критерии, случай аддитивной записи

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняются условия:

1) если $a, b \in H$, то $a + b \in H$;
2) если $a \in H$, то $-a \in H$.

Теорема

Непустое конечное множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если $a, b \in H$, то $a + b \in H$.

Подгруппы

Критерии, случай аддитивной записи

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняются условия:

1) если $a, b \in H$, то $a + b \in H$;
2) если $a \in H$, то $-a \in H$.

Теорема

Непустое конечное множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если $a, b \in H$, то $a + b \in H$.

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если $a, b \in H$, то $a - b \in H$.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что любой элемент $b \in G$ может быть представлен в виде $b = a^k$ для некоторого целого k.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что любой элемент $b \in G$ может быть представлен в виде $b = a^k$ для некоторого целого k.
Элемент a называется образующим элементом циклической группы G.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что любой элемент $b \in G$ может быть представлен в виде $b = a^k$ для некоторого целого k.
Элемент a называется образующим элементом циклической группы G.

Замечание

Если в группе используется аддитивная запись, то соотношение $b = a^k$ заменяется равенством $b = ka$.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что любой элемент $b \in G$ может быть представлен в виде $b = a^k$ для некоторого целого k.
Элемент a называется образующим элементом циклической группы G.

Замечание

Если в группе используется аддитивная запись, то соотношение $b = a^k$ заменяется равенством $b = ka$.

Замечание

Из равенства $a^m a^n = a^n a^m$, m, $n \in \mathbb{Z}$, вытекает коммутативность любой циклической группы. Поэтому любая некоммутативная группа циклической не будет.

Циклические группы
Примеры

1) Единичная группа $\{e\}$ циклическая.

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

Циклические группы

Примеры

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

    $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
   Образующим будет также элемент $-i$.

Циклические группы

Примеры

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

   Образующим будет также элемент $-i$.

   Элементы 1 и -1 образующими не будут.

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
   Образующим будет также элемент $-i$.
   Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
Образующим будет также элемент $-i$.
Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
$\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
Образующим будет также элемент $-i$.
Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
$\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,
$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

   Образующим будет также элемент $-i$.

   Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.

   $\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,

   $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,

   элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
   Образующим будет также элемент $-i$.
   Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
   $\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,
   $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,
   элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим,
   группа $\mathbb{U}_n$ циклическая.
4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.

1) Единичная группа $\{e\}$ циклическая.

2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

Образующим будет также элемент $-i$.

Элементы 1 и -1 образующими не будут.

3) Группа $\mathbb{U}_n$.

$\mathbb{U}_n = \{\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k = 0, 1, \dots, n-1\}$,

$\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^k$, $k = 0,\ 1,\ \dots,\ n-1$,

элемент $a = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ является образующим,

группа $\mathbb{U}_n$ циклическая.

4) Группа $\mathbb{Z}_n = \{0, 1, 2, \dots n-1\}$, $n \geqslant 2$.

Выписываем кратные элемента 1: 0, 1, 2,…, $n-1$,

группа $\mathbb{Z}_n$ циклическая.

1) Единичная группа $\{e\}$ циклическая.

2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

Образующим будет также элемент $-i$.

Элементы 1 и -1 образующими не будут.

3) Группа $\mathbb{U}_n$.

$\mathbb{U}_n = \{\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,

$\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,

элемент $a = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ является образующим,

группа $\mathbb{U}_n$ циклическая.

4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.

Выписываем кратные элемента 1: 0, 1, 2,..., $n-1$,

группа $\mathbb{Z}_n$ циклическая.

5) Группа $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

1) Единичная группа $\{e\}$ циклическая.

2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.

$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.

Образующим будет также элемент $-i$.

Элементы 1 и -1 образующими не будут.

3) Группа $\mathbb{U}_n$.

$\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,

$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,

элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим,

группа $\mathbb{U}_n$ циклическая.

4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.

Выписываем кратные элемента 1: 0, 1, 2,..., $n-1$,

группа $\mathbb{Z}_n$ циклическая.

5) Группа $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

Выписываем степени элемента 3:

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
Образующим будет также элемент $-i$.
Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
$\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,
$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,
элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим,
группа $\mathbb{U}_n$ циклическая.
4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.
Выписываем кратные элемента 1: 0, 1, 2,..., $n-1$,
группа $\mathbb{Z}_n$ циклическая.
5) Группа $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
Выписываем степени элемента 3:
$3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
$i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
Образующим будет также элемент $-i$.
Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
$\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,
$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,
элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим,
группа $\mathbb{U}_n$ циклическая.
4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.
Выписываем кратные элемента 1: 0, 1, 2,..., $n-1$,
группа $\mathbb{Z}_n$ циклическая.
5) Группа $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
Выписываем степени элемента 3:
$3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$,

Циклические группы

Примеры

1) Единичная группа $\{e\}$ циклическая.
2) Группа $\mathbb{U}_4 = \{1, -1, i, -i\}$.
   $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$.
   Образующим будет также элемент $-i$.
   Элементы 1 и -1 образующими не будут.
3) Группа $\mathbb{U}_n$.
   $\mathbb{U}_n = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1\}$,
   $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k$, $k = 0,\ 1,\ \ldots,\ n-1$,
   элемент $a = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ является образующим,
   группа $\mathbb{U}_n$ циклическая.
4) Группа $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$, $n \geqslant 2$.
   Выписываем кратные элемента 1: 0, 1, 2,$\ldots$, $n-1$,
   группа $\mathbb{Z}_n$ циклическая.
5) Группа $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
   Выписываем степени элемента 3:
   $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$,
   группа $\mathbb{Z}_7^*$ циклическая.

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
степени элемента 2: $1,\ 2,\ 4,\ 8,\ 1,\ \ldots$

6) Группа $\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
степени элемента 2: 1, 2, 4, 8, 1, … ,
степени элемента 7: 1, 7, 4, 13, 1, …

6) Группа $\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, …,

степени элемента 7: 1, 7, 4, 13, 1, …,

степени элемента 11: 1, 11, 1, …

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, $\ldots$,

степени элемента 7: 1, 7, 4, 13, 1, $\ldots$,

степени элемента 11: 1, 11, 1, $\ldots$,

степени элемента 13: 1, 13, 4, 7, 1, $\ldots$

6) Группа $\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, ... ,

степени элемента 7: 1, 7, 4, 13, 1, ... ,

степени элемента 11: 1, 11, 1, ... ,

степени элемента 13: 1, 13, 4, 7, 1, ... ,

степени элемента 14: 1, 14, 1, ...

6) Группа $\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, . . . ,

степени элемента 7: 1, 7, 4, 13, 1, . . . ,

степени элемента 11: 1, 11, 1, . . . ,

степени элемента 13: 1, 13, 4, 7, 1, . . . ,

степени элемента 14: 1, 14, 1, . . . ,

группа $\mathbb{Z}_{15}^{*}$ не является циклической.

Циклические группы
Примеры

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
степени элемента 2: 1, 2, 4, 8, 1, ... ,
степени элемента 7: 1, 7, 4, 13, 1, ... ,
степени элемента 11: 1, 11, 1, ... ,
степени элемента 13: 1, 13, 4, 7, 1, ... ,
степени элемента 14: 1, 14, 1, ... ,
группа $\mathbb{Z}_{15}^*$ не является циклической.
7) Группа $\mathbb{Z}$.

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, ... ,

степени элемента 7: 1, 7, 4, 13, 1, ... ,

степени элемента 11: 1, 11, 1, ... ,

степени элемента 13: 1, 13, 4, 7, 1, ... ,

степени элемента 14: 1, 14, 1, ... ,

группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.

Кратные числа 1: $\ldots -2, -1, 0, 1, 2, 3, \ldots$

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, . . . ,

степени элемента 7: 1, 7, 4, 13, 1, . . . ,

степени элемента 11: 1, 11, 1, . . . ,

степени элемента 13: 1, 13, 4, 7, 1, . . . ,

степени элемента 14: 1, 14, 1, . . . ,

группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.

Кратные числа 1: $\ldots -2$, -1, 0, 1, 2, 3, $\ldots$,

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, … ,

степени элемента 7: 1, 7, 4, 13, 1, … ,

степени элемента 11: 1, 11, 1, … ,

степени элемента 13: 1, 13, 4, 7, 1, … ,

степени элемента 14: 1, 14, 1, … ,

группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.

Кратные числа 1: $\ldots -2$, -1, 0, 1, 2, 3, …,

группа циклическая

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,

степени элемента 2: 1, 2, 4, 8, 1, . . . ,

степени элемента 7: 1, 7, 4, 13, 1, . . . ,

степени элемента 11: 1, 11, 1, . . . ,

степени элемента 13: 1, 13, 4, 7, 1, . . . ,

степени элемента 14: 1, 14, 1, . . . ,

группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.

Кратные числа 1: $\ldots -2, -1, 0, 1, 2, 3, \ldots,$

группа циклическая,

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
   степени элемента 2: 1, 2, 4, 8, 1, . . . ,
   степени элемента 7: 1, 7, 4, 13, 1, . . . ,
   степени элемента 11: 1, 11, 1, . . . ,
   степени элемента 13: 1, 13, 4, 7, 1, . . . ,
   степени элемента 14: 1, 14, 1, . . . ,
   группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.
   Кратные числа 1: $\ldots -2$, -1, 0, 1, 2, 3, $\ldots$,
   группа циклическая,
   образующим является и число -1

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
   степени элемента 2: 1, 2, 4, 8, 1, ... ,
   степени элемента 7: 1, 7, 4, 13, 1, ... ,
   степени элемента 11: 1, 11, 1, ... ,
   степени элемента 13: 1, 13, 4, 7, 1, ... ,
   степени элемента 14: 1, 14, 1, ... ,
   группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.
   Кратные числа 1: ... −2, −1, 0, 1, 2, 3, ...,
   группа циклическая,
   образующим является и число −1,

6) Группа $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$,
степени элемента 2: 1, 2, 4, 8, 1, ..., ,
степени элемента 7: 1, 7, 4, 13, 1, ..., ,
степени элемента 11: 1, 11, 1, ..., ,
степени элемента 13: 1, 13, 4, 7, 1, ..., ,
степени элемента 14: 1, 14, 1, ..., ,
группа $\mathbb{Z}_{15}^*$ не является циклической.

7) Группа $\mathbb{Z}$.
Кратные числа 1: $\ldots -2$, -1, 0, 1, 2, 3, ...,
группа циклическая,
образующим является и число -1,
других образующих элементов нет.

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.
Эта группа не является циклической,
$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической,

$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической,

$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.

Эта группа не является циклической

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической,

$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.

Эта группа не является циклической,

$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.
Эта группа не является циклической,
$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.
9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.
Эта группа не является циклической,
$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу,
$a > 0$, среди степеней нет отрицательных чисел

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.
Эта группа не является циклической,
$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.
Эта группа не является циклической,
$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу,
$a > 0$, среди степеней нет отрицательных чисел,
$a < 0$, положительными являются только четные степени a

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической,

$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.

Эта группа не является циклической,

$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу,

$a > 0$, среди степеней нет отрицательных чисел,

$a < 0$, положительными являются только четные степени a,

$a^2 \neq 1$

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.
Эта группа не является циклической,
$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.
Эта группа не является циклической,
$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу,
$a > 0$, среди степеней нет отрицательных чисел,
$a < 0$, положительными являются только четные степени a,
$a^2 \neq 1$,
$\{a^{2n}\}_{n=-\infty}^{\infty}$ строго возрастает или строго убывает

8) Группа $\mathbb{Q}$, аддитивная группа рациональных чисел.

Эта группа не является циклической,

$a \in \mathbb{Q}$, $a \neq 0$, число $a/2 \in \mathbb{Q}$ не является кратным числа a.

9) Группа $\mathbb{Q}^*$, мультипликативная группа ненулевых рациональных чисел.

Эта группа не является циклической,

$\forall a \in \mathbb{Q}^*$ степени элемента a не исчерпывают всю группу,

$a > 0$, среди степеней нет отрицательных чисел,

$a < 0$, положительными являются только четные степени a,

$a^2 \neq 1$,

$\{a^{2n}\}_{n=-\infty}^{\infty}$ строго возрастает или строго убывает,

ни одно рациональное число, находящееся строго между двумя членами последовательности, не является степенью числа a.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,

x, $y \in \langle a \rangle$

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,

x, $y \in \langle a \rangle$, $x = a^m$, $y = a^n$, m, $n \in \mathbb{Z}$

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,

$x, y \in \langle a \rangle$, $x = a^m$, $y = a^n$, $m, n \in \mathbb{Z}$,

$xy^{-1} = a^{m-n} \in \langle a \rangle$.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,
x, $y \in \langle a \rangle$, $x = a^m$, $y = a^n$, m, $n \in \mathbb{Z}$,
$xy^{-1} = a^{m-n} \in \langle a \rangle$.
Если $|a| = n$, то $\langle a \rangle = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,

x, $y \in \langle a \rangle$, $x = a^m$, $y = a^n$, m, $n \in \mathbb{Z}$,

$xy^{-1} = a^{m-n} \in \langle a \rangle$.

Если $|a| = n$, то $\langle a \rangle = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$, $|\langle a \rangle| = |a|$.

10) Любая циклическая группа является конечным или счетным множеством (не более, чем счетным).

Поэтому любая группа, элементы которой образуют несчетное множество, не является циклической.

Например, это группы $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$.

11) G — группа, $a \in G$, $\langle a \rangle$ — множество всех элементов, представимых в виде степени элемента a.

Множество $\langle a \rangle$ является циклической подгруппой группы G,
$x,\ y \in \langle a \rangle$, $x = a^m$, $y = a^n$, $m,\ n \in \mathbb{Z}$,
$xy^{-1} = a^{m-n} \in \langle a \rangle$.
Если $|a| = n$, то $\langle a \rangle = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$, $|\langle a \rangle| = |a|$.
Если $|a| = \infty$, то все элементы a^n, $n \in \mathbb{Z}$ попарно различны, и $\langle a \rangle = \left\{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\right\}$,
подгруппа $\langle a \rangle$ бесконечная, $|\langle a \rangle| = |a|$.

Циклические группы

Альтернативное определение циклической группы.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.
Обратно, $a \in G$ и $|a| = |G|$.

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.
Обратно, $a \in G$ и $|a| = |G|$.
$\langle a \rangle \subset G$

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.
Обратно, $a \in G$ и $|a| = |G|$.
$\langle a \rangle \subset G$, $|\langle a \rangle| = |a| = |G|$

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.
Обратно, $a \in G$ и $|a| = |G|$.
$\langle a \rangle \subset G$, $|\langle a \rangle| = |a| = |G|$, $G = \langle a \rangle$

Циклические группы

Альтернативное определение циклической группы.

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что $G = \langle a \rangle$.

Теорема

Конечная группа G является циклической в том и только том случае, когда существует элемент $a \in G$, порядок которого равен порядку группы.

Циклическая группа G, образующий элемент a.
$G = \langle a \rangle$, $|G| = |\langle a \rangle| = |a|$.
Обратно, $a \in G$ и $|a| = |G|$.
$\langle a \rangle \subset G$, $|\langle a \rangle| = |a| = |G|$, $G = \langle a \rangle$, группа G циклическая. $\square$

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

a^k является образующим $\Leftrightarrow |a^k| = n$

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

a^k является образующим $\Leftrightarrow |a^k| = n \;\Leftrightarrow \frac{n}{(n,k)} = n$

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

a^k является образующим $\Leftrightarrow |a^k| = n \;\Leftrightarrow \frac{n}{(n,k)} = n \quad \Leftrightarrow (n,k) = 1.$

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

a^k является образующим $\Leftrightarrow |a^k| = n \;\Leftrightarrow \frac{n}{(n,k)} = n \quad \Leftrightarrow (n,k) = 1.$
$G = \{a^k : k = 0, 1, \ldots, n-1\}$

Циклические группы

Следствие

Элемент конечной циклической группы является образующим тогда и только тогда, когда его порядок равен порядку группы.

Следствие

Пусть G — циклическая группа конечного порядка n с образующим элементом a. Элемент a^k $(k \in \mathbb{Z})$ является образующим группы G тогда и только тогда, когда числа k и n взаимно простые. Число образующих элементов группы G равно $\varphi(n)$.

a^k является образующим $\Leftrightarrow |a^k| = n \ \Leftrightarrow \frac{n}{(n,k)} = n \quad \Leftrightarrow (n,k) = 1$.
$G = \{a^k : k = 0, 1, \ldots, n-1\}$,
количество чисел в последовательности $0,\ 1,\ \ldots,\ n-1$, взаимно простых с n, равно $\varphi(n)$. $\square$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.

$H = \{e\}$ циклическая.

$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,

$x = a^k$, $k \in \mathbb{N}$.

$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.

$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.

Доказываем обратное вложение.

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$, $r = 0$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$, $r = 0$, $n = dq$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$, $r = 0$, $n = dq$, $x = (a^d)^q \in \langle a^d \rangle$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$, $r = 0$, $n = dq$, $x = (a^d)^q \in \langle a^d \rangle$,
$H \subset \langle a^d \rangle$

Циклические группы

Теорема

Любая подгруппа циклической группы является циклической.

G циклическая группа с образующим элементом a, H ее подгруппа.
$H = \{e\}$ циклическая.
$H \neq \{e\}$, $x \in H$, $x \neq e$, $x = a^k$, $k \in \mathbb{Z}$, $k \neq 0$, $x^{-1} = a^{-k}$,
$x = a^k$, $k \in \mathbb{N}$.
$d = \min\{k : k \in \mathbb{N}, a^k \in H\}$.
$a^d \in H \Rightarrow \langle a^d \rangle \subset H$.
Доказываем обратное вложение.
$x \in H$, $x = a^n$, $n \in \mathbb{Z}$, $n = dq + r$, $0 \leqslant r < d$, $x = a^{dq+r}$,
$a^r = \underbrace{x}_{\in H} \underbrace{(a^d)^{-q}}_{\in H} \in H$, $r = 0$, $n = dq$, $x = (a^d)^q \in \langle a^d \rangle$,
$H \subset \langle a^d \rangle$, $H = \langle a^d \rangle$. □

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0, 1, 2, \ldots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0,\ 1,\ 2,\ \ldots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

$$
\begin{aligned}
&0\mathbb{Z} = \{0\},\\
&1\mathbb{Z} = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2\},\\
&2\mathbb{Z} = \mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4\},\\
&3\mathbb{Z} = \mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0,\ 1,\ 2,\ \ldots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

$$
\begin{aligned}
&0\mathbb{Z} = \{0\},\\
&1\mathbb{Z} = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2\},\\
&2\mathbb{Z} = \mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4\},\\
&3\mathbb{Z} = \mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

$H \neq \{0\}$

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0,\ 1,\ 2,\ \dots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

$$
\begin{aligned}
&0\mathbb{Z} = \{0\},\\
&1\mathbb{Z} = \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2\},\\
&2\mathbb{Z} = \mathbb{Z} = \{\dots, -4, -2, 0, 2, 4\},\\
&3\mathbb{Z} = \mathbb{Z} = \{\dots, -6, -3, 0, 3, 6\},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned}
$$

$H \neq \{0\}$, $H = \langle d \rangle$, $d \in \mathbb{N}$

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0,\ 1,\ 2,\ \ldots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

$$
\begin{aligned}
&0\mathbb{Z} = \{0\},\\
&1\mathbb{Z} = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2\},\\
&2\mathbb{Z} = \mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4\},\\
&3\mathbb{Z} = \mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

$H \neq \{0\}$, $H = \langle d \rangle$, $d \in \mathbb{N}$, $H = \{\ldots, -2d, -d, 0, d, 2d, \ldots\}$

Циклические группы

Следствие

Множества $k\mathbb{Z}$, $k = 0,\ 1,\ 2,\ \ldots$ являются подгруппами группы $\mathbb{Z}$, все эти подгруппы попарно различны и ими исчерпываются все подгруппы группы $\mathbb{Z}$.

$$
\begin{aligned}
&0\mathbb{Z} = \{0\},\\
&1\mathbb{Z} = \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2\},\\
&2\mathbb{Z} = \mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4\},\\
&3\mathbb{Z} = \mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

$H \neq \{0\}$, $H = \langle d\rangle$, $d \in \mathbb{N}$, $H = \{\ldots, -2d, -d, 0, d, 2d, \ldots\} = d\mathbb{Z}$. $\square$

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x + y) = f(x)f(y)$, $f(xy) = f(x) + f(y)$, $f(x + y) = f(x) + f(y)$.

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x + y) = f(x)f(y)$, $f(xy) = f(x) + f(y)$, $f(x + y) = f(x) + f(y)$.
Свойства гомоморфизмов:

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых $x, y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x+y) = f(x)f(y)$, $f(xy) = f(x) + f(y)$, $f(x+y) = f(x) + f(y)$.
Свойства гомоморфизмов:

- 1) $f(e_1) = e_2$;

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x+y) = f(x)f(y)$, $f(xy) = f(x) + f(y)$, $f(x+y) = f(x) + f(y)$.
Свойства гомоморфизмов:

- 1) $f(e_1) = e_2$;
- 2) $\forall a \in G_1 \;\; f(a^{-1}) = (f(a))^{-1}$;

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x + y) = f(x)f(y)$,
$f(xy) = f(x) + f(y)$, $f(x + y) = f(x) + f(y)$.
Свойства гомоморфизмов:

- 1) $f(e_1) = e_2$;
- 2) $\forall a \in G_1 \ f(a^{-1}) = (f(a))^{-1}$;
- 3) $\forall a \in G_1, \forall n \in \mathbb{Z} \ f(a^n) = (f(a))^n$;

Гомоморфизмы

Пусть G_1 и G_2 — произвольные группы.

Определение

Отображение $f : G_1 \to G_2$ называется гомоморфизмом, если для любых x, $y \in G_1$ выполняется соотношение $f(xy) = f(x)f(y)$.

Альтернативные варианты записи: $f(x + y) = f(x)f(y)$, $f(xy) = f(x) + f(y)$, $f(x + y) = f(x) + f(y)$.
Свойства гомоморфизмов:

- 1) $f(e_1) = e_2$;
- 2) $\forall a \in G_1 \ f(a^{-1}) = (f(a))^{-1}$;
- 3) $\forall a \in G_1, \forall n \in \mathbb{Z} \ f(a^n) = (f(a))^n$;
- 4) $a \in G_1$, $|a| = m < \infty \Rightarrow |f(a)| = n < \infty$, $n|m$.

Доказательство.

Доказательство.
1)

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$

Гомоморфизмы

Доказательство.
1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1) f(e_1) = f(e_1)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

Гомоморфизмы

Доказательство.
1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$
2)

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$

Доказательство.

1) $e_1e_1 = e_1,\ f(e_1e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2$

Гомоморфизмы

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

Гомоморфизмы

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3)

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$:

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1)$

Гомоморфизмы

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1) f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ □

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ □

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$: $a^0 = e_1,\ f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0,$

$n = 1$:

Гомоморфизмы

Доказательство.
1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □
2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □
3) $f(a^n) \stackrel{?}{=} (f(a))^n$.
$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,
$n = 1$: $f(a^1) = f(a)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \overset{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \overset{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$:

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ □

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ □

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$: $a^0 = e_1,\ f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0,$

$n = 1$: $f(a^1) = f(a) = (f(a))^1,$

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$: $a^0 = e_1,\ f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0,$

$n = 1$: $f(a^1) = f(a) = (f(a))^1,$

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \overset{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \overset{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$:

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n)$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n})$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n}$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ □

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ □

3) $f(a^n) \overset{?}{=} (f(a))^n.$

$n = 0\colon\ a^0 = e_1,\ f(a^0) = f(e_1) \overset{1)}{=} e_2 = (f(a))^0,$

$n = 1\colon\ f(a^1) = f(a) = (f(a))^1,$

$n \geqslant 1\colon\ f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1},$

$n \leqslant -1\colon\ f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \overset{2)}{=} ((f(a))^{-1})^{-n}$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$: $a^0 = e_1,\ f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0,$

$n = 1$: $f(a^1) = f(a) = (f(a))^1,$

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1},$

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n.$ $\square$

Гомоморфизмы

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,
$n = 1$: $f(a^1) = f(a) = (f(a))^1$,
$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,
$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n$. □

4)

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1$, $f(e_1 e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \overset{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \overset{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \overset{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n$. $\square$

4) $|a| = m$

Гомоморфизмы

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. □

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. □

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n$. □

4) $|a| = m$, $a^m = e_1$

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^na) = f(a^n)f(a) = (f(a))^nf(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n$. $\square$

4) $|a| = m$, $a^m = e_1$, $f(a^m) = f(e_1)$, $(f(a))^m = e_2$

Доказательство.

1) $e_1e_1 = e_1$, $f(e_1e_1) = f(e_1)$, $f(e_1)f(e_1) = f(e_1)$, $f(e_1) = e_2$. $\square$

2) $aa^{-1} = e_1$, $f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2}$, $f(a)f(a^{-1}) = e_2$,

$f(a^{-1}) = (f(a))^{-1}$. $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n$.

$n = 0$: $a^0 = e_1$, $f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0$,

$n = 1$: $f(a^1) = f(a) = (f(a))^1$,

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1}$,

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n$. $\square$

4) $|a| = m$, $a^m = e_1$, $f(a^m) = f(e_1)$, $(f(a))^m = e_2 \Rightarrow |f(a)| < \infty$

Гомоморфизмы

Доказательство.

1) $e_1 e_1 = e_1,\ f(e_1 e_1) = f(e_1),\ f(e_1)f(e_1) = f(e_1),\ f(e_1) = e_2.$ $\square$

2) $aa^{-1} = e_1,\ \ f(a)f(a^{-1}) = \underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1}) = e_2,$

$f(a^{-1}) = (f(a))^{-1}.$ $\square$

3) $f(a^n) \stackrel{?}{=} (f(a))^n.$

$n = 0$: $a^0 = e_1,\ f(a^0) = f(e_1) \stackrel{1)}{=} e_2 = (f(a))^0,$

$n = 1$: $f(a^1) = f(a) = (f(a))^1,$

$n \geqslant 1$: $f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = (f(a))^n f(a) = (f(a))^{n+1},$

$n \leqslant -1$: $f(a^n) = f((a^{-1})^{-n}) = (f(a^{-1}))^{-n} \stackrel{2)}{=} ((f(a))^{-1})^{-n} =$
$= (f(a))^n.$ $\square$

4) $|a| = m,\ a^m = e_1,\ f(a^m) = f(e_1),\ (f(a))^m = e_2 \Rightarrow |f(a)| < \infty,$
$|f(a)| = n$

Доказательство.

1) $e_1e_1=e_1,\ f(e_1e_1)=f(e_1),\ f(e_1)f(e_1)=f(e_1),\ f(e_1)=e_2.$ □

2) $aa^{-1}=e_1,\ \ f(a)f(a^{-1})=\underbrace{f(e_1)}_{e_2},\ \ f(a)f(a^{-1})=e_2,$

$f(a^{-1})=(f(a))^{-1}.$ □

3) $f(a^n)\stackrel{?}{=}(f(a))^n.$

$n=0$: $a^0=e_1,\ f(a^0)=f(e_1)\stackrel{1)}{=}e_2=(f(a))^0,$

$n=1$: $f(a^1)=f(a)=(f(a))^1,$

$n\geqslant 1$: $f(a^{n+1})=f(a^na)=f(a^n)f(a)=(f(a))^nf(a)=(f(a))^{n+1},$

$n\leqslant -1$: $f(a^n)=f((a^{-1})^{-n})=(f(a^{-1}))^{-n}\stackrel{2)}{=}((f(a))^{-1})^{-n}=$
$=(f(a))^n.$ □

4) $|a|=m,\ a^m=e_1,\ f(a^m)=f(e_1),\ (f(a))^m=e_2\Rightarrow|f(a)|<\infty,$
$|f(a)|=n,\ n|m.$ □

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \ \Rightarrow e_1 \in \ker f$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing$.

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \ \Rightarrow e_1 \in \ker f \ \Rightarrow \ker f \neq \varnothing$.

$a,\ b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f$.

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \ \Rightarrow e_1 \in \ker f \ \Rightarrow \ker f \neq \varnothing$.

$a,\ b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f$.

$f(ab^{-1})$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing.$

$a,\, b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f.$

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

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing.$

$a,\, b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f.$

$f(ab^{-1}) = f(a)(f(b))^{-1} = e_2 e_2^{-1}$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing.$

$a,\, b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f.$

$f(ab^{-1}) = f(a)(f(b))^{-1} = e_2 e_2^{-1} = e_2$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing$.

$a,\, b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f$.

$f(ab^{-1}) = f(a)(f(b))^{-1} = e_2 e_2^{-1} = e_2 \Rightarrow ab^{-1} \in \ker f$

Гомоморфизмы

Определение

Ядром гомоморфизма групп $f : G_1 \to G_2$ называется множество $\ker f = \{x : x \in G_1, f(x) = e_2\}$.

Теорема

Ядро гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_1.

$f(e_1) = e_2 \;\Rightarrow e_1 \in \ker f \;\Rightarrow \ker f \neq \varnothing$.

$a,\, b \in \ker f \overset{?}{\Rightarrow} ab^{-1} \in \ker f$.

$f(ab^{-1}) = f(a)(f(b))^{-1} = e_2 e_2^{-1} = e_2 \Rightarrow ab^{-1} \in \ker f$. $\square$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1}$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1} = e_2$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.
2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1} = e_2$, $ab^{-1} \in \ker f$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1} = e_2$, $ab^{-1} \in \ker f$, $ab^{-1} = e_1$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.
2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1} = e_2$, $ab^{-1} \in \ker f$, $ab^{-1} = e_1$, $a = b$

Гомоморфизмы

Теорема

Гомоморфизм $f : G_1 \to G_2$ является инъективным отображением тогда и только тогда, когда его ядро тривиально.

1) f инъективное, $x \in \ker f$, $f(x) = e_2$, $f(e_1) = e_2, x = e_1$, $\ker f = \{e_1\}$.

2) $\ker f = \{e_1\}$, a, $b \in G_1$, $f(a) = f(b)$, $f(ab^{-1}) = f(a)(f(b))^{-1} = e_2$, $ab^{-1} \in \ker f$, $ab^{-1} = e_1$, $a = b$. $\square$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,

$a, b \in \operatorname{im} f$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,
$a, b \in \operatorname{im} f \ \stackrel{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f$.

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2,\ e_2 \in \operatorname{im} f,\ \operatorname{im} f \neq \varnothing,$
$a,\ b \in \operatorname{im} f \ \stackrel{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f.$
$u,\ v \in G_1,\ f(u) = a,\ f(v) = b\ ,\ f(uv^{-1})$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюрьективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$$f(e_1) = e_2,\ e_2 \in \operatorname{im} f,\ \operatorname{im} f \neq \varnothing,$$
$$a,\ b \in \operatorname{im} f \ \overset{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f.$$
$$u,\ v \in G_1,\ f(u) = a,\ f(v) = b\ ,\ f(uv^{-1}) = f(u)(f(v))^{-1}$$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,
$a, b \in \operatorname{im} f \overset{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f$.
$u, v \in G_1$, $f(u) = a$, $f(v) = b$, $f(uv^{-1}) = f(u)(f(v))^{-1} = ab^{-1}$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,
$a, b \in \operatorname{im} f \overset{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f$.
$u, v \in G_1$, $f(u) = a$, $f(v) = b$, $f(uv^{-1}) = f(u)(f(v))^{-1} = ab^{-1}$,

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,
$a, b \in \operatorname{im} f \;\overset{?}{\Rightarrow}\; ab^{-1} \in \operatorname{im} f$.
$u, v \in G_1$, $f(u) = a$, $f(v) = b$, $f(uv^{-1}) = f(u)(f(v))^{-1} = ab^{-1}$,
$ab^{-1} \in \operatorname{im} f$

Гомоморфизмы

Определение

Образом гомоморфизма групп $f : G_1 \to G_2$ называется множество $f(G_1) = \{f(x) : x \in G_1\}$.
Образ гомоморфизма f обозначается через $\operatorname{im} f$.

Замечание

Гомоморфизм $f : G_1 \to G_2$ является сюръективным отображением тогда и только тогда, когда $\operatorname{im} f = G_2$.

Теорема

Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой группы G_2.

$f(e_1) = e_2$, $e_2 \in \operatorname{im} f$, $\operatorname{im} f \neq \varnothing$,
$a, b \in \operatorname{im} f \overset{?}{\Rightarrow} ab^{-1} \in \operatorname{im} f$.
$u, v \in G_1$, $f(u) = a$, $f(v) = b$, $f(uv^{-1}) = f(u)(f(v))^{-1} = ab^{-1}$,
$ab^{-1} \in \operatorname{im} f$. $\square$