Математические основы защиты информации

Лекция 4

Пилиди Владимир Ставрович

14 апреля 2020 года

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:
для $a \in G$, $n \in \mathbb{N}$ полагаем $a^{-n} = (a^{-1})^n$.

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:
для $a \in G$, $n \in \mathbb{N}$ полагаем $a^{-n} = (a^{-1})^n$.
Сохраняются свойства степеней:

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:
для $a \in G$, $n \in \mathbb{N}$ полагаем $a^{-n} = (a^{-1})^n$.
Сохраняются свойства степеней:

- $a^m a^n = a^{m+n}$, $m, n \in \mathbb{Z}$;

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:
для $a \in G$, $n \in \mathbb{N}$ полагаем $a^{-n} = (a^{-1})^n$.
Сохраняются свойства степеней:

- $a^m a^n = a^{m+n}$, m, $n \in \mathbb{Z}$;
- $(a^m)^n = a^{mn}$, m, $n \in \mathbb{Z}$;

Группы

В случае групп дополнительно вводятся отрицательные целые степени элементов:
для $a \in G$, $n \in \mathbb{N}$ полагаем $a^{-n} = (a^{-1})^n$.
Сохраняются свойства степеней:

- $a^m a^n = a^{m+n}$, $m, n \in \mathbb{Z}$;
- $(a^m)^n = a^{mn}$, $m, n \in \mathbb{Z}$;
- если $ab = ba$, то $(ab)^n = a^n b^n$, $n \in \mathbb{Z}$.

Определение

Говорят, что элемент a группы G имеет конечный порядок, если существует такое натуральное число n, что $a^n = e$. В этом случае наименьшее натуральное число n, для которого выполняется такое равенство, называется порядком элемента a и обозначается через $|a|$. Если для любого $n \in \mathbb{N}$ выполняется соотношение $a^n \neq e$, говорят, что элемент a имеет бесконечный порядок.

Определение

Говорят, что элемент a группы G имеет конечный порядок, если существует такое натуральное число n, что $a^n = e$. В этом случае наименьшее натуральное число n, для которого выполняется такое равенство, называется порядком элемента a и обозначается через $|a|$. Если для любого $n \in \mathbb{N}$ выполняется соотношение $a^n \neq e$, говорят, что элемент a имеет бесконечный порядок.

Замечания

Определение

Говорят, что элемент a группы G имеет конечный порядок, если существует такое натуральное число n, что $a^n = e$. В этом случае наименьшее натуральное число n, для которого выполняется такое равенство, называется порядком элемента a и обозначается через $|a|$. Если для любого $n \in \mathbb{N}$ выполняется соотношение $a^n \neq e$, говорят, что элемент a имеет бесконечный порядок.

Замечания

- Если элемент a имеет бесконечный порядок, то используется обозначение $|a| = \infty$.

Определение

Говорят, что элемент a группы G имеет конечный порядок, если существует такое натуральное число n, что $a^n = e$. В этом случае наименьшее натуральное число n, для которого выполняется такое равенство, называется порядком элемента a и обозначается через $|a|$. Если для любого $n \in \mathbb{N}$ выполняется соотношение $a^n \neq e$, говорят, что элемент a имеет бесконечный порядок.

Замечания

- Если элемент a имеет бесконечный порядок, то используется обозначение $|a| = \infty$.
- Запись $|a| < \infty$ означает, что a — элемент конечного порядка.

Определение

Говорят, что элемент a группы G имеет конечный порядок, если существует такое натуральное число n, что $a^n = e$. В этом случае наименьшее натуральное число n, для которого выполняется такое равенство, называется порядком элемента a и обозначается через $|a|$. Если для любого $n \in \mathbb{N}$ выполняется соотношение $a^n \neq e$, говорят, что элемент a имеет бесконечный порядок.

Замечания

- Если элемент a имеет бесконечный порядок, то используется обозначение $|a| = \infty$.
- Запись $|a| < \infty$ означает, что a — элемент конечного порядка.
- В случае аддитивной записи соотношения $a^n = e$, $a^n \neq e$ заменяются соответственно на $na = 0$, $na \neq 0$.

Примеры.

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

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

$$\begin{array}{rrrrrrr}
1, & 1, & 1, & \ldots, & & & \\
-1, & 1, & -1, & 1, & -1, & \ldots, & \\
i, & -1, & -i, & 1, & i, & -1, & \ldots, \\
-i, & -1, & i, & 1, & -i, & -1, & \ldots\ .
\end{array}$$

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

$$\begin{array}{rrrrrrr} 1, & 1, & 1, & \ldots, & & & \\ -1, & 1, & -1, & 1, & -1, & \ldots, & \\ i, & -1, & -i, & 1, & i, & -1, & \ldots, \\ -i, & -1, & i, & 1, & -i, & -1, & \ldots\ . \end{array}$$

Порядки элементов 1, -1, i, $-i$ равны соответственно 1, 2, 4 и 4.

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

$$\begin{array}{rrrrrrr}
\textcolor{red}{1}, & 1, & 1, & \ldots, & & & \\
-1, & \textcolor{red}{1}, & -1, & 1, & -1, & \ldots, & \\
i, & -1, & -i, & \textcolor{red}{1}, & i, & -1, & \ldots, \\
-i, & -1, & i, & \textcolor{red}{1}, & -i, & -1, & \ldots\ .
\end{array}$$

Порядки элементов 1, -1, i, $-i$ равны соответственно 1, 2, 4 и 4.
2) Группа $\mathbb{Z}$: все элементы, кроме нулевого, имеют бесконечный порядок.

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

$$
\begin{array}{rrrrrrr}
{\color{red}1}, & 1, & 1, & \ldots, & & & \\
-1, & {\color{red}1}, & -1, & 1, & -1, & \ldots, & \\
i, & -1, & -i, & {\color{red}1}, & i, & -1, & \ldots, \\
-i, & -1, & i, & {\color{red}1}, & -i, & -1, & \ldots\ .
\end{array}
$$

Порядки элементов 1, -1, i, $-i$ равны соответственно 1, 2, 4 и 4.
2) Группа $\mathbb{Z}$: все элементы, кроме нулевого, имеют бесконечный порядок.

$$
\begin{array}{rrrrr}
1, & 2, & 3, & 4, & \ldots \\
2, & 4, & 6, & 8, & \ldots \\
3, & 6, & 9, & 12, & \ldots \\
\multicolumn{5}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots}
\end{array}
$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,... a^{n-1} попарно различны.

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,$\ldots a^{n-1}$ попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,... a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. □

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$n|k$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,$\ldots$ a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$n|k$, $k = nm$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$n|k$, $k = nm$, $a^k = a^{nm}$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i - j \leqslant n-1$, $i = j$. □

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,... a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1\,,\ a^{i-j} = e\,,\ 0 \leqslant i-j \leqslant n-1\,,\ i = j.$ $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,$\ldots a^{n-1}$ попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i - j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\; k = nm\,,\; a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,... a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$n|k$, $k = nm$, $a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e$.

$a^k = e$, $k = mn + r, 0 \leqslant r \leqslant n-1$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. □

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e,\ k = mn + r, 0 \leqslant r \leqslant n-1,\ a^k = a^{mn+r}$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, $a^2, \ldots a^{n-1}$ попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e,\ k = mn + r, 0 \leqslant r \leqslant n-1,\ a^k = a^{mn+r} = (a^n)^m a^r$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e,\ k = mn + r, 0 \leqslant r \leqslant n-1,\ a^k = a^{mn+r} = (a^n)^m a^r = a^r$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,... a^{n-1} попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$n|k$, $k = nm$, $a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$

$a^k = e$, $k = mn + r, 0 \leqslant r \leqslant n-1$, $a^k = a^{mn+r} = (a^n)^m a^r = a^r$,
$a^r = e$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,$\ldots a^{n-1}$ попарно различны.

$a^i = a^j$, $0 \leqslant j \leqslant i \leqslant n-1$, $a^{i-j} = e$, $0 \leqslant i-j \leqslant n-1$, $i = j$. $\square$

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\ k = nm\,,\ a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e,\ k = mn + r, 0 \leqslant r \leqslant n-1,\ a^k = a^{mn+r} = (a^n)^m a^r = a^r,$$
$$a^r = e\,,\ r = 0$$

Свойство

$|a| = 1$ в том и только том случае, когда $a = e$

Свойство

Если $|a| = n > 1$, то элементы e, a, a^2,… a^{n-1} попарно различны.

$a^i = a^j,\, 0 \leqslant j \leqslant i \leqslant n-1\,,\, a^{i-j} = e\,,\, 0 \leqslant i-j \leqslant n-1\,,\, i = j.$ □

Свойство

Если $|a| = n$, $k \in \mathbb{Z}$, то $a^k = e$ в том и только том случае, когда $n|k$.

$$n|k\,,\; k = nm\,,\; a^k = a^{nm} = (\underbrace{a^n}_{=e})^m = e.$$

$$a^k = e,\, k = mn + r, 0 \leqslant r \leqslant n-1,\, a^k = a^{mn+r} = (a^n)^m a^r = a^r,$$
$$a^r = e\,,\, r = 0\,,\, n|k.$$ □

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,,\; a^{n+1} = a^n a = a$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,,\; a^{n+1} = a^n a = a\,,\; a^{n+2} = a^n a^2 = a^2, \;\ldots \qquad \square$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \dots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,,\; a^{n+1} = a^n a = a\,,\; a^{n+2} = a^n a^2 = a^2, \;\dots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}},\ a^n = e\,,\ a^{n+1} = a^n a = a\,,\ a^{n+2} = a^n a^2 = a^2,\ \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\ aa^{n-1} = e$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,,\; a^{n+1} = a^n a = a\,,\; a^{n+2} = a^n a^2 = a^2, \;\ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\; aa^{n-1} = e\,,\; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \ldots \quad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\; aa^{n-1} = e\,,\; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,, \; aa^{n-1} = e\,, \; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

$|G| < \infty$, $a \in G$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\; aa^{n-1} = e\,,\; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

$|G| < \infty$, $a \in G$, $\quad a,\ a^2,\ a^3,\ \ldots$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\; aa^{n-1} = e\,,\; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

$$|G| < \infty, \, a \in G, \quad a, \, a^2, \, a^3, \, \ldots, \quad a^i = a^j, \, 1 \leqslant j < i$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,,\; aa^{n-1} = e\,,\; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

$$|G| < \infty, \; a \in G, \quad a, \; a^2, \; a^3, \; \ldots, \quad a^i = a^j, \; 1 \leqslant j < i, \quad a^{i-j} = e$$

Свойство

Если $|a| = n$, то последовательность степеней элемента a является периодической с периодом n.

$$\underbrace{e, a, a^2, \ldots a^{n-1}}_{\text{попарно различны}}, \; a^n = e\,, \; a^{n+1} = a^n a = a\,, \; a^{n+2} = a^n a^2 = a^2, \; \ldots \qquad \square$$

Свойство

Если $|a| = n$, то $a^{-1} = a^k$ для некоторого $k \in \mathbb{N}$.

Если $n > 1$, то $a^n = e\,, \; aa^{n-1} = e\,, \; a^{-1} = a^{n-1}$.
Если $n = 1$, то $a = e$, $e^{-1} = e^1$. $\square$

Свойство

Порядки всех элементов конечной группы являются конечными.

$|G| < \infty$, $a \in G$, $\quad a, a^2, a^3, \ldots, \quad a^i = a^j$, $1 \leqslant j < i$, $\quad a^{i-j} = e$,
$|a| < \infty$. $\square$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n, k) = d$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$.

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.

$(a^k)^m = e$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n|km$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n|km \Leftrightarrow \frac{n}{d}|\frac{k}{d}m$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \overset{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n|km \Leftrightarrow \frac{n}{d}|\frac{k}{d}m \Leftrightarrow \frac{n}{d}|m$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.

$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n | km \Leftrightarrow \frac{n}{d} | \frac{k}{d} m \Leftrightarrow \frac{n}{d} | m \Leftrightarrow m = \frac{n}{d}, 2\frac{n}{d}, 3\frac{n}{d}, \ldots$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n|km \Leftrightarrow \frac{n}{d}\big|\frac{k}{d}m \Leftrightarrow \frac{n}{d}|m \Leftrightarrow m = \frac{n}{d}, 2\frac{n}{d}, 3\frac{n}{d}, \ldots$
$\Rightarrow |a^k| = \frac{n}{d}$. $\square$

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n,k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n | km \Leftrightarrow \frac{n}{d} \big| \frac{k}{d} m \Leftrightarrow \frac{n}{d} | m \Leftrightarrow m = \frac{n}{d}, 2\frac{n}{d}, 3\frac{n}{d}, \ldots$
$\Rightarrow |a^k| = \frac{n}{d}$. $\square$

Свойство

Если $|a| = \infty$, то для любого $k \in \mathbb{Z} \setminus \{0\}$ имеет место равенство
Если $|a^k| = \infty$,

Свойство

Если $|a| < \infty$, то для любого $k \in \mathbb{Z}$ имеет место равенство $|a^k| = \frac{|a|}{(|a|,k)}$.

Обозначим $|a| = n$, $(n, k) = d$, $|a^k| \stackrel{?}{=} \frac{n}{d}$. Пусть $m \in \mathbb{N}$.
$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n|km \Leftrightarrow \frac{n}{d}|\frac{k}{d}m \Leftrightarrow \frac{n}{d}|m \Leftrightarrow m = \frac{n}{d}, 2\frac{n}{d}, 3\frac{n}{d}, \ldots$
$\Rightarrow |a^k| = \frac{n}{d}$. $\square$

Свойство

Если $|a| = \infty$, то для любого $k \in \mathbb{Z} \setminus \{0\}$ имеет место равенство
Если $|a^k| = \infty$,

Если $(a^k)^n = e$ для некоторого $n \in \mathbb{N}$, то $a^{kn} = e$, $kn \neq 0$,
$|a| < \infty$. $\square$

Следствие

Для любого элемента a имеет место равенство $|a^{-1}| = |a|$.

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn}$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn}$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^kb^k$, $a^kb^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \;\Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$, $n|k$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$, $n|k$, $mn|k$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn.$
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$, $n|k$, $mn|k$,
$k \geqslant mn$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$, $n|k$, $mn|k$,
$k \geqslant mn \quad \Rightarrow k = mn$. $\square$

Свойство

Предположим, что порядки элементов a и b конечные, взаимно простые и выполняется равенство $ab = ba$. Тогда элемент ab имеет конечный порядок и $|ab| = |a| \cdot |b|$.

$|a| = m$, $|b| = n$.
$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e \Rightarrow |ab| \leqslant mn$.
$k = |ab|$, $k \leqslant mn$.
$(ab)^k = a^k b^k$, $a^k b^k = e$, $a^k = b^{-k}$, $a^{kn} = b^{-kn} = e$, $m|k$, $n|k$, $mn|k$,
$k \geqslant mn \quad \Rightarrow k = mn$. □

Следствие

Если элементы $a_1, a_2, \ldots, a_k$ попарно перестановочные, их порядки конечные и попарно взаимно простые, то элемент $a = a_1 a_2 \ldots a_k$ имеет конечный порядок, равный произведению порядков сомножителей.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.
$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \qquad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\qquad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*;$ $\qquad n \in \mathbb{N}, \mathbb{U}_n \subset \mathbb{U}$

Подгруппы

Определение и примеры

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.
$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\quad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$; $\quad n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,

$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,

$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\quad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $\quad n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$, $\quad k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $\quad n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,
G, $\{e\}$ и G.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$; $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,

$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,

G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,
G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

G — группа с единичным элементом e, H — подгруппа с единичным элементом e'.

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\quad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $\quad n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,

$\mathbb{U}_2 \subset \mathbb{U}_4$, $\quad k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $\quad n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,

G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

G — группа с единичным элементом e, H — подгруппа с единичным элементом e'.

$e'e' = e'$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,
G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

G — группа с единичным элементом e, H — подгруппа с единичным элементом e'.
$e'e' = e'$, $e' \in G \Rightarrow ee' = e'$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$, $k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,
G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

G — группа с единичным элементом e, H — подгруппа с единичным элементом e'.
$e'e' = e'$, $e' \in G \Rightarrow ee' = e'$, $e'e' = ee'$

Определение

Пусть G — некоторая группа. Непустое множество $H \subset G$ называется подгруппой группы G, если множество H само является группой с операцией, введенной в группе G.

Примеры подгрупп.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\quad \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, $\quad n \in \mathbb{N}$, $\mathbb{U}_n \subset \mathbb{U}$,
$\mathbb{U}_2 \subset \mathbb{U}_4$, $\quad k|n \Rightarrow \mathbb{U}_k \subset \mathbb{U}_n$, $\quad n \geqslant 2$, $\mathbb{A}_n \subset \mathbb{S}_n$,
G, $\{e\}$ и G.

Замечание

Единичный элемент подгруппы совпадает с единичным элементом самой группы.

G — группа с единичным элементом e, H — подгруппа с единичным элементом e'.
$e'e' = e'$, $e' \in G \Rightarrow ee' = e'$, $e'e' = ee' \quad \Rightarrow e' = e$.

Подгруппы

Примеры

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \ldots n\}$

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \ldots n\}$, $(a, b) \mapsto \max\{a, b\}$

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \ldots n\}$, $(a, b) \mapsto \max\{a, b\}$, $a \in S$, $S_0 = \{a\}$

Подгруппы

Примеры

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \ldots n\}$, $(a, b) \mapsto \max\{a, b\}$, $a \in S$, $S_0 = \{a\}$, $(a, a) \mapsto a$. $\square$

Подгруппы
Примеры

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \dots n\}$, $(a, b) \mapsto \max\{a, b\}$, $a \in S$, $S_0 = \{a\}$, $(a, a) \mapsto a$. $\square$

Замечание

Пусть H — подгруппа группы G, $a \in H$. Тогда элемент, обратный к a в самой группе, совпадает с обратным к a в подгруппе H

Следствие

В любой группе G подгруппа $\{e\}$ является единственной подгруппой порядка 1.

Замечание

В случае моноидов аналог последнего утверждения места не имеет.

$S = \{0, 1, 2, \ldots n\}$, $(a, b) \mapsto \max\{a, b\}$, $a \in S$, $S_0 = \{a\}$, $(a, a) \mapsto a$. □

Замечание

Пусть H — подгруппа группы G, $a \in H$. Тогда элемент, обратный к a в самой группе, совпадает с обратным к a в подгруппе H

Оба элемента являются решениями уравнения $ax = e$. □

Теорема

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

Подгруппы

Критерии

Теорема

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

1) если a, $b \in H$, то $ab \in H$;

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H$

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.

$(a, b) \mapsto ab$ — бинарная операция в множестве H.

$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H$

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.

$(a, b) \mapsto ab$ — бинарная операция в множестве H.

$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H\,,\ e \in H.$$ □

Подгруппы

Критерии

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$. $\square$

Теорема

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

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$. $\square$

Теорема

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

$a \in H$

Теорема

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

1) если $a,\, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.
$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H,\ e \in H.$ $\square$

Теорема

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

$a \in H,\ a^2 \in H$

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.

$(a, b) \mapsto ab$ — бинарная операция в множестве H.

$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$. $\square$

Теорема

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

$a \in H$, $a^2 \in H$, $a^3 \in H \ldots$

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$. □

Теорема

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

$a \in H$, $a^2 \in H$, $a^3 \in H \ldots$, $a^i = a^j$, $1 \leqslant j < i$

Теорема

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

1) если $a, b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H\,,\ e \in H.$ $\square$

Теорема

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

$a \in H,\ a^2 \in H,\ a^3 \in H \ldots,\ a^i = a^j,\ 1 \leqslant j < i,\ |a| < \infty$

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.

$(a, b) \mapsto ab$ — бинарная операция в множестве H.

$(ab)c = a(bc)$ выполняется.

$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H$, $e \in H$. $\square$

Теорема

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

$a \in H$, $a^2 \in H$, $a^3 \in H \ldots$, $a^i = a^j$, $1 \leqslant j < i$, $|a| < \infty$, $a^{-1} = a^k$, $k \in \mathbb{N}$

Подгруппы
Критерии

Теорема

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

1) если a, $b \in H$, то $ab \in H$;
2) если $a \in H$, то $a^{-1} \in H$.

Выполняются 1) и 2) $\overset{?}{\Rightarrow}$ H является группой.
$(a, b) \mapsto ab$ — бинарная операция в множестве H.
$(ab)c = a(bc)$ выполняется.

$$H \neq \varnothing \Rightarrow \exists a \in H \overset{2)}{\Rightarrow} a^{-1} \in H \overset{1)}{\Rightarrow} aa^{-1} \in H\,,\ e \in H.$$ □

Теорема

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

$a \in H$, $a^2 \in H$, $a^3 \in H\ldots$, $a^i = a^j$, $1 \leqslant j < i$, $|a| < \infty$, $a^{-1} = a^k$, $k \in \mathbb{N}$, $a^{-1} \in H$. □

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$,
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 $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$,
a, $b \in H$, $b^{-1} \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$,
a, $b \in H$, $b^{-1} \in H$, $a(b^{-1})^{-1} \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$,
a, $b \in H$, $b^{-1} \in H$, $a(b^{-1})^{-1} \in H$, $ab \in H$

Теорема

Непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда выполняется условие: если a, $b \in H$, то $ab^{-1} \in H$.

$c \in H$, $cc^{-1} \in H$, $e \in H$,
$a \in H$, $ea^{-1} \in H$, $a^{-1} \in H$,
a, $b \in H$, $b^{-1} \in H$, $a(b^{-1})^{-1} \in H$, $ab \in H$. $\square$