Математические основы защиты информации

Лекция 7

Пилиди Владимир Ставрович

12 мая 2020 года

Группа $\mathbb{S}_3$.

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

Группа $\mathbb{S}_3$.

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

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

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

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

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

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Группа $\mathbb{S}_3$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$,
$fH = \{fe, fa, fb\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$,
$fH = \{fe, fa, fb\} = \{f, c, d\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$,
$fH = \{fe, fa, fb\} = \{f, c, d\}$.
Два левых смежных класса: $\{e, a, b\}$ и $\{c, d, f\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$,
$fH = \{fe, fa, fb\} = \{f, c, d\}$.
Два левых смежных класса: $\{e, a, b\}$ и $\{c, d, f\}$.
Правые смежные классы: $He = Ha = Hb = \{e, a, b\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H = \{e, a, b\}$.
$eH = H$, $aH = \{ae, a^2, ab\} = H$, $bH = \{be, ba, b^2\} = H$,
$cH = \{ce, ca, cb\} = \{c, d, f\}$, $dH = \{de, da, db\} = \{d, f, c\}$,
$fH = \{fe, fa, fb\} = \{f, c, d\}$.
Два левых смежных класса: $\{e, a, b\}$ и $\{c, d, f\}$.
Правые смежные классы: $He = Ha = Hb = \{e, a, b\}$,
$Hc = Hd = Hf = \{c, d, f\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1 e = \{e, c\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1 e = \{e, c\}$, $\quad H_1 a$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1e = \{e, c\}$, $\quad H_1a = \{ea, ca\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1e = \{e, c\}$, $\quad H_1a = \{ea, ca\} = \{a, d\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1e = \{e, c\}$, $\quad H_1a = \{ea, ca\} = \{a, d\}$,
$H_1b = \{eb, cb\}$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1e = \{e, c\}$, $H_1a = \{ea, ca\} = \{a, d\}$,
$H_1b = \{eb, cb\} = \{b, f\}$.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Подгруппа $H_1 = \{e, c\}$.
$eH_1 = H_1$, $aH_1 = \{ae, ac\} = \{a, f\}$,
$bH_1 = \{be, bc\} = \{b, d\}$,
$\{e, c\}$, $\{a, f\}$, $\{b, d\}$.
$H_1e = \{e, c\}$, $H_1a = \{ea, ca\} = \{a, d\}$,
$H_1b = \{eb, cb\} = \{b, f\}$.
$\{e, c\}$, $\{a, d\}$, $\{b, f\}$.

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH,\ f(x) = ax$

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH,\ f(x) = ax\ ,\ f(x_1) = f(x_2)$

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH$, $f(x) = ax$, $f(x_1) = f(x_2)$, $ax_1 = ax_2$

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH$, $f(x) = ax$, $f(x_1) = f(x_2)$, $ax_1 = ax_2$, $x_1 = x_2$

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH$, $f(x) = ax$, $f(x_1) = f(x_2)$, $ax_1 = ax_2$, $x_1 = x_2$. □

Замечание

Два множества A и B называются равномощными, если существует биективное отображение $f : A \to B$.

Отношение равномощности является отношением эквивалентности.
Конечные множества являются равномощными тогда и только тогда, когда они имеют одинаковое число элементов.

Теорема

Любые два смежных класса группы G по ее подгруппе H являются равномощными.

$f : H \to aH$, $f(x) = ax$, $f(x_1) = f(x_2)$, $ax_1 = ax_2$, $x_1 = x_2$. □

Следствие

Число элементов произвольного смежного класса по конечной подгруппе H равно порядку этой подгруппы.

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$, $A^{-1} = (xH)^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$, $A^{-1} = (xH)^{-1} = H^{-1}x^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$, $A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$, $A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}$.

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}$, $A = xH$, $x \in G$, $A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}$.
$B \in X_{\text{п}}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A)$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A))$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A)) = g(A^{-1})$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A)) = g(A^{-1}) = (A^{-1})^{-1}$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A)) = g(A^{-1}) = (A^{-1})^{-1} = A$

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A)) = g(A^{-1}) = (A^{-1})^{-1} = A\,.$
Отображение f биективное

Теорема

Множество всех левых смежных классов группы G по ее подгруппе H равномощно множеству всех правых смежных классов группы G по этой подгруппе.

$X_{\text{л}}$ — множество всех левых смежных классов группы G по подгруппе H.
$X_{\text{п}}$ — множество всех правых смежных классов группы G по подгруппе H.
$A \in X_{\text{л}}\,,\ A = xH,\ x \in G\,,\ A^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in X_{\text{п}}.$
$B \in X_{\text{п}} \ \Rightarrow B^{-1} \in X_{\text{л}}.$
$f : X_{\text{л}} \to X_{\text{п}}, f : A \mapsto A^{-1}\,,$
$g : X_{\text{п}} \to X_{\text{л}}, g : B \mapsto B^{-1}\,,$
$(gf)(A) = g(f(A)) = g(A^{-1}) = (A^{-1})^{-1} = A\,.$
Отображение f биективное.

Следствие

Множества $X_{\text{л}}$ и $X_{\text{п}}$ одновременно являются конечными или бесконечными, и в первом случае имеют одинаковое число элементов.

Следствие

Множества $X_{\text{л}}$ и $X_{\text{п}}$ одновременно являются конечными или бесконечными, и в первом случае имеют одинаковое число элементов.

Определение

Если множество всех левых смежных классов группы G по подгруппе H конечное, говорят, что подгруппа H имеет конечный индекс.

Следствие

Множества $X_{\text{л}}$ и $X_{\text{п}}$ одновременно являются конечными или бесконечными, и в первом случае имеют одинаковое число элементов.

Определение

Если множество всех левых смежных классов группы G по подгруппе H конечное, говорят, что подгруппа H имеет конечный индекс.
В этом случае число левых смежных классов называют индексом подгруппы H в группе G и обозначают через $|G : H|$.

Следствие

Множества $X_{\text{л}}$ и $X_{\text{п}}$ одновременно являются конечными или бесконечными, и в первом случае имеют одинаковое число элементов.

Определение

Если множество всех левых смежных классов группы G по подгруппе H конечное, говорят, что подгруппа H имеет конечный индекс.
В этом случае число левых смежных классов называют индексом подгруппы H в группе G и обозначают через $|G : H|$.
Если множество этих смежных классов бесконечное, говорят, что подгруппа имеет бесконечный индекс, и пишут $|G : H| = \infty$.

Теорема Лагранжа

Пусть G — конечная группа, H — ее подгруппа.
Тогда имеет место равенство $|G| = |G : H| \cdot |H|$.

Теорема Лагранжа

Пусть G — конечная группа, H — ее подгруппа.
Тогда имеет место равенство $|G| = |G : H| \cdot |H|$.

Группа G является объединением $|G : H|$ попарно не пересекающихся левых смежных классов, каждый из которых содержит $|H|$ элементов.

Теорема Лагранжа

Пусть G — конечная группа, H — ее подгруппа.
Тогда имеет место равенство $|G| = |G : H| \cdot |H|$.

Группа G является объединением $|G : H|$ попарно не пересекающихся левых смежных классов, каждый из которых содержит $|H|$ элементов.
Число элементов группы равно произведению $|G : H| \cdot |H|$. □

Теорема Лагранжа

Пусть G — конечная группа, H — ее подгруппа.
Тогда имеет место равенство $|G| = |G : H| \cdot |H|$.

Группа G является объединением $|G : H|$ попарно не пересекающихся левых смежных классов, каждый из которых содержит $|H|$ элементов.
Число элементов группы равно произведению $|G : H| \cdot |H|$. □

Следствие

Порядок и индекс произвольной подгруппы конечной группы делят порядок этой группы.

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$, $|\mathbb{Z}_m^*| = \varphi(m)$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$, $|\mathbb{Z}_m^*| = \varphi(m)$, $a \in \mathbb{Z}$, $(a, m) = 1$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$, $|\mathbb{Z}_m^*| = \varphi(m)$, $a \in \mathbb{Z}$, $(a, m) = 1$, $a \bmod m \in \mathbb{Z}_m^*$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$, $|\mathbb{Z}_m^*| = \varphi(m)$, $a \in \mathbb{Z}$, $(a, m) = 1$, $a \bmod m \in \mathbb{Z}_m^*$,

$a^{\varphi(m)} \equiv (a \bmod m)^{\varphi(m)} \equiv 1 (\bmod m)$

Следствие

Порядок любого элемента конечной группы делит порядок этой группы.

$a \in G$, $H = \langle a \rangle$, $|a| = |H|$. □

Это утверждение обобщает теорему Эйлера.

$m \geqslant 2$, $|\mathbb{Z}_m^*| = \varphi(m)$, $a \in \mathbb{Z}$, $(a, m) = 1$, $a \bmod m \in \mathbb{Z}_m^*$,

$a^{\varphi(m)} \equiv (a \bmod m)^{\varphi(m)} \equiv 1 (\bmod m)$. □

Теорема (о подгруппах конечной циклической группы)

Теорема (о подгруппах конечной циклической группы)

Пусть G — циклическая группа порядка n с образующим элементом a.

Теорема (о подгруппах конечной циклической группы)

Пусть G — циклическая группа порядка n с образующим элементом a.
Тогда для любого делителя k числа n существует единственная подгруппа группы G порядка k.

Теорема (о подгруппах конечной циклической группы)

Пусть G — циклическая группа порядка n с образующим элементом a.
Тогда для любого делителя k числа n существует единственная подгруппа группы G порядка k.
Эта циклическая подгруппа порождается элементом $a^{n/k}$ и состоит из всех элементов $x \in G$, удовлетворяющих условию $x^k = e$.

Теорема (о подгруппах конечной циклической группы)

Пусть G — циклическая группа порядка n с образующим элементом a.
Тогда для любого делителя k числа n существует единственная подгруппа группы G порядка k.
Эта циклическая подгруппа порождается элементом $a^{n/k}$ и состоит из всех элементов $x \in G$, удовлетворяющих условию $x^k = e$.
Указанными подгруппами исчерпываются все подгруппы группы G.

Теорема (о подгруппах конечной циклической группы)

Пусть G — циклическая группа порядка n с образующим элементом a.
Тогда для любого делителя k числа n существует единственная подгруппа группы G порядка k.
Эта циклическая подгруппа порождается элементом $a^{n/k}$ и состоит из всех элементов $x \in G$, удовлетворяющих условию $x^k = e$.
Указанными подгруппами исчерпываются все подгруппы группы G.
Подгруппы H_1, H_2 группы G удовлетворяют условию $H_1 \subset H_2$ в том и только том случае, когда порядок подгруппы H_1 делит порядок подгруппы H_2.

$H \subset G$

$H \subset G$, $|H| = k$

Группы

Смежные классы

$H \subset G$, $|H| = k$, $k|n$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d|$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k}$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k} = (a^{n/l})^m$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k} = (a^{n/l})^m \in H_2$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k} = (a^{n/l})^m \in H_2 \Rightarrow \langle a^{n/k} \rangle \subset H_2$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k} = (a^{n/l})^m \in H_2 \Rightarrow \langle a^{n/k} \rangle \subset H_2$, $H_1 \subset H_2$

$H \subset G$, $|H| = k$, $k|n$, $\forall x \in H\ x^k = e$.
Найдем число решений уравнения $x^k = e$ в группе G.
$x \in G$, $x^k = e$, $x = a^m$, $m \in \mathbb{Z}$, $0 \leqslant m < n$,
$x^k = e \Leftrightarrow a^{mk} = e \Leftrightarrow n|mk \Leftrightarrow \frac{n}{k} \Big| m$, $m = \frac{n}{k}t$, $t \in \mathbb{Z}$,
$m = 0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}$,
число решений уравнения равно k,
$H = \{x \in G : x^k = e\}$,
группа порядка k единственная.
$k|n$, $d = \frac{n}{k}$, $H = \langle a^d \rangle$,
$|H| = |a^d| = \frac{|a|}{(d,|a|)} = \frac{n}{(d,n)} = \frac{n}{d} = k$.
Анализ соотношения $H_1 \subset H_2$, $|H_1| = k$, $|H_2| = l$.
1) $H_1 \subset H_2 \Rightarrow k|l$.
2) $k|l$, $H_1 = \langle a^{n/k} \rangle$, $H_2 = \langle a^{n/l} \rangle$, $m = l/k \in \mathbb{N}$,
$a^{n/k} = (a^{n/l})^{l/k} = (a^{n/l})^m \in H_2 \Rightarrow \langle a^{n/k} \rangle \subset H_2$, $H_1 \subset H_2$. □

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n\,,\ H \subset G, |H| = k$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$, $H = \langle x \rangle$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G, |x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G, |x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G, |x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$,
группа порядка k единственная

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$,
группа порядка k единственная,

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$,
группа порядка k единственная,
все элементы порядка k содержатся в подгруппе H и являются образующими этой группы.

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$,
группа порядка k единственная,
все элементы порядка k содержатся в подгруппе H и являются образующими этой группы.
Количество образующих элементов циклической группы порядка k равно $\varphi(k)$

Следствие

Пусть G — циклическая группа порядка n. Тогда для любого делителя k числа n группа содержит ровно $\varphi(k)$ элементов порядка k.

$k \mid n$, $H \subset G, |H| = k$, H циклическая,
ее образующие элементы имеют порядок k.
$x \in G$, $|x| = k$, $H = \langle x \rangle$, $|H| = |x| = k$, $k \mid n$,
группа порядка k единственная,
все элементы порядка k содержатся в подгруппе H и являются образующими этой группы.
Количество образующих элементов циклической группы порядка k равно $\varphi(k)$. □

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

$|G| = n$ — четное число

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

$|G| = n$ — четное число , $2|n$

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

$|G| = n$ — четное число , $2|n$,
количество элементов второго порядка равно $\varphi(2) = 1$

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

$|G| = n$ — четное число , $2|n$,
количество элементов второго порядка равно $\varphi(2) = 1$. □

Следствие

Циклическая группа четного порядка содержит единственный элемент второго порядка.

$|G| = n$ — четное число , $2|n$,
количество элементов второго порядка равно $\varphi(2) = 1$. □

Следствие

Имеет место равенство $\sum_{d|n} \varphi(d) = n$.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.
1) Существует $a \in G$, $|a| = \infty$.
$H = \langle a \rangle$ — бесконечная циклическая группа ,
она содержит бесконечное множество подгрупп.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.
1) Существует $a \in G$, $|a| = \infty$.
$H = \langle a \rangle$ — бесконечная циклическая группа ,
она содержит бесконечное множество подгрупп.
2) Все элементы группы G имеют конечные порядки.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.
1) Существует $a \in G$, $|a| = \infty$.
$H = \langle a \rangle$ — бесконечная циклическая группа ,
она содержит бесконечное множество подгрупп.
2) Все элементы группы G имеют конечные порядки.
Все циклические подгруппы являются конечными.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.
1) Существует $a \in G$, $|a| = \infty$.
$H = \langle a \rangle$ — бесконечная циклическая группа ,
она содержит бесконечное множество подгрупп.
2) Все элементы группы G имеют конечные порядки.
Все циклические подгруппы являются конечными.
$H_1, H_2, \ldots, H_n$ — различные циклические группы.

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G$

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G$,

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G\,, \quad a \in G \setminus \bigcup\limits_{i=1}^{n} H_i$

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G\,, \quad a \in G \setminus \bigcup\limits_{i=1}^{n} H_i\ , H_{n+1} = \langle a \rangle$

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G\,, \quad a \in G \setminus \bigcup\limits_{i=1}^{n} H_i\ , H_{n+1} = \langle a \rangle\,,$

$H_{n+1} \neq H_i,\ i = 1, 2, \ldots, n$

Теорема

Множество подгрупп бесконечной группы является бесконечным.

Множество циклических подгрупп бесконечной группы является бесконечным.

1) Существует $a \in G$, $|a| = \infty$.

$H = \langle a \rangle$ — бесконечная циклическая группа ,

она содержит бесконечное множество подгрупп.

2) Все элементы группы G имеют конечные порядки.

Все циклические подгруппы являются конечными.

$H_1, H_2, \ldots, H_n$ — различные циклические группы.

$\bigcup\limits_{i=1}^{n} H_i \neq G\,, \quad a \in G \setminus \bigcup\limits_{i=1}^{n} H_i\ , H_{n+1} = \langle a \rangle\,,$

$H_{n+1} \neq H_i,\ i = 1, 2, \ldots, n\ .$ □

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа , $k|n$, $1 < k < n$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа , $k|n$, $1 < k < n$,
$H_0 \subset G$, $|H_0| = k$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа , $k|n$, $1 < k < n$,
$H_0 \subset G$, $|H_0| = k$, $H_0 \neq \{e\}$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа , $k|n$, $1 < k < n$,
$H_0 \subset G$, $|H_0| = k$, $H_0 \neq \{e\}$, $H_0 \neq G$

Теорема

Группа не имеет собственных подгрупп тогда и только тогда, когда она конечная и ее порядок равен единице или является простым числом.

$|G| = \infty$,
множество всех подгрупп бесконечное ,
множество всех собственных подгрупп бесконечное .
$|G| = n$, n — простое , $H \subset G$, $|H| = k$,
$k|n$, $k = 1$, $H = \{e\}$, $k = n$, $H = G$.
n составное , $a \in G$, $a \neq e$, $H =< a >$, $H \neq \{e\}$.
$H \neq G \Rightarrow H$ собственная подгруппа.
$H = G$, G — циклическая группа , $k|n$, $1 < k < n$,
$H_0 \subset G$, $|H_0| = k$, $H_0 \neq \{e\}$, $H_0 \neq G$. □

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$, $Hx^{-1} \subset x^{-1}H$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная, $x \in G$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная, $x \in G$, $Hx = xH$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная, $x \in G$, $Hx = xH$, $x^{-1}(Hx) = x^{-1}(xH)$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная, $x \in G$, $Hx = xH$, $x^{-1}(Hx) = x^{-1}(xH)$,
$x^{-1}Hx = H$

Определение

Подгруппа H группы G называется нормальной, если для любого $x \in G$ имеет место равенство $xH = Hx$, то есть любой левый смежный класс является одновременно и правым смежным классом.

Вместо термина «нормальная подгруппа» используются также термины «инвариантная подгруппа» и «нормальный делитель».

Теорема

Подгруппа H группы G является нормальной в том и только том случае, когда $x^{-1}Hx \subset H$ для любого $x \in G$.

1) $\forall x \in G\ x^{-1}Hx \subset H$, $x(x^{-1}Hx) \subset xH$, $Hx \subset xH$,
$Hx^{-1} \subset x^{-1}H$, $x(Hx^{-1})x \subset x(x^{-1}H)x$,
$xH \subset Hx$, $xH = Hx$.
2) H нормальная, $x \in G$, $Hx = xH$, $x^{-1}(Hx) = x^{-1}(xH)$,
$x^{-1}Hx = H$, $x^{-1}Hx \subset H$. □