ДИСКРЕТНАЯ МАТЕМАТИКА

ГУИМЦ, ИУ5,8 - 3 семестр

Лекция 7. АЛГЕБРЫ: ГРУППЫ

Формы записи бинарной операции группы.

Аддитивная запись.

Бинарную операцию группы называют **сложением**, $+$,
нейтральный элемент — **0**,
обратный элемент к a — **противоположный** к a, $-a$.

Мультипликативная запись.

Бинарную операцию группы называют **умножением**.
Обозначают знаком $\cdot$,
нейтральный элемент — **1**, элемент,
обратный к a — a^{-1}.
Элемент $a \cdot b$ —**произведение** элементов a и b (ab).

Пример 7.1.

а. Алгебра $(\mathbb{Z}, +)$ — коммутативная группа.

На множестве $\mathbb{Z}$ операция сложения ассоциативна и коммутативна.

Число 0 есть нейтральный элемент.

Для каждого целого числа n существует обратный по сложению элемент, число $-n$, противоположное n.

Аддитивная группа целых чисел.

б. Симметрическая группа множества A.

Множество всех *биекций* некоторого множества A на себя с операцией композиции отображений есть группа.

Композиция двух биекций есть биекция.

Операция композиции ассоциативна.

Нейтральный элемент — тождественное отображение id_A — есть биекция.

Для всякой биекции $f\colon A \to A$ отображение f^{-1}, обратное биекции f, определено, является биекцией и выполнены равенства $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_A$.

Симметрическая группа степени n

Если множество A конечно, — **группа подстановок** множества A.

Если $|A| = n$, — **симметрическая группа степени** n, обозначение — S_n (*группа подстановок* n *-й степени*).

в. Алгебры $(\mathbb{Q} \setminus \{0\}, \cdot)$ и $(\mathbb{R} \setminus \{0\}, \cdot)$ есть коммутативные группы. **Мультипликативная группа рациональных чисел** и **мультипликативная группа действительных чисел**.

Нейтральный элемент (единица) группы. Число 1.
Обратный элемент. $x^{-1} = 1/x$.

г. Для произвольно фиксированного множества A рассмотрим алгебру $(2^A, \triangle)$, где $\triangle$ — операция вычисления *симметрической разности множеств*.

Операция $\triangle$ ассоциативна и коммутативна.
Нейтральный элемент. $(\forall X), X \subseteq A$, $X \triangle \varnothing = X$.
Обратный элемент. $X \triangle Y = \varnothing \Leftrightarrow X = Y$, (каждый элемент обратен сам себе).
Алгебра $(2^A, \triangle)$ — абелева группа.

д. Аддитивная группа вычетов по модулю k
Алгебра $\mathbb{Z}_k^+ = (\{0, 1, \ldots, k-1\}, \oplus_k)$. Операция $\oplus_k$ (**сложения по модулю k**):
для любых двух m и n число $m \oplus_k n$, называемое **суммой** чисел m и n **по модулю** k, равно остатку от деления арифметической суммы $m + n$ на k.
$\mathbb{Z}_k^+$ коммутативная группа.
Нейтральный элемент — число 0.
Обратный элемент к числу n — $k - n$ ($n \oplus_k (k - n) = 0$).

е. Множество всех невырожденных числовых квадратных матриц порядка n с операцией умножения матриц является группой M_n.
Произведение двух невырожденных матриц снова есть невырожденная матрица.
Нейтральный элемент — единичная матрица порядка n, невырожденная.
Обратный элемент —обратная матрица, (матрица,обратная к невырожденной, является невырожденной).

Теорема 1. Пусть $\mathcal{G} = (G, \cdot)$ — группа. Для любых элементов $a, b \in G$ верны тожества

$$1.(a \cdot b)^{-1} = b^{-1} \cdot a^{-1};$$
$$2.(a^{-1})^{-1} = a.$$

◄ 1. В силу ассоциативности умножения группы:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = ((a \cdot b) \cdot b^{-1}) \cdot a^{-1}.$$
$$((a \cdot b) \cdot b^{-1}) \cdot a^{-1} = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = \mathbf{1}.$$

$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = \mathbf{1}$.
$(b^{-1} \cdot a^{-1})(a \cdot b) = \mathbf{1}$ доказывается аналогично.
Элемент $b^{-1} \cdot a^{-1}$ является обратным к элементу $a \cdot b$.
2. $(a^{-1})^{-1} = a$.
$(a^{-1})^{-1}$ — обратный элемент к a^{-1}.
По определению элемента, обратного к данному $a^{-1} \cdot a = a \cdot a^{-1} = \mathbf{1}$, элемент a — обратный элемент к a^{-1}.
В любой группе $\mathcal{G} = (G, \cdot)$ для каждого $a \in G$ элемент, обратный к a, единственный т.е. $a = (a^{-1})^{-1}$. ►

Теорема 2. В любой группе $\mathcal{G} = (G, \cdot, \mathbf{1})$ справедливы **левый** и **правый законы сокращения**:
если $a \cdot x = a \cdot y$, то $x = y$, и если $x \cdot a = y \cdot a$, то $x = y$.

◄ Пусть $a \cdot x = a \cdot y$.
Умножим обе части этого равенства слева на элемент a^{-1}.

$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y)$
в силу ассоциативности операции вгруппе $(a^{-1} \cdot a) \cdot x = (a^{-1} \cdot a) \cdot y$.
т.к. $a^{-1} \cdot a = \mathbf{1} \Rightarrow \mathbf{1} \cdot x = \mathbf{1} \cdot y \Rightarrow x = y$

Доказан левый закон сокращения. Аналогично доказывается и правый закон. ►

Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — группа, a, b — фиксированные элементы G.
Рассмотрим задачу решения уравнений

$$a \cdot x = b, \tag{7.1}$$

$$x \cdot a = b \tag{7.2}$$

в группе $\mathcal{G}$.
Т.е. поиск всех таких элементов $x \in G$, для которых уравнение (7.1) (или (7.2)) превращается в тождество.

Теорема 3. В любой группе $\mathcal{G}$ уравнения вида $a \cdot x = b$ (7.1)
и $x \cdot a = b$ (7.2)
имеют решения, и притом единственные.

◄ $x = a^{-1} \cdot b$ — решение (7.1).
$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1} \cdot b) = b$.
Единственность решения.
Пусть для фиксированных a и b и некоторого x выполнено равенство

$$a \cdot x = b. \tag{7.3}$$

$\mathcal{G}$ группа $\Rightarrow (\forall a)\exists a^{-1} | a^{-1}a = \mathbf{1}$
Умножим на a^{-1} обе части равенства (7.3) .

$$\begin{aligned} & a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b \ \Rightarrow \\ \Rightarrow \ & (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b \ \Rightarrow \\ \Rightarrow \ & \mathbf{1} \cdot x = a^{-1} \cdot b \ \Rightarrow \ x = a^{-1} \cdot b. \end{aligned}$$

Решение единственное в силу единственности обратного элемента.
Аналогично из $x \cdot a = b$ получаем $x = b \cdot a^{-1}$, и это решение также единственное. ►

Разность

При использовании аддитивной записи операции для коммутативной группы $\mathcal{G} = (G, +, \mathbf{0})$ уравнения (7.1) и (7.2) сводятся к:

$$a + x = b. \tag{7.4}$$

$x = b + (-a)$ — решение уравнения (7.4).

$b + (-a)$ в коммутативной группе называют **разностью** элементов b и a и обзначают $b - a$.

Операцию, сопоставляющую упорядоченной паре (a, b) разность $b - a$, называют операцией **вычитания**.

В коммутативной группе можно записать так: $x = b - a$.

В случае коммутативной группы при мультипликативной записи решения уравнений (7.1) и (7.2) имеют вид $x = b \cdot a^{-1}$.

В полугруппе в общем случае законы сокращения и разрешимость уравнений типа (7.1) и (7.2) могут не иметь места.

В полугруппе квадратных матриц фиксированного порядка с операцией умножения матриц из матричного равенства $AX = AY$ не следует, что $X = Y$ (только, если $\det A \neq 0$).

7.1. Циклическая полугруппа

В свободном моноиде, порожденном некоторым конечным множеством, оба закона сокращения справедливы, но обратных элементов не существует.
В полугруппе можно умножать любой элемент a сам на себя, элемент $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}}$ определен однозначно в силу ассоциативности операции полугруппы .

Определение 7.1.
В полугруппе $(A, \cdot)$ n **-я степень элемента** a есть элемент $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a \cdot a^{n-1}$, $n = 2, 3, \ldots$
Если $(A, \cdot, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.
Если $(A, \cdot, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \ldots$ (Отрицательная степень элемента a группы есть положительная степень элемента, обратного к a .)

Сформулируем утверждения о свойствах степеней (без доказательства).

Утверждение 7.1. Для любой полугруппы $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (m, $n \in \mathbb{N}$).

Утверждение 7.2. Для любой группы $a^{-n} = (a^n)^{-1}$ $(n \in \mathbb{N})$, $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (m, $n \in \mathbb{Z}$).

Определение 7.2. Полугруппу (в частности, группу) $(A, \cdot)$ называют **циклической**, если существует такой элемент a, что любой элемент x полугруппы является некоторой (целой) степенью элемента a.
Элемент a называют **образующим элементом полугруппы (группы)**.

Пример 7.2.

а. Полугруппа $(\mathbb{N}, +)$ циклическая, с образующим элементом 1. При аддитивной записи бинарной операции возведение элемента a в положительную степень n есть сумма n этих элементов, $n \cdot a$ (или na, без знака умножения).

б. Группа $(\mathbb{Z}, +, 0)$ также циклическая. Образующие элементы: 1 или -1.

Элемент 1. $0 \cdot 1 = 0$, $n \cdot 1 = \underbrace{1 + \ldots + 1}_{n \text{ раз}} = n$ ($n > 0$) и $(-1) \cdot 1 = -1$,

$(-n) \cdot 1 = n \cdot (-1) = \underbrace{(-1) + \ldots + (-1)}_{n \text{ раз}} = -n$ ($n > 0$).

Элемент -1. $0 \cdot (-1) = 0$, отрицательные целые числа получаются как положительные „степени“ -1, а положительные — как отрицательные „степени“ -1. Например, $(-2) \cdot (-1) = 2$, $4 \cdot (-1) = -4$.

в. Группа $(\mathbb{Z}_3, \oplus_3, 0)$ вычетов по модулю 3 циклическая, любой ее ненулевой элемент является образующим.

$\mathbb{Z}_3 = \{0, 1, 2\}$. 1: $1 \oplus_3 1 = 2$, $1 \oplus_3 1 \oplus_3 1 = 0$.

2: $2^2 = 2 \oplus_3 2 = 1$, $2 \oplus_3 2 \oplus_3 2 = 0$. #

Конечные циклические группы.

Конечная алгебра (конечная группа) — это алгебра, носитель которой — конечное множество.

Порядком конечной группы называют количество элементов в этой группе.

Например, аддитивная группа вычетов по модулю k имеет порядок k.

Симметрическая группа степени n, т.е. группа подстановок S_n, имеет порядок $n!$.

Мультипликативная группа вычетов по модулю p, где p — простое число, имеет порядок $p-1$.

Порядок элемента a циклической группы — это наименьшее положительное n, такое, что $a^n = \mathbf{1}$.

Теорема 4. Порядок образующего элемента конечной циклической группы равен порядку самой группы.

◄ Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — конечная циклическая группа,
a — образующий элемент группы $\mathcal{G}$,
$n > 0$ — порядок образующего элемента.

1. Все степени $a^0 = \mathbf{1}$, $a^1 = a, \ldots, a^{n-1}$ попарно различны.

Если $a^k = a^l$, $0 < l < k < n$, то

$$a^{k-l} = a^{k+(-l)} = a^k a^{-l} = a^l a^{-l} = a^{l-l} = \mathbf{1}.$$

Найдена степень $k-l<n$, $a^{k-l} = \mathbf{1}$ Противоречие с выбором n как порядка элемента a.

2. Любая степень элемента a принадлежит множеству $\{\mathbf{1}, a, \ldots, a^{n-1}\}$.

$$\forall\,(m \in \mathbb{Z})\ \exists\,(n, k \in \mathbb{Z})\big|\ (m = kn + q), \text{где } (q \in \mathbb{Z}\ \wedge 0 \le q < n)$$

Тогда

$$a^m = a^{kn+q} = a^{kn} \cdot a^q = (a^n)^k \cdot a^q = \mathbf{1} \cdot a^q = a^q \in \{\mathbf{1}, a, \ldots, a^{n-1}\}.$$

Поскольку каждый элемент группы $\mathcal{G}$ есть некоторая степень элемента a, то $G = \{\mathbf{1}, a, \ldots, a^{n-1}\}$ и порядок группы равен n. ►

В бесконечной циклической группе не существует такого $n > 0$, что для образующего элемента a группы выполняется равенство $a^n = \mathbf{1}$

7.2. Группа подстановок

Подстановкой n-элементного множества $\{1, 2, \ldots, n\}$ называют взаимнооднозначное отображение этого множества в себя (биекцию).

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Образ 1 (при отображении σ) есть α_1, образ 2 есть α_2, ..., образ n есть α_n.

Циклом длины k называют подстановку, которая отображает β_1 в β_2, β_2 в $\beta_3, \ldots, \beta_{k-1}$ в β_k, а β_k в β_1, где $\beta_i \in \{1, \ldots, n\}$, $i = 1, \ldots, k$ и все β_i попарно различны, а все элементы, отличные от $\beta_1, \ldots, \beta_k$, отображаются сами в себя.
Цикл записывают ее в виде $(\beta_1\ \beta_2\ \ldots\ \beta_k)$.

Группа S_4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3\ 4)$$

Цикл длины 2 называют *транспозицией*.
Транспозиция представляет такое отображение множества $\{1, \ldots, n\}$ в себя, при котором два элемента меняются местами, а остальные остаются на своих местах.

Полная запись транспозиции $(3\ 4)$ в S_4 :

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

Тождественная подстановка

$$\xi = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix},$$

Обратная подстановка
Подстановка, обратная подстановке

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

есть подстановка, которая отображает α_1 в 1, α_2 в 2, $\ldots$ α_n в n, элементы первой строки записываются в обычном порядке: $1, \ldots, n$.
$\forall A \in S_n,\ A \circ A^{-1} = \xi$

Решение уравнений в группе подстановок

Решить уравнение в группе S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ X \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Обозначим

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ C = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Умножим обе части уравнения слева на A^{-1} и уравнение справа на B^{-1}

$$A^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$B^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$A^{-1} \circ A \circ X \circ B \circ B^{-1} = A^{-1} \circ C \circ B^{-1}$$

получим

$$X = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2).$$

7.3. Подгруппы.Циклические подгруппы.

Пусть $\mathcal{G} = (G, *)$ — произвольный группоид и $H \subseteq G$ — некоторое подмножество множества G.

Определение 7.3. Множество $H \subseteq G$ замкнуто относительно операции $*$, если $x * y \in H$ для любых x, $y \in H$.

Подмножество H с операцией $*$ будет группоидом $\mathcal{H} = (H, *)$, если $H \subseteq G$ **замкнуто относительно операции** $*$. Его называют **подгруппоидом** группоида $\mathcal{G}$.

Если подмножество H замкнуто относительно бинарной операции $*$ и бинарная операция $*$ ассоциативна на множестве G, то операция останется ассоциативной и при ее ограничении на подмножество H.

Если группоид $\mathcal{G}$ является полугруппой, то и всякий его подгруппоид будет полугруппой, называемой подполугруппой полугруппы $\mathcal{G}$.

Если группоид является *моноидом* (*группой*), утверждать, что любой подгруппоид является также моноидом (группой) нельзя.

Пример 7.3. Группоид — **аддитивная группа целых чисел** $(\mathbb{Z}, +)$.

$\mathbb{N} \subseteq \mathbb{Z}$ Подмножество натуральных чисел замкнуто относительно операции сложения $+$, группоид $(\mathbb{N}, +)$ будет подгруппоидом группоида $(\mathbb{Z}, +)$.
Операция сложения чисел ассоциативна, $(\mathbb{N}, +)$ — подполугруппа.
0 нейтральный элемент относительно операции сложения в множестве $\mathbb{N}$ отсутствует.
Следовательно, $(\mathbb{N}, +)$ не является группой (не является и моноидом).

Определение 7.4. Моноид $\mathcal{P} = (P, \cdot, \mathbf{1})$ есть подмоноид моноида $\mathcal{M} = (M, \cdot, \mathbf{1})$ тогда и только тогда, когда множество P замкнуто относительно бинарной операции $\cdot$ моноида $\mathcal{M}$, а также относительно его нульарной операции $\mathbf{1}$.

Определение 7.5. Пусть $\mathcal{G} = (G, \cdot, {}^{-1}, \mathbf{1})$ — группа, $H \subseteq G$, H замкнуто относительно операции $\cdot$ группы $\mathcal{G}$, содержит нейтральный элемент $\mathbf{1}$ этой группы ($\mathbf{1} \in H$) и вместе с каждым элементом $x \in H$ содержит **элемент** x^{-1}, **обратный** к x, т.е. замкнутое относительно унарной операции ${}^{-1}$ взятия обратного.
Тогда $\mathcal{H} = (H, \cdot, {}^{-1}, \mathbf{1})$ также есть группа, которую называют **подгруппой** группы $\mathcal{G}$.

Пусть ω — унарная операция на множестве G моноида $\mathcal{G}$, $\mathcal{H}$ — некоторый его подмоноид.

Подмоноид $\mathcal{H}$ моноида $\mathcal{G}$ называется замкнутым относительно унарной операции ω, если для каждого $x \in H$ имеет место $\omega(x) \in H$.

Группа $\mathcal{H} = (H, \cdot, {}^{-1}, \mathbf{1})$ есть подгруппа группы $\mathcal{G} = (G, \cdot, {}^{-1}, \mathbf{1})$ в том и только в том случае, когда множество H замкнуто относительно всех операций $\cdot$, ${}^{-1}$, $\mathbf{1}$ сигнатуры группы $\mathcal{G}$.

Единица моноида (группы) служит одновременно единицей любого его подмоноида (любой подгруппы).

Пример 7.4.

а. Подмножество всех натуральных четных чисел есть подполугруппа полугруппы $(\mathbb{N}, +)$ (подмножество всех натуральных четных чисел замкнуто относительно сложения, операция сложения ассоциативна).

б. Аддитивная полугруппа натуральных чисел с нулем $(\mathbb{N} \cup \{0\}, +)$ — моноид с нейтральным элементом 0.

Подмножество всех положительных (> 0) четных чисел с операцией сложения не будет подмоноидом моноида $(\mathbb{N} \cup \{0\}, +, 0)$, ее носитель не содержит нуля — единицы моноида.

Подмножество всех натуральных чисел вместе с нулем, делящихся на заданное число $k > 1$, замкнуто относительно операции сложения; на нем может быть определен подмоноид моноида $(\mathbb{N} \cup \{0\}, +, 0)$.

в. Группа рациональных чисел $\mathbb{Q}$ с операцией умножения, является подгруппой группы действительных чисел с операцией умножения $(\mathbb{R} \setminus \{0\}, \cdot, 1)$.

г. Алгебра $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ не является подгруппой группы $(\mathbb{R} \setminus \{0\}, \cdot, 1)$, т.к. не содержит вместе с каждым целым числом m обратного к нему числа $\frac{1}{m}$.

Данное множество будет моноидом т.к. оно замкнуто относительно операции умножения и содержит единицу.

7.4. Циклические подгруппы

Пусть $\mathcal{G} = (G, \cdot, {}^{-1}, \mathbf{1})$ — группа.

Произведение любых **степеней элемента** a есть снова некоторая степень элемента a, нулевая степень дает единицу группы, а обратным к элементу a^k является элемент a^{-k}.

Таким образом, множество всех степеней фиксированного элемента a группы $\mathcal{G}$ является подгруппой группы $\mathcal{G}$.

Определение 7.6. Подгруппу группы $\mathcal{G}$, заданную на множестве всех степеней фиксированного элемента a, называют **циклической подгруппой** группы $\mathcal{G}$, **порожденной элементом** a.

Пример 7.5. В группе $\mathbb{Z}_{13}^*$ (мультипликативной группе вычетов по модулю 13) построить циклическую подгруппу, порожденную элементом 5.

$5^0 = 1$, $5^1 = 5$, $5^2 = 5 \odot_{13} 5 = 12$, $5^3 = 5 \odot_{13} 12 = 8$, $5^4 = 5 \odot_{13} 8 = 1$.

Порядок этой циклической подгруппы равен 4.

Она состоит из элементов: 1, 5, 8 и 12.

7.5. Теорема Лагранжа

Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — группа, а $\mathcal{H} = (H, \cdot, \mathbf{1})$ — ее подгруппа.

Левым смежным классом подгруппы $\mathcal{H}$ по элементу $a \in G$ называют множество

$$aH = \{y\colon y = a \cdot h,\ h \in H\}\,.$$

Соответственно **правый смежный класс подгруппы $\mathcal{H}$ по элементу** $a \in G$ — это множество

$$Ha = \{y\colon y = h \cdot a,\ h \in H\}\,.$$

Очевидно, что в коммутативной группе $aH = Ha$.

Утверждение 7.3.

$$a \in H \Rightarrow aH = H$$

◀ Рассмотрим левые смежные классы.
Метод двух включений:
1. $aH \subseteq H$.

$(x \in aH) \wedge (a \in H) \Rightarrow \ \exists h \in H \ \ x = ah \wedge (a \in H)$
(множество H замкнуто относительно умножения группы) $\mathcal{G} \ \Rightarrow \ x \in H.$

2. $H \subseteq aH$.

$$x \in H \Rightarrow \ x = \mathbf{1} \cdot x = (aa^{-1})x = a(a^{-1}x) = ah$$

где $h = a^{-1}x \in H \Rightarrow \ x \in aH.$
Окончательно получим $aH = H$.▶

можно Построение отношения эквивалентности с использованием смежных классов.

Бинарное отношение $\sim_H$ на множестве G:
элементы a и b связаны отношением $\sim_H$ ($a \sim_H b$), если и только если левые смежные классы подгруппы $\mathcal{H}$ по элементам a и b совпадают ($aH = bH$).

Теорема 5. Бинарное отношение $\sim_H$ есть эквивалентность на G, причем класс эквивалентности произвольного элемента $a \in G$ совпадает с левым смежным классом aH.

◄ Докажем, что $\sim_H$ является эквивалентностью на G.

$\forall a \in G\ (aH = aH) \Rightarrow a \sim_H a \Rightarrow$ бинарное отношение $\sim_H$ **рефлексивно**;

$a \sim_H b \Rightarrow (aH = bH) \Rightarrow (bH = aH) \Rightarrow (b \sim_H a) \Rightarrow$

$\Rightarrow$ отношение $\sim_H$ **симметрично**;

$a \sim_H b \wedge b \sim_H c \Rightarrow (aH = bH) \wedge (bH = cH) \Rightarrow a \sim_H c \Rightarrow$

$\Rightarrow$ отношение $\sim_H$ **транзитивно**

$\sim_H$ есть эквивалентность

Класс эквивалентности произвольного элемента a равен aH $[a]_{\sim_H} = aH$.
Метод двух включений.
1. $[a]_{\sim_H} \subseteq aH$.

$x \in [a]_{\sim_H} \Rightarrow x \sim_H a \Rightarrow$
$\Rightarrow xH = aH \ (xH = \{xh_1 | h_1 \in H\}, aH = \{ah | h \in H\}) \Rightarrow$
$\Rightarrow (\forall ah) ah \in aH, h \in H \ (\exists xh_1) xh_1 \in xH | ah = xh_1 \Rightarrow$
$\Rightarrow x = ahh_1^{-1} = ah_2,$ где $h_2 = hh_1^{-1}, h_2 \in H$
(силу замкнутости подгруппы $\mathcal{H}$ относительно групповой операции)

Следовательно, $[a]_{\sim_H} \subseteq aH$.

2. $aH \subseteq [a]_{\sim_H}$.
Пусть

$$x \in aH, \text{ тогда } \exists h \in H \mid x = ah \Rightarrow xH = ahH.$$

$$ahH = \{(ah)h_3 | h_3 \in H\} = \{a(hh_3) | h_3 \in H\} = \{ah_4 | h_4 \in H\} = aH$$

$$\Rightarrow xH = aH \Rightarrow (x \sim_H a) \Rightarrow x \in [a]_{\sim_H} \Rightarrow aH \subseteq [a]_{\sim_H}$$

►