

# Симметрическая и знакопеременная группы

**Алгебраические операции.** Пусть  $X$  – некоторое произвольное множество. В частности, качестве  $X$  можно рассматривать любое подмножество одного из следующих множеств:

- множества  $\mathbb{N} = \{1, 2, \dots\}$  всех натуральных чисел;
- множества  $\mathbb{Z}$  всех целых чисел, множества  $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$  всех целых неотрицательных чисел и множества  $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ ;
- множества  $\mathbb{Q}$  всех рациональных чисел и множества  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ ;
- множества  $\mathbb{R}$  всех вещественных чисел и множества  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ;
- множества  $\mathbb{C}$  всех комплексных чисел и множества  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ;
- множества  $\mathfrak{S}(\Omega)$  всех подмножеств некоторого множества  $\Omega$ ;
- множества  $\mathfrak{T}(\Omega)$  всех отображений некоторого множества  $\Omega$  в себя или множества  $\mathfrak{T}^*(\Omega)$  всех биективных отображений  $\Omega$  в себя;
- множества  $M_n(E)$  всех  $n \times n$ -матриц с элементами из некоторого числового множества  $E$  при  $n \in \mathbb{N}$  и т.д.

Напомним, что  $X \times X = \{(x, y) : x, y \in X\}$ . Напомним также, что величина  $|X|$  определяется следующим образом:  $|X| = N$ ,  $N \in \mathbb{N}$ , если множество  $X$  состоит из  $N$  элементов и  $|X| = \infty$ , если  $X$  состоит из бесконечного числа элементов (в этом обозначении мы не будем различать бесконечные счетные множества и бесконечные множества, имеющие мощность континуума).

**Определение.** *Бинарной операцией на множестве  $X$  называется любое отображение  $\tau : X \times X \rightarrow X$ , определенное на всем множестве  $X \times X$ .*

Другими словами, если на множестве  $X$  задана *бинарная операция*  $\tau$ , то любой (упорядоченной) паре  $(a, b)$  элементов  $a \in X, b \in X$  поставлен в соответствие некоторый элемент  $c = \tau(a, b)$  множества  $X$ . Аналогичным образом можно определить *унарную* операцию на  $X$  как отображение  $X$  в себя, *тернарную* операцию на  $X$  как отображение множества  $X \times X \times X$  в  $X$  и так далее.

Для записи бинарных операций используют два стандартных способа: *функциональный* (при этом результат применения операции  $\tau$  к элементам  $a$  и  $b$  записывается в виде  $\tau(a, b)$ ) и *операторный* (в этом случае результат применения операции  $\tau$  к элементам  $a$  и  $b$  записывается в виде  $a \tau b$ ).

Функциональную форму записи бинарных операций часто называют *префиксной*, а операторную – *инфиксной*.

Традиционно, для записи бинарных операций используют операторную форму, а в качестве символов, обозначающих операции, используют стандартные *знаки операций*, например  $+$ ,  $-$ ,  $*$ ,  $\cdot$ ,  $\times$ ,  $\circ$ ,  $/$ ,  $\div$ ,  $\cup$ ,  $\cap$  и т.д. Всюду в дальнейшем для упрощения обозначений выражение  $a \cdot b$  будет записываться в виде  $ab$ .



**Алгебраические структуры.** На каждом множестве  $X$  можно задать много различных алгебраических операций. Множество  $X$  с заданной на нем алгебраической операцией  $*$  обозначается символом  $(X, *)$ . Во многих случаях на множестве  $X$  целесообразно рассматривать не одну, а две, три или более различных алгебраических операций  $*_1, \dots, *_N$ ,  $N > 1$ . В этом случае используется обозначение  $(X, \{*_1, \dots, *_N\})$  или  $(X, *_1, \dots, *_N)$ .

**Определение.** *Объект  $(X, \{*_1, \dots, *_N\})$ , где  $X$  – некоторое множество, а  $*_j$ ,  $j = 1, \dots, N$  – некоторые заданные на  $X$  алгебраические операции, называется алгебраической структурой.*

**Пример 1.1.** Простейшими примерами алгебраических структур являются

$$(\mathbb{Z}, +), \quad (\mathbb{Z}, \cdot), \quad (\mathbb{Q}, +), \quad (\mathbb{Q}, \cdot), \quad (\mathbb{R}, +), \quad (\mathbb{R}, \cdot), \quad (\mathbb{R}, \{+, \cdot\}),$$

где символы  $+$  и  $\cdot$  обозначают операции сложения и умножения, определенные на соответствующих (числовых) множествах традиционным образом.

Алгебраическими структурами будут также

$$(M_n(\mathbb{R}), +), \quad \text{и} \quad (M_n(\mathbb{R}), \times),$$

где  $+$  и  $\times$  – это операции матричного сложения и умножения.

Приведем также несколько примеров алгебраических структур, заданных на стандартных множествах (таких, как  $\mathbb{Z}$  или  $\mathbb{R}$ ), но при помощи совершенно нестандартных операций:

$$(\mathbb{Z}, \diamond), \quad (\mathbb{Z}, \circ), \quad (\mathbb{R}, \circ), \quad \dots,$$

где  $x \diamond y = -x - y$ , а  $x \circ y = x + y + xy$ .

Нам понадобится понятие замкнутости множества относительно алгебраической операции. Пусть  $(X, *)$  – некоторая алгебраическая структура, а  $Y$  – некоторое подмножество  $X$ .

**Определение.** Говорят, что множество  $Y$  замкнуто относительно операции  $*$ , если  $y_1 * y_2 \in Y$  для любых  $y_1, y_2 \in Y$ .

**Определение.** Пусть на множестве  $X$  задана бинарная операция  $*$ . Она называется ассоциативной, если для любых  $a, b, c \in X$  выполняется равенство

$$(a * b) * c = a * (b * c).$$

Если для любых  $a, b \in X$  выполняется равенство

$$a * b = b * a,$$

то операция  $*$  называется коммутативной.

**Замечание.** Ассоциативность и коммутативность – это независимые свойства, поскольку существуют операции, обладающие одним из этих свойств, но не другим. В самом деле, операция умножения на множестве  $M_n(\mathbb{R})$  является, как известно из курса линейной алгебры, ассоциативной, но не коммутативной. А операция  $\diamond$  на множестве  $\mathbb{Z}$ , определенная соотношением  $x \diamond y = -x - y$ , является коммутативной так как для любых  $x, y \in \mathbb{Z}$  имеет место равенство

$$x \diamond y = -x - y = -(x + y) = -(y + x) = -y - x = y \diamond x,$$

но не является ассоциативной, так как

$$(1 \diamond 2) \diamond 3 = (-1 - 2) \diamond 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 \diamond (2 \diamond 3).$$



**Определение.** Алгебраическая структура  $(X, *)$ , где  $X$  – некоторое множество, а  $*$  – ассоциативная операция на  $X$ , называется полугруппой.

Если  $(X, *)$  – полугруппа и если операция  $*$  коммутативна, то полугруппа  $X$  называется коммутативной полугруппой.

Говорят также, что множество  $X$  образует полугруппу (является полугруппой) относительно операции  $*$ . Часто используют более короткую терминологию и говорят, что  $X$  – полугруппа. При этом имеется в виду, что соответствующая операция  $*$  однозначно восстанавливается из контекста.

Если в полугруппе  $(X, *)$  операция  $*$  – это операция *умножения*, то такая полугруппа называется *мультипликативной*. А если  $*$  – это операция *сложения*, то полугруппа  $X$  называется *аддитивной*. Безусловно, использование терминов “мультипликативная полугруппа” и “аддитивная полугруппа” носит довольно условный характер. Дело в том, что термин “умножение” часто используется для обозначения общей ассоциативной бинарной операции, а термин “сложение” – для обозначения общей ассоциативной и коммутативной бинарной операции.

Хорошим примером, демонстрирующим естественность такой терминологии являются операции сложения и умножения матриц из  $M_n(\mathbb{R})$ , так как матричное сложение – это ассоциативная и коммутативная операция, а матричное умножение – это ассоциативная, но не коммутативная операция.

Простейшими примерами полугрупп являются, например, такие алгебраические структуры, как  $(\mathbb{N}, +)$ ,  $(\mathbb{N}, \cdot)$ ,  $(\mathbb{R}, +)$  или  $(\mathbb{R}, \cdot)$ , где  $+$  и  $\cdot$  – это стандартные операции сложения и умножения чисел. Среди простых примеров полугрупп с нестандартными операциями можно привести, например,  $(\mathbb{Z}, *)$ , где  $x * y = \text{НОД}(x, y)$ . В то же самое время алгебраические структуры  $(\mathbb{Z}, \diamond)$  и  $(\mathbb{Z}, *)$  при  $x * y = x^y$  не будут полугруппами, так как соответствующие операции не ассоциативны.



**Определение.** Элемент  $e_L \in X$  называется *левым единичным* (или *левым нейтральным*) элементом алгебраической структуры  $(X, *)$ , если для любого элемента  $x \in X$  имеет место равенство  $e_L * x = x$ . Аналогично, элемент  $e_R \in X$  называется *правым единичным* (или *правым нейтральным*), если  $x * e_R = x$  для любого  $x \in X$ .

В полугруппе  $(\mathbb{R}, +)$  число 0 будет и левым и правым единичным элементом. Аналогично, в полугруппе  $(\mathbb{R}, \cdot)$  левым и, одновременно, правым единичным элементом будет число 1. Оказывается, имеет место следующее свойство левых и правых единичных элементов.

**Предложение.** Пусть в алгебраической структуре  $(X, *)$  существуют левый единичный элемент  $e_L$  и правый единичный элемент  $e_R$ . Тогда  $e_L = e_R$ .

**Проверка.** В самом деле, из определения левого и правого единичных элементов вытекает, что  $e_R = e_L * e_R = e_L$ . □

Приведем пример алгебраической структуры, в которой не существует правого единичного элемента, но существует бесконечно много левых единичных элементов.

**Определение.** Элемент  $e \in X$  называется *единичным* (или *нейтральным*) элементом алгебраической структуры  $(X, *)$ , если для любого элемента  $x \in X$  имеет место равенство  $e * x = x * e = x$ .

**Предложение.** Если в алгебраической структуре  $(X, *)$  существует единичный элемент, то он является единственным.

**Проверка.** В самом деле, пусть в алгебраической структуре  $(X, *)$  существуют два единичных элемента, скажем  $e_1$  и  $e_2$ . Тогда, по определению единичного элемента  $e_1 = e_1 * e_2 = e_2$ .  $\square$

**Определение.** Если  $X$  – полугруппа относительно операции  $*$  и если в алгебраической структуре  $(X, *)$  существует единичный элемент  $e$ , то  $X$  называется *полугруппой с единицей*, или *моноидом*.

Пусть  $X$  – полугруппа относительно операции  $*$  и пусть  $Y$  – замкнутое относительно операции  $*$  подмножество множества  $X$ . Тогда  $Y$  будет полугруппой относительно операции  $*$ .

**Определение.**  $Y$  называется *подполугруппой* полугруппы  $X$ .

Пусть теперь  $X$  является полугруппой с единицей (моноидом) относительно операции  $*$ , а  $Y$  – замкнутым относительно операции  $*$  подмножеством  $X$  таким, что  $e \in Y$  (где  $e$  – единица полугруппы  $X$ ). В этом случае оправдано следующее определение:

**Определение.**  $Y$  называется *подмоноидом* моноида  $X$ .

Так, при натуральном  $n > 1$ , структура  $(n\mathbb{Z}, \cdot)$  – это подполугруппа полугруппы  $(\mathbb{Z}, \cdot)$ , а структура  $(n\mathbb{Z}, +)$  – это подмоноид моноида  $(\mathbb{Z}, +)$ .

**Замечание.** Если есть желание или необходимость подчеркнуть, что алгебраическая структура  $(X, *)$  является полугруппой с единицей  $e$ , то пишут, что  $(X, *, e)$  – полугруппа с единицей.



**Предложение 1.6.** Пусть  $*$  – ассоциативная бинарная операция на множестве  $X$ . Для любого натурального  $n > 1$  и для любых элементов  $x_1, \dots, x_n \in X$  значение выражения  $x_1 * x_2 * \dots * x_n$  не зависит от порядка выполнения операций при его вычислении.

**Доказательство.** Используем индукцию по  $n$ . При  $n = 2$  доказываемое утверждение очевидно, а при  $n = 3$  оно непосредственно вытекает из определения ассоциативности операции. Для краткости будем называть операцию  $*$  умножением, а элементы  $a$  и  $b$  в выражении  $a * b$  – сомножителями. Предположим теперь, что  $n > 3$  и, что для числа сомножителей, меньшего  $n$ , доказываемое условие справедливо. Нам необходимо показать, что из этого следует справедливость доказываемого утверждения для произведения  $n$  сомножителей.

Так как по предположению индукции результат вычисления произведения  $m < n$  сомножителей не зависит от способа расстановки скобок, для любого натурального  $m < n$  и для любых  $x_1, \dots, x_m \in X$  имеет место равенство

$$x_1 * \dots * x_m = ((\dots (x_1 * x_2) * \dots) * x_{m-1}) * x_m,$$

причем способ записи (вычисления) произведения, использованный в правой части этого равенства естественно назвать *каноническим*.

Для доказательства справедливости рассматриваемого утверждения для произведения  $n$  сомножителей надо показать, что такое произведение равно соответствующему каноническому произведению независимо от способа его вычисления.

Пусть произведение  $x_1 * x_2 * \cdots * x_n$  вычисляется следующим образом (здесь  $k$  – натуральное число,  $1 \leq k \leq n - 1$ )

$$(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n),$$

а порядок вычисления произведений в скобках не имеет значения в силу предположения индукции (так как  $k < n$  и  $n - k < n$ ). Если  $k = n - 1$ , то

$$x_1 * \cdots * x_n = (x_1 * \cdots * x_{n-1}) * x_n = ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n,$$

а последнее произведение уже имеет канонический вид. При  $k < n - 1$

$$(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n) = (x_1 * \cdots * x_k) * ((x_{k+1} * \cdots * x_{n-1}) * x_n)$$

по предположению индукции (во второй скобке порядок вычисления можно выбирать произвольно). Далее,

$$(x_1 * \cdots * x_k) * ((x_{k+1} * \cdots * x_{n-1}) * x_n) = ((x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_{n-1})) * x_n$$

в силу ассоциативности операции  $*$ . Еще раз применяя предположение индукции получаем, что

$$((x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_{n-1})) * x_n = (x_1 * \cdots * x_{n-1}) * x_n,$$

а последнее произведение, как уже было показано выше, равно соответствующему каноническому произведению.  $\square$

**Определение.** Элементы  $x \in X$  и  $y \in X$  произвольной (не обязательно коммутативной) полугруппы  $(X, *)$  называются **коммутирующими** (говорят также, что элементы  $x$  и  $y$  коммутируют), если

$$x * y = y * x.$$

**Предложение 1.7.** Пусть элементы  $x$  и  $y$  моноида  $X$  коммутируют в  $X$ . Тогда для любого  $n \in \mathbb{Z}_+$  верно равенство

$$(x * y)^n = x^n * y^n. \quad (1.2)$$

**Доказательство.** Равенство (1.2) легко проверяется по индукции. В самом оно верно при  $n = 0, 1$  и, из того, что  $(x * y)^{n-1} = x^{n-1} * y^{n-1}$  и из равенства  $x * y = y * x$  вытекает, что  $y^{n-1} * x = x * y^{n-1}$  и, окончательно,

$$(x * y)^n = (x * y)^{n-1} * (x * y) = x^{n-1} * y^{n-1} * x * y = x^{n-1} * x * y^{n-1} * y = x^n * y^n.$$

□



Пусть  $(X, *, e)$  – полугруппа с единицей.

**Определение.** Элемент  $a \in X$  называется *обратимым*, если существует элемент  $b \in X$  такой, что  $a * b = b * a = e$ . Этот элемент  $b$  называется *обратным* для элемента  $a$ .

Если элемент  $a \in X$  обратим, а  $b \in X$  – соответствующий обратный элемент, то ясно, что  $b$  также является обратимым элементом.

**Предложение.** Если элемент  $a \in X$  обратим, то обратный для него элемент  $b \in X$  является единственным.

**Проверка.** Пусть  $a \in X$  и пусть  $b_1 \in X$  и  $b_2 \in X$  – два обратных для  $a$  элемента. Тогда  $b_2 = e * b_2 = b_1 * a * b_2 = b_1 * e = b_1$ .  $\square$

**Определение.** Обратный элемент для  $a$  обозначают  $a^{-1}$ .

**Предложение.**  $(a^{-1})^{-1} = a$ .

**Проверка.** В самом деле,  $(a^{-1})^{-1} * a^{-1} = e$  и, аналогично,  $a^{-1}(a^{-1})^{-1} = e$ .  $\square$

**Предложение.** Если  $X$  – полугруппа с единицей,  $x, y \in X$  и если существуют  $x^{-1}$  и  $y^{-1}$ , то  $(x * y)^{-1}$  существует и  $(x * y)^{-1} = y^{-1} * x^{-1}$ .

**Проверка.** В самом деле,  $(x * y) * (y^{-1} * x^{-1}) = x * (y y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$ , а  $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = y^{-1} * y = e$ .  $\square$

**Следствие.** Если  $X$  – моноид, то множество  $U(X)$  состоящее из всех обратимых элементов моноида  $X$  является подмоноидом в  $X$ .

**Определение.** Полугруппа с единицей  $G$  такая, что для любого элемента  $x \in G$  существует обратный элемент  $x^{-1} \in G$  называется группой. Число  $|G|$  называется порядком группы  $G$ .

Другими словами, множество  $G$  с определенной на нем бинарной операцией  $*$  является группой, если (1) операция  $*$  является ассоциативной, (2) в  $G$  существует нейтральный элемент  $e$  относительно операции  $*$  и (3) для любого  $x \in G$  существует (единственный) элемент  $x^{-1} \in G$  такой, что  $x * x^{-1} = x^{-1} * x = e$ .

**Определение.** Если  $G$  – группа (относительно операции  $*$ ), то ее подмножество  $G_1$  называется подгруппой, если  $e \in G_1$  и для любых элементов  $x, y \in G_1$  выполнены условия  $x * y \in G_1$  и  $x^{-1} \in G_1$ .

Другими словами,  $G_1$  – подгруппа группы  $G$ , если  $G_1$  – подмоноид  $G$  и множество  $G_1$  замкнуто относительно операции взятия обратного элемента.

Подгруппа  $H$  группы  $G$  называется *собственной*, если  $H \neq \{e\}$  и  $H \neq G$ .



**Определение.** Группа  $G$  называется *коммутативной*, если  $G$  является коммутативной как полугруппа, т.е., если для любых элементов  $g, h \in G$  справедливо равенство  $g * h = h * g$ .

**Замечание.** Часто коммутативные группы называют также *абелевыми* (в честь норвежского математика Абеля).

**Определение.** Величина  $[x, y] = x * y * x^{-1} * y^{-1}$ , где  $x$  и  $y$  – произвольные элементы группы  $G$  называется *коммутатором* элементов  $x$  и  $y$ .

Термин “коммутатор” возник в силу следующего равенства

$$x * y = [x, y] * y * x,$$

которое справедливо для любых  $x \in G$  и  $y \in G$ . Кроме того, элементы  $x \in G$  и  $y \in G$  коммутируют (т.е.  $x * y = y * x$ ) если и только если их коммутатор  $[x, y] = 1$ .

Как отмечалось выше, множество  $\mathfrak{S}^*(\Omega)$  всех биективных отображений некоторого множества  $\Omega$  на себя образует группу относительно операции композиции отображений.

**Определение.** Множество  $S_n = \mathfrak{S}^*({1, 2, \dots, n})$ , где  $n \in \mathbb{N}$ , рассматриваемое вместе с операцией композиции отображений, называется *симметрической группой степени  $n$* . Элементы множества  $S_n$  называются *перестановками*.

В качестве упражнения предлагается проверить, что  $|S_n| = n!$ .

Традиционно, перестановки обозначаются греческими буквами. Каждую перестановку  $\pi : k \mapsto \pi(k)$ ,  $k = 1, 2, \dots, n$  для наглядности можно изобразить в виде  $2 \times n$  матрицы

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

где  $k_j = \pi(j)$  – все числа из множества  $\{1, 2, \dots, n\}$  взятые по одному разу в каком-то порядке. Единичная перестановка обозначается символом  $e : j \mapsto e(j) = j$ ,  $j = 1, 2, \dots, n$ . Для перестановок определена операция *умножения*, которая определяется

как композиция соответствующих отображений: произведение  $\sigma\tau$  перестановок  $\sigma \in S_n$  и  $\tau \in S_n$  определяется как перестановка  $j \mapsto \sigma(\tau(j))$ ,  $j = 1, 2, \dots, n$ . Например, если

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \text{а} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

то произведения  $\sigma\tau$  и  $\tau\sigma$  вычисляются так

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \\ \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \end{aligned}$$

так что  $\sigma\tau \neq \tau\sigma$ .



**Предложение 1.10.** *Каждая перестановка  $\pi \neq e$  из  $S_n$  является произведением независимых циклов длины, большей или равной 2. Это разложение в произведение однозначно с точностью до порядка следования сомножителей.*

Введем еще одно важное понятие, связанное с перестановками. Цикл длины 2 будем называть *транспозицией*. Любая транспозиция имеет вид  $(ab)$  и оставляет на месте все символы, отличные от  $a$  и  $b$ . Из предложения 1.10 вытекает следующее утверждение

**Предложение 1.11.** *Каждая перестановка  $\pi \in S_n$  может быть представлена в виде произведения транспозиций.*

Для доказательства достаточно заметить, что

$$(1, 2, \dots, m - 1, m) = (1, m)(1, m - 1)(1, m - 2) \times \dots \times (1, 3)(1, 2)$$

(здесь в записи циклов для удобства чтения элементы разделены запятыми). Разумеется, разложение перестановки в произведение транспозиций не является единственным. Например, в  $S_4$  имеют место следующие разложения

$$(123) = (13)(12) = (23)(13) = (13)(24)(12)(14).$$

Более того, в общем случае имеет место равенство  $\sigma\tau^2 = \sigma$  для любых транспозиций  $\sigma$  и  $\tau$  (проверка оставляется в качестве *упражнения*). Таким образом, количество транспозиций в разложении перестановки  $\pi \in S_n$  зависит не только от  $\pi$ , но и от способа разложения.

**Определение.** Функция  $f$  от  $n$  переменных называется *кососимметрической*, если  $\tau \circ f = -f$  для любой транспозиции  $\tau \in S_n$ .

**Предложение 1.12.** Пусть  $\pi$  – перестановка из  $S_n$  и пусть  $\pi = \tau_1 \times \cdots \times \tau_k$  – некоторое разложение  $\pi$  в произведение транспозиций. Тогда число  $\varepsilon_\pi := (-1)^k$  полностью определяется перестановкой  $\pi$  и не зависит от способа ее разложения в произведение транспозиций. **По определению**, число  $\varepsilon_\pi$  называется *четностью* подстановки  $\pi$ . Если  $\varepsilon_\pi = 1$ , то  $\pi$  называется *четной*, а если  $\varepsilon_\pi = -1$ , то  $\pi$  называется *нечетной*. Далее,  $\varepsilon_{\alpha\beta} = \varepsilon_\alpha \varepsilon_\beta$  для любых перестановок  $\alpha, \beta \in S_n$ .

**Замечание.** 1) Произведение перестановок одинаковой четности дает четную перестановку, а произведение перестановок различной четности дает нечетную перестановку.

2) Количество четных и нечетных перестановок в  $S_n$  одинаково и равно  $n!/2$ .

3) Множество  $A_n$  состоящее из всех *четных* перестановок степени  $n$  является подгруппой группы  $S_n$ .

**Определение.** *Группа  $A_n$  называется знакопеременной группой (степени  $n$ ).*