2. ТЕОРИЯ ПОЙА

2.1. ПРЕОБРАЗОВАНИЯ МНОЖЕСТВА

2.1.1. Преобразования и подстановки

2.1.1.1. Операции и алгебры

Будем говорить, что на множестве A задана *n-местная операция* φ, если каждому вектору $\langle a_1, a_2, \dots, a_n\rangle \in A^n$ ставится в соответствие единственный элемент $a \in A$. Обозначается такая операция $\varphi: A^n \to$ $\to A$. По аналогии с бинарными отношениями n-местную операцию можно также называть *функцией* из A^n в A и применять запись $a = \varphi(a_1, a_2, \dots, a_n)$, означающую, что элемент a ставится в соответствие вектору $\langle a_1, a_2, \dots, a_n\rangle$. Координаты вектора называются *аргументами* этой функции. Таким образом, n-местная операция представляет собой функцию n аргументов, принимающих значения в множестве A. Понятно, что на произвольном множестве можно задать несколько (для бесконечного числа элементов в A бесконечно много) операций. *Сигнатурой* множества A называется некоторое подмножество $\Phi = \{\varphi_1, \varphi_2, \dots\}$ этих операций. Множество A с его сигнатурой называется *алгеброй* и обозначается $\mathcal{A}(A, \Phi)$. Множество A называется *основным множеством алгебры.*

Особое значение имеют двухместные, или *бинарные*, операции. Будем применять для них не функциональную запись, а специальные знаки. Пусть на множестве A определены две бинарные операции $+$ и $\cdot$ (употребление знаков сложения и умножения не означает, что эти операции обязательно аналогичны сложению и умножению чисел). Операция $\cdot$ называется *ассоциативной*, если для любых a, b, $c \in A$ выполняется равенство

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

коммутативной, если для любых a, $b \in A$

$$a \cdot b = b \cdot a.$$

Операция $\cdot$ *дистрибутивна* относительно $+$, если для любых a, b, $c \in A$ верны равенства

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

(дистрибутивность слева);

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

(дистрибутивность справа). Для коммутативной операции $\cdot$ свойства дистрибутивности слева и справа эквивалентны.

Элемент $\mathbb{I}$ называется *нейтральным*, или *единичным*, относительно операции $\cdot$, если для любого $a \in A$

$$a \cdot \mathbb{I} = \mathbb{I} \cdot a = a.$$

В любой алгебре существует не более одного единичного элемента. Действительно, если $\mathbb{I}$, $\mathbb{I}'$ — два различных нейтральных элемента, то из равенства $\mathbb{I} = \mathbb{I} \cdot \mathbb{I}' = \mathbb{I}' \cdot \mathbb{I} = \mathbb{I}'$ следовало бы противоречие. Элемент a^{-1} называется *обратным* к элементу $a \in A$ относительно операции $\cdot$, если $a \cdot a^{-1} = a^{-1} \cdot a = \mathbb{I}$.

Например, в алгебре множеств (подраздел 1.1.1) операцией $\cdot$ является пересечение, $+$ — объединение множеств. Нейтральным элементом относительно пересечения является универсум $\mathbb{U}$, так как для любого множества A верно $A \cap \mathbb{U} = \mathbb{U} \cap A = A$, относительно объединения — $\emptyset$ ($A \cup \emptyset = \emptyset \cup A = A$). Обе операции коммутативны, ассоциативны и дистрибутивны относительно друг друга. Обратных элементов не существует. В алгебре производящих функций (подраздел 1.3.1) операциями $\cdot$ и $+$ являются соответственно умножение и сложение. Нейтральным элементом $\mathbb{I}$ относительно умножения является ряд $\mathbb{I}$ — производящая функция последовательности $\langle 1, 0, 0, \dots \rangle$, обратный к ряду F_a элемент — ряд

$$F_a^{-1} = \frac{\mathbb{I}}{F_a}.$$

Нейтральным относительно сложения элементом является нулевой ряд $\mathbb{0}$, обратным к производящей функции F_a — противоположный ряд $-F_a$.

Пусть $A' \subseteq A$. Обозначим через

$$\varphi(A') = \{a \in A | a = \varphi(a_1, a_2, \ldots, a_n), a_i \in A', i = 1, \ldots, n\}$$

образ A' при операции φ. Множество A' называется *замкнутым* относительно n-местной операции φ на A, если $\varphi(A') \subseteq A'$. Если множество $A' \subseteq A$ замкнуто относительно всех операций сигнатуры алгебры, то оно является основным множеством алгебры $\mathcal{A}'(A', \Phi)$ с той же сигнатурой. Эта алгебра называется *подалгеброй* $\mathcal{A}(A, \Phi)$.

2.1.1.2. Гомоморфизм

Пусть имеются две алгебры $\mathcal{A}(A, \Phi)$, $\mathcal{B}(B, \Psi)$ с сигнатурами $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, $\Psi = \{\psi_1, \psi_2, \ldots, \psi_k\}$, состоящими из одинакового числа операций, причём для всех $i = 1, 2, \ldots, k$ операции φ_i, ψ_i являются функциями n_i аргументов.

Функция $f: A \to B$, удовлетворяющая условиям

$$f\left(\varphi_i\left(a_{j_1}, a_{j_2}, \ldots, a_{j_{n_i}}\right)\right) = \psi_i\left(f(a_{j_1}), f(a_{j_2}), \ldots, f\left(a_{j_{n_i}}\right)\right)$$

для всех $i = 1, 2, \ldots, k$ и всех $a_{j_s} \in A$, называется *гомоморфизмом* алгебры $\mathcal{A}(A, \Phi)$ в алгебру $\mathcal{B}(B, \Psi)$. Таким образом, гомоморфизм — функциональное отображение A в B, сохраняющее операции сигнатур Φ и Ψ. Взаимно однозначный (биективный) гомоморфизм называется *изоморфизмом.*

Гомоморфизм алгебры в некоторую подалгебру называется *гомоморфизмом в себя.* Изоморфизм алгебры в себя называется *автоморфизмом*.

Примером изоморфизма алгебры $\mathcal{A}(A, +)$ на алгебру $\mathcal{B}(B, +)$ является функция $f(n) = 2n$, если её рассматривать как $f: \mathbb{Z} \to \mathbb{Z}'$, где $\mathbb{Z}$ — множество целых чисел, $\mathbb{Z}'$ — чётных целых чисел и $A = \mathbb{Z}$, $B = \mathbb{Z}'$. Если же $f: \mathbb{Z} \to \mathbb{Z}$, $B = \mathbb{Z}$, то f становится автоморфизмом алгебры $\mathcal{A}(A, +)$.

2.1.1.3. Группы

Алгебра $\mathcal{A}(A, \ \cdot)$, у которой сигнатура состоит из единственной ассоциативной операции $\cdot$, называется *полугруппой*. Если операция $\cdot$ коммутативна, то полугруппа называется *коммутативной*, или *абеле-*

вой. Полугруппа $\mathcal{G}$ с нейтральным элементом I, в которой для каждого элемента g существует обратный, называется *группой*. Элемент I называется *единицей* группы. В дальнейшем и сами группы, и их основные множества будем обозначать одними и теми же буквами. *Абелева (коммутативная) группа* — группа с коммутативной операцией $\cdot$. Совокупность $\mathcal{H}$ элементов группы $\mathcal{G}$, образующая группу относительно операции $\cdot$, называется *подгруппой*. Если основное множество группы $\mathcal{G}$ конечно, то группа называется *конечной,* число элементов в $\mathcal{G}$ называется *порядком* группы.

Например, множество целых чисел $\mathbb{Z}$ образует абелеву группу относительно сложения; множество рациональных чисел без нуля образует абелеву группу относительно умножения. Эти группы бесконечны.

Пример конечной группы: совокупность преобразований плоскости, переводящих квадрат в себя. Здесь умножение преобразований означает их композицию, т. е. последовательное применение. Нетрудно убедиться, что таких преобразований всего восемь, для каждого в группе существует обратное. Нейтральный элемент — тождественное преобразование, т. е. такое, при котором каждая точка плоскости остаётся на месте.

Обозначим $g^k = \underbrace{g \cdot g \cdot \dots \cdot g}_{k}$ — k-я степень элемента $g \in \mathcal{G}$, $k \geq 0$ (полагаем $g^0 = \mathrm{I}$). Тогда операции над степенями элементов определяются следующим образом:

$$g^{k+s} = g^k \cdot g^s,\ (g^k)^s = g^{ks}.$$

Обратным к элементу g^k будет $g^{-k} = (g^{-1})^k$. Действительно, в силу ассоциативности операции $\cdot$

$$g^k \cdot g^{-k} = g^k \cdot (g^{-1})^k =$$

$$= \left(\underbrace{g \cdot g \cdot \dots \cdot g}_{k}\right) \cdot \left(\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{k}\right) =$$

$$= \Big(\underbrace{g \cdot g \cdot \dots \cdot g}_{k-1}\Big) \cdot (g \cdot g^{-1}) \cdot \Big(\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{k-1}\Big) =$$
$$= \Big(\underbrace{g \cdot g \cdot \dots \cdot g}_{k-1}\Big) \cdot \mathrm{I} \cdot \Big(\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{k-1}\Big) =$$
$$= \Big(\underbrace{g \cdot g \cdot \dots \cdot g}_{k-1}\Big) \cdot \Big(\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{k-1}\Big) = \dots = g \cdot g^{-1} = \mathrm{I}.$$

Аналогично доказывается, что $g^{-k} \cdot g^{k} = \mathrm{I}$. Итак,

$$(g^{k})^{-1} = g^{-k}. \tag{2.1.1}$$

Пусть $\mathcal{G}' = \{g_1, g_2, \dots, g_s\}$ — непустое подмножество основного множества группы $\mathcal{G}$. Совокупность всех элементов $\mathcal{G}$, представимых виде

$$g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_s^{\alpha_s}, \tag{2.1.2}$$

где α_1, α_2, … , α_s принимают всевозможные целочисленные значения, образует подгруппу $\mathcal{G}$. Действительно, эта совокупность содержит нейтральный элемент I, так как $\mathrm{I} = g_1^0 \cdot g_2^0 \cdot \dots \cdot g_s^0 = \mathrm{I} \cdot \mathrm{I} \cdot \dots \cdot \mathrm{I}$. Для любого элемента вида (2.1.2) существует обратный

$$g_s^{-\alpha_s} \cdot g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}$$

также вида (2.1.2). В самом деле, в силу ассоциативности $\cdot$ и формулы (2.1.1)

$$\left(g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_s^{\alpha_s}\right) \cdot \left(g_s^{-\alpha_s} \cdot g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}\right) =$$
$$= \left(g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_{s-1}^{\alpha_{s-1}}\right) \cdot \left(g_s^{\alpha_s} \cdot g_s^{-\alpha_s}\right) \cdot \left(g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}\right) =$$
$$= \left(g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_{s-1}^{\alpha_{s-1}}\right) \cdot \mathrm{I} \cdot \left(g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}\right) =$$
$$= \left(g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_{s-1}^{\alpha_{s-1}}\right) \cdot \left(g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}\right) = \dots = g_1^{\alpha_1} \cdot g_1^{-\alpha_1} = \mathrm{I}.$$

Аналогично доказывается, что

$$\left(g_s^{-\alpha_s} \cdot g_{s-1}^{-\alpha_{s-1}} \cdot \dots \cdot g_1^{-\alpha_1}\right) \cdot \left(g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_s^{\alpha_s}\right) = \mathrm{I}.$$

Эта подгруппа называется *подгруппой, порождённой множеством* $\mathcal{G}'$, и обозначается $[\mathcal{G}']$ или $[g_1, g_2, \dots, g_s]$. Множество $\mathcal{G}'$ называется *системой образующих* подгруппы $[\mathcal{G}']$, его элементы — *образующими*. Если $[\mathcal{G}']$ совпадает со всей $\mathcal{G}$, то $\mathcal{G}'$ — система образующих группы $\mathcal{G}$.

Подгруппа группы $\mathcal{G}$, порождённая элементом $g \in \mathcal{G}$, называется *циклической* (обозначается $[g]$). Циклическая подгруппа состоит из степеней одного и того же элемента, она всегда абелева, поскольку $g^k \cdot g^s = g^{k+s} = g^{s+k} = g^s \cdot g^k$. Если для элемента $g \in \mathcal{G}$ существует натуральное число p, такое, что

$$g^p = \mathrm{I}, \qquad (2.1.3)$$

то говорят, что g *имеет конечный порядок*. Наименьшее число, удовлетворяющее условию (2.1.3), называется *порядком* элемента g. Циклическая группа, порождённая элементом g порядка p, конечна и имеет вид $[g] = \{\mathrm{I}, g, g^2, \dots, g^{p-1}\}$, т. е. содержит p элементов. Действительно, любое натуральное число k единственным образом представимо в виде $k = sp + r$, где r — остаток от деления k на p ($0 \le$ $\le r \le p - 1$). Поэтому $g^k = g^{sp+r} = g^{sp} \cdot g^r = (g^p)^s \cdot g^r = \mathrm{I}^s \cdot g^r =$ $= \mathrm{I} \cdot g^r = g^r$.

2.1.1.4. Смежные классы

Пусть $\mathcal{H}$ — подгруппа группы $\mathcal{G}$. *Левым смежным классом* группы $\mathcal{G}$ по подгруппе $\mathcal{H}$ называется множество $g\mathcal{H}$ элементов вида $g \cdot h$ где $h \in \mathcal{H}$, g — фиксированный элемент группы $\mathcal{G}$, который называется *представителем* смежного класса. Аналогично определяется *правый смежный класс* $\mathcal{H}g$.

Лемма 2.1.1

Левые (правые) смежные классы образуют разбиение группы.

Доказательство

Проведём для левых смежных классов. Для правых доказательство аналогично. Поскольку в подгруппе $\mathcal{H}$ имеется нейтральный элемент, то любой элемент $g \in \mathcal{G}$ представим в виде $g = g \cdot \mathrm{I}$, $\mathrm{I} \in \mathcal{H}$, а значит, каждый элемент группы g входит в свой смежный класс $g\mathcal{H}$. Рассмотрим два смежных класса $g_i\mathcal{H}$, $g_j\mathcal{H}$ и докажем, что они либо не пересекаются, либо совпадают. Пусть $g_i \neq g_j$ (в противном случае классы $g_i\mathcal{H}$, $g_j\mathcal{H}$ совпадают) и $g_i\mathcal{H} \cap g_j\mathcal{H} \neq \emptyset$. Тогда существует элемент $g \in g_i\mathcal{H} \cap g_j\mathcal{H}$. Из условия $g \in g_i\mathcal{H}$ следует $g = g_i \cdot h_1$, из

$g \in g_j\mathcal{H}$ — $g = g_j \cdot h_2$. Следовательно,

$$g_i \cdot h_1 = g_j \cdot h_2 \;\Rightarrow\; g_i = g_j \cdot h_2 \cdot h_1^{-1}.$$

По определению подгруппы $h_1^{-1} \in \mathcal{H}$ и $h_2 \cdot h_1^{-1} \in \mathcal{H}$, значит, $g_i \in$ $\in g_j\mathcal{H}$, что доказывает включение $g_i\mathcal{H} \subseteq g_j\mathcal{H}$. Из равенства $g_j = g_i \cdot$ $\cdot h_1 \cdot h_2^{-1}$ следует $g_j \in g_i\mathcal{H}$ и вместе с тем обратное включение. Доказано, что при наличии у смежных классов хотя бы одного общего элемента они совпадают. ■

Множество левых (правых) смежных классов группы $\mathcal{G}$ по подгруппе $\mathcal{H}$ обозначим через $\mathcal{G} \,/\, \mathcal{H}$ ($\mathcal{H} \,/\, \mathcal{G}$).

Если группа $\mathcal{G}$ конечна, то из леммы следует *теорема Лагранжа.*

Теорема 2.1.1 (Лагранжа)

Для конечной группы $\mathcal{G}$ и любой её подгруппы $\mathcal{H}$ справедливо равенство

$$|\mathcal{G}| = |\mathcal{H}||\mathcal{G} \,/\, \mathcal{H}|$$

($|\mathcal{G}| = |\mathcal{H}||\mathcal{H} \,/\, \mathcal{G}|$ для правых смежных классов).

Следствие

Порядок любого элемента группы является делителем порядка группы. Если порядок группы — простое число, то группа — циклическая.

Доказательство

Циклическая группа, порождённая элементом g конечной группы $\mathcal{G}$, имеет вид $[g] = \{\mathrm{I}, g, g^2, \dots, g^{p-1}\}$, т. е. содержит p элементов (p — порядок g) и является подгруппой $\mathcal{G}$. Далее применяем к ней теорему Лагранжа и получаем утверждение. ■

Подгруппа $\mathcal{H}$ группы $\mathcal{G}$ называется *нормальным делителем* $\mathcal{G}$, если $g\mathcal{H} = \mathcal{H}g$ для любого $g \in \mathcal{G}$, т. е. левые и правые смежные классы по нормальному делителю $\mathcal{H}$ совпадают. *Нормализатором* подгруппы $\mathcal{H}'$ в группе $\mathcal{G}$ называется множество $N(\mathcal{H}') = \{g \in \mathcal{G} \mid g\mathcal{H}'g^{-1} = \mathcal{H}'\}$, где $g\mathcal{H}'g^{-1} = \{h \in \mathcal{G} | h = gh'g^{-1}, h' \in \mathcal{H}'\}$. Если $\mathcal{H}' = \mathcal{H}$, где $\mathcal{H}$ — нормальный делитель группы $\mathcal{G}$, то $H(\mathcal{H}) = \mathcal{G}$. Действительно, равенство $h = gh'g^{-1}$ можно записать в виде $gh' =$

$= hg$, которое в случае h, h' из нормального делителя $\mathcal{H}$ выполняется при любых $g \in \mathcal{G}$. Пусть $\varphi: \mathcal{G} \to \mathcal{G}'$ — гомоморфизм из группы $\mathcal{G}$ в группу $\mathcal{G}'$. *Ядром* гомоморфизма φ называется множество $\ker\varphi = \{g \in \mathcal{G} \mid \varphi(g) = \mathrm{I}'$, где I' — нейтральный элемент группы $\mathcal{G}'$.

Лемма 2.1.2

Ядро гомоморфизма $\varphi: \mathcal{G} \to \mathcal{G}'$ является нормальным делителем группы $\mathcal{G}$.

Доказательство

Сначала надо доказать, что $\ker\varphi$ является подгруппой $\mathcal{G}$. Пусть $a,\ b \in \ker\varphi$. Тогда $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \mathrm{I}' \cdot \mathrm{I}' = \mathrm{I}'$, поэтому $a \cdot b \in \ker\varphi$. Далее,

$$\varphi(\mathrm{I}) = \varphi(\mathrm{I} \cdot \mathrm{I}) = \varphi(\mathrm{I}) \cdot \varphi(\mathrm{I}). \qquad (2.1.4)$$

Так как $\varphi(\mathrm{I}) \in \mathcal{G}'$, то в подгруппе $\mathcal{G}'$ существует обратный к $\varphi(\mathrm{I})$ элемент $(\varphi(\mathrm{I}))^{-1}$. Тогда из равенства (2.1.4) следует $\varphi(\mathrm{I}) = \mathrm{I}'$, поэтому $\mathrm{I} \in \ker\varphi$. Наконец, покажем, что каждый элемент $a \in \ker\varphi$ имеет в $\ker\varphi$ обратный. Для произвольного $a \in \ker\varphi \subseteq \mathcal{G}$ в $\mathcal{G}$ имеется обратный элемент a^{-1}. Убедимся в том, что он принадлежит $\ker\varphi$. Выше было доказано, что $\mathrm{I} \in \ker\varphi$. Поэтому

$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(\mathrm{I}) = \mathrm{I}' \Rightarrow \varphi(a^{-1}) = \big(\varphi(a)\big)^{-1} = \\ = (\mathrm{I}')^{-1} = \mathrm{I}'.$$

Отсюда получаем, что $a^{-1} \in \ker\varphi$. Итак, $\ker\varphi$ — подгруппа группы $\mathcal{G}$.

Теперь докажем, что она является нормальным делителем. Обозначим $\mathcal{H} = \ker\varphi$. Пусть

$$g \cdot a \cdot g^{-1} \in g\mathcal{H}g^{-1},$$

где $g \in \mathcal{G}$, a — произвольный элемент из $\mathcal{H}$. Из равенства

$$\varphi(g \cdot a \cdot g^{-1}) = \varphi(g) \cdot \varphi(a) \cdot \varphi(g^{-1}) = \varphi(g) \cdot \mathrm{I}' \cdot \varphi(g^{-1}) = \\ = \varphi(g) \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(\mathrm{I}) = \mathrm{I}'$$

следует, что $g \cdot a \cdot g^{-1} \in \mathcal{H}$, а значит, $g\mathcal{H}g^{-1} \subseteq \mathcal{H}$. Если теперь взять произвольный элемент $a \in \mathcal{H}$, то аналогично доказывается, что $\varphi(g^{-1} \cdot a \cdot g) = \mathrm{I}'$, $g \in \mathcal{G}$, $g^{-1} \cdot a \cdot g \in \mathcal{H}$, следовательно, верно, что $a \in g\mathcal{H}g^{-1}$ и $\mathcal{H} \subseteq g\mathcal{H}g^{-1}$. Из доказанных включений следует $\mathcal{H} =$

$= g\mathcal{H}g^{-1}$, что эквивалентно $g\mathcal{H} = \mathcal{H}g$. Подгруппа $\mathcal{H}$ является нормальным делителем $\mathcal{G}$. ■

2.1.1.5. Кольца и поля

Алгебра $\mathcal{A}(A, +, \cdot)$ называется *кольцом*, если множество A с операцией $+$ образует абелеву группу, а операция $\cdot$ дистрибутивна относительно $+$. Нейтральный элемент относительно $+$ обозначается 0 и называется *нулём*, если существует нейтральный элемент относительно $\cdot$, то он обозначается 1 и называется *единицей* кольца. Если операция $\cdot$ коммутативна, кольцо называется *коммутативным,* если ассоциативна — *ассоциативным*.

Примеры: множество целых чисел $\mathbb{Z}$ с операциями сложения и умножения образует коммутативное ассоциативное кольцо; множество числовых квадратных матриц размерности n на n с операциями сложения и умножения — ассоциативное некоммутативное кольцо. Эти кольца бесконечны.

Примером конечного кольца является кольцо *вычетов по модулю* m. Введём на множестве $\mathbb{Z}$ целых чисел бинарное отношение *сравнимости по модулю* m: числа $a, b \in \mathbb{Z}$ принадлежат этому отношению, если их разность делится на m или, что то же самое, a и b имеют одинаковые остатки при делении на m. Записывается это условие так: $a = b(\operatorname{mod} m)$ (читается: a равно b по модулю m). Легко проверить, что отношение сравнимости является эквивалентностью, следовательно, $\mathbb{Z}$ разбивается на классы эквивалентности по этому отношению. Они называются классами *вычетов по модулю* m и обозначаются $K_0, K_1, \dots, K_{m-1}$. Класс K_i содержит все целые числа, дающие остаток i при делении на m; i является наименьшим таким неотрицательным числом и берётся в качестве представителя класса K_i. Таким образом, числа $0, 1, \dots, m-1$ образуют полную систему наименьших неотрицательных вычетов.

Введём на множестве классов операции сложения $+$ и умножения $\cdot$. Считаем, что $K_i + K_j = K_l$, если $i' + j' = l'(\operatorname{mod} m)$, $i' \in K_i$,

$j' \in K_j$, $l' \in K_l$. Нетрудно убедиться в том, что результат этой операции не зависит от выбора чисел i', j' в классах K_i, K_j, т. е. последнее равенство определяет единственный класс K_l, поэтому в качестве i', j' можно брать представители i и j и определять сумму $K_i + K_j = K_l$ равенством $i + j = l (\mathrm{mod}\, m)$. Аналогично определяется операция умножения: $K_i \cdot K_j = K_l$, если $ij = l (\mathrm{mod}\, m)$.

Определив эти операции на K_0, K_1, … , K_{m-1}, получаем *кольцо классов вычетов* по модулю m $\mathcal{K}(K, +, \cdot)$ $(K = \{K_0, K_1, \dots, K_{m-1}\})$. То, что это действительно кольцо, т. е. операция $+$ ассоциативна, коммутативна, замкнута в K относительно взятия обратного элемента, а $\cdot$ дистрибутивна относительно $+$, нетрудно доказать (рекомендуется самостоятельно провести доказательство). Нулём кольца, очевидно, является класс K_0.

Если в произвольном кольце произведение двух отличных от нуля элементов равно нулю, то они называются *делителями нуля*. Кольцо без делителей нуля называется *областью целостности.*

Возвращаясь к примеру с кольцом вычетов, заметим, что в нём делители нуля могут быть в том и только том случае, когда m является составным числом. Действительно, из условия $K_i \cdot K_j = 0$ следует $ij = 0 (\mathrm{mod}\, m)$, т. е. ij делится на m без остатка, что невозможно при m простом и $i \neq 0$, $j \neq 0$ (напомним, что i, j — представители классов K_i, K_j, т. е. остатки при делении на m).

Кольцо с единицей называется *полем*, если множество ненулевых элементов образует абелеву группу относительно операции $\cdot$. Это значит, что в поле операция $\cdot$ коммутативна, ассоциативна и обратима, т. е. для каждого $a \neq 0$ в этом поле существует обратный элемент a^{-1}. Множество ненулевых элементов называется *мультипликативной группой поля*.

Примеры: поле действительных чисел с операциями сложения и умножения, поле рациональных чисел с такими же операциями.

Поле называется *конечным*, если её основное множество конечно. Конечные поля также называют *полями Галуа* и обозначают $GF(p)$, число p равно количеству элементов в поле. Примером конечного поля является *поле классов вычетов по простому модулю* p. Очевидно, что единицей поля является класс K_1. Докажем, что в множестве $K' = \{K_1, K_2, \dots, K_{p-1}\}$ каждый элемент имеет обратный относительно умножения. Пусть $K_i \in K'$. Рассмотрим совокупность наименьших неотрицательных вычетов по модулю p, соответствующих числам i, $2i$, … , $(p-1)i$. Все они не сравнимы по модулю p, так как

$$\alpha i = \beta i (\operatorname{mod} p) \;\Rightarrow\; \alpha = \beta$$

при $i \neq 0$ и простом p. Следовательно, рассматриваемая система вычетов является полной, и существует единственный элемент j от 1 до $p-1$, при котором $ij = 1 (\operatorname{mod} p)$. Поэтому

$$K_i \cdot K_j = K_1 = 1 \;\Rightarrow\; K_i^{-1} = K_j \in K'.$$

Важное свойство конечных полей состоит в следующем.

Теорема 2.1.2

Мультипликативная группа поля Галуа $GF(p)$ является циклической группой порядка $p-1$.

Доказательство приведено в пункте 2.1.1.3. Образующий элемент g мультипликативной группы называется *примитивным элементом.*

2.1.1.6. Полугруппы преобразований

Пусть имеется множество A. Будем называть *преобразованием* A любую функцию $f: A \to A$. Как было отмечено в пункте 1.1.3.2, в случае конечного (n)-множества A преобразование можно записывать в виде двухстрочной матрицы

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}.$$

Рассмотрим множество преобразований A. Определим на нём бинарную операцию умножения $\cdot$, состоящую в последовательном применении двух преобразований, т. е. для преобразований f_1, f_2 при всех $a \in A$ $(f_1 \cdot f_2)(a) = f_2(f_1(a))$. В дальнейшем для краткости знак умножения $\cdot$ будем опускать.

Пример: $A = \{1, 2, 3, 4, 5\}$,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 3 & 5 & 4 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix};$$

$$f_1 f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 4 & 1 \end{pmatrix}, f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 3 & 4 & 5 \end{pmatrix},$$

$$f_1 f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 5 & 1 & 4 & 3 \end{pmatrix}, f_2 f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix},$$

$$f_1 f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 3 & 5 & 4 & 3 \end{pmatrix}.$$

Эта операция ассоциативна, так как для любого $a \in A$ $\big(f_1(f_2 f_3)\big)(a) =$ $= \big((f_1 f_2) f_3\big)(a) = f_3\big(f_2(f_1(a))\big)$. Следовательно, если совокупность преобразований множества A замкнута относительно операции умножения, то она образует полугруппу — *полугруппу преобразований*. Множество элементов этой полугруппы, замкнутое относительно умножения, называется *подполугруппой преобразований.*

Если A — (n)-множество, то полугруппа всех его преобразований называется *симметрической полугруппой степени* n и обозначается $\mathfrak{F}_n$. Любая полугруппа преобразований (n)-множества является подполугруппой $\mathfrak{F}_n$.

2.1.1.7. Группы подстановок

В пункте 1.1.3.2 было введено понятие подстановки. Из предыдущего пункта следует, что подстановка является взаимно однозначным (биективным) преобразованием. Рассмотрим множество $\mathfrak{S}_n$ всех подстановок (n)-множества. Число n называется *степенью подстановки*. Докажем, что эти подстановки образуют группу относительно операции умножения.

Нейтральным элементом является тождественная подстановка

$$\mathrm{I} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix},$$

оставляющая каждый элемент множества на своём месте.

Каждой подстановке $s \in \mathfrak{S}_n$ соответствует единственная обратная подстановка $s^{-1} \in \mathfrak{S}_n$. Её можно построить следующим образом. Пусть

$$s = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}.$$

Переставим в этой матрице строки. Поскольку преобразование s сюръективно, в первой строке получившейся матрицы будут присутствовать все индексы от 1 до n. Переставим теперь столбцы таким образом, чтобы индексы в первой строке шли в порядке возрастания. Получим матрицу обратной подстановки s^{-1}. Следовательно, $\mathfrak{S}_n$ является группой относительно операции последовательного применения подстановок.

Группа $\mathfrak{S}_n$ называется *симметрической группой степени* n. Любое множество подстановок степени n, замкнутое относительно операций умножения и взятия обратного элемента, является группой. Каждая группа подстановок степени n есть подгруппа симметрической группы $\mathfrak{S}_n$.

Пример: $A = \{1, 2, 3\}$, группа $\mathfrak{S}_3$ состоит из подстановок

$$s_0 = \mathrm{I} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Можно непосредственно проверить, что любое произведение подстановок принадлежит $\mathfrak{S}_3$, например:

$$s_3 s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = s_5,$$

$$s_1 s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s_3.$$

Обратные подстановки строим перестановкой строк и столбцов, как описано выше:

$$s_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_1, s_2^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2, s_3^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s_3,$$

$$s_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = s_5, s_5^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = s_4.$$

2.1.2. Орбиты и циклы

2.1.2.1. Орбиты подстановок

Рассматривается группа подстановок (n)-множества A, s — некоторая подстановка из этой группы. Определим на A бинарное отношение $\sim$ следующим образом. Считается, что $a \sim b$ для $a, b \in A$ тогда и только тогда, когда существует такое целое число k, что $b = s^k(a)$ (s^k — k-я степень подстановки s). Это бинарное отношение рефлексивно, поскольку $a = \mathrm{I}(a) = s^0(a)$, а значит, $a \sim a$, симметрично, так как из равенства $b = s^k(a)$ вытекает $a = s^{-k}(b)$, поэтому из $a \sim b$ следует $b \sim a$. Наконец, оно транзитивно, поскольку если $b = s^k(a)$, $c = s^l(b)$, то $c = s^l(b) = s^l(s^k(a)) = s^{k+l}(a)$, значит, из $a \sim b$, $b \sim c$ следует $a \sim c$. Следовательно, $\sim$ является эквивалентностью.

Согласно теореме 1.1.1 классы эквивалентности $A/\sim$ образуют разбиение множества A. Блоки $A_1, A_2, \dots, A_k$ этого разбиения называются *орбитами*, или *классами транзитивности*, подстановки $s \in \mathfrak{S}_n$. Докажем следующие утверждение.

Лемма 2.1.3

Для любого $i = 1, \dots, k$:

1) $s(A_i) = A_i$, $s(A_i)$ — образ орбиты A_i при подстановке s;

2) сужения $s|A_i$ подстановки s на орбиту A_i снова являются подстановками.

Доказательство

1) Докажем включение $s(A_i) \subseteq A_i$. Пусть $x \in s(A_i)$. Это значит, что $x = s(a)$ при некотором $a \in A_i$. Тогда по определению класса транзитивности $x \in A_i$.

Докажем $A_i \subseteq s(A_i)$. Пусть $a \in A_i$, тогда $a = s^l(x)$ при некотором $x \in A_i$. Отсюда следует:

$$a = s^l(x) = (s^{l-1}s)(x) = s(s^{l-1}(x)) = s(y),$$

где $y = s^{l-1}(x) \in A_i$, так как $x \sim y$. Итак, получаем, что при некотором $y \in A_i$ элемент a равен $s(y)$, значит, $a \in s(A_i)$.

Равенство $s(A_i) = A_i$, $s(A_i)$ доказано.

2) Поскольку s является подстановкой A, сужение s на $A_i \subseteq A$ инъективно, а из доказанной первой части леммы следует, что оно и сюръективно. Следовательно, $s|A_i$ есть биекция из A_i на A_i, а значит, подстановка A_i. ■

2.1.2.2. Циклы

Сужение $s|A_i$ подстановки s на орбиту A_i называется *циклом* этой подстановки. Он представляет собой подстановку степени $n_i = |A_i|$ множества A_i. Пусть a — некоторый элемент орбиты A_i. Поскольку все остальные элементы A_i имеют вид $s^l(a)$, а число их равно $n_i - 1$, то подстановку $s|A_i$ можно записать в виде цикла длины n_i:

$$\left(a, s_i(a), s_i^2(a), \dots, s_i^{n_i-1}(a)\right) \tag{2.1.5}$$

(здесь введено обозначение $s_i = s|A_i$). Тогда

$$\left.\begin{array}{c} s_i^{n_i}(a) = a, \\ s_i^{n_i+1}(a) = s_i(a), \\ \vdots \end{array}\right\} \tag{2.1.6}$$

Теперь можно всю подстановку s разложить на циклы:

$$s = \left(a_1, s_1(a_1), s_1^2(a_1), \dots, s_1^{n_1-1}(a_1)\right)\cdots$$
$$\cdots\left(a_k, s_k(a_k), s_k^2(a_k), \dots, s_k^{n_k-1}(a_k)\right).$$

Если подстановки s_1, s_2, … , s_k доопределить до подстановок степени n, полагая $s_i(a) = a$ при $a \in A \backslash A_i$, то получим разложение подстановки s в произведение независимых циклов $s_1 s_2 \cdots s_k$. Поскольку орбиты как классы эквивалентности попарно не пересекаются, это произведение не зависит от порядка сомножителей. Заметим также, что из условий (2.1.6) следует однозначность записи цикла в виде (2.1.5) с точностью до циклического сдвига, т. е.

$$s_i = \left(s_i^{\upsilon}(a), s_i^{\upsilon+1}(a), \dots, s_i^{n_i+\upsilon-1}(a)\right), 0 \le \upsilon \le n_i - 1, \tag{2.1.7}$$

в частности, при $\upsilon = 0$ получаем представление (2.1.5).

Назовём *порядком* подстановки $s \in \mathfrak{S}_n$ наименьшее целое неотрицательное число p, удовлетворяющее условию $s^p = \mathrm{I}$. Его значение можно найти по следующей лемме.

Лемма 2.1.4

Порядок подстановки равен наименьшему общему кратному длин циклов, входящих в её разложение.

Доказательство

Если $s = s_1 s_2 \cdots s_k$, то $s^p = s_1^p s_2^p \cdots s_k^p$. Из равенства $s_i^{n_i}(a) = a$ для произвольного $a \in A_i$ (см. (2.1.6)) следует, что $s_i^{n_i} = \mathrm{I}$ ($i = 1, \dots, k$). Поэтому p совпадает с наименьшим общим кратным чисел n_1, $n_2, \dots, n_k$. ■

Цикл (a, b) длины 2 называется *транспозицией*. Он представляет собой подстановку, оставляющую на месте все элементы, кроме a и b. Любой цикл можно представить в виде произведения транспозиций, например, следующим образом:

$(a_1, a_2, \dots, a_l) = (a_1, a_2)(a_1, a_3)(a_1, a_4) \cdots (a_1, a_{l-1})(a_1, a_l)$. Следовательно, каждая перестановка может быть представлена в виде произведения транспозиций. Таким образом, множество всех транспозиций является системой образующих группы $\mathfrak{S}_n$ подстановок (n)-множества A:

$$\mathfrak{S}_n = [(a_1, a_2), \dots, (a_1, a_n), (a_2, a_3), \dots, (a_2, a_n), \dots, (a_{n-1}, a_n)].$$

П р и м е р: для подстановки степени 8

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 8 & 5 & 2 & 6 \end{pmatrix}$$

имеет место следующее разложение на циклы:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 8 & 5 & 2 & 6 \end{pmatrix} =$$
$$= (1 \quad 3 \quad 4)(2 \quad 7)(5 \quad 8 \quad 6).$$

Длины циклов равны 3, 2, 2. Наименьшее общее кратное этих чисел 6, поэтому $p = 6$. Нетрудно убедиться непосредственным вычислением, что $s^6 = \mathrm{I}$.

2.1.2.3. Цикловые классы

Очевидно, что любая подстановка $s \in \mathfrak{S}_n$ может содержать в разложении циклы длин $1, 2, \dots, n$. *Цикловым классом* будем называть символическую запись $1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}$, где $\alpha_1 + 2\alpha_2 + \cdots +$

$+n\alpha_n = n$. Будем говорить, что подстановка $s \in \mathfrak{S}_n$ принадлежит цикловому классу $1^{\alpha_1}2^{\alpha_2} \dots n^{\alpha_n}$, если её разложение содержит α_j циклов длины j, $j = 1, \dots, n$. Решим задачу нахождения числа $C(\alpha_1, \alpha_2, \dots, \alpha_n)$ подстановок в цикловом классе $1^{\alpha_1}2^{\alpha_2} \dots n^{\alpha_n}$. Докажем, что

$$C(\alpha_1, \alpha_2, \dots, \alpha_n) = \frac{n!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \alpha_1! \, \alpha_2! \cdots \alpha_n!}. \quad (2.1.8)$$

Рассмотрим разложение подстановки $s \in \mathfrak{S}_n$ из циклового класса $1^{\alpha_1}2^{\alpha_2} \dots n^{\alpha_n}$ в произведение циклов:

$$s = (a_1)(a_2) \cdots (a_{\alpha_1})(b_1, c_1)\,(b_2, c_2) \cdots (b_{\alpha_2}, c_{\alpha_2}) \cdots.$$

Переставляя буквы в этой записи с сохранением скобок на своих местах, можно получить любую другую подстановку из данного класса. Всего имеются $n!$ таких перестановок. Но те из них, которые осуществляют циклические сдвиги внутри скобок, очевидно, не дают новых подстановок (см. представление цикла (2.1.7)). Число циклических сдвигов цикла равно его длине, поэтому существуют j^{α_j} перестановок, осуществляющих циклические сдвиги букв в α_j циклах длины j, а всего $1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n}$ перестановок для всех циклов. Далее, перестановки циклов одинаковой длины также не дадут новых подстановок. Количество таких перестановок равно $\alpha_j!$ для циклов длины j и $\alpha_1! \, \alpha_2! \cdots \alpha_n!$ для всех циклов. Следовательно, $1^{\alpha_1} \times$ $\times\, 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \alpha_1! \, \alpha_2! \cdots \alpha_n!$ различных перестановок букв соответствуют единственной подстановке данного циклового класса. Если умножить теперь это число на количество подстановок в цикловом классе $C(\alpha_1, \alpha_2, \dots, \alpha_n)$, то получим общее число перестановок $n!$:

$$1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \alpha_1! \, \alpha_2! \cdots \alpha_n! \, C(\alpha_1, \alpha_2, \dots, \alpha_n) = n!,$$

откуда и следует доказываемая формула.

Если просуммировать (2.1.8) по всем упорядоченным наборам решений уравнения $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n$ в неотрицательных целых числах, то получим равенство

$$\sum_{\substack{\langle \alpha_1,\alpha_2,\dots,\alpha_n\rangle \\ 0\le\alpha_i\le n \\ i=1,\dots,n \\ \alpha_1+2\alpha_2+\dots+n\alpha_n=n}} \frac{1}{1^{\alpha_1}\cdot 2^{\alpha_2}\cdot \dots \cdot n^{\alpha_n}\alpha_1!\,\alpha_2!\cdots\alpha_n!} = 1.$$

2.1.2.4. Подстановки с заданным числом циклов. Числа Стирлинга

Обозначим через $C(n,k)$ число подстановок степени n, имеющих k циклов. Тогда из формулы (2.1.8) следует

$$C(n,k) = \sum_{\substack{\langle \alpha_1,\alpha_2,\dots,\alpha_n\rangle \\ 0\le\alpha_i\le n \\ i=1,\dots,n \\ \alpha_1+2\alpha_2+\dots+n\alpha_n=n \\ \alpha_1+\alpha_2+\dots+\alpha_n=k}} \frac{n!}{1^{\alpha_1}\cdot 2^{\alpha_2}\cdot \dots \cdot n^{\alpha_n}\alpha_1!\,\alpha_2!\cdots\alpha_n!}.$$

Выведем рекуррентное соотношение для чисел $C(n,k)$. Разобьём множество подстановок с k циклами на два класса: в первый включим подстановки, оставляющие на месте фиксированный элемент a, во второй — все остальные подстановки. В первом классе содержатся $C(n-1,k-1)$ подстановок, так как остающийся на месте элемент образует цикл длины 1 в разложении в произведение циклов. Подсчитаем число подстановок во втором классе. Элемент a должен присутствовать в каком-либо цикле длины от 2 до n. Включив его в один такой цикл, для остальных элементов имеем $C(n-1,k)$ подстановок. Значит, всего имеется $(n-1)C(n-1,k)$ подстановок, сдвигающих элемент a. Очевидно, что классы не пересекаются, поэтому по правилу суммы получаем рекуррентное соотношение

$$C(n,k) = C(n-1,k-1) + (n-1)C(n-1,k), \quad (2.1.9)$$

$k = 1, \dots, n-1$. Положив $C(0,0) = 1$, $C(n,0) = 0$, $n > 0$, $C(n,k) = 0$, $k > n$ или когда $k < 0$ или $n < 0$, его можно распространить на все целочисленные значения n и k.

Для вычисления $C(n,k)$ с помощью соотношения (2.1.9) применим метод производящих функций. Умножив (2.1.9) на z^k и просуммировав полученные выражения по k от 0 до n, получим

$$\sum_{k=0}^{n} C(n,k)z^k =$$
$$= \sum_{k=0}^{n} C(n-1,k-1)z^k + (n-1)\sum_{k=0}^{n} C(n-1,k)\,z^k =$$
$$= \sum_{k=0}^{n-1} C(n-1,k)z^{k+1} + (n-1)\sum_{k=0}^{n-1} C(n-1,k)\,z^k =$$
$$= z\sum_{k=0}^{n-1} C(n-1,k)z^k + (n-1)\sum_{k=0}^{n-1} C(n-1,k)\,z^k$$

(здесь использованы условия $C(n,k) = 0$, при $k > n$ и при $k < 0$). Далее, многочлен

$$F_{C,n}(z) = \sum_{k=0}^{n} C(n,k)z^k$$

является производящей функцией чисел $C(n,k)$. Подставив его в последнее полученное равенство, имеем

$$F_{C,n}(z) = zF_{C,n-1}(z) + (n-1)F_{C,n-1}(z) =$$
$$= (z+n-1)F_{C,n-1}(z).$$

Производя в этом равенстве последовательно подстановку, получим с учётом того, что $F_{C,0}(z) = C(0,0) = 1$

$$F_{C,n}(z) = z(z+1)\cdots(z+n-1). \qquad (2.1.10)$$

Итак, числа подстановок степени n с k циклами $C(n,k)$ являются коэффициентами при z^k многочлена (2.1.10). Можно выписать явную формулу для $C(n,k)$, используя числа Стирлинга.

Равенства

$$(z)_n = \sum_{k=0}^{n} s(n,k)z^k,$$

$$z^n = \sum_{k=0}^{n} \sigma(n,k)(z)_k$$

определяют *числа Стирлинга* $s(n,k)$, $\sigma(n,k)$ *первого* и *второго рода*, соответственно. Здесь

$$(z)_n = z(z-1)\cdots(z-n+1) \text{ —}$$

факториальная функция (при $z = m \geq n$ натуральном $(m)_n = m(m-1)\cdots(m-n+1) = A_m^n$ — число размещений без повторений из m элементов по n). Полагаем $s(0,0) = \sigma(0,0) = 1$, $s(n,k) = \sigma(n,k) = 0$ при $n < k$.

Из определения чисел Стирлинга следует соотношение ортогональности для них:

$$\sum_{j=k}^{n} s(n,j)\,\sigma(j,k) = \delta_{nk} = \begin{cases} 1, n = k, \\ 0, n \neq k \end{cases}$$

(δ_{nk} — символ Кронекера).

Заменим в равенстве, определяющем числа Стирлинга первого рода, z на $-z$ и умножим обе его части на $(-1)^n$. Получим

$$(-1)^n(-z)_n = z(z+1)\cdots(z+n-1) = \\ = \sum_{k=0}^{n}(-1)^{n+k}s(n,k)z^k.$$

Итак, получаем, что

$$F_{C,n}(z) = \sum_{k=0}^{n} C(n,k)z^k = z(z+1)\cdots(z+n-1) = \\ = \sum_{k=0}^{n}(-1)^{n+k}s(n,k)z^k,$$

откуда следует формула $C(n,k) = (-1)^{n+k}s(n,k)$, связывающая величины $C(n,k)$ с числами Стирлинга первого рода, а через соотношение ортогональности и с числами второго рода.

2.1.2.5. Цикловой индекс группы подстановок

Пусть $\mathcal{G}$ — группа подстановок степени n и $k_i(g)$ — число циклов длины i в подстановке $g \in \mathcal{G}$, $i = 1, \dots, n$. Многочлен

$$P_{\mathcal{G}}(z_1, z_2, \dots, z_n) = \frac{1}{|\mathcal{G}|}\sum_{g \in \mathcal{G}} z_1^{k_1(g)}\, z_2^{k_2(g)} \cdots z_n^{k_n(g)}$$

называется *цикловым индексом* группы подстановок.

Для симметрической группы $\mathfrak{S}_n$ степени n ($|\mathfrak{S}_n| = n!$) слагаемые в $P_{\mathcal{G}}(z_1, z_2, \dots, z_n)$, соответствующие подстановке s из циклового класса $1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}$, одинаковы, а их количество равно числу элементов в цикловом классе $1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}$, т. е. $C(\alpha_1, \alpha_2, \dots, \alpha_n)$. Поэтому цикловой индекс группы $\mathfrak{S}_n$ равен

$$P_{\mathfrak{S}_n}(z_1, z_2, \dots, z_n) = \frac{1}{n!} \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ 0 \le \alpha_i \le n \\ i = 1, \dots, n \\ \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n}} C(\alpha_1, \alpha_2, \dots, \alpha_n) z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}.$$

Суммирование ведётся по всем неотрицательным целым решениям уравнения $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n$, или, что то же самое, по всем разбиениям числа n. С учётом формулы (2.1.8) цикловой индекс группы $\mathfrak{S}_n$ можно записать в виде

$$P_{\mathfrak{S}_n}(z_1, z_2, \dots, z_n) =$$

$$= \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ 0 \le \alpha_i \le n \\ i = 1, \dots, n \\ \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n}} \frac{1}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \alpha_1! \, \alpha_2! \cdots \alpha_n!} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} =$$

$$= \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ 0 \le \alpha_i \le n \\ i = 1, \dots, n \\ \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n}} \frac{1}{\alpha_1! \, \alpha_2! \cdots \alpha_n!} \left(\frac{z_1}{1}\right)^{\alpha_1} \left(\frac{z_2}{2}\right)^{\alpha_2} \cdots \left(\frac{z_n}{n}\right)^{\alpha_n}.$$

Для нескольких первых значений n имеем следующие цикловые индексы $\mathfrak{S}_n$:

$$P_{\mathfrak{S}_1}(z_1) = z_1;$$

$$P_{\mathfrak{S}_2}(z_1, z_2) = \frac{1}{2}(z_1^2 + z_2);$$

$$P_{\mathfrak{S}_3}(z_1, z_2, z_3) = \frac{1}{6}(z_1^3 + 3z_1 z_2 + 2z_3^3);$$

$$P_{\mathfrak{S}_4}(z_1, z_2, z_3, z_4) = \frac{1}{24}(z_1^4 + 6z_1^2 z_2 + 3z_2^2 + 8z_1 z_3 + 6z_4).$$

Отметим, что каждая подстановка относится к некоторому цикловому классу, поэтому сумма всех $C(\alpha_1, \alpha_2, \dots, \alpha_n)$ в $P_{\mathfrak{S}_n}(z_1, z_2, \dots, z_n)$ равна $n!$, а значит, сумма всех числовых коэффициентов $P_{\mathfrak{S}_n}(z_1, z_2, \dots, z_n)$ равна 1. Отсюда получаем *тождество Коши*:

$$\sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ 0 \le \alpha_i \le n \\ i=1,\dots,n \\ \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n}} \frac{1}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \alpha_1! \, \alpha_2! \cdots \alpha_n!} = 1.$$

Рассмотрим теперь циклическую группу $\mathcal{C}_n$ подстановок степени n, все элементы которой представляют собой степени одной и той же подстановки

$$C = \begin{pmatrix} 1 & 2 & \dots & n \\ n & 1 & \dots & n-1 \end{pmatrix}$$

(без потери общности можно считать, что основное множество группы $\mathcal{C}_n$ есть $\{1, 2, \dots, n\}$). Эта группа имеет вид $\mathcal{C}_n = \{I, C, C^2, \dots, C^{n-1}\}$, $|\mathcal{C}_n| = n$. Подстановка C^j имеет $d(n, j)$ циклов длины $\frac{n}{d(n,j)}$, где $d(n, j)$ — наибольший общий делитель чисел n, j. Цикловой индекс группы $\mathcal{C}_n$ равен

$$P_{\mathcal{C}_n}(z_1, z_2, \dots, z_n) = \frac{1}{n} \sum_{j=0}^{n-1} z_{n/d(n,j)}^{d(n,j)}.$$

Его можно записать через *функцию Эйлера* ϕ, равную для каждого натурального k количеству чисел, не превосходящих k и взаимно простых с ним (см. пункт 1.2.1.6).

Можно заметить, что число целых j, $0 \le j \le n-1$, удовлетворяющих равенству $d(n, j)k = n$, равно $\phi(k)$. Поэтому цикловой индекс циклической группы подстановок степени n вычисляется по формуле

$$P_{\mathcal{C}_n}(z_1, z_2, \dots, z_n) = \frac{1}{n} \sum_{k|n} \phi(k) z_k^{\frac{n}{k}}, \qquad (2.1.11)$$

здесь суммирование ведётся по всем делителям d числа n.

2.2. ТЕОРЕМА ПОЙА

2.2.1. Группы и эквивалентность функций

2.2.1.1. GH-эквивалентность

Рассмотрим множества $X = \{1, 2, \dots, m\}$ и $Y = \{y_1, y_2, \dots, y_n\}$. Каждой функции $f: X \to Y$ поставим в соответствие вектор $\sigma = \langle f(1), f(2), \dots, f(m) \rangle$. Пусть $\mathcal{G}$ — группа подстановок степени m, действующая на множестве X, $\mathcal{H}$ — группа подстановок степени n на Y. Для подстановок $g \in \mathcal{G}$ и $h \in \mathcal{H}$ определим операцию действия g и h на функцию f слева и справа, соответственно, приводящую к новой функции $f': X \to Y$, следующим образом. Будем считать, что $f' = g \circ \circ f \circ h$, если для соответствующих векторов σ и σ' имеет место равенство

$$\langle f'(1), f'(2), \dots, f'(m) \rangle =$$
$$= \langle h\Big(f\big(g(1)\big)\Big), h\Big(f\big(g(2)\big)\Big), \dots, h\Big(f\big(g(1)\big)\Big) \rangle.$$

Введём на множестве Y^X всех функций из X в Y бинарное отношение $\sim$: $f \sim f'$ в том и только том случае, когда существуют такие $g \in \mathcal{G}$ и $h \in \mathcal{H}$, что $f' = g \circ f \circ h$. Если взять $g = \mathrm{I}$, $h = \mathrm{I}$, то $f = g \circ \circ f \circ h$, поэтому $\sim$ рефлексивно. Далее, если $f' = g \circ f \circ h$, то $f = = g^{-1} \circ f' \circ h^{-1}$, $g^{-1} \in \mathcal{G}$, $h^{-1} \in \mathcal{H}$, следовательно, из $f \sim f'$ следует $f' \sim f$ и $\sim$ симметрично. Наконец, пусть $f \sim f'$, $f' \sim f''$. Это значит, что $f' = g \circ f \circ h$, $g \in \mathcal{G}$, $h \in \mathcal{H}$, $f'' = g' \circ f' \circ h'$, $g' \in \mathcal{G}$, $h' \in \mathcal{H}$. Тогда $f'' = g' \circ f' \circ h' = g' \circ (g \circ f \circ h) \circ h' = (g' \cdot g) \circ f \circ (h \cdot h')$.

По определению группы $g' \cdot g \in \mathcal{G}$, $h \cdot h' \in \mathcal{H}$, следовательно, $f \sim f''$ и бинарное отношение $\sim$ транзитивно. Итак, доказано, что $\sim$ является эквивалентностью. Будем называть его *GH-эквивалентностью*. Как любая эквивалентность, она разбивает множество Y^X функций f, а значит, и множество соответствующих векторов f', на классы *GH*-эквивалентности. Их удобнее описывать именно как классы векторов f'.

Пример: пусть $X = \{1, 2, 3\}$, $Y = \{a, b\}$, множество векторов, соответствующих функциям из Y^X: $\{\langle a, a, a \rangle, \langle b, a, a \rangle, \langle a, b, a \rangle, \langle a, a, b \rangle,$

$\langle b,b,a\rangle, \langle b,a,b\rangle, \langle b,b,a\rangle, \langle b,b,b\rangle\}$, $\mathcal{G}$ — группа подстановок степени 3:

$$\mathcal{G} = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\};$$

$\mathcal{H}$ — симметрическая группа степени 2:

$$\mathcal{H} = \left\{\begin{pmatrix}a & b\\ a & b\end{pmatrix}, \begin{pmatrix}a & b\\ b & a\end{pmatrix}\right\}.$$

Тогда на множестве Y^X имеются два класса GH-эквивалентности, представителями которых могут быть векторы $\langle a,a,a\rangle$ и $\langle a,a,b\rangle$.

2.2.1.2. Лемма Бернсайда

Пусть $\mathcal{G}$ — группа подстановок, действующая на множестве $A = \{1, 2, \dots, n\}$ (в качестве A можно взять любое (n)-множество). Определим на элементах A бинарное отношение $\sim$, полагая, что $a \sim b$ для a, $b \in A$ в том случае, если существует такая подстановка $g \in \mathcal{G}$, что $b = g(a)$. Нетрудно доказать, что $\sim$ является эквивалентностью, следовательно, фактор-множество $A/\sim$ является разбиением A. Блоки этого разбиения называются *орбитами* группы $\mathcal{G}$, или её *областями транзитивности.* Введённое в пункте 2.1.2.1 понятие орбиты подстановки совпадает с определением орбиты группы в случае циклической группы, состоящей из всех степеней этой подстановки.

Стабилизатором $\mathcal{G}(a)$ элемента $a \in A$ относительно группы $\mathcal{G}$ называется множество подстановок из $\mathcal{G}$, оставляющих a на месте, т. е. $\mathcal{G}(a) = \{g \in \mathcal{G} | g(a) = a\}$. Очевидно, что для любого $a \in A$ стабилизатор $\mathcal{G}(a)$ является подгруппой группы $\mathcal{G}$, так как $\mathrm{I} \in \mathcal{G}(a)$, $(g \cdot g')(a) = g'(g(a)) = g'(a) = a$, если g, $g' \in \mathcal{G}(a)$; для любого $g \in \mathcal{G}(a)$ g^{-1} также принадлежит $\mathcal{G}(a)$, поскольку равенство $g(a) = a$ равносильно $a = g^{-1}(a)$. Если $b = g(a)$, $g \in \mathcal{G}$ (это означает, что a и b лежат в одной и той же орбите группы $\mathcal{G}$), то стабилизаторы $\mathcal{G}(a)$ и $\mathcal{G}(b)$ сопряжены в $\mathcal{G}$, т. е.

$$\mathcal{G}(b) = g^{-1}\mathcal{G}(a)g. \tag{2.2.1}$$

Действительно, если $g' \in \mathcal{G}(b)$, то $b = g'(b)$. Отсюда следует

$$g(a) = g'(b) \Leftrightarrow a = g^{-1}\big(g'(b)\big) = g^{-1}\Big(g'\big(g(a)\big)\Big) =$$

$$= (g \cdot g' \cdot g^{-1})(a) \;\Rightarrow\; g'' = g \cdot g' \cdot g^{-1} \in \mathcal{G}(a) \;\Leftrightarrow$$

$$\Leftrightarrow\ g' = g^{-1} \cdot g'' \cdot g,\ g'' \in \mathcal{G}(a),$$

а это значит, что $g' \in g^{-1}\mathcal{G}(a)g$. Этим доказано $\mathcal{G}(b) \subseteq g^{-1}\mathcal{G}(a)$. Включение $g^{-1}\mathcal{G}(a)g \subseteq \mathcal{G}(b)$ доказывается обратной цепочкой рассуждений. Равенство (2.2.1) доказано.

Лемма 2.2.1 (Бернсайда)

Число орбит $N(\mathcal{G})$ группы $\mathcal{G}$ подстановок, действующих на множестве A, равно среднему арифметическому чисел циклов единичной длины в подстановках группы $\mathcal{G}$:

$$N(\mathcal{G}) = \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} k_1(g),$$

где $k_1(g)$ — число циклов единичной длины в подстановке g.

Доказательство

Рассмотрим разбиение группы $\mathcal{G}$ на правые смежные классы по стабилизатору $\mathcal{G}(a)$: $\mathcal{G} = \mathcal{G}(a) \cup \mathcal{G}(a)g_1 \cup \ldots \cup \mathcal{G}(a)g_{l-1}$, где $a \in A$, l — число представителей смежных классов группы $\mathcal{G}$. Пусть $a_i = g_i(a)$, $i = 1,\ 2, \ldots, l-1$, покажем, что множество $\tilde{A} = \tilde{A}(a) = \{a, a_1, a_2, \ldots, a_{l-1}\}$ представляет собой орбиту группы $\mathcal{G}$, представителем которой является элемент a. Поскольку все g_i являются представителями смежных классов $\mathcal{G}$, $a_i = g_i(a)$, то все a_i принадлежат орбите $\mathcal{G}$ с представителем a. Докажем, что других элементов в этой орбите быть не может. Предположим, что в орбите существует элемент $\bar{a} \notin \tilde{A}$. Это значит, что при некоторой подстановке $\bar{g} \in \mathcal{G}$ $\bar{a} = \bar{g}(a)$. Так как смежные классы образуют разбиение, то $\bar{g}$ принадлежит одному из них, который обозначим $\mathcal{G}(a)g_i$. Тогда при некоторой подстановке $g \in \mathcal{G}(a)$ $\bar{g} = g \cdot g_i$. Отсюда следует, что

$$\bar{a} = \bar{g}(a) = (g \cdot g_i)(a) = g_i(g(a)) = g_i(a) = a_i \in \tilde{A},$$

а это противоречит предположению. Итак, получаем, что $l = \left|\tilde{A}(a)\right|$ и по теореме Лагранжа

$$\left|\tilde{A}(a)\right||\mathcal{G}(a)| = |\mathcal{G}|, \tag{2.2.2}$$

т. е. для любого элемента a из орбиты $\tilde{A}(a)$ группы $\mathcal{G}$ справедливо равенство (2.2.2).

Пусть $A_1,\ A_2,\ \dots,\ A_{N(\mathcal{G})}$ — орбиты группы $\mathcal{G}$ на множестве A и для всех $i = 1,\ 2,\ \dots,\ N(\mathcal{G})$ элемент a_i принадлежит A_i. Тогда согласно формуле (2.2.2) имеем

$$|\mathcal{G}| = \left|\tilde{A}(a_i)\right||\mathcal{G}(a_i)| = |A_i||\mathcal{G}(a_i)|. \qquad (2.2.3)$$

Если теперь просуммировать равенства (2.2.3) по всем i от 1 до $N(\mathcal{G})$, то получим

$$N(\mathcal{G})|\mathcal{G}| = \sum_{i=1}^{N(\mathcal{G})} |A_i||\mathcal{G}(a_i)|.$$

Выше мы убедились в том, что если a и a_i принадлежат одной и той же орбите, то $|\mathcal{G}(a)| = |\mathcal{G}(a_i)| = l$, поэтому последнее соотношение можно записать так:

$$N(\mathcal{G})|\mathcal{G}| = \sum_{i=1}^{N(\mathcal{G})} \sum_{a\in A_i} |\mathcal{G}(a)| = \sum_{a\in A} |\mathcal{G}(a)|.$$

С другой стороны,

$$\sum_{a\in A} |\mathcal{G}(a)| = \sum_{a\in A} \sum_{g\in\mathcal{G}(a)} 1 =$$

$$= \sum_{g\in\mathcal{G}} \sum_{\substack{a\in A \\ g(a)=a}} 1 = \sum_{g\in\mathcal{G}} k_1(g).$$

Приравнивая выражения для одной о той же величины, получаем

$$N(\mathcal{G})|\mathcal{G}| = \sum_{g\in\mathcal{G}} k_1(g),$$

откуда и следует утверждение леммы. ■

2.2.1.3. Число классов GH-эквивалентности

Пусть $\mathcal{G}$ и $\mathcal{H}$ — группы подстановок, действующие на множествах X, Y, соответственно (здесь используются обозначения пункта 2.2.1.1). Построим множество подстановок $\mathcal{H}^{\mathcal{G}}$, действующих на Y^X. Будем считать, что пара $\langle g, h\rangle \in \mathcal{H}^{\mathcal{G}}$, $g \in \mathcal{G}$, $h \in \mathcal{H}$, действует на элемент $f \in Y^X$ следующим образом: $\langle g, h\rangle(f) = f'$ тогда и только тогда, когда $g \circ f \circ h = f'$, $f, f' \in Y^X$.

На множестве $\mathcal{H}^{\mathcal{G}}$ определим операцию умножения $\otimes$, полагая

$$\langle g, h\rangle \otimes \langle g', h'\rangle = \langle g \cdot g', h \cdot h'\rangle. \qquad (2.2.4)$$

Эта операция ассоциативна в силу ассоциативности операций умножения $\cdot$ в группах $\mathcal{G}$ и $\mathcal{H}$. Обратным по отношению к элементу $\langle g, h\rangle$ является элемент $\langle g^{-1}, h^{-1}\rangle$, в чём можно убедиться непосредственной подстановкой. Единичный элемент в $\mathcal{H}^{\mathcal{G}}$ имеет вид $\langle \mathrm{I}, \mathrm{I}'\rangle$, где I, I'— единичные элементы в группах $\mathcal{G}$ и $\mathcal{H}$, соответственно. Следовательно, множество $\mathcal{H}^{\mathcal{G}}$ является группой подстановок. Эту группу называют *степенной группой.* Степень группы равна числу элементов в Y^X, т. е. $|Y|^{|X|} = n^m$. Порядок равен числу её элементов, т. е. $|\mathcal{G}||\mathcal{H}|$.

Определим теперь на Y^X бинарное отношение $\sim$ по аналогии с такими же отношениями на других множествах с действующими на них группами: $f \sim f'$ тогда и только тогда, когда $\langle g, h\rangle(f) = f'$ для некоторого элемента $\langle g, h\rangle \in \mathcal{H}^{\mathcal{G}}$. Нетрудно доказать, что $\sim$ является эквивалентностью, следовательно, Y^X разбивается на классы эквивалентности по $\sim$ — орбиты группы $\mathcal{H}^{\mathcal{G}}$.

Применяя лемму Бернсайда, найдём число классов GH-эквивалентности.

Теорема 2.2.1

Число классов GH-эквивалентности на множестве Y^X равно

$$N(\mathcal{G}, \mathcal{H}) =$$

$$= \frac{1}{|\mathcal{G}||\mathcal{H}|} \sum_{g \in \mathcal{G}} \sum_{h \in \mathcal{H}} \prod_{j=1}^{m} \left(\sum_{r|j} r k_r(h) \right)^{k_j(g)},$$

где внутреннее суммирование ведётся по всем делителям j, $k_j(g)$ — число циклов длины j в подстановке g.

Доказательство

Из определения следует, что GH-эквивалентность совпадает с эквивалентностью, определяемой степенной группой $\mathcal{H}^{\mathcal{G}}$ на множестве Y^X. Поэтому по лемме Бернсайда имеем

$$N(\mathcal{G},\mathcal{H}) = \frac{1}{|\mathcal{G}||\mathcal{H}|}\sum_{g\in\mathcal{G}}\sum_{h\in\mathcal{H}}\sum_{\substack{f\in Y^X\\ g\circ f\circ h=f}} 1,$$

внутренняя сумма берётся по всем неподвижным точкам подстановки $\langle g,h\rangle$, т. е. её циклам длины 1. Для доказательства теоремы осталось вычислить эту сумму, т. е. найти число функций $f\in Y^X$, удовлетворяющих условию $g\circ f\circ h=f$.

Пусть орбита подстановки $g\in\mathcal{G}$, содержащая элемент $x\in X$, состоит из элементов x, $g(x), \dots,$ $g^{j-1}(x)$. Тогда их образами при функции f, удовлетворяющей условию $g\circ f\circ h=f$, будут соответственно элементы $f(x)$, $h^{-1}(f(x)), \dots,$ $h^{-j+1}(f(x))$ (проверяется непосредственным вычислением). Отсюда следует, что если r — число элементов орбиты подстановки $h\in\mathcal{H}$, содержащей элемент $f(x)$, то r является делителем j. В данном случае (т. е. когда $g\circ f\circ h=f$) функция f однозначно определяется указанием в качестве образа x одного из r элементов области транзитивности цикла длины r подстановки h. Поэтому число способов выбора образа элемента x, который принадлежит орбите с j элементами подстановки $h\in\mathcal{H}$, равно

$$\sum_{r|j} rk_r(h).$$

Поскольку выбор значений образов различных элементов осуществляется независимо, то по правилу произведения

$$\sum_{\substack{f\in Y^X\\ g\circ f\circ h=f}} 1 = \prod_{j=1}^{m}\left(\sum_{r|j} rk_r(h)\right)^{k_j(g)},$$

где

$$\left(\sum_{r|j} rk_r(h)\right)^{k_j(g)} = 1,$$

$$k_j(g) = 0.$$

Теорема доказана. ■

2.2.2. Теорема Пойа о перечислении и её применение

2.2.2.1. Основная теорема

Пусть $f: X \to Y$ — функция из (m)-множества X в (n)-множество Y. В теории Пойа такие функции называются *отображениями.* В рамках этой теории разработан наиболее общий алгебраический метод перечисления классов эквивалентности отображений относительно групп подстановок. По терминологии Пойа элементы множества X называются *местами*, элементы Y — *фигурами*, элементы множества Y^X всех отображений X в Y — *конфигурациями.*

Группа подстановок $\mathcal{G}$ действует на множестве X и определяет отношение эквивалентности на Y^X по традиционному правилу: f эквивалентно f' (f, $f' \in Y^X$) в том и только том случае, когда $f' = gf$ при некоторой подстановке $g \in \mathcal{G}$. То, что описанное бинарное отношение на Y^X действительно является эквивалентностью, доказывается аналогично всем предыдущим эквивалентностям $\sim$.

Каждому элементу Y поставим в соответствие вектор длины k с координатами из некоторого дискретного числового кольца $\mathcal{K}$. Этот вектор называется *характеристикой фигуры* y и обозначается $\omega(y) = \langle \omega_1, \omega_2, \dots, \omega_k \rangle$, $\omega_i \in \mathcal{K}$. Характеристика $\omega(y)$ является образом фигуры y при некотором отображении $\omega: Y \to \mathcal{K}^k$, которое называется *весом фигур.*

Характеристику конфигурации $f \in Y^X$ определим формулой

$$W(f) = \sum_{x \in X} \omega(f(x)),$$

т. е. она равна сумме характеристик всех фигур (сумма векторов понимается как вектор, координаты которого равны суммам соответствующих координат слагаемых). Таким образом, определено отображение $W: Y^X \to \mathcal{K}^k$, которое будем называть *весом конфигураций*.

Пусть $a(\omega_1, \omega_1, \dots, \omega_k)$ — число фигур $y \in Y$, имеющих характеристику $\langle \omega_1, \omega_2, \dots, \omega_k \rangle$. Составим для неё формальный степенной ряд

$$F(z_1, z_2, \dots, z_k) = \sum_{\langle \omega_1, \omega_2, \dots, \omega_k \rangle} a(\omega_1, \omega_1, \dots, \omega_k) z_1^{\omega_1} z_2^{\omega_2} \cdots z_k^{\omega_k},$$

где суммирование ведётся по всем значениям весов фигур. По аналогии с (одномерной) производящей функцией, $F(z_1, z_2, \dots, z_k)$ будем называть *производящей функцией весовой спецификации фигур*. Из определения характеристики конфигурации следует, что для эквивалентных относительно группы подстановок $\mathcal{G}$ конфигураций их веса совпадают (это обусловливается коммутативностью сложения в числовом поле $\mathcal{K}$). Обозначим через $b_m(\omega_1, \omega_1, \dots, \omega_k)$ число неэквивалентных конфигураций $f \in Y^X$ с характеристикой $\langle \omega_1, \omega_2, \dots, \omega_k \rangle$ и составим для $b_m(\omega_1, \omega_1, \dots, \omega_k)$ производящую функцию

$$\Phi_m(z_1, z_2, \dots, z_k) = \sum_{\langle \omega_1, \omega_2, \dots, \omega_k \rangle} b_m(\omega_1, \omega_1, \dots, \omega_k) z_1^{\omega_1} z_2^{\omega_2} \cdots z_k^{\omega_k},$$

где суммирование ведётся по всем значениям весов конфигураций. Функция $\Phi_m(z_1, z_2, \dots, z_k)$ называется *производящей функцией весовой спецификации конфигураций*, не эквивалентных относительно группы $\mathcal{G}$. Цикловой индекс группы $\mathcal{G}$ представляет собой многочлен

$$P_{\mathcal{G}}(z_1, z_2, \dots, z_m) =$$
$$= \frac{1}{|\mathcal{G}|} \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_m \rangle \\ 0 \le \alpha_i \le m \\ i = 1, \dots, m \\ \alpha_1 + 2\alpha_2 + \dots + m\alpha_m = m}} C_{\mathcal{G}}(\alpha_1, \alpha_2, \dots, \alpha_m) z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_m^{\alpha_m}, \qquad (2.2.5)$$

где $C_{\mathcal{G}}(\alpha_1, \alpha_2, \dots, \alpha_m)$ — число элементов группы подстановок $\mathcal{G}$ циклового класса $1^{\alpha_1} 2^{\alpha_2} \dots m^{\alpha_m}$, и суммирование ведётся по всем таким векторам $\langle \alpha_1, \alpha_2, \dots, \alpha_m \rangle$, что $\alpha_1 + 2\alpha_2 + \dots + m\alpha_m = m$. Теперь можно сформулировать *теорему Пойа*.

Теорема 2.2.2 (теорема Пойа)

$$\Phi_m(z_1, z_2, \dots, z_k) =$$
$$= P_{\mathcal{G}}(F(z_1, z_2, \dots, z_k), F(z_1^2, z_2^2, \dots, z_k^2), \dots, F(z_1^m, z_2^m, \dots, z_k^m)).$$

Доказательство

Определим гомоморфизм $\varphi: \mathcal{G} \to \mathcal{G}'$, где $\mathcal{G}' = \varphi(\mathcal{G})$ — образ группы подстановок $\mathcal{G}$ при гомоморфизме φ, являющийся группой подстановок на множестве Y^X, следующим образом. Полагаем $\varphi(g) = g'$, $g \in \mathcal{G}$, $g' \in \mathcal{G}'$, если

$$g'(f) = f\big(g(x)\big) \tag{2.2.6}$$

для всех $x \in X$, $f \in Y^X$. Очевидно, $\mathcal{G}'$ является степенной группой с группой подстановок, действующих на Y, состоящей из единственной, тождественной, подстановки. Тогда то, что отображение φ гомоморфно, следует из (2.2.6) и из определения операции умножения $\otimes$ (2.2.4) на степенных группах.

С помощью группы $\mathcal{G}'$ можно ввести на множестве Y^X отношение эквивалентности $\approx$: $f \approx f'$, если $g'(f) = f'$ при некотором $g' \in \mathcal{G}'$. Очевидно, что если $f \sim f'$, где $\sim$ есть G-эквивалентность (т. е. $f \sim f'$ в том случае, когда $f(x) = f(g(x))$ при некотором $g \in \mathcal{G}$), то $f \approx f'$ и наоборот. Следовательно, отношения $\sim$ и $\approx$ совпадают.

Обозначим через $b_m(\omega_1, \omega_1, \dots, \omega_k;\ g')$ число неэквивалентных конфигураций с характеристикой $\langle \omega_1, \omega_2, \dots, \omega_k \rangle$, являющихся неподвижными точками подстановки $g' \in \mathcal{G}'$. По лемме Бернсайда

$$b_m(\omega_1, \omega_1, \dots, \omega_k) = \frac{1}{|\mathcal{G}'|} \sum_{g' \in \mathcal{G}'} b_m(\omega_1, \omega_1, \dots, \omega_k;\ g').$$

Пусть $\mathcal{H}g$ — правый смежный класс группы $\mathcal{G}$ по подгруппе $\mathcal{H} = \ker \varphi$ (напомним, что $\ker \varphi$ — ядро гомоморфизма φ). Из условия (2.2.6) следует $f(h(g(x))) = f(x)$ для любого $x \in X$, где $h \in \mathcal{H}$. Следовательно, если $\mathcal{S}$ — произвольная система представителей правых смежных классов $\mathcal{G}$ по подгруппе $\mathcal{H}$, то

$$\frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} b_m(\omega_1, \omega_1, \dots, \omega_k;\ g) = \frac{1}{|\mathcal{G}|} \sum_{s \in \mathcal{S}} \sum_{h \in \mathcal{H}} b_m(\omega_1, \omega_1, \dots, \omega_k; h \cdot s) =$$

$$= \frac{1}{|\mathcal{G}'|} \sum_{g' \in \mathcal{G}'} b_m(\omega_1, \omega_1, \dots, \omega_k;\ g')$$

(здесь были применены лемма 2.1.1 и теорема Лагранжа из пункта 2.1.1.4). Теперь из леммы Бернсайда следует

$$b_m(\omega_1, \omega_1, \dots, \omega_k) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} b_m(\omega_1, \omega_1, \dots, \omega_k;\ g). \qquad (2.2.7)$$

Составим производящую функцию чисел $b_m(\omega_1, \omega_1, \dots, \omega_k;\ g)$:

$$\Phi_m(z_1, z_2, \dots, z_k; g) = \sum_{\langle \omega_1, \omega_2, \dots, \omega_k \rangle} b_m(\omega_1, \omega_1, \dots, \omega_k; g) z_1^{\omega_1} z_2^{\omega_2} \cdots z_k^{\omega_k},$$

где суммирование ведётся по всем векторам характеристик конфигураций, не изменяющихся при действии подстановки $g \in \mathcal{G}$, т. е. по классам не эквивалентных относительно g конфигураций.

Пусть $f\big(g(x)\big) = f(x)$ для всех $g \in \mathcal{G}$ и всех $x \in X$, т. е. f — неподвижная точка гомоморфизма φ. Разложим подстановку $g \in \mathcal{G}$ в произведение независимых циклов $g = g_1 g_2 \cdots g_t$. Если X_j — орбита из l_j элементов, на которой действует цикл g_j, то для $x \in X_j$ имеют место равенства $f\left(g_j(x)\right) = f\left(g_j^2(x)\right) = \cdots = f\left(g_j^{l_j}(x)\right) = f(x)$. Это означает, что конфигурация f постоянна на X_j. Следовательно, любая конфигурация, инвариантная относительно действия подстановки g, может быть однозначно определена значениями f на орбитах X_1, X_2, … , X_t подстановки g. Пусть $b_m\big(\omega_1^{(j)},\ \omega_2^{(j)}, \dots,\ \omega_k^{(j)};\ g_j\big)$ — число конфигураций с характеристикой $\left\langle \omega_1^{(j)}, \dots, \omega_k^{(j)} \right\rangle$, являющихся сужениями на орбиту X_j всего множества конфигураций, инвариантных относительно действия цикла g_j. Тогда число конфигураций — неподвижных точек φ, т. е. инвариантных при всей подстановке g, имеющих характеристику $\langle \omega_1, \omega_2, \dots, \omega_k \rangle$, равно

$$b_m(\omega_1, \omega_2, \dots, \omega_k; g) =$$

$$= \sum_{\substack{\omega_1^{(1)} + \omega_1^{(2)} + \cdots + \omega_1^{(t)} = \omega_1 \\ \omega_2^{(1)} + \omega_2^{(2)} + \cdots + \omega_2^{(t)} = \omega_2 \\ \vdots \\ \omega_k^{(1)} + \omega_k^{(2)} + \cdots + \omega_k^{(t)} = \omega_k}} b_m\big(\omega_1^{(1)}, \omega_2^{(1)}, \dots, \omega_k^{(1)};\ g_1\big) \times \qquad (2.2.8)$$

$$\times\, b_m\big(\omega_1^{(2)}, \omega_2^{(2)}, \dots, \omega_k^{(2)};\ g_2\big) \cdots b_m\big(\omega_1^{(t)}, \omega_2^{(t)}, \dots, \omega_k^{(t)};\ g_t\big).$$

Суммирование здесь ведётся по всем весовым векторам $\left\langle\omega_1^{(1)},\omega_2^{(1)},\dots,\omega_k^{(1)}\right\rangle$, $\langle\omega_1^{(2)},\omega_2^{(2)},\dots,\omega_k^{(2)}\rangle,\dots$, $\langle\omega_1^{(t)},\omega_2^{(t)},\dots,\omega_k^{(t)}\rangle$, удовлетворяющим указанным под знаком суммы равенствам.

Для каждого цикла g_j построим производящую функцию чисел конфигураций, инвариантных при действии g_j:

$$\Phi_m(z_1,z_2,\dots,z_k;g_j)=\sum_{\langle\omega_1,\omega_2,\dots,\omega_k\rangle} b_m(\omega_1,\omega_1,\dots,\omega_k;g_j)z_1^{\omega_1}z_2^{\omega_2}\cdots z_k^{\omega_k}.$$

Производящая функция чисел $b_m(\omega_1,\omega_1,\dots,\omega_k;\ g)$ с учётом (2.2.8) равна

$$\Phi_m(z_1,z_2,\dots,z_k;g)=$$

$$=\sum_{\langle\omega_1,\omega_2,\dots,\omega_k\rangle}\left(\sum_{\substack{\omega_1^{(1)}+\omega_1^{(2)}+\cdots+\omega_1^{(t)}=\omega_1\\ \vdots\\ \omega_k^{(1)}+\omega_k^{(2)}+\cdots+\omega_k^{(t)}=\omega_k}} b_m\left(\omega_1^{(1)},\omega_2^{(1)},\dots,\omega_k^{(1)};\ g_1\right)\times\right.$$

$$\left.\times\, b_m\left(\omega_1^{(2)},\omega_2^{(2)},\dots,\omega_k^{(2)};\ g_2\right)\cdots b_m\left(\omega_1^{(t)},\omega_2^{(t)},\dots,\omega_k^{(t)};\ g_t\right)\right)\times$$

$$\times\, z_1^{\omega_1}z_2^{\omega_2}\cdots z_k^{\omega_k}=$$

$$=\Phi_m(z_1,z_2,\dots,z_k;g_1)\Phi_m(z_1,z_2,\dots,z_k;g_2)\cdots\Phi_m(z_1,z_2,\dots,z_k;g_t).$$

Пусть $f(g(x))=f(x)$ для всех $g\in\mathcal{G}$ и для всех $x\in X$, а $\overline{y}$ — постоянное значение, принимаемое конфигурацией f на орбите X_j длины l_j, соответствующей циклу g_j подстановки $g\in\mathcal{G}$. Если $\omega(\overline{y})=$ $=\langle\omega_1,\omega_2,\dots,\omega_k\rangle$, то характеристика сужения конфигурации на орбиту X_j равна $\langle\omega_1 l_j,\ \omega_2 l_j,\dots,\omega_k l_j\rangle$. Следовательно, производящая функция $\Phi_m(z_1,z_2,\dots,z_k;g_j)$ равна

$$\Phi_m(z_1,z_2,\dots,z_k;g_j)=\sum_{\langle\omega_1,\omega_2,\dots,\omega_k\rangle} a(\omega_1,\omega_1,\dots,\omega_k)z_1^{\omega_1 l_j}z_2^{\omega_2 l_j}\cdots z_k^{\omega_k l_j}.$$

Поэтому для производящей функции чисел $a(\omega_1,\omega_1,\dots,\omega_k)$ фигур $y\in Y$ с характеристикой $\langle\omega_1,\omega_2,\dots,\omega_k\rangle$ имеет место соотношение

$$F\left(z_1^{\omega_1 l_j}, z_2^{\omega_2 l_j}, \dots, z_k^{\omega_k l_j}\right) = \Phi_m\big(z_1, z_2, \dots, z_k; g_j\big). \quad (2.2.9)$$

Теперь найдём производящую функцию весовой спецификации конфигураций, не эквивалентных относительно группы $\mathcal{G}$. С учётом равенства (2.2.7) получаем

$$\Phi_m(z_1, z_2, \dots, z_k) = \sum_{\langle\omega_1, \omega_2, \dots, \omega_k\rangle} b_m(\omega_1, \omega_1, \dots, \omega_k) z_1^{\omega_1} z_2^{\omega_2} \cdots z_k^{\omega_k} =$$

$$= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \Phi_m(z_1, z_2, \dots, z_k; g) =$$

$$= \frac{1}{|\mathcal{G}|} \sum_{j_1 + 2j_2 + \dots + mj_m = m} C(j_1, j_2, \dots, j_m;\ \mathcal{G})\, \Phi_m(z_1, z_2, \dots, z_k; g_1) \times$$

$$\times\, \Phi_m(z_1, z_2, \dots, z_k; g_2) \cdots \Phi_m(z_1, z_2, \dots, z_k; g_t).$$

Подставляя в последнюю формулу (2.2.8), имеем

$$\Phi_m(z_1, z_2, \dots, z_k) = \frac{1}{|\mathcal{G}|} \sum_{j_1 + 2j_2 + \dots + mj_m = m} C(j_1, j_2, \dots, j_m;\ \mathcal{G}) \times$$

$$\times\, F^{j_1}(z_1, z_2, \dots, z_k) F^{j_2}(z_1^2, z_2^2, \dots, z_k^2) \cdots F^{j_m}(z_1^m, z_2^m, \dots, z_k^m).$$

Если теперь сравнить это выражение с определением циклового индекса (2.2.5), то приходим к доказываемой формуле. ■

Теорема Пойа о перечислении, основанная на математическом аппарате теории групп, является очень эффективным инструментом для решения перечислительных комбинаторных задач. Далее рассматриваются конкретные примеры применения теоремы Пойа.

2.2.2.2. Задача о числе (m)-мультимножеств

Пусть Y^X — совокупность отображений (функций) $f: X \to Y$, где $X = \{1, 2, \dots, m\}$, $Y = \{y_1, y_2, \dots, y_n\}$. На множестве X действует группа подстановок $\mathcal{G}$, определяющая отношение G-эквивалентности на Y^X: $f \sim f'$, f, $f' \in Y^X$, в том и только том случае, когда $f(g(x)) = f'(x)$ для всех $x \in X$ при некотором $g \in \mathcal{G}$. В качестве характеристики фигуры $y_i \in Y$ возьмём n-мерный вектор $\omega(y_i) = \langle 0, \dots, 0, \underbrace{1}_{i}, 0, \dots, 0\rangle$,

в котором единственная i-я ненулевая координата равна 1. При этих условиях производящая функция весовой спецификации фигур имеет вид $F(z_1, z_2, \dots, z_n) = z_1 + z_2 + \dots + z_n$.

Каждой конфигурации соответствует m-мультимножество первичной спецификации $y_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$, составленное из α_1 элементов y_1, α_2 элементов y_2, … , α_n элементов y_n, где α_i — количество чисел x от 1 до m (элементов множества X), для которых $f(x) = y_i$ $(\alpha_1 + \alpha_2 + \dots + \alpha_n = m)$. Очевидно, что конфигурация f имеет первичную спецификацию $y_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$ в том, и только том случае, когда её вес равен $\omega(f) = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$. Составим производящую функцию чисел $C_m(\alpha_1, \alpha_2, \dots, \alpha_n; \mathcal{G})$ конфигураций, имеющих первичную спецификацию $y_1^{\alpha_1}\, y_2^{\alpha_2} \dots y_n^{\alpha_n}$, не эквивалентных относительно группы $\mathcal{G}$:

$$\Phi_m(z_1, z_2, \dots, z_n; \mathcal{G}) = \\ = \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ \alpha_1 + +\alpha_2 + \dots + \alpha_n = m}} C_m(\alpha_1, \alpha_2, \dots, \alpha_n;\, \mathcal{G})\, z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}.$$

Согласно теореме Пойа она равна

$$\Phi_m(z_1, z_2, \dots, z_n; \mathcal{G}) = \\ = P_{\mathcal{G}}(z_1 + \dots + z_n, z_1^2 + \dots + z_n^2, \dots, z_1^m + \dots + z_n^m), \quad (2.2.10)$$

где $P_{\mathcal{G}}(t_1, t_2, \dots, t_m)$ — цикловой индекс группы $\mathcal{G}$. Из этой формулы при $z_1 = z_2 = \dots = z_n = 1$ следует выражение для числа классов G-эквивалентности на множестве Y^X:

$$C_{mn}(\mathcal{G}) = P_{\mathcal{G}}(n, n, \dots, n). \quad (2.2.11)$$

Пусть $\mathcal{G} = \mathfrak{S}_m$ — симметрическая группа степени m. В этом случае два отображения f, $f' \in Y^X$ G-эквивалентны, если существует такая подстановка $g \in \mathfrak{S}_m$, что $g \circ f = f'$ (знак $\circ$ означает последовательное применение подстановки g и отображения f), или $f'(i) = f\big(g(i)\big)$, $i = 1, \dots, m$. Отсюда следует, что $f \sim f'$ тогда и только тогда, когда первичные спецификации f, f' совпадают, поэтому для произвольного представителя класса эквивалентности f его первичная спецификация $y_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$ $(\alpha_1 + \alpha_2 + \dots + \alpha_n = m)$ однозначно определяет этот класс эквивалентности. Фактически каждый класс эквивалентности однозначно определяется вектором $\langle \alpha_1, \alpha_2, \dots, \alpha_m \rangle$ с целыми неотрицательными координатами, в котором $\alpha_1 + \alpha_2 + \dots +$ $+\alpha_n = m$. Следовательно,

$$C_m(\alpha_1, \alpha_2, \dots, \alpha_n; \mathfrak{S}_m) = 1. \qquad (2.2.12)$$

Описанная комбинаторная схема называется *коммутативным несимметричным* (n)-базисом. Элемент системы представителей классов G-эквивалентности в рассматриваемом случае называется (m)-выборкой данного базиса. Каждой (m)-выборке ставится в соответствие совокупность векторов вида

$$\langle f(g(1)), f\big(g(2)\big), \dots, f\big(g(m)\big) \rangle,$$

где g принимает значения во всей симметрической группе подстановок $\mathfrak{S}_m$. Эта совокупность определяет (m)-сочетание с повторениями из n элементов ((m)-мультимножество). Отсюда следует, что каждой (m)-выборке в коммутативном несимметричном (n)-базисе взаимно однозначным образом соответствует повторное (m)-сочетание из n различных элементов.

Другим примером комбинаторной схемы отбора, описываемой коммутативной несимметричной схемой, является размещение m одинаковых предметов в n разных ячейках. Понятно, что каждое такое размещение однозначно определяется вектором $\langle \alpha_1, \alpha_2, \dots, \alpha_m \rangle$, где α_1, α_2, ..., α_m — целые неотрицательные числа, удовлетворяющие уравнению $\alpha_1 + \alpha_2 + \dots + \alpha_n = m$. Из изложенного выше следует, что размещениям m одинаковых предметов в n различных ячейках ставятся во взаимно однозначное соответствие (m)-выборки в коммутативном несимметричном (n)-базисе.

К примеру, статистика неразличимых частиц, в которой различные состояния (группы, ячейки) равновероятны (*статистика Бозе-Эйнштейна*), как раз и описывается схемой коммутативного несимметричного базиса.

С помощью теоремы Пойа вычислим количество классов эквивалентности в коммутативном несимметричном (n)-базисе. Из (2.2.12) следует, что

$$\Phi_m(z_1, z_2, \dots, z_n; \mathfrak{S}_m) = \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ \alpha_1 + + \alpha_2 + \dots + \alpha_n = m}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \Rightarrow$$

$$\Rightarrow \sum_{m=0}^{\infty} \Phi_m(z_1, z_2, \dots, z_n; \mathfrak{S}_m) t^m =$$

$$= \sum_{m=0}^{\infty} \left(\sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ \alpha_1 + + \alpha_2 + \dots + \alpha_n = m}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \right) t^m.$$

Далее, запишем следующее формальное равенство:

$$\frac{1}{1 - z_1 t} \cdot \frac{1}{1 - z_2 t} \cdot \dots \cdot \frac{1}{1 - z_n t} =$$

$$= (1 + z_1 t + z_1^2 t^2 + \cdots)(1 + z_2 t + z_2^2 t^2 + \cdots) \times$$

$$\times \cdots (1 + z_n t + z_n^2 t^2 + \cdots) =$$

$$= \left(\sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \\ \alpha_1 + + \alpha_2 + \dots + \alpha_n = m}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \right) t^m$$

(здесь применена известная формула суммы бесконечно убывающей геометрической прогрессии). Отсюда следует, что функция

$$f_{\Phi_m}(t) = \prod_{j=1}^{n} \left(1 - z_j t\right)^{-1}$$

является производящей для величин $\Phi_m(z_1, z_2, \dots, z_n; \mathfrak{S}_m)$. Преобразуем f_{Φ_m} следующим образом:

$$f_{\Phi_m}(t) = \prod_{j=1}^{n} \left(1 - z_j t\right)^{-1} = \exp\left(\sum_{j=1}^{n} \ln\left(1 - z_j t\right)^{-1} \right) =$$

$$= \exp\left(\sum_{k=1}^{\infty} \left(\sum_{j=1}^{n} z_j^k \right) \frac{t^k}{k} \right). \qquad (2.2.13)$$

Здесь было применено известное из математического анализа разложение функции $\ln(1 + z)$ в степенной ряд:

$$\ln(1+z)=\sum_{k=1}^{\infty}(-1)^{k-1}\frac{z^k}{k}.$$

Теперь, используя формулу(2.2.10), получаем из (2.2.12)

$$\sum_{m=0}^{\infty}\Phi_m(z_1,z_2,\dots,z_n;\mathcal{S}_m)t^m=$$

$$=\sum_{m=0}^{\infty}P_{\mathcal{G}}(z_1+\dots+z_n,z_1^2+\dots+z_n^2,\dots,z_1^m+\dots+z_n^m)t^m=$$

$$=\exp\left(\sum_{k=1}^{\infty}\left(\sum_{j=1}^{n}z_j^k\right)\frac{t^k}{k}\right).$$

Если в обеих частях последнего равенства положить $z_1=\dots=z_n=1$, то с учётом (2.2.13) находим

$$\sum_{m=0}^{\infty}P_{\mathfrak{S}_n}(n,n,\dots,n)\,t^m=\sum_{m=0}^{\infty}C_{mn}(\mathcal{S}_n)\,t^m=\exp\left(n\sum_{k=1}^{\infty}\frac{t^k}{k}\right)=$$

$$=\big(\exp(-\ln(1-t))\big)^n=(1-t)^{-n}. \qquad (2.2.14)$$

Применяя известное разложение функции $(1-t)^{-n}$ в ряд Ньютона

$$(1-t)^{-n}=\sum_{m=0}^{\infty}C_{n+m-1}^{m}t^m,$$

из (2.2.14) получаем

$$C_{mn}(\mathcal{S}_n)=C_{n+m-1}^{m}\text{ —}$$

общее число (m)-мультимножеств из n элементов, т. е. (m)-выборок в коммутативном несимметричном (n)-базисе.

2.2.2.3. Задача об ожерельях

Пусть имеется запас из n бусинок, содержащий по δ_i бусинок цвета c_i, $i=1,\,2,\,\dots,\,k$ $(\delta_1+\delta_2+\dots+\delta_k=n)$, бусинки одного цвета считаются неразличимыми. Расположим $m\le n$ выбранных из n бусинок в m равноотстоящих точках окружности. Класс таких расположений, совмещающихся циклическим сдвигом (поворотом) окружности, будем называть *ожерельем.* Таким образом, число различных ожерелий из m бусинок, взятых из данного запаса, равно количеству классов эквивалентности расположений бусинок на окружности относительно циклической группы C_m, состоящей из поворотов окружности на угол $\frac{\pi n}{m}$, $0 \le n \le m-1$.

Присвоим каждой бусинке номер от 1 до n, $Y = \{1, 2, \dots, n\}$ — множество номеров, $X = \{1, 2, \dots, m\}$ — множество позиций на окружности, на которые расставляются бусинки. Тогда каждое расположение бусинок на окружности определяется некоторым отображением $f: X \to Y$. Каждому ожерелью ставится во взаимно обратное соответствие класс эквивалентности на множестве Y^X, порождаемый циклической группой C_m. Отношение эквивалентности в данном случае определяется следующим образом. Отображение f эквивалентно f', если векторы $\langle f(1), f(2), \dots, f(m)\rangle$, $\langle f'(1), f'(2), \dots, f'(m)\rangle$ отличаются циклическим сдвигом.

Пусть $c_1^{\alpha_1} c_2^{\alpha_2} \dots c_k^{\alpha_k}$ — первичная спецификация цветов, где α_i — число бусинок цвета c_i в расположении на окружности, $1 \le i \le k$; $D_{C_m}(\alpha_1, \alpha_2, \dots, \alpha_k)$ — число не эквивалентных относительно группы C_m отображений $f \in Y^X$, имеющих первичную спецификацию $c_1^{\alpha_1} c_2^{\alpha_2} \dots c_k^{\alpha_k}$, т. е. ожерелий цветового состава, соответствующего спецификации. Тогда производящая функция весовой спецификации конфигураций имеет вид (напоминаем, что в качестве характеристики фигуры $y_i = i \in Y$ берётся k-вектор $\omega(y_i) = \langle 0, \dots, 0, 1, 0, \dots, 0\rangle$):

$$\Phi_m(z_1, z_2, \dots, z_k; C_m) =$$
$$= \sum_{\substack{\langle \alpha_1, \alpha_2, \dots, \alpha_k\rangle \\ 0 \le \alpha_i \le \delta_i \\ \alpha_1 + \alpha_2 + \dots + \alpha_k = m}} D_{C_m}(\alpha_1, \alpha_2, \dots, \alpha_k) z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_k^{\alpha_k}.$$

Цикловой индекс циклической группы C_m вычисляется по формуле (см. (2.1.11))

$$P_{C_m}(t_1, t_2, \dots, t_k) = \frac{1}{m} \sum_{d|m} \phi(d) t_d^{\frac{m}{d}},$$

где ф — функция Эйлера, суммирование ведётся по всем делителям числа m. Тогда для $\Phi_m(z_1, z_2, \dots, z_k; \mathcal{C}_m)$ в силу теоремы Пойа имеем формулу

$$\Phi_m(z_1, z_2, \dots, z_k; \mathcal{C}_m) = \frac{1}{m} \sum_{d|m} \phi(d) \left(\delta_1 z_1^d + \delta_2 z_2^d + \dots + \delta_k z_k^d\right)^{\frac{m}{d}}.$$

Преобразуем $\Phi_m(z_1, z_2, \dots, z_k; \mathcal{C}_m)$, используя полиномиальную формулу:

$$\Phi_m(z_1, z_2, \dots, z_k; \mathcal{C}_m) = \frac{1}{m} \sum_{d|\langle \alpha_1, \alpha_2, \dots, \alpha_k \rangle} \phi(d) \frac{(m/d)!}{(\alpha_1/d)! \cdots (\alpha_k/d)!} \times$$
$$\times\, \delta_1^{\frac{\alpha_1}{d}} \delta_2^{\frac{\alpha_2}{d}} \cdots \delta_k^{\frac{\alpha_k}{d}} z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_k^{\alpha_k},$$

где суммирование ведётся по всем делителям d наибольшего общего делителя чисел α_1, α_2, ..., α_k. Отсюда следует формула для числа ожерелий $D_{\mathcal{C}_m}(\alpha_1, \alpha_2, \dots, \alpha_k)$:

$$D_{\mathcal{C}_m}(\alpha_1, \alpha_2, \dots, \alpha_k) = \frac{1}{m} \sum_{d|\langle \alpha_1, \alpha_2, \dots, \alpha_k \rangle} \phi(d) \frac{(m/d)!}{(\alpha_1/d)! \cdots (\alpha_k/d)!} \times$$
$$\times\, \delta_1^{\frac{\alpha_1}{d}} \delta_2^{\frac{\alpha_2}{d}} \cdots \delta_k^{\frac{\alpha_k}{d}}.$$

3. ГРАФЫ

3.1. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ГРАФОВ

3.1.1. Граф. Компоненты и виды графов

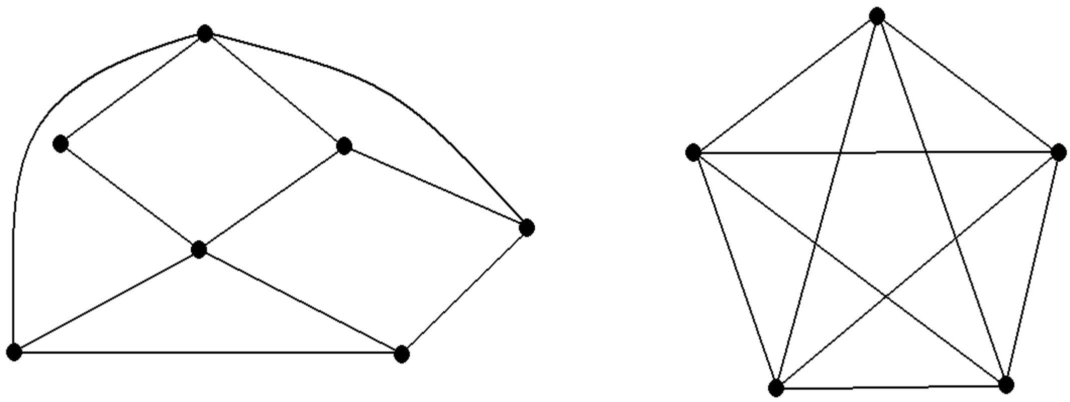
3.1.1.1. Понятие графа

Графом G называется абстрактный теоретико-множественный объект, представляющий собой упорядоченную пару множеств $G = \langle V, X \rangle$, где V — множество не более чем счётной мощности (т. е. либо конечное, либо счётно-бесконечное), X — некоторое подмножество множества неупорядоченных пар элементов V. Множество V называется *множеством вершин*, его элементы — *вершинами* графа, число $n = |V|$ называется *порядком* графа; X — *множество рёбер*, его элементы — *рёбра*. Если $X \subseteq V^2$, т. е. элементы X являются упорядоченными парами, то G называется *ориентированным графом*, или *орграфом.* Его рёбра называются *дугами.* Рёбра графа будем обозначать парой вершин в фигурных скобках, например, $x = \{u, v\}$ — ребро, соединяющее вершины u и v. Дуги будем обозначать парой вершин в угловых скобках: $x = \langle u, v \rangle$.

Пусть $x = \{u, v\} \in X$. В этом случае будем говорить, что вершины u и v *смежны*, ребро x инцидентно u и v; u, v — *концевые вершины* ребра x. Аналогично, если $x = \langle u, v \rangle$, то дуга x инцидентна u и v, которые являются концевыми вершинами дуги x, при этом u — *начальная*, v — *конечная* вершины x. Таким образом, отношение инцидентности есть отношение между разнородными элементами графа. Инцидентными или не инцидентными могут быть вершина и ребро или вершина и дуга.

Рёбра (дуги) называются *смежными*, если они инцидентны одной и той же вершине. Таким образом, смежность — отношение между однородными элементами графа: смежными или несмежными могут быть ребра (дуги) или вершины.

Граф $G = \langle V, X \rangle$ может быть изображён геометрически. Если вершинам поставить в соответствие точки плоскости, а рёбрам — линии, соединяющие точки, соответствующие их концевым вершинам, то получившийся рисунок называется *диаграммой* графа. Если при этом линии не пересекаются нигде, кроме вершин, то диаграмма графа называется его *топологической реализацией.* Не всякий граф имеет топологическую реализацию. На рис. 3.1.1 изображены диаграммы графов, допускающих (а) и не допускающих (б) такие реализации. Граф (б) играет важную роль в теории. Он имеет своё обозначение K_5.



а) Топологическая реализация графа (плоский граф)

б) Граф, не допускающий топологическую реализацию

Рис. 3.1.1

Граф, допускающий топологическую реализацию, называется *планарным.* Его топологическую реализацию, т. е. диаграмму, в которой линии пересекаются только в точках, соответствующих вершинам, будем называть *плоским* графом.

Орграф геометрически изображается точками, соответствующими вершинам, и стрелками, соответствующими дугам, причём стрелка направлена от начальной к конечной точке.

Граф называется *пустым*, если $V = \emptyset$, $X = \emptyset$. Обозначается пустой граф Λ. Противоположным пустому является *полный* граф — такой граф, в котором любые две несовпадающие вершины смежны. Полный граф с n вершинами обозначается K_n. Например, K_5 — полный граф с 5 вершинами.

Ребро (дугу), у которой обе концевые вершины совпадают, будем называть *петлёй.* Граф (орграф), содержащий петли, называется *псевдографом.* Рёбра, имеющие общие концевые вершины, называются *кратными.* Дуги называются *кратными,* если у них совпадают начальные и конечные вершины. Дуги называются *противоположными*, если начальная вершина одной является конечной вершиной другой и наоборот. Граф (орграф), содержащий кратные рёбра (дуги), называется *мультиграфом.* Граф называется *конечным*, если его множества вершин и рёбер конечны, если же хотя бы одно из этих множеств бесконечно, граф называется *бесконечным.* Конечный граф без петель и кратных рёбер называется *простым.*

3.1.1.2. Степень вершины графа

Звездой вершины v графа (орграфа) G называется множество инцидентных v рёбер (дуг). Обозначать звезду будем $\delta(v)$. *Степенью вершины* v называется величина $\deg(v) = |\delta(v)|$, т. е. степень вершины равна числу инцидентных ей рёбер (дуг). Для орграфов различают *полустепени захода* и *исхода* вершины. Полустепень захода обозначается $\delta_+(v)$ и равна числу дуг звезды, для которых v является конечной вершиной (такие дуги называются *входящими)*, соответственно, полустепень исхода $\delta_-(v)$ есть число дуг, для которых v — начальная вершина (*исходящих* дуг). Очевидно, что $\delta_+(v) + \delta_-(v) = deg(v)$.

Для любого графа справедливо следующее очевидное утверждение.

Лемма 3.1.1

$$\sum_{v \in V} \deg(v) = 2|X|.$$

Следствие

Число вершин нечётной степени в любом графе нечётно.

Вершина $v \in V$ называется *концевой вершиной графа* $G = \langle V, X \rangle$, если $\deg(v) = 1$. Вершина называется *изолированной*, если её степень равна нулю. На рис. 3.1.2 изображена диаграмма графа, у которого вершина u — изолированная, v — концевая.

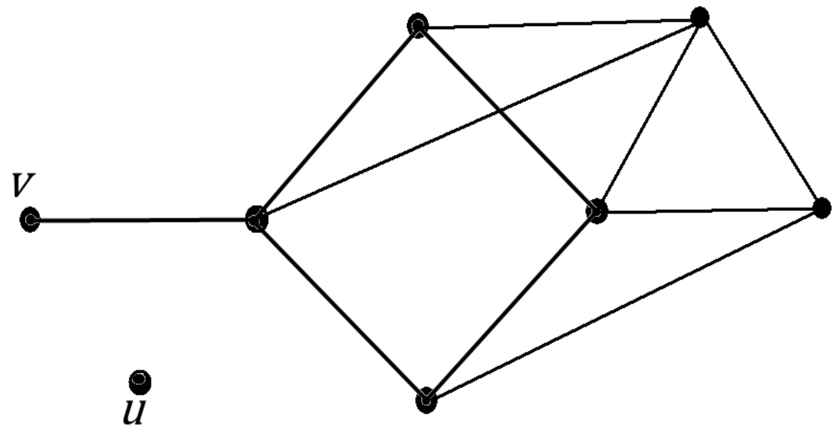
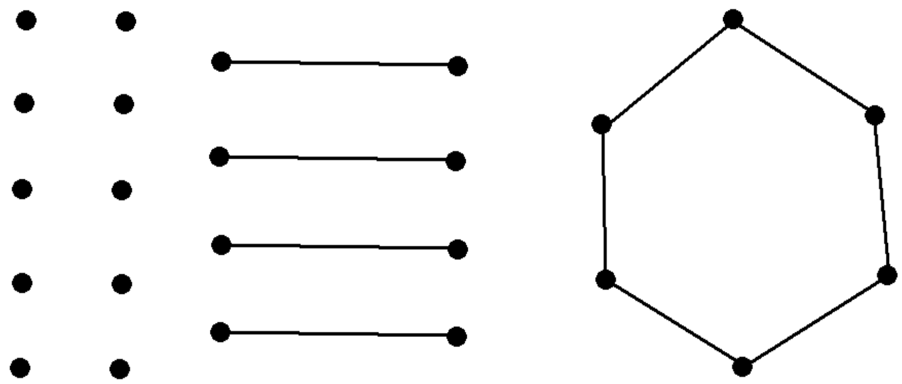


Рис. 3.1.2. Граф с изолированной и концевой вершинами

Граф называется *регулярным* (*равномерным*) *степени* d, если степени всех его вершин одинаковы и равны d. На рис. 3.1.3 показаны диаграммы равномерных графов степени 0 (а), 1 (б), 2 (в).



а) $d = 0$ *б*) $d = 1$ *в*) $d = 2$

Рис. 3.1.3. Регулярные графы

На рис. 3.1.4 показан регулярный граф степени 3 — *граф Куратовского* $K_{3,3}$, имеющий большое значение в теории графов. Очевидно, что полный граф с n вершинами является регулярным степени $n - 1$.

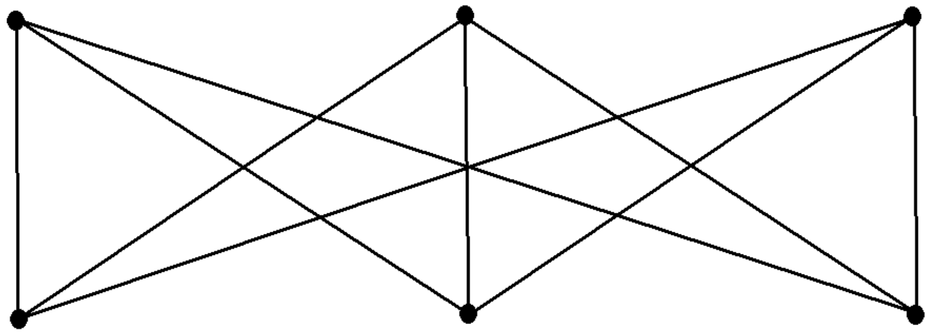


Рис. 3.1.4. Граф Куратовского

3.1.1.3. Способы задания графа

Способы задания графов делятся на теоретико-множественные, графический и матричные.

Теоретико-множественные способы задают граф как множество элементов. Таких способов два. Первый — задание графа (орграфа) по его определению, т. е. списком вершин $V = \{v_1, v_2, \dots, v_n\}$ и рёбер (дуг) $X = \{x_1, x_2, \dots, x_m\}$, где $x_1 = \{v_{i_1}, v_{j_1}\}$, $x_2 = \{v_{i_2}, v_{j_2}\}$, … , $x_m = \{v_{i_m}, v_{j_m}\}$, ($x_1 = \langle v_{i_1}, v_{j_1}\rangle$, $x_2 = \langle v_{i_2}, v_{j_2}\rangle$, … , $x_m = \langle v_{i_m}, v_{j_m}\rangle$ в случае орграфа). Второй способ — списки инцидентности. Для каждой вершины указывается множество инцидентных ей рёбер, для орграфа — множества исходящих и входящих дуг:

$$v_1\colon x_{i_1}, x_{i_2}, \dots$$
$$v_2\colon x_{j_1}, x_{j_2}, \dots$$
$$\vdots$$

Теоретико-множественные способы задания просты и понятны, но неудобны для практического применения, например, при реализации различных алгоритмов на графах.

Графический способ задания — диаграммы — был уже рассмотрен в 3.1.1.1. Здесь только заметим, что его единственное преимущество в простоте и наглядности. Поэтому он незаменим при обучении основам теории графов. Но для практического применения он также непригоден.

Матричные способы являются самыми важными с практической точки зрения. Различают два основных вида матриц, задающих графы: матрицы смежности вершин и инцидентности.

Отношение смежности между вершинами является бинарным отношением на множестве вершин V. Матрица этого отношения называется *матрицей смежности вершин.* Она обозначается $\Omega(G)$, и её элементы вычисляются по правилу: $\Omega_{ij} = 1$, если вершины v_i, v_j смежны (т. е. в G есть ребро $\{v_i, v_j\}$), $\Omega_{ij} = 0$ в противном случае. Если в графе есть кратные рёбра, то тогда Ω_{ij} равно числу рёбер $\{v_i, v_j\}$.

Можно выделить некоторые свойства матрицы $\Omega(G)$:

1) для неориентированного графа $\Omega(G)$ симметрична ($\Omega_{ij} = \Omega_{ji}$, $i, j = 1, 2, \dots, n$; n — число вершин);

2) если граф содержит петли, то на главной диагонали есть ненулевые числа, в противном случае все элементы главной диагонали — нули;

3) если в графе нет кратных рёбер, то матрица $\Omega(G)$ бинарная, т. е. содержит только нули и единицы, в противном случае в ней есть числа, большие 1;

4) сумма элементов строки (столбца) равна степени вершины, которой соответствует эта строка (столбец), таким образом, изолированной вершине соответствует нулевая строка (столбец), концевой — единичная строка (столбец);

5) если граф G полный, то в $\Omega(G)$ все элементы единицы, только на главной диагонали стоят нули.

Матрица смежности вершин орграфа заполняется по следующему правилу: $\Omega_{ij} = 1$, если в G есть дуга $\langle v_i, v_j \rangle$, $\Omega_{ij} = 0$ в противном случае. При наличии кратных дуг Ω_{ij} равна числу дуг $\langle v_i, v_j \rangle$. Некоторые свойства матрицы $\Omega(G)$ орграфа G:

1) в общем случае матрица несимметрична;

2) если орграф содержит петли, то на главной диагонали есть ненулевые числа;

3) если в орграфе нет кратных дуг, то матрица $\Omega(G)$ бинарная, в противном случае в ней есть числа, большие 1;

4) противоположным дугам соответствуют равные числа в ячейках, симметричных относительно главной диагонали: $\Omega_{ij} = \Omega_{ji}$, если $\langle v_i, v_j \rangle$, $\langle v_j, v_i \rangle$ — противоположные дуги;

5) сумма элементов строки равна полустепени исхода соответствующей вершины, столбца — полустепени захода, следовательно, сумма элементов i-й строки и i-го столбца равна $\deg(v_i)$;

6) для изолированной вершины v_i сумма элементов i-й строки и i-го столбца равна нулю, для концевой — единице.

Второй вид матричного задания — матрица инцидентности. Она обозначается $\varepsilon(G)$, её элементы вычисляются по правилу (в случае неориентированных графов): $\varepsilon_{ij} = 1$, если вершина v_i инцидентна ребру x_j, $i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, m$; n — число вершин, m — число рёбер. Таким образом, матрица $\varepsilon(G)$ имеет размерность n на m.

Некоторые свойства матрицы $\varepsilon(G)$:

1) для неориентированных графов матрица бинарная, в каждом столбце при отсутствии петель ровно по две единицы, если же есть петли, то им соответствуют единичные столбцы (имеются в виду столбцы единичной матрицы), нулевых столбцов не должно быть;

2) кратным рёбрам соответствуют одинаковые столбцы, следовательно, если в матрице все столбцы разные, то в графе нет кратных рёбер;

3) сумма элементов строки равна степени соответствующей вершины, значит, изолированной вершине соответствует нулевая строка, концевой — строка с одной единицей;

4) матрица полного графа имеет n строк и C_n^2 столбцов, в каждой строке ровно по $n-1$ единиц.

В случае ориентированного графа $\varepsilon_{ij} = 1$, если v_i является конечной вершиной дуги x_j, $\varepsilon_{ij} = -1$, если v_i — начальная вершина x_j и $\varepsilon_{ij} = 0$, если v_i не инцидентна x_j.

Некоторые свойства матрицы $\varepsilon(G)$ орграфа G:

1) если в G нет петель, то в матрице присутствуют только 1, -1 и 0, если же есть петли, то им соответствуют столбцы, в которых одна позиция должна содержать и 1, и -1 одновременно, в остальных — нули. В этом случае применяют какой-либо особый символ, например, ± 1;

2) если в орграфе нет петель, то в каждом столбце стоит ровно одно число 1 и одно -1, нулевых столбцов не должно быть;

3) кратным дугам соответствуют одинаковые столбцы, противоположным — столбцы, сумма которых равна нулевому;

4) для каждой строки сумма единиц равна полустепени захода соответствующей вершины, сумма чисел -1 равна по модулю полустепени исхода. Таким образом, сумма модулей элементов строки равна степени вершины, соответствующей строке.

И матрица инцидентности, и матрица смежности полностью определяют граф (орграф), т.е. являются равноправными способами его задания. Выбор их зависит от конкретной решаемой задачи.

3.1.1.4. Маршруты, пути, цепи, циклы

Пусть дан граф (орграф) $G = \langle V, X \rangle$. *Маршрутом* в G, соединяющим вершины v_0 и v_l, называется последовательность вершин и рёбер (дуг) вида

$$v_0 x_1 v_1 x_2 v_2 \dots v_{l-1} x_l v_l, \tag{3.1.1}$$

где ребро (дуга) x_i инцидентна вершинам v_{i-1}, v_i для всех $i = 1, 2, \dots, l$. Вершина v_0 называется *начальной*, v_l — *конечной вершиной* маршрута, число l — его *длиной*. Если v_0 совпадает с v_l, маршрут называется *замкнутым*, в противном случае — *открытым.*

Маршрут называется *простым,* если все рёбра (дуги) в нём различны. Простой маршрут, в котором все вершины различны, называется *цепью.* На рис. 3.1.5 показан пример диаграммы простого маршрута, не являющегося цепью. Стрелками показано направление движения по маршруту. Маршрут (цепь), соединяющий вершины u и v, будем называть (u, v)-*маршрутом* ((u, v)-*цепью*).

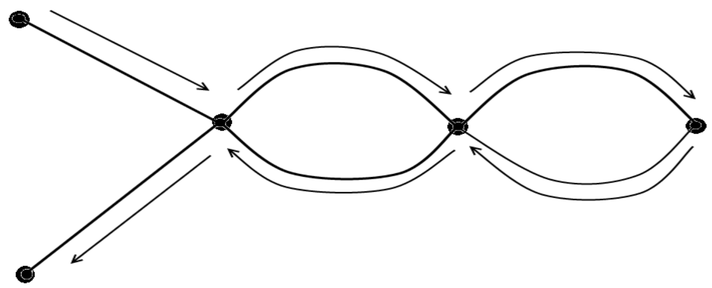


Рис. 3.1.5. Простой маршрут, не являющийся цепью

Теорема 3.1.1

Если в графе G существует маршрут, соединяющий две различные вершины u, v, то из его рёбер можно составить (u, v)-цепь.

Доказательство

Пусть маршрут $u = v_0 x_1 v_1 x_2 v_2 \dots v_{l-1} x_l v_l = v$ соединяет вершины u, v. Из всех (u, v)-маршрутов, множества рёбер которых являются подмножествами совокупности x_1, x_2, … , x_l, выберем самый короткий (содержащий наименьшее число рёбер). Обозначим его $u = v_0 = v'_0 x'_1 v'_1 \dots v'_{k-1} x'_k v'_k = v_l = v$. Покажем, что его вершины v'_0, v'_1, … , v'_k различны, т. е. он представляет собой (u, v)-цепь. Предположим, что $v'_i = v'_j$ $(i < j)$. Тогда составим (u, v)-маршрут

$$u = v_0 = v'_0 x'_1 v'_1 \dots v'_i x'_{j+1} v'_{j+1} \dots v'_{k-1} x'_k v'_k = v_l = v.$$

Его длина будет равна $k - (j - i) < k$, что противоречит предположению о минимальности k. Таким образом, (u, v)-маршрут из рёбер исходного маршрута, имеющий минимальную длину, является цепью. ■

Из этой теоремы следует, что существование (u, v)-маршрута эквивалентно существованию (u, v)-цепи, поэтому в дальнейшем будем говорить именно о цепи между двумя вершинами.

Замкнутый простой маршрут, в котором все вершины различны, называется *циклом.* Следующая теорема является аналогом теоремы 1 для замкнутых маршрутов.

Теорема 3.1.2

Если в графе G существует замкнутый простой маршрут, то из его рёбер можно составить цикл.

Доказательство

Предположим, что последовательность $v_0 x_1 v_1 x_2 v_2 \dots v_{l-1} x_l v_l = v_0$ является замкнутым простым маршрутом. Если все вершины в нём различны, то он является циклом. В противном случае из совокупности его рёбер выберем подмножество, образующее замкнутый маршрут минимальной длины. Обозначим этот маршрут $v_0 = v'_0 x'_1 v'_1 \dots v'_{k-1} x'_k v'_k = v_l = v_0$. Покажем, что все его вершины различны. Действительно, если какая-либо из вершин входит в последовательность $v'_0, v'_1, \dots, v'_{k-1}$ дважды, то найдётся целое число s $(1 \leq s \leq k - 1)$ такое, что все вершины $v'_0, v'_1, \dots, v'_s$ различны, а v'_{s+1} совпадает с одной из $v'_0, v'_1, \dots, v'_s$. Пусть $v'_i = v'_{s+1}$ $(0 \leq i \leq s)$. Тогда маршрут $v'_i x'_{i+1} \dots v'_s x'_{s+1} v'_{s+1} = v'_i$ будет замкнутым простым маршрутом длины $s - i + 1 \leq k$, что противоречит предположению о минимальности k. ■

Замечание

Условие простоты маршрута существенно. Например, замкнутый маршрут $v_0 x_1 v_1 x_1 v_0$ не является простым, и из его единственного ребра x_1 построить цикл нельзя.

Маршрут (3.1.1) в орграфе, в котором $x_i = \langle v_{i-1}, v_i \rangle$ для всех i от 1 до l, называется *путём*. Таким образом, движение в пути происходит только по направлениям дуг. Замкнутый простой путь, в котором все вершины различны, называется *контуром.* Для путей и контуров справедливы теоремы, аналогичные доказанным выше.

Теорема 3.1.3

Если в орграфе G существует путь от вершины u к вершине v, то из его дуг можно составить (u, v)-путь, являющийся цепью.

Теорема 3.1.4

Если в орграфе G существует замкнутый простой путь, то из его дуг можно составить контур.

3.1.2. Связность

3.1.2.1. Компоненты связности

Граф называется *связным*, если между любыми его несовпадающими вершинами существует цепь. Иными словами, в связном графе можно пройти по рёбрам от любой вершины к любой другой вершине. Для определения компонент связности и блоков необходимо ввести некоторые понятия.

Подграфом G' графа $G = \langle V, X\rangle$ называется граф $G' = \langle V', X'\rangle$, у которого $V' \subseteq V$, $X' \subseteq X$ (записывается $G' \subseteq G$). Понятно, что для любого графа G $\Lambda \subseteq G$ (Λ — пустой граф) и $G \subseteq G$. Эти подграфы называются *несобственными.* Подграфы, отличные от Λ и самого графа G, называются *собственными.* Для собственных подграфов G' применяется запись $G' \subset G$.

Пусть V' — некоторое непустое подмножество множества V вершин графа $G = \langle V, X\rangle$, $X(V')$ — множество всех рёбер $x = \{u, v\} \in$ $\in X$ таких, что $u \in V'$, $v \in V'$. Подграф $G(V') = \langle V', X(V')\rangle$ графа G называется *подграфом, порождённым множеством вершин* V'.

Определим на множестве вершин V графа $G = \langle V, X\rangle$ бинарное отношение $\equiv$, считая, что $u \equiv v$ тогда и только тогда, когда $u = v$ или в G существует (u, v)-цепь. Очевидно, что это отношение рефлексивно ($v = v$ для любой вершины $v \in V$, поэтому $v \equiv v$). Если в графе есть (u, v)-цепь, то она же будет и (v, u)-цепью, поэтому $\equiv$ симметрично. Наконец, пусть в графе есть (u, v)-цепь $u = v_0 x_1 v_1 \dots x_l v_l = v$ и (v, s)-цепь $v = v'_0 x'_1 v'_1 \dots x'_k v'_k = s$. Объединяя их, получаем (u, s)-цепь $u = v_0 x_1 v_1 \dots x_l v_l x'_1 v'_1 \dots x'_k v'_k = s$. Следовательно, отношение $\equiv$ транзитивно. Итак, доказано, что $\equiv$ — эквивалентность. По теореме о разбиении на классы эквивалентности множество вершин V распадается на непересекающиеся подмножества V_1, V_2, … , V_d — классы эквивалентности по $\equiv$. В пределах каждого V_i, $i = 1, 2, \dots, d$, можно из одной вершины достичь любую другую по рёбрам графа G.

Подграфы $G_1 = \langle V_1, X(V_1)\rangle$, … , $G_d = \langle V_d, X(V_d)\rangle$, порождённые подмножествами $V_1, V_2, \dots, V_d$, называются *компонентами связности* графа G, число d — степенью связности. Очевидно, что связный граф имеет степень связности 1, и единственная его компонента связности совпадает с самим графом. Понятно, что каждое ребро принадлежит ровно одной компоненте связности.

3.1.2.2. Мосты

Пусть x — некоторое ребро графа $G = \langle V, X \rangle$. Если у G удалить ребро x, то получится граф с тем же множеством вершин и множеством рёбер $X \backslash \{x\}$. Обозначим его $G \backslash x$.

Теорема 5

В связном графе G ребро x принадлежит некоторому циклу тогда и только тогда, когда граф $G \backslash x$ также является связным.

Доказательство

Докажем необходимость. Пусть ребро x принадлежит циклу

$$v_0 x v_1 x_2 v_2 \dots x_l v_l = v_0. \qquad (3.1.2)$$

Рассмотрим произвольную пару вершин u и v графа G. Так как он связный, между ними существует (u, v)-цепь. Если она не содержит ребро x, то и в графе $G \backslash x$ она будет соединять u и v. Предположим теперь эта цепь проходит через x. Заменим в ней участок $v_0 x v_1$ последовательностью $v_0 = v_l x_l \dots v_2 x_2 v_1$, т. е. частью цикла (3.1.2) без ребра x. Вновь получим (u, v)-цепь, но уже составленную из рёбер графа $G \backslash x$, что и доказывает его связность.

Докажем достаточность. Пусть $x = \{u, v\}$. Поскольку граф $G \backslash x$ связный, между любыми его вершинами, а значит, и между u и v существует цепь $u = v_0 x_1 v_1 x_2 v_2 \dots v_{l-1} x_l v_l = v$. Тогда, присоединяя к ней ребро x с инцидентными ей вершинами, получаем цикл $u =$ $= v_0 x_1 v_1 \, x_2 v_2 \dots v_{l-1} x_l v x u$ в графе G. ■

Ребро x называется *мостом* (*перешейком*, *разделяющим ребром*), если его удаление ведёт к увеличению степени связности графа. На рис. 3.1.6 показана диаграмма графа с мостом x. Если граф G не является связным, то при удалении ребра x изменяется лишь компонента связности, содержащая x. Отсюда и из теоремы 3.1.5 следует необходимое и достаточное условие того, что x является мостом.

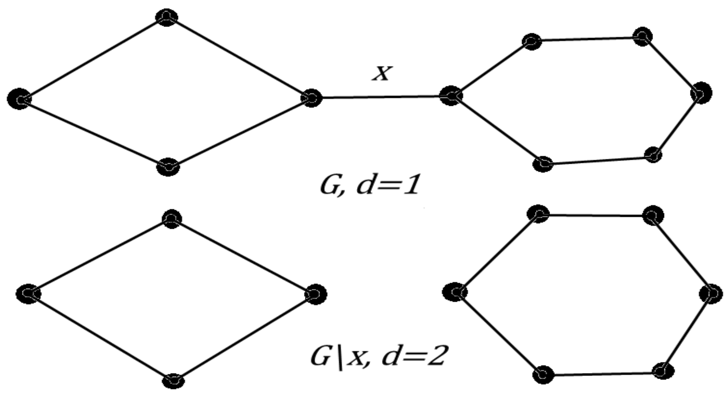


Рис. 3.1.6. Мост

Теорема 3.1.6

Ребро графа является мостом тогда и только тогда, когда в графе нет циклов, содержащих его.

3.1.2.3. Блоки

Вершина $v \in V$ графа $G = \langle V, X \rangle$ называется *точкой сочленения,* если её удаление вместе с рёбрами её звезды увеличивает степень связности G. Связный граф, не имеющий точек сочленения, называется *блоком.* При числе вершин $n = 1$ понятие блока не определено. При $n = 2$ граф, состоящий из единственного ребра, является блоком. При $n > 2$ имеет место следующее утверждение.

Теорема 3.1.7

В любом связном графе, имеющем не менее двух вершин, найдутся по крайней мере две вершины, не являющиеся точками сочленения.

Доказательство

Пусть граф G имеет по крайней мере две вершины. Рассмотрим цепь максимальной длины в нём, u и v — её начальная и конечная вершины. Докажем, что v не является точкой сочленения. Предположим противное. Тогда существует вершина s, принадлежащая той компоненте связности графа G, которая не содержит u (u и v соединены цепью, поэтому принадлежат одной компоненте, а s лежит в другой, появляющейся после удаления v). Следовательно, все (u, s)-цепи содержат вершину v, поэтому длина любой (u, s)-цепи больше длины (u, v)-цепи, что невозможно в силу предположения о максимальности её длины. Точно так же доказывается, что u не является точкой сочленения. ■

Для произвольного связного графа, т. е. имеющего точки сочленения, определяется его блок. *Блоком связного графа G* называется его максимальный связный нетривиальный (т. е. имеющий не менее двух вершин) подграф, являющийся блоком. Максимальность понимается в том смысле, что любой подграф-блок содержится в блоке графа.

3.1.3. Деревья

3.1.3.1. Теоремы о деревьях

Граф, не содержащий циклов, называется *лесом.* Связный граф без циклов называется *деревом.* Таким образом, деревья являются компонентами связности леса. Деревья и леса — виды *ациклических графов.* На рис. 3.1.7 изображены примеры диаграмм деревьев. На рис. 3.1.8 показано бинарное дерево — граф, имеющий особое значение в теории алгоритмов.

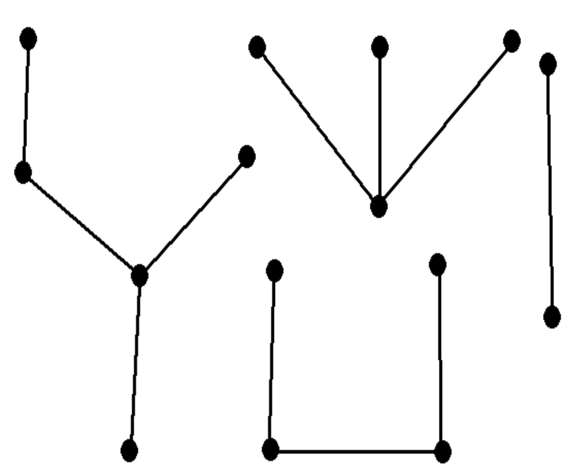


Рис. 3.1.7. Деревья

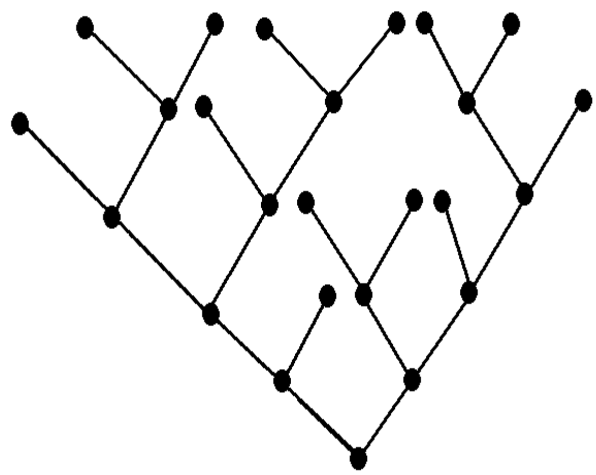


Рис. 3.1.8. Бинарное дерево

В следующих теоремах сформулированы характеристические свойства деревьев, т. е. по сути их можно считать альтернативными определениями дерева.

Теорема 3.1.8

Граф является деревом тогда и только тогда, когда между любыми его двумя несовпадающими вершинами существует одна и только одна цепь

Доказательство

Доказательство необходимости. Пусть G — дерево. Предположим, что в G существуют две различные (u, v)-цепи $u = v_0 x_1 v_1 \dots v_{k-1} x_k v_k = v$, $u = v_0' x_1' v_1' \dots v_{l-1}' x_l' v_l' = v$. Если они не имеют общих вершин, кроме u и v, то очевидно, что в совокупности обе цепи образуют цикл, что противоречит тому, что G является деревом. Поэтому считаем, что эти цепи имеют по крайней мере одну общую вершину, отличную от u или v. Пусть $s = v_i$ — первая вершина из первой цепи $(s \neq u)$, принадлежащая обеим цепям такая, что ей предшествующие $v_1, v_2, \dots, v_{i-1}$ не принадлежат второй цепи. Если $t = v_j$ $(j > i)$ — следующая вершина первой цепи, принадлежащая также и второй, такая, что ей предшествующие, кроме s, не принадлежат второй цепи (t может быть равна v, поэтому она обязательно существует), то участки обеих цепей между s и t образуют цикл. Полученное противоречие доказывает необходимость.

Докажем достаточность. Поскольку между любыми двумя вершинами графа существует цепь, то он связный, а из единственности такой цепи следует ацикличность (если бы в графе был цикл, то любые две вершины этого цикла были бы соединены двумя цепями). ■

Теорема 3.1.9

Дерево, содержащее не менее двух вершин, имеет по крайней мере две концевые вершины.

Доказательство

Пусть в дереве G цепь $u = v_0 x v_1 x_2 v_2 \dots x_l v_l = v$ имеет максимальную длину. Покажем, что начальная и конечная вершины этой цепи являются концевыми для дерева.

Итак, требуется доказать, что вершина v инцидентна только ребру x_l. Предположим, что существует отличное от x_l инцидентное v ребро x_{l+1}, v_{l+1} — другая его концевая вершина. Так как в G нет циклов, то v_{l+1} не может совпадать ни с одной из вершин v_0, v_1, … , v_l, а это значит, что последовательность $v_0 x v_1 x_2 v_2 \dots x_l v_l x_{l+1} v_{l+1}$ также является цепью и имеет длину $l + 1$, что противоречит тому, что l — максимальная длина цепи в G. ■

Для доказательства следующей теоремы нам понадобится вспомогательное утверждение.

Лемма 3.1.2

Если удалить из дерева одну из его концевых вершин вместе с инцидентным ей ребром, то получившийся граф также будет деревом.

Доказательство

Пусть $G = \langle V, X \rangle$, v — концевая вершина дерева G, x — инцидентное её ребро. Очевидно, что в графе $G' = \langle V \backslash \{v\}, X \backslash \{x\} \rangle$ не будет циклов. Также очевидно, что любая цепь, соединяющая вершины u, $u' \in V \backslash \{v\}$, не содержит ни v, ни x. Следовательно, (u, u')-цепь в графе G' можно построить только из рёбер $X \backslash \{x\}$, а это означает, что граф G' связный. ■

Теорема 3.1.10

Связный граф является деревом тогда и только тогда, когда

$$m = n - 1, \qquad (3.1.3)$$

где n — число вершин, m — число рёбер.

Доказательство

Необходимость докажем индукцией по числу вершин n. База индукции ($n = 1$) очевидна: в дереве с одной вершиной рёбер быть не должно (единственное возможное в таком графе ребро — петля — образовало бы цикл), поэтому $m = 0$, равенство $m = n - 1$ верно. Предположение индукции: в любом дереве с $k \leq n$ вершинами число рёбер на единицу меньше числа вершин. Доказываем индукционный шаг. Рассмотрим дерево с $n + 1$ вершинами ($n + 1 \geq 2$). Согласно теореме 3.1.9 в нём есть хотя бы две концевые вершины. Удалим из него концевую вершину с инцидентным ей ребром. Из леммы 3.1.2 следует, что получившийся граф будет деревом с n вершинами. В нём, согласно предположению индукции, число рёбер на единицу меньше числа вершин. Поскольку были удалены одна вершина и одно ребро, то и в исходном дереве было такое же соотношение. Индукционный шаг доказан.

Теперь докажем достаточность. Пусть в связном графе G выполняется соотношение (3.1.3). Предположим, что он не является деревом. Тогда в нём есть циклы, количество которых обозначим s. Удалим из какого-либо цикла ребро. Из теоремы 3.1.5 следует, что получившийся граф будет связным, число циклов в нём $s - 1$ (понятно, что если удалённое ребро принадлежало сразу двум циклам, то всё равно количество циклов уменьшилось на 1). Будем также далее удалять по одному ребру из циклов и каждый раз согласно теореме 3.1.5 получать связный граф. После того, как исчезнет последний цикл, получим дерево с n вершинами и $m - s$ рёбрами. По доказанной необходимости для этого дерева верно равенство $m - s = n - 1$, откуда, принимая во внимание (3.1.3), получаем, что $s = 0$. А это означает, что исходный граф был деревом. ■

Следствие

Для любого связного графа $n - m + 1 \geq 0$.

Остовным поддеревом (*остовом, покрывающим поддеревом*) графа G называется его подграф, содержащий все вершины G и являющийся деревом.

Теорема 3.1.11

В любом связном графе существует остовное поддерево.

Доказательство

Если граф является деревом, то он сам представляет собой своё остовное поддерево. Если же в нём есть циклы, то действуя так же, как в доказательстве достаточности теоремы 3.1.10, можно построить покрывающее поддерево. ■

3.1.3.2. Цикломатическое число

Число $\mu = m - n + d$, где n — число вершин, m — число рёбер, d — степень связности графа, называется *цикломатическим числом.* Если G_1, G_2, … , G_d — компоненты связности графа G, имеющие по n_1, n_2, … , n_d вершин и m_1, m_2, … , m_d рёбер, соответственно, то для каждой из них цикломатическое число определяется формулой

$$\mu_i = m_i - n_i + 1. \quad (3.1.4)$$

Очевидно, что

$$\mu_i = \sum_{i=1}^{d} \mu_i. \quad (3.1.5)$$

Теорема 3.1.12

1) Для любого графа цикломатическое число $\mu \geq 0$.

2) Граф является деревом тогда и только тогда, когда его цикломатическое число $\mu = 0$.

3) Цикломатическое число графа $\mu=1$ тогда и только тогда, когда в нём существует единственный цикл.

Доказательство

Утверждения теоремы (1) и (2) вытекают из теоремы 3.1.10, следствия из неё — из формул (3.1.4), (3.1.5). Остаётся доказать (3).

Пусть цикломатическое число графа G равно 1. Если G несвязен, то из (3.1.5) и утверждения (1) следует, что одна из его компонент связности имеет цикломатическое число 1, остальные — 0. Следовательно, согласно утверждению (2), все компоненты связности, кроме одной, с цикломатическим числом 1, являются деревьями. Поэтому достаточно доказать утверждение для связного графа. В этом случае G не является деревом, значит, в нём существуют циклы. Допустим, что в G есть два несовпадающих цикла, следовательно, найдётся хотя бы одно ребро, принадлежащее первому и не принадлежащее второму циклу. Если исключить его, то получится связный граф (теорема 3.1.5) с цикломатическим числом 0, содержащий цикл, что противоречит утверждению (2). Следовательно, в G имеется ровно один цикл.

Обратно, пусть G содержит ровно один цикл. Если G несвязен, то все его компоненты, кроме той, что содержит цикл, являются деревьями, тогда из утверждения (2) и формулы (3.1.5) следует, что цикломатическое число G равно цикломатическому числу этой компоненты. Поэтому достаточно доказать утверждение для связного графа. В этом случае удаление любого ребра цикла превращает G в дерево (получившийся граф связен, что следует из теоремы 3.1.5, и из него исчезает единственный цикл). Поскольку цикломатическое число дерева равно 0, и было удалено одно ребро, то для исходного графа G $\mu = 1$. ■

3.2. ПЕРЕЧИСЛИТЕЛЬНЫЕ ЗАДАЧИ НА ГРАФАХ

3.2.1. Помеченные графы

3.2.1.1. Понятие помеченного графа

Пусть дан граф $G = \langle V, X \rangle$, где $|V| = n$. Будем называть его *помеченным*, если на множестве V задана биекция $\wp: V \to \{1, 2, \dots, n\}$, т. е. каждой вершине приписывается целое число от 1 до n, которое называется *пометкой* вершины. Таким образом, помеченный граф можно определить как тройку $G^{\wp} = \langle V, X, \wp \rangle$. Поскольку функции $\wp$ являются подстановками множества вершин V, их общее число равно $n!$, однако количество помеченных графов с n вершинами может быть меньше $n!$.

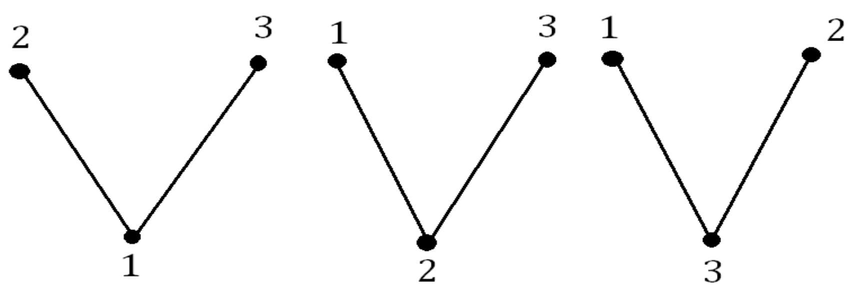


Рис. 3.2.1. Помеченные графы с двумя рёбрами

Например, на рис. 3.2.1 изображены диаграммы трех различных графов порядка 3 с двумя рёбрами. На рис. 3.2.2 показаны остальные три диаграммы с помеченными вершинами, но очевидно, что каждая из них эквивалента ровно одной диаграмме на рис. 3.2.1.

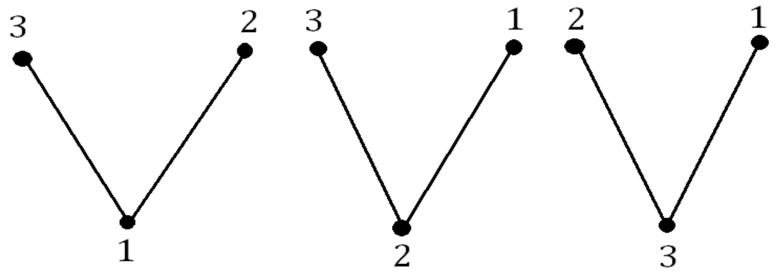
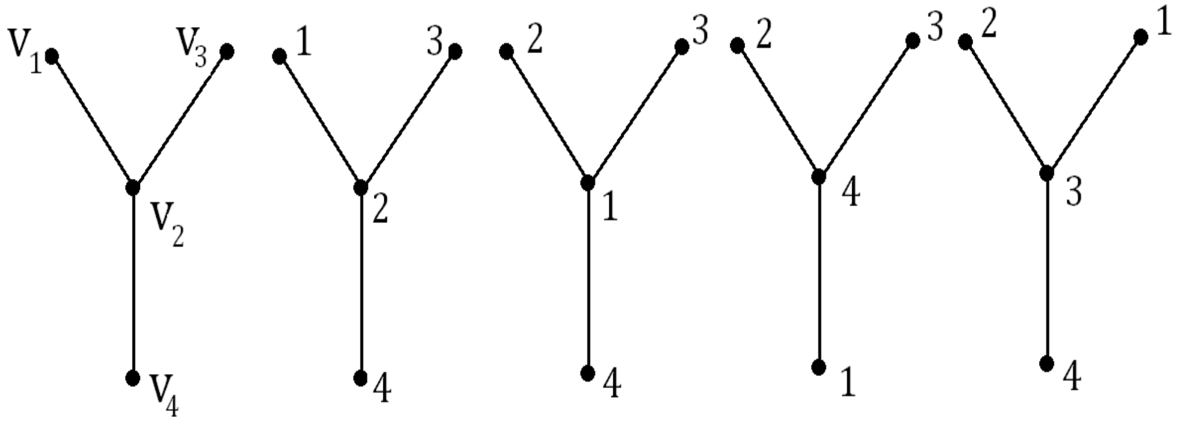


Рис. 3.2.2. Эквивалентные помеченные графы

Таким образом, существуют три различных помеченных графа с тремя вершинами. Как видно из приведённого примера, некоторые из помеченных графов можно считать одинаковыми. Определим такие графы как изоморфные.

Помеченные графы $G_1^{\wp} = \langle V_1, X_1, \wp_1 \rangle$, $G_2^{\wp} = \langle V_2, X_2, \wp_2 \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение f множества $\wp_1(V_1)$ на $\wp_2(V_2)$, сохраняющее отношение смежности вершин с соответствующими пометками, т. е. v_1 и v_2 тогда и только тогда смежны в $G_1^{\wp}$, когда $f(v_1)$ и $f(v_2)$ смежны в $G_2^{\wp}$. На множестве всех неориентированных графов можно ввести отношение изоморфизма, считая изоморфные пары графов принадлежащими этому отношению. Нетрудно доказать, что оно является эквивалентностью, поэтому разбивает всё множество графов на классы эквивалентности, содержащие изоморфные друг другу графы. На рис. 3.2.3, *а* показана диаграмма графа с четырьмя вершинами и тремя рёбрами, а на рис. 3.2.3, *б* — диаграммы четырех различных соответствующих ему помеченных графов.

Таким образом, число элементов класса эквивалентности, которому принадлежит данный граф, равно количеству способов пометить его вершины, т. е. числу различных соответствующих помеченных графов.



а) б)

Рис. 3.2.3. Граф (а) и соответствующие ему помеченные графы (б)

3.2.1.2. Перечисление помеченных графов

Найдём число помеченных графов порядка n. Для этого сначала найдём, сколько существует помеченных графов с m рёбрами. Из понятия помеченного графа как элемента класса изоморфных друг другу графов следует, что он определяется парами смежных вершин. Всего имеется C_n^2 неупорядоченных пар вершин, каждая из которых может быть смежной или несмежной. Если выбрать из них m пар, которые будут соединены рёбрами, то получим помеченный граф. Это можно сделать $C_{C_n^2}^m$ способами. Следовательно, существует $C_{C_n^2}^m$ помеченных графов с m рёбрами. Отсюда и из того, что производящей функцией сочетаний является бином Ньютона, следует теорема.

Теорема 3.2.1

Производящая функция f_n чисел помеченных графов q_n порядка n задаётся формулой

$$f_n(z) = (1 + z)^{C_n^2}.$$

Понятно, что общее число помеченных графов Q_n порядка n есть сумма коэффициентов в разложении производящей функции f_n по степеням z, которая легко находится подстановкой в f_n вместо z единицы:

$$Q_n = f_n(1) = 2^{C_n^2}.$$

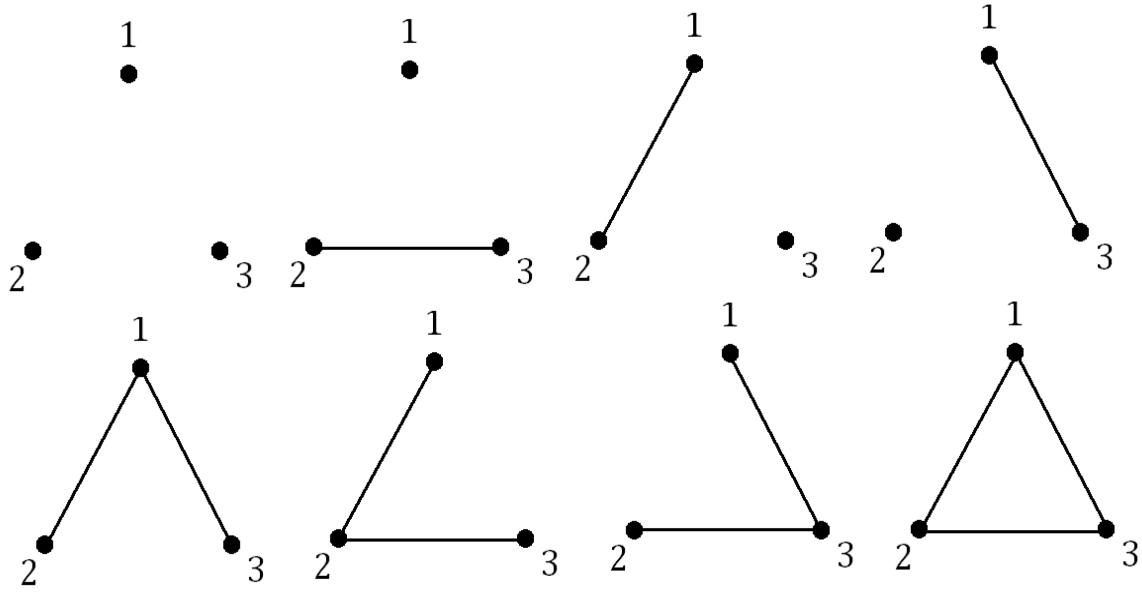


Рис. 3.2.4. Помеченные графы порядка 3

На рис. 3.2.4 изображены все помеченные графы порядка 3. Нетрудно увидеть, что они принадлежат четырем различным классам эквивалентности, т. е. соответствуют четырем разным непомеченным графам. Их диаграммы показаны на рис. 3.2.5. Таким образом, графы G_1, G_2, G_3, G_4 на рис. 3.2.5 можно пометить соответственно 1, 3, 3, 1 способами.

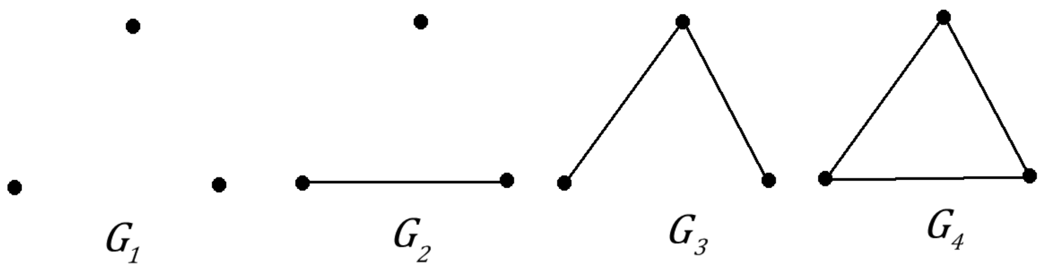


Рис. 3.2.5. Непомеченные графы порядка 3

Возникает общая задача о числе помеченных графов, соответствующих данному непомеченному. Для её решения нужно рассмотреть *автоморфизмы*, или *симметрии*, графа. В пункте 3.2.1.1 было определено изоморфное отображение одного графа в другой. Если при этом граф переходит в самого себя, то такое отображение назовём автоморфизмом. Более точно, автоморфизмом графа $G = = \langle V, X \rangle$ называется взаимно однозначное отображение $g: V \to V$ такое, что если $\{u, v\} \in X$, то $\{g(u), g(v)\} \in X$. Таким образом, автоморфизм представляет собой подстановку множества вершин X. Нетрудно доказать, что совокупность всех автоморфизмов образует группу $\Gamma(G)$, называемую *группой автоморфизмов* графа G. Полный граф K_n имеет своей группой симметрическую группу $\mathfrak{S}_n$, верно и обратное утверждение: если $\mathfrak{S}_n$ является группой автоморфизмов графа G, то G — полный граф K_n. Граф, диаграмма которого изображена на рис. 3.2.3 a, имеет ровно шесть автоморфизмов ($|\Gamma(G)| = 6$), которые можно записать с использованием представления в виде произведения циклов ($V = = \{v_1, v_2, v_3, v_4\}$): $(v_1)(v_2)(v_3)(v_4)$, $(v_2)(v_3)(v_1 v_4)$, $(v_1)(v_2)(v_3 v_4)$, $(v_2)(v_4)(v_1 v_3)$, $(v_2)(v_1 v_3 v_4)$, $(v_2)(v_1 v_4 v_3)$.

Пусть $s(G) = |\Gamma(G)|$ — порядок группы $\Gamma(G)$, равный числу симметрий графа G. Тогда справедлива следующая теорема, дающая решение задачи о количестве помеченных графов.

Теорема 3.2.2

Число различных способов пометить данный граф G порядка n равно

$$l(G) = \frac{n!}{s(G)}.$$

Доказательство

Группа автоморфизмов $\Gamma(G)$ является подгруппой симметрической группы $\mathfrak{S}_n$, порядок которой равен $n!$. Число помеченных графов, соответствующих G, совпадает с мощностью смежного класса $\mathfrak{S}_n$ по элементу $\Gamma(G)$. Теперь теорема следует из теоремы Лагранжа (пункт 2.1.1.4). ■

3.2.1.3. Перечисление помеченных деревьев

Задача вычисления количества помеченных деревьев была решена А. Кэли. Впоследствии было найдено много других независимых доказательств его результата.

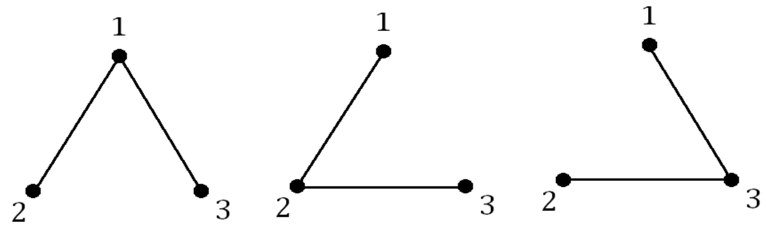


Рис. 3.2.6. Помеченные деревья с 3 вершинами

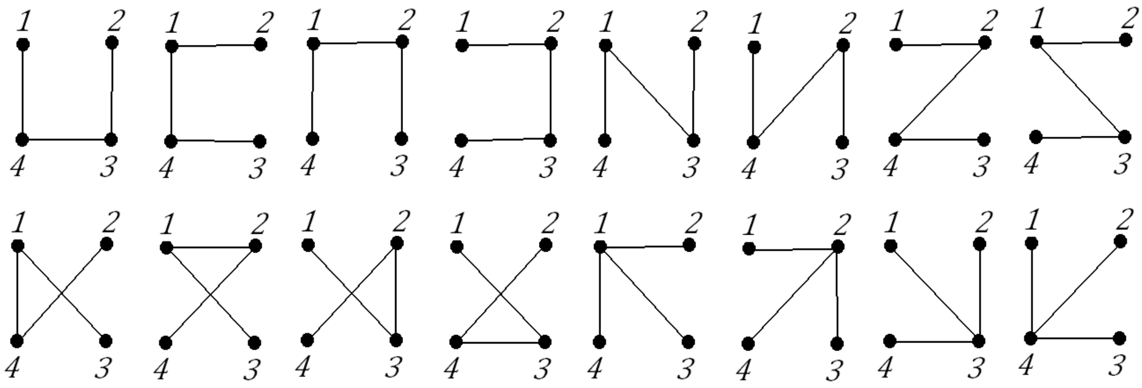


Рис. 3.2.7. Помеченные деревья с 4 вершинами

На рис. 3.2.6 показаны все помеченные деревья с тремя, а на рис. 3.2.7 — с четырьмя вершинами. Как видно, их количества равны соответственно 3 и 16. Для вывода формулы Кэли нам понадобится *матричная теорема о деревьях* (*теорема Кирхгофа*). При её доказательстве будет использован следующий результат из линейной алгебры. Пусть P и Q — прямоугольные матрицы размерностей m на n и n на m, соответственно ($m \leq n$). Главным определителем матрицы P будем называть определитель порядка m, составленный из каких-либо m столбцов P, главным определителем Q соответственно будем называть определитель, составленный из каких-либо m строк Q. Пару таких определителей будем называть соответствующей, если в них входят строки матрицы P и столбцы Q с одинаковыми номерами. Теперь сформулируем утверждение, известное в линейной алгебре как *теорема Бине-Коши.*

Лемма 3.2.1

Определитель матрицы PQ равен сумме попарных произведений всех соответствующих главных определителей матриц P и Q.

Пусть $\widehat{\Omega}(G)$ — матрица, полученная из матрицы $-\Omega(G)$ (напомним, $\Omega(G)$ — матрица смежности вершин) заменой элемента $\left(\Omega(G)\right)_{ii}$ на главной диагонали на $\deg(v_i)$.

Теорема 3.2.3 (теорема Кирхгофа)

Пусть G — связный помеченный граф, $\Omega(G)$ — его матрица смежности вершин. Тогда все алгебраические дополнения $\widehat{\Omega}(G)$ равны между собой, и их общее значение совпадает с числом остовов графа G.

Доказательство

Заменим в каждом столбце матрицы инцидентности $\varepsilon(G)$ одну из единиц на -1. Тогда $\varepsilon(G)$ перейдёт в матрицу $\varepsilon(G')$, являющуюся матрицей инцидентности орграфа G', полученного из G введением направлений на всех рёбрах. Очевидно, что элемент $\varepsilon(G')\left(\varepsilon(G')\right)^T$ (A^T означает транспонирование матрицы A) имеет вид

$$\left(\varepsilon(G')\left(\varepsilon(G')\right)^T\right)_{ij} = \sum_{k=1}^{m}\left(\varepsilon(G')\right)_{ik}\left(\varepsilon(G')\right)_{jk}$$

и равен $deg(v_i)$, если $i = j$, равен -1, если вершины v_i, v_j смежны, и 0 во всех остальных случаях (m — число рёбер графа G). Следовательно, $\varepsilon(G')\left(\varepsilon(G')\right)^T = \widehat{\Omega}(G)$.

Рассмотрим любую подматрицу матрицы $\varepsilon(G')$ с n строками и $n-1$ столбцами (n — число вершин графа G). Она соответствует остовному подорграфу G'' орграфа G' с $n-1$ дугами (остовный подграф — подграф, содержащий все вершины исходного графа). Удалив из подматрицы произвольную строку, например, k-ю, получим квадратную матрицу M размерности $n-1$.

Покажем, что $|\det M|$ равен 1 или 0 в зависимости от того, является ли G'' деревом (ордеревом) или нет. Пусть G'' — не дерево. Тогда орграф G'' имеет n вершин и $n-1$ дуг, следовательно, он не связен, и существует компонента связности, не содержащая v_k. Строки M, соответствующие вершинам этой компоненты, линейно зависимы, поэтому M имеет неполный ранг, и $|\det M| = 0$.

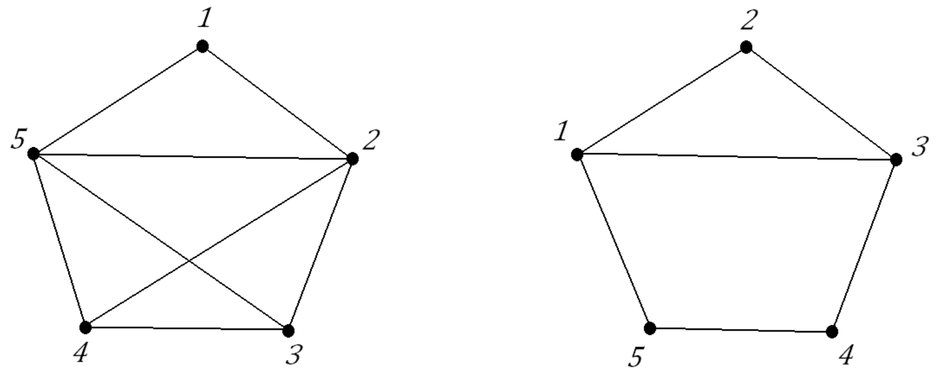
Предположим, что G'' — дерево. Пометим его вершины, отличные от v_k, следующим образом. Присвоим пометку 1 концевой вершине $v \neq v_k$ подордерева G'' (её существование гарантирует теорема 3.1.9). Если удалить из G'' вершину v с инцидентной ей дугой, вновь получим ордерево (лемма 3.1.2). Пометим числом 2 любую концевую его вершину и так далее. Приходим к новому помеченному ордереву $\tilde{G}''$, которому соответствует матрица M', полученная из M перестановкой строк и столбцов. Поэтому $\det M' = \det M$. Но M' — нижняя треугольная матрица, у которой на главной диагонали стоят либо 1, либо -1, следовательно, $|\det M| = |\det M'| = 1$.

Вычислим теперь с помощью леммы 1 алгебраическое дополнение A_{11} элемента $\left(\widehat{\Omega}(G)\right)_{11}$ матрицы $\widehat{\Omega}(G)$. Пусть D_1 — подматрица размера $n-1$ на m, полученная из $\varepsilon(G')$ вычёркиванием первой строки. Согласно лемме 1 получаем, что A_{11} равно сумме попарных произведений соответствующих главных определителей матриц D_1 и D_1^T. Очевидно, что эти главные определители равны между собой, выше было доказано, что их произведение равно 1, если столбцы D_1 определяют остов графа G, и 0 в противном случае.

Таким образом, сумма этих произведений, т. е. A_{11}, равна в точности числу остовов G. Из структуры матрицы $\widehat{\Omega}(G)$ очевидно следует, что в ней все суммы по строкам и все суммы по столбцам равны нулю. Известно, что в таких матрицах все алгебраические дополнения элементов равны между собой. Теорема доказана. ■

Для иллюстрации матричной теоремы о деревьях рассмотрим помеченный граф G, диаграмма которого изображена на рис. 3.2.8, *а*.

Его матрица смежности вершин:



а) б)

Рис. 3.2.8. Примеры помеченных графов

$$\Omega(G) = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Матрица $\widehat{\Omega}(G)$:

$$\widehat{\Omega}(G) = \begin{pmatrix} 2 & -1 & 0 & 0 & -1 \\ -1 & 4 & -1 & -1 & -1 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & -1 & 4 \end{pmatrix}.$$

Алгебраическое дополнение, например, элемента $\left(\widehat{\Omega}(G)\right)_{22}$, равно

$$A_{22} = \begin{vmatrix} 2 & 0 & 0 & 1 \\ 0 & 3 & -1 & -1 \\ 0 & -1 & 3 & -1 \\ -1 & -1 & -1 & 4 \end{vmatrix} = 56,$$

поэтому G имеет 56 остовов. Для графа G с диаграммой на рис. 3.2.8, *б* соответствующие матрицы равны

$$\Omega(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \widehat{\Omega}(G) = \begin{pmatrix} 3 & -1 & -1 & 0 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ -1 & -1 & 3 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Алгебраическое дополнение элемента $\left(\widehat{\Omega}(G)\right)_{41}$ равно

$$A_{41} = -\begin{vmatrix} -1 & -1 & 0 & -1 \\ 2 & -1 & 0 & 0 \\ -1 & 3 & -1 & 0 \\ 0 & 0 & -1 & 2 \end{vmatrix} = 11.$$

Граф G имеет 11 помеченных остовов, их диаграммы показаны на рис. 3.2.9.

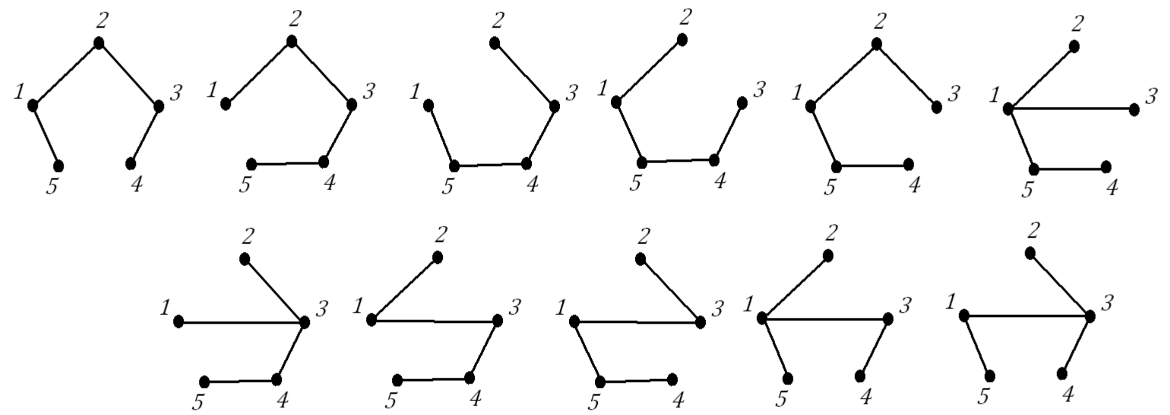


Рис. 3.2.9. Помеченные остовные поддеревья графа G

Из теоремы Кирхгофа непосредственно следует результат Кэли.

Теорема 3.2.4 (теорема Кэли)

Число помеченных деревьев с n вершинами равно n^{n-2}.

Доказательство

Применим матричную теорему о деревьях к полному помеченному графу K_n порядка n. Матрица $\widehat{\Omega}(K_n)$ имеет вид

$$\widehat{\Omega}(K_n) = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix}.$$

Алгебраическое дополнение любого диагонального элемента $\widehat{\Omega}(K_n)$ является определителем $(n-1)$-го порядка вида

$$\begin{vmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{vmatrix}.$$

Вычитая первую строку из всех остальных, получим определитель

$$\begin{vmatrix} n-1 & -1 & -1 & \cdots & -1 \\ -n & n & 0 & & 0 \\ \vdots & & & \ddots & \vdots \\ -n & 0 & 0 & \cdots & n \end{vmatrix}.$$

Затем последовательно прибавим 2, 3, ..., $(n-2)$-й столбцы к первому. Придём к верхнетреугольному определителю

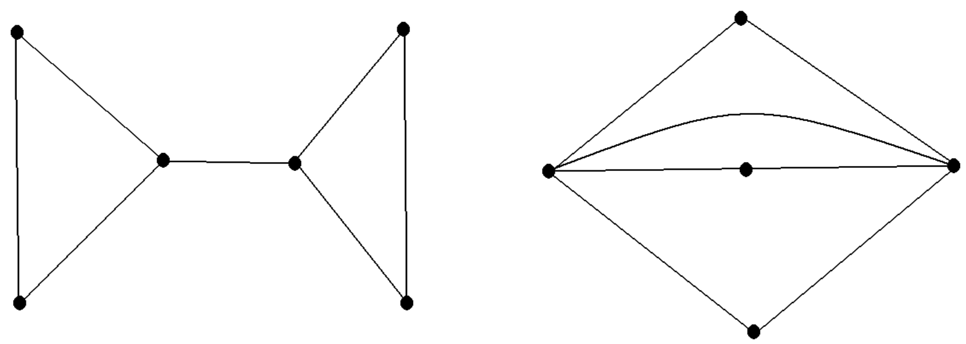
$$\begin{vmatrix} 1 & -1 & \cdots & -1 \\ 0 & n & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{vmatrix},$$

равному n^{n-2}. Значит, число помеченных остовных поддеревьев K_n равно n^{n-2}, а это и есть количество помеченных деревьев с n вершинами. ■

3.2.2. Обходы графов

3.2.2.1. Эйлеровы графы

Эйлеровой цепью графа называется простой маршрут, содержащий все его рёбра. *Эйлеровым циклом* графа называется содержащий все его рёбра замкнутый простой маршрут. Заметим, что эйлеров цикл не является циклом в смысле общего определения, так как в нём вершины могут проходиться неоднократно. Граф, в котором имеется эйлеров цикл, называется *эйлеровым.* Понятно, что эйлеров граф должен быть связным. На рис. 3.2.10, *а* показана диаграмма графа, не являющегося эйлеровым, на рис. 3.2.10, *б* — диаграмма эйлерова графа.



а. Неэйлеров граф б. Эйлеров граф

Рис. 3.2.10

Теорема 3.2.5

Для любого связного графа G эквивалентны следующие утверждения:

1) G — эйлеров граф;

2) каждая вершина имеет чётную степень;

3) существует разбиение множества рёбер графа на подмножества, при котором рёбра каждого подмножества образуют вместе с инцидентными им вершинами цикл.

Доказательство

(1) $\Rightarrow$ (2). При прохождении эйлерова цикла вход в вершину и выход из неё осуществляются по разным рёбрам, т. е. проход вершины вносит 2 в её степень, а поскольку каждое ребро появляется в цикле ровно один раз, любая вершина должна иметь чётную степень.

(2) $\Rightarrow$ (3). По условию G — связный граф, в котором каждая вершина имеет степень, не меньшую двух, поэтому в G существует цикл. Включим его рёбра в первый блок разбиения и удалим из G. Получится остовный подграф G_1 графа G, в котором каждая вершина также имеет чётную степень. Если в нём нет рёбер, то нужное разбиение построено. В противном случае применим те же рассуждения, что и к исходному графу G, получим второй блок разбиения и придём к остовному подграфу G_2, в котором степени всех вершин чётны и так далее. За конечное число шагов будет получен остовный подграф с пустым множеством рёбер, и построено разбиение рёбер G на блоки, каждый из которых образует цикл.

(3) $\Rightarrow$ (1). Пусть X_1 — один из блоков разбиения. Если рёбра X_1 вместе инцидентными вершинами составляют весь граф G, то очевидно, что G — эйлеров граф. В противном случае выберем блок X_2 такой, что существует вершина v, принадлежащая и циклу из рёбер X_1, и циклу из рёбер X_2 (такой блок найдётся в силу связности G). Если $v = v_0 x_1 v_1 \dots v_{k-1} x_k v_k = v$ — цикл из рёбер блока X_1, $v = u_0 y_1 u_1$ $y_2 u_2 \dots u_{s-1} y_s u_s = v$ — цикл из рёбер X_2, то $v = v_0 x_1 v_1 \dots v_{k-1}$ $x_k v_k y_1 u_1 y_2 u_2 \dots u_{s-1} y_s u_s = v$ — простой замкнутый маршрут (по-

второв рёбер в нём не может быть, потому что блоки разбиения X_1 и X_2 не пересекаются), содержащий рёбра $X_1 \cup X_2$. Продолжая эту процедуру, можно построить простой замкнутый маршрут, содержащий все рёбра G, следовательно, G — эйлеров граф. ■

Следствие

Граф имеет эйлерову цепь тогда и только тогда, когда он:

1) является связным;

2) содержит две вершины нечётной степени.

Доказательство

Необходимость очевидна, поэтому докажем только достаточность условий (1), (2). Пусть u и v — две вершины графа G, имеющие нечётную степень. Добавим к G ребро $\{u, v\}$, тогда все вершины расширенного графа G' будут иметь чётную степень. В силу связности G, а значит, и G' по теореме 3.2.5 в G' существует эйлерова цепь. Если из неё удалить ребро $\{u, v\}$, то получится открытый простой маршрут, соединяющий u и v и содержащий все рёбра исходного графа G. ■

3.2.2.2. Эйлеровы контуры в орграфах

Эйлеровым контуром называется замкнутый путь в орграфе, содержащий все вершины, в который каждая дуга входит ровно один раз. Заметим, что эйлеров контур не является контуром в смысле общего определения, так как в нём вершины могут повторяться. Орграф, в котором существует эйлеров контур, называется *эйлеровым.* Известен достаточно очевидный критерий того, что орграф является эйлеровым.

Теорема 3.2.6

Орграф является эйлеровым тогда и только тогда, когда:

1) он связен;

2) для каждой его вершины полустепень захода равна полустепени исхода.

Доказательство аналогично доказательству теоремы 3.2.5.

На рис. 3.2.11 представлены примеры диаграмм эйлеровых орграфов.

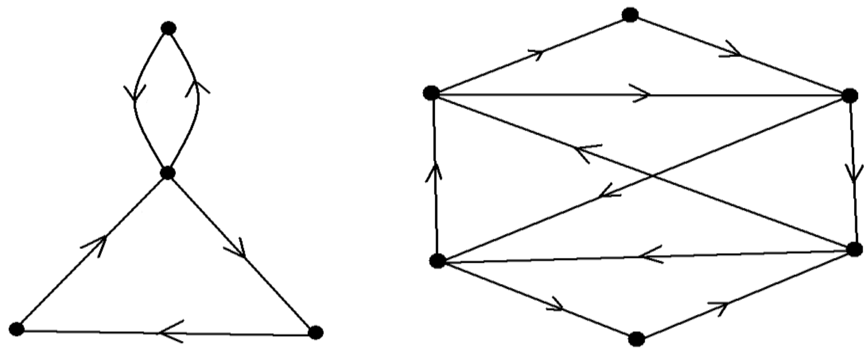


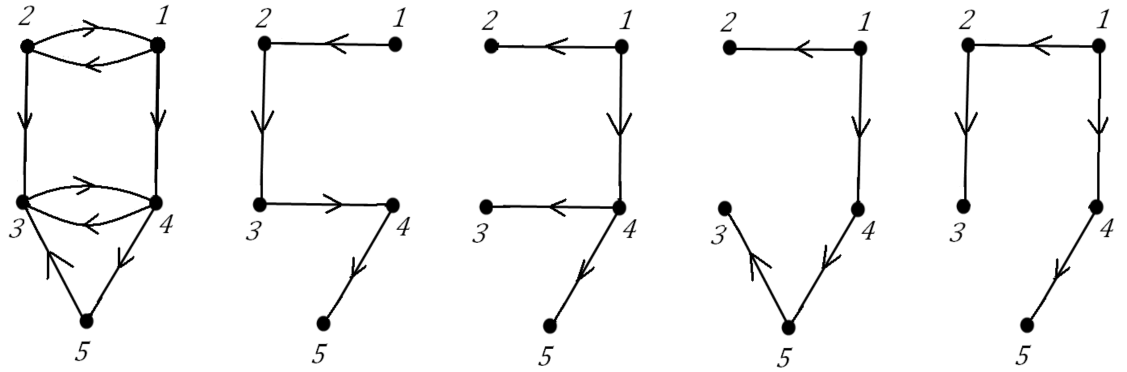
Рис. 3.2.11. Эйлеровы орграфы

Очевидно, что в помеченном эйлеровом орграфе существует несколько эйлеровых контуров. Решим задачу нахождения их числа в данном эйлеровом орграфе. Для этого сформулируем матричную теорему о деревьях для орграфов. Пусть G — орграф с матрицей смежности $\Omega(G)$. Определим диагональную матрицу $M_-(G)$, у которой $\left(M_-(G)\right)_{ii} = \delta_-(v_i)$ ($\delta_-(v)$— полустепень исхода вершины v). Далее вводим матрицу $C_-(G) = M_-(G) - \Omega(G)$.

Таким образом, сумма всех элементов каждой строки матрицы $C_-(G)$ равна 0, кроме того, из теоремы 6 следует, что сумма элементов каждого столбца равна 0 тогда и только тогда, когда G — эйлеров орграф. Аналогично определяется матрица $C_+(G) = M_+(G) - \Omega(G)$, где $M_+(G)$ — диагональная матрица, у которой $\left(M_+(G)\right)_{ii} = \delta_+(v_i)$ ($\delta_+(v)$— полустепень захода вершины v). Сумма всех элементов каждого столбца $C_+(G)$ равна 0, а сумма элементов каждой строки равна 0 тогда и только тогда, когда G — эйлеров орграф.

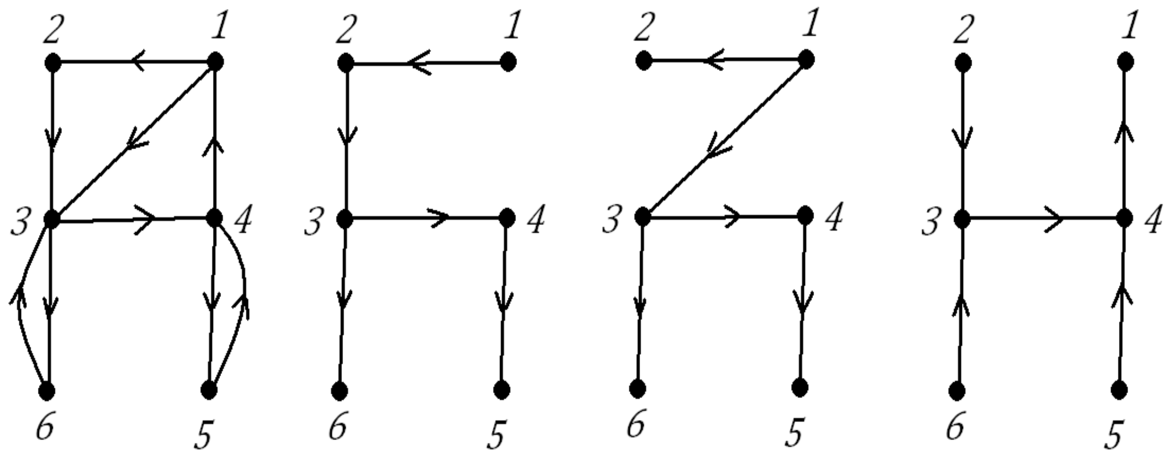
Корневым деревом называется дерево с выделенной вершиной — *корнем.* Пусть имеется орграф G. Будем говорить, что остовное корневое подордерево T_+ с корнем v *входит в вершину* v, если все его дуги ориентированы по направлению к v. Более строго, T_+ содержит только пути, составленные из дуг орграфа G, в которых v является конечной вершиной. Аналогично, остовное корневое подордерево T_- с корнем v *выходит из вершины* v, если все его дуги ориентированы по направлению от v, т. е. T_- содержит только пути из дуг G, начинающиеся в v.

Помеченный орграф, диаграмма которого показана на рис. 3.2.12, *а*, имеет 4 выходящих из вершины с пометкой 1 остовных подордерева, изображённых на рис. 3.2.12, *б*. Ориентированных остовов, входящих в вершину 1, нет.



а) б)

Рис. 3.2.12. Орграф (а) и выходящие из вершины деревья (б)



а) б) в)

Рис. 3.2.13. Орграф (а), выходящие (б) и входящие (в) деревья

У помеченного орграфа, диаграмма которого изображена на рис. 3.2.13, *а*, существуют два ориентированных остова, выходящих из корня с пометкой 1 (рис. 3.2.13, *б*), и один входящий (рис. 3.2.13, *в*). Теперь можно сформулировать *матричную теорему о деревьях для орграфов.*

Теорема 3.2.7

Пусть G — связный помеченный орграф.

1) Все алгебраические дополнения i-й строки матрицы $C_{-}(G)$ равны между собой, и их общее значение равно числу остовных подордеревьев, входящих в вершину v_i.

2) Все алгебраические дополнения j-го столбца матрицы $C_{+}(G)$ равны между собой, и их общее значение равно числу остовных подордеревьев, выходящих из вершины v_j.

Проиллюстрируем теорему на примере орграфов с рис. 3.2.12 и 3.2.13. Орграф, диаграмма которого изображена на рис. 3.2.12, a, имеет следующую матрицу смежности вершин:

$$\Omega(G)=\begin{pmatrix} 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Соответствующая матрица $C_{-}(G)$:

$$C_{-}(G)=M_{-}(G)-\Omega(G)=$$

$$=\begin{pmatrix} 2 & 0 & 0 & 0 & 0\\ 0 & 2 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}-\begin{pmatrix} 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}=$$

$$=\begin{pmatrix} 2 & -1 & 0 & -1 & 0\\ -1 & 2 & -1 & 0 & 0\\ 0 & 0 & 1 & -1 & 0\\ 0 & 0 & -1 & 2 & -1\\ 0 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

Вычислим алгебраическое дополнение элемента $\left(C_{-}(G)\right)_{11}$:

$$A_{11}=\begin{vmatrix} 2 & -1 & 0 & 0\\ 0 & 1 & -1 & 0\\ 0 & -1 & 2 & -1\\ 0 & -1 & 0 & 1 \end{vmatrix}=0.$$

Поэтому согласно теореме ориентированных остовов, входящих в вершину, помеченную 1, нет. Найдём с помощью теоремы число остовов, выходящих из вершины с пометкой 1. Матрица $C_{+}(G)$:

$$C_{+}(G)=M_{+}(G)-\Omega(G)=$$

$$=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & -1 & 0 & -1 & 0 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 3 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

Вычислим алгебраическое дополнение, например, элемента $\left(C_+(G)\right)_{21}$:

$$A_{21} = -\begin{vmatrix} -1 & 0 & -1 & 0 \\ 0 & 3 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & -1 & 0 & 1 \end{vmatrix} = 4.$$

Обратимся к графу с диаграммой на рис. 3.2.13, a. Его матрица смежности:

$$\Omega(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Далее вычисляем $C_-(G)$:

$$C_-(G) = M_-(G) - \Omega(G) =$$

$$= \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 2 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 & 0 & -1 \\ -1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

Алгебраическое дополнение элемента $\left(C_-(G)\right)_{11}$:

$$A_{11}=\begin{vmatrix}1&-1&0&0&0\\0&2&-1&0&-1\\0&0&2&-1&0\\0&0&-1&1&0\\0&-1&0&0&1\end{vmatrix}=1.$$

Найдём число выходящих из вершины с пометкой 1 остовов:

$$C_+(G)=M_+(G)-\Omega(G)=$$
$$=\begin{pmatrix}1&-1&-1&0&0&0\\0&1&-1&0&0&0\\0&0&3&-1&0&-1\\-1&0&0&2&-1&0\\0&0&0&-1&1&0\\0&0&-1&0&0&1\end{pmatrix}.$$

Алгебраическое дополнение элемента $\left(C_+(G)\right)_{11}$:

$$A_{11}=\begin{vmatrix}1&-1&0&0&0\\0&3&-1&0&-1\\0&0&2&-1&0\\0&0&-1&1&0\\0&-1&0&0&1\end{vmatrix}=2.$$

Итак, теорема даёт тот же результат, что был получен по диаграмме: орграф G имеет 2 ориентированных остова, выходящих из вершины с пометкой 1, и 1 входящий.

Теперь можно применить матричную теорему о деревьях для орграфов к выводу формулы числа эйлеровых контуров в данном орграфе. Так как в эйлеровом орграфе для каждой вершины $v_i \in V$ $\delta_+(v_i)=\delta_-(v_i)$, обозначим это число δ_i (v_i — вершина, помеченная числом i). Далее, поскольку $C_-(G)=C_+(G)$, если G — эйлеров орграф, то обозначим эту матрицу $C(G)$, a — общее значение алгебраических дополнений элементов матрицы $C(G)$ (понятно, что в этом случае все алгебраические дополнения матрицы $C(G)$ совпадают и равны числу остовов, входящих в произвольную вершину (исходящих из произвольной вершины)).

Теорема 3.2.8

Число $e(G)$ эйлеровых контуров в помеченном эйлеровом орграфе G порядка n, у которого алгебраические дополнения элементов матрицы $C(G)$ равны a, определяется формулой

$$e(G) = a\prod_{i=1}^{n}(\delta_i - 1)!.$$

Доказательство

Пусть v — произвольная вершина G. Покажем, что каждый эйлеров контур E в G определяет единственный остов T_+, входящий в вершину v.

Итак, имеются эйлеров контур E и вершина $v \in V$. Построим ориентированный остов, входящий в v и соответствующий E. Назовём последней дугой вершины $u \in V$, $u \neq v$, дугу, выходящую из u и проходимую последней при движении по контуру E, если начальной (и конечной) вершиной является v. Таким образом, во всём контуре E только v не будет иметь последней дуги. Составим подграф G из последних дуг и инцидентных им вершин. Понятно, что он будет остовным (E — эйлеров контур), а поскольку в нём полустепень исхода v равна 0, полустепени исхода всех остальных вершин — 1, то он является ордеревом, входящим в v, т. е. искомым остовом T_+. Из построения видно, что T_+ единственен.

Теперь покажем, что каждый такой остов T_+ определяет в точности $(\delta_1 - 1)!\,(\delta_2 - 1)! \cdots (\delta_n - 1)!$ эйлеровых контуров. Построим все такие контуры, связанные с T_+. Из любой вершины $v_i \in V$ (в том числе и из v) выходят δ_i дуг. Каждому эйлерову контуру соответствует упорядочение (перестановка) дуг, но одна дуга при этом не учитывается, поскольку она должна проходиться последней при движении по контуру. Кроме того, одна дуга, выходящая из v, также не переставляется при пересчёте контуров, так как она резервируется в качестве первой дуги контура E. Следовательно, для каждой вершины v_i существует ровно $(\delta_i - 1)!$ различных упорядочений дуг, исходящих из v_i, по их появлению в контуре E. Так как выборы дуг при каждой вершине происходят независимо друг от друга, по правилу произведения получаем число эйлеровых контуров, определяемых остовом T_+:

$$\prod_{i=1}^{n}(\delta_i - 1)!.$$

Учитывая, что количество ориентированных остовов, входящих в v, равно a, приходим к доказываемой формуле. ■

Следствие

Если в эйлеровом орграфе каждое δ_i, $i = 1, 2, \dots, n$, равно либо 1, либо 2, то число эйлеровых контуров равно количеству остовов, входящих в произвольную вершину.

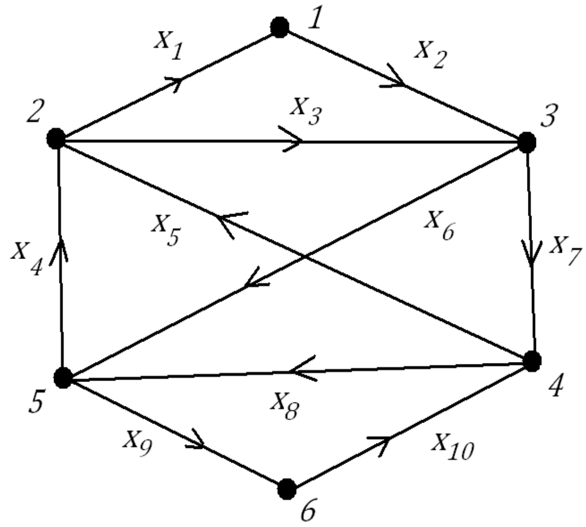


Рис. 3.2.14. Эйлеров орграф с δ_i, равными 1 или 2

Продемонстрируем это утверждение на примере помеченного эйлерова орграфа G с диаграммой на рис. 3.2.14. Все его δ_i равны либо 1, либо 2. Найдём число остовов, входящих в вершину с пометкой 1. Матрица $C(G)$:

$$C(G) = M_-(G) - \Omega(G) =$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & -1 & 0 & 2 & -1 & 0 \\ 0 & -1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

Матрица $e(G)$:

$$e(G) = a = A_{11} =$$

$$= \begin{vmatrix} 2 & -1 & 0 & 0 & 0 \\ 0 & 2 & -1 & -1 & 0 \\ -1 & 0 & 2 & -1 & 0 \\ -1 & 0 & 0 & 2 & -1 \\ 0 & 0 & -1 & 0 & 1 \end{vmatrix} = 6.$$

Получаем, что в G имеются 6 эйлеровых контуров. Они соответствуют 6 остовным подордеревьям, входящим в вершину, помеченную 1. Их диаграммы представлены на рис. 3.2.15. Ниже даны эти эйлеровы циклы в соответствии с остовами с рис. 3.2.15:

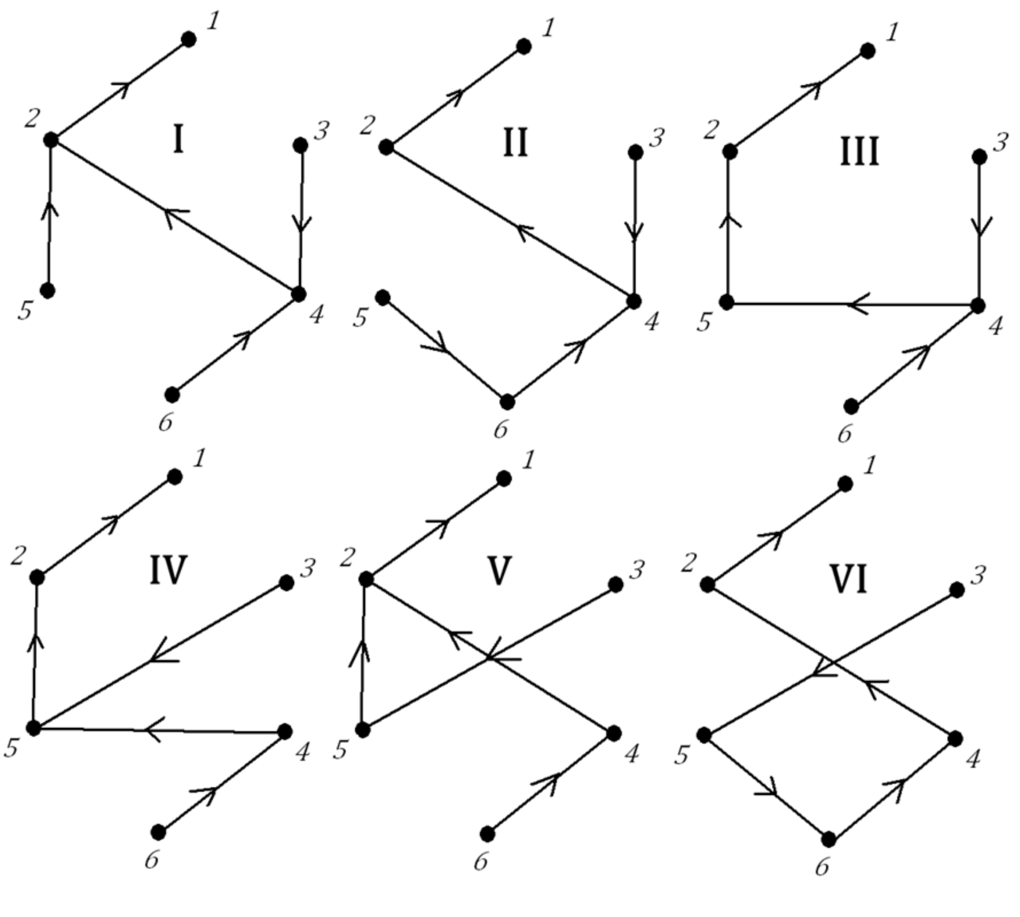


Рис. 3.2.15. Остовные поддеревья, входящие в вершину 1

I. $1x_2 3x_6 5x_9 6x_{10} 4x_8 5x_4 2x_3 3x_7 4x_5 2x_1 1$;
II. $1x_2 3x_6 5x_4 2x_3 3x_7 4x_8 5x_9 6x_{10} 4x_5 2x_1 1$;
III. $1x_2 3x_6 5x_9 6x_{10} 4x_5 2x_3 3x_7 4x_8 5x_4 2x_1 1$;
IV. $1x_2 3x_7 4x_5 2x_3 3x_6 5x_9 6x_{10} 4x_8 5x_4 2x_1 1$;
V. $1x_2 3x_7 4x_8 5x_9 6x_{10} 4x_5 2x_3 3x_6 5x_4 2x_1 1$;
VI. $1x_2 3x_7 4x_8 5x_4 2x_3 3x_6 5x_9 6x_{10} 4x_5 2x_1 1$.

3.2.2.3. Гамильтоновы графы

Гамильтоновым циклом в графе называется цикл, содержащий все его вершины. Если в графе имеется гамильтонов цикл, то он называется *гамильтоновым.* Таким образом, в гамильтоновом графе можно обойти все вершины по рёбрам и вернуться в начальную точку, причём каждая вершина (кроме начальной) будет пройдена ровно один раз. Задача эффективного описания гамильтоновых графов в настоящее время до конца не решена, известно лишь несколько необходимых и несколько достаточных условий существования гамильтоновых циклов. В данном пункте приведена одна теорема, дающая достаточное условие того, что граф гамильтонов.

Теорема 3.2.9 (теорема Поша)

Пусть граф G имеет $n \geq 3$ вершин. Если для любого p, $1 \leq p < \frac{n-1}{2}$, число вершин со степенями, не превосходящими p, меньше p, и для нечётного n число вершин степени $\frac{n-1}{2}$ не превосходит $\frac{n-1}{2}$, то G является гамильтоновым графом.

Доказательство

Предположим, что теорема неверна, G — максимальный негамильтонов граф порядка n, удовлетворяющий условиям теоремы. Очевидно, что добавление любого ребра в граф, обладающий указанными в формулировке теоремы свойствами, приводит к графу, также обладающему этими свойствами. В силу максимальности G добавление к нему любого ребра даёт гамильтонов граф, поэтому любые две насмежные вершины в G можно соединить цепью, содержащей все вершины G.

Покажем, что всякая вершина, степень которой не меньше $\frac{n-1}{2}$, смежна с каждой вершиной со степенью, большей $\frac{n-1}{2}$. Допустим, что $\deg(v_1) \geq \frac{n-1}{2}$, $\deg(v_s) > \frac{n-1}{2}$, но v_1 и v_s несмежны. Тогда существует (v_1, v_s)-цепь $v_1 v_2 \dots v_s$, содержащая все вершины G (в обозначении цепи опущены рёбра). Обозначим вершины, смежные v_1, через v_{i_1}, $v_{i_2}, \dots, v_{i_p}$, где $p = \deg(v_1)$, $2 = i_1 < i_2 < \dots < i_p$. Очевидно, что v_s не может быть смежна ни с одной вершиной v_{i_j-1}, поскольку тогда в G существовал бы гамильтонов цикл $v_1 v_2 \dots v_{i_j-1} v_s v_{s-1} \dots v_{i_j} v_1$. Поскольку $p = \deg(v_1) \geq \frac{n-1}{2}$, то $\deg(v_s) \leq n - 1 - p < \frac{n}{2}$, что невозможно в силу того, что $\deg(v_s) > \frac{n-1}{2}$. Поэтому v_1 и v_s смежны.

Отсюда вытекает, что из условия $\deg(v) \geq \frac{n}{2}$ для всех $v \in V$, следует, что G — гамильтонов граф. В силу доказанного выше и того, что G удовлетворяет условиям теоремы, каждая пара вершин смежна, т. е. G — полный граф. Но нетрудно доказать, что при любом $n \geq 3$ полный граф K_n является гамильтоновым.

Таким образом, в G существует хотя бы одна вершина степени, меньшей $\frac{n}{2}$. Пусть m — наибольшая среди степеней всех таких вершин и пусть $\deg(v_1) = m$. По условию теоремы число вершин со степенями, не превосходящими m, не больше $m < \frac{n}{2}$, поэтому должно быть больше m вершин со степенями, превосходящими m, а значит, не меньшими $\frac{n}{2}$. Следовательно, найдётся вершина v_s степени, не меньшей $\frac{n}{2}$, не смежная v_1. Выше было доказано, что тогда существует (v_1, v_s)-цепь $v_1 v_2 \dots v_s$, содержащая все вершины G. Вновь обозначим через $v_{i_1}, v_{i_2}, \dots, v_{i_m}$ смежные v_1 вершины G. Как было показано выше, v_s не может быть смежна ни одной из m вершин v_{i_j-1} $(1 \leq j \leq$ $\leq m)$. Но v_1 и v_s несмежны, v_s имеет степень, не меньшую $\frac{n}{2}$, поэтому, как было показано в первой части доказательства, $m < \frac{n-1}{2}$. Так как по условию число вершин со степенями, не превосходящими m, меньше m, то хотя бы одна из m вершин v_{i_j-1} $(1 \leq j \leq m)$ должна иметь степень, не меньшую $\frac{n}{2}$. Пусть v' — одна из таких вершин (может быть, единственная). Итак, установлено, что степени двух несмежных вершин v_s и v' не меньше $\frac{n}{2}$. Получили противоречие с доказанным в первой части (любые пары вершин, в которых степень одной не меньше $\frac{n-1}{2}$, а степень другой больше $\frac{n-1}{2}$, должны быть смежны). Теорема доказана. ■

Замечание

Данное в теореме достаточное условие не является необходимым. На рис. 3.2.16 приведена диаграмма гамильтонова графа, не удовлетворяющего условиям Поша.

Следствие 1 (теорема Оре)

Если $n \geq 3$ и $\deg(u) + \deg(v) \geq n$ для любой пары несмежных вершин u и v графа G, то G — гамильтонов граф.

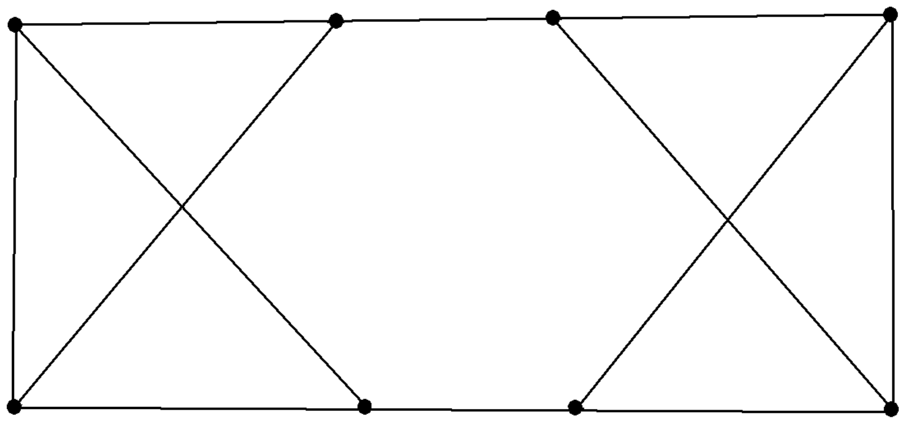


Рис. 3.2.16. Гамильтонов граф, не удовлетворяющий условиям Поша

Следствие 2 (теорема Дирака)

Если $n > 3$ и $\deg(v) \geq \frac{n}{2}$ для любой вершины v графа G, то G — гамильтонов граф.

3.2.3. Раскраски графов

3.2.3.1. Хроматическое число

Пусть $G = \langle V, X \rangle$ — произвольный граф без петель. *Раскрашенным графом* будем называть граф $G^C = \langle V, X, R^C \rangle$ с введённым на множестве V отношением эквивалентности R^C, при котором ни одна пара смежных вершин не принадлежит одному классу эквивалентности. Эти классы называются *цветами*. Таким образом, можно говорить, что вершины, входящие в один класс окрашены в один цвет, и никакие две смежные вершины не окрашены в один цвет. Если число цветов равно k, то граф будем называть *k-раскрашенным.* Два k-раскрашенных графа $G_1^C = \langle V_1, X_1, R_1^C \rangle$, $G_2^C = \langle V_2, X_2, R_2^C \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение $f: V_1 \to V_2$, сохраняющее смежность и цвета вершин. Более точно, если u и v смежны в G_1^C, то $f(u)$ и $f(v)$ смежны в G_2^C, если $\langle u, v \rangle \in R_1^C$, $u, v \in V_1$, то $\langle f(u), f(v) \rangle \in V_2$.

Хроматическое число $\chi(G)$ графа $G = \langle V, X \rangle$ определяется как наименьшее число k, при котором существует k-раскрашенный граф $G^C = \langle V, X, R^C \rangle$ (в этом случае говорят, что граф G имеет k-раскраску). Граф G называется *k-раскрашиваемым*, если $\chi(G) \leq k$, и *k-хроматическим*, если $\chi(G) = k$. Очевидно, что для любого графа G порядка n существуют n-раскраска и $\chi(G)$-раскраска, поэтому он должен иметь также k-раскраску для любого k, удовлетворяющего условию $\chi(G) < k < n$. Например, граф с диаграммой, изображённой на рис. 3.2.17, является *2*-хроматическим. На рис. 3.2.18 показаны его k-раскраски для $k = 2,\ 3,\ 4,\ 5$. Хроматические числа некоторых графов легко находятся, например, для полного графа K_n $\chi(K_n) = n$, $\chi(K_n \backslash x) = n - 1$, x — произвольное ребро K_n; $\chi(T) = 2$ для любого дерева T с не менее чем двумя вершинами; $\chi(C) = 2$, если C — цикл чётной длины, $\chi(C) = 3$ для цикла C нечётной длины. Очевидно, что граф является *1*-хроматическим тогда и только тогда, когда он регулярный степени 0 (такие графы называются *вполне несвязными*).

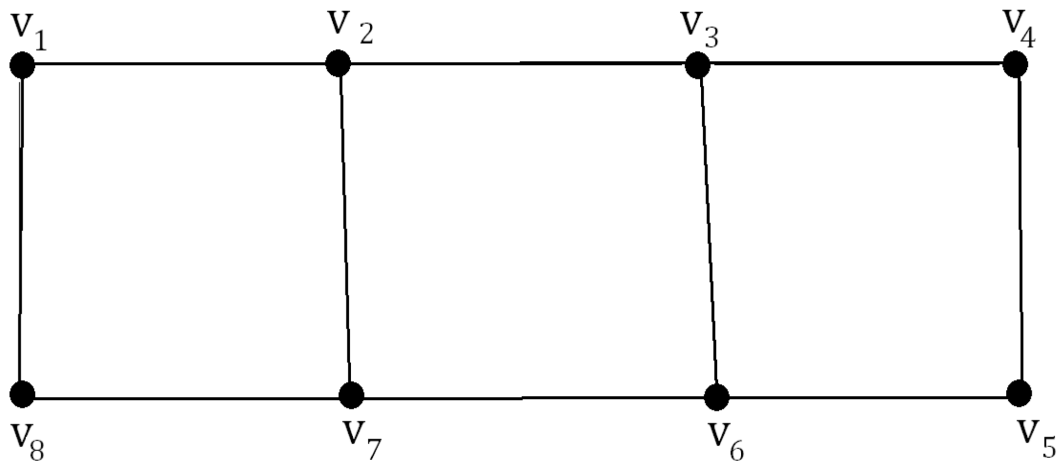


Рис. 3.2.17. *2*-хроматический граф

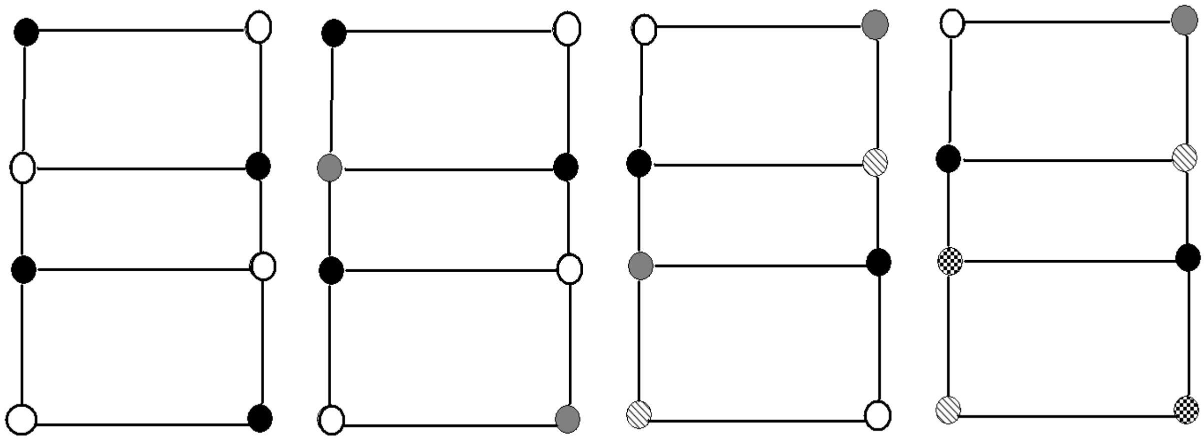


Рис. 3.2.18. 2, 3, 4, 5-раскраски *2*-хроматического графа

Описание *2*-раскрашиваемых графов дано в следующей теореме.

Теорема 3.2.10 (теорема Кёнига)

Граф является *2*-раскрашиваемым тогда и только тогда, когда он не содержит циклов нечётной длины.

Проблема описания k-раскрашиваемых графов при $k \geq 3$ до сих пор эффективно не решена, неизвестны также методы определения хроматического числа произвольного графа.

3.2.3.2. Хроматический многочлен

Пусть G — помеченный граф. *Раскраской графа* t *цветами* называется любая его k-раскраска, у которой $k \leq t$. Две раскраски графа t цветами будем считать различными, если по крайней мере одной вершине приписываются разные цвета.

Обозначим через $f_G(z)$ число различных раскрасок помеченного графа G z цветами. Очевидно, что $f_G(z) = 0$ при $z < \chi(G)$ и наименьшее z, для которого $f_G(z) > 0$, равно $\chi(G)$. Непосредственным подсчётом можно найти $f_G(z)$ для полного и вполне несвязного графов.

Лемма 3.2.2

1) $f_{K_n}(z) = z(z-1)\cdots(z-n+1) = (z)_n$;

2) $f_G(z) = z^n$, если G — вполне несвязный граф порядка n.

Убедимся в том, что $f_G(z)$ для любого графа является многочленом от z. Для этого установим вспомогательное утверждение.

Лемма 3.2.3

Если u и v — несмежные вершины графа G, то

$$f_G(z) = f_{G+\{u,v\}}(z) + f_{G'}(z),$$

где $G + \{u, v\}$ — граф G с добавленным ребром $\{u, v\}$, G' — граф, полученный из G отождествлением вершин u и v.

Доказательство

Разобьём все раскраски графа G t цветами (их число равно $f_G(z)$) на два класса. В первый включим те из них, в которых u и v окрашены в разные цвета, во второй — те, при которых они окрашены в один цвет. Очевидно, что первый класс насчитывает $f_{G+\{u,v\}}(z)$ раскрасок, второй — $f_{G'}(z)$. Поскольку классы не пересекаются, по правилу суммы получаем нужную формулу. ■

Теорема 3.2.11

Для любого графа G $f_G(z)$ является многочленом от z.

Доказательство

Если G — неполный граф с n вершинами и m рёбрами, то согласно лемме 3 существуют такие графы G_1 с $m+1$ рёбрами и G_2 с $n-1$ вершинами, что $f_G(z) = f_{G_1}(z) + f_{G_2}(z)$. Применим снова лемму 3 к $f_{G_1}(z)$ и $f_{G_2}(z)$ и так далее до тех пор, пока в получаемых графах не исчезнут несмежные вершины, т. е. пока в сумме не будут фигурировать только $f_G(z)$ полных графов. Но по лемме 3.2.2 все такие $f_G(z)$ равны $(z)_n$, т. е. являются многочленами от z. Следовательно, $f_G(z)$

исходного графа представляет собой сумму многочленов, а значит, является многочленом. ■

Многочлен f_G называется *хроматическим многочленом* графа G. Лемма 3.2.3 даёт алгоритм рекуррентного построения хроматического многочлена.

Найдём, например, f_G графа G, диаграмма которого показана на рис. 3.2.19, *а*. Согласно лемме $f_G(z) = f_{K_4}(z) + f_{K_3}(z)$ (см. рис. 3.2.19, *б*). Отсюда получаем

$$f_G(z) = z(z-1)(z-2)(z-3) + z(z-1)(z-2) =$$
$$= z^4 - 5z^3 + 8z^2 - 4z.$$

В частности, G можно раскрасить в 3 цвета $f_G(3) = 6$ способами, в 4 цвета — $f_G(4) = 48$ способами.

Непосредственно из леммы 3.2.3 вытекают свойства хроматических многочленов, данные в следующей теореме.

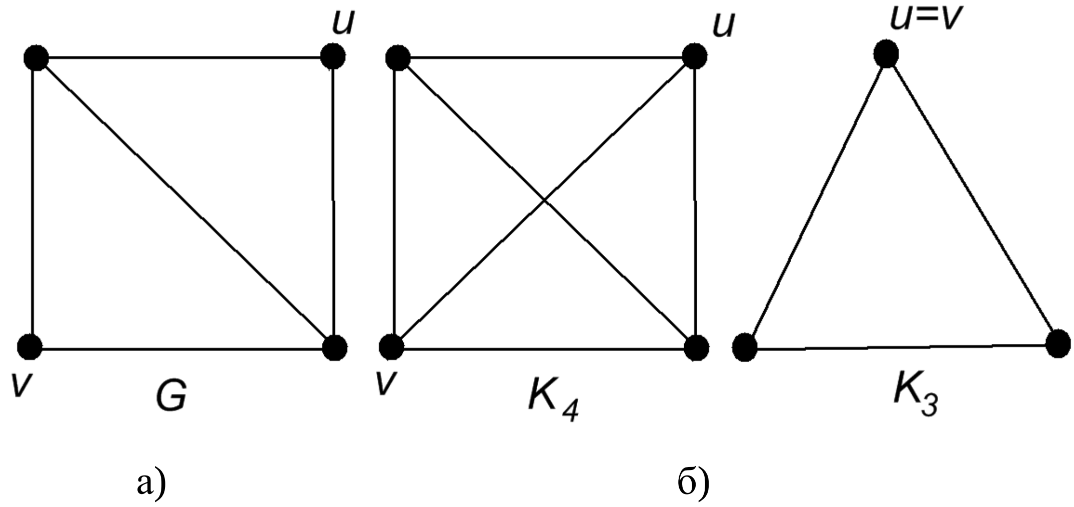


Рис. 3.2.19. Граф G (а) и его разложение на K_4 и K_3 (б)

Теорема 3.2.12

Пусть G — граф с n вершинами, m рёбрами и d компонентами связности $G_1, G_2, \ldots, G_d$. Тогда:

1) многочлен f_G имеет степень n;

2) старший коэффициент f_G равен 1;

3) коэффициент при z^{n-1} равен $-m$;

4) свободный член f_G равен нулю;

5) $f_G(z) = f_{G_1}(z) f_{G_2}(z) \cdots f_{G_d}(z)$;

6) наименьший показатель степени z, входящей в f_G с ненулевым коэффициентом, равен d.

Понятно, что любые два изоморфных помеченных графа имеют один и тот хроматический многочлен. Однако существуют неизоморфные графы, имеющие один и тот же f_G.

Теорема 3.2.13

Граф G порядка n является деревом тогда и только тогда, когда $f_G(z) = z(z-1)^{n-1}$.

Доказательство

Пусть T_n — помеченное дерево с n вершинами. Индукцией по n докажем, что $f_{T_n}(z) = z(z-1)^{n-1}$. База индукции $n = 1$ очевидна. Предположение индукции: хроматический многочлен любого дерева с n вершинами имеет вид $z(z-1)^{n-1}$. Доказываем индукционный шаг. Рассмотрим дерево T_{n+1}, пусть v — его концевая вершина (её существование гарантируется теоремой 3.1.9), u — единственная инцидентная v вершина T_{n+1}. По индукционному предположению хроматический многочлен дерева $T_n' = T_{n+1} \setminus \{u, v\}$ (то, что T_n' является деревом, следует из леммы 3.1.2) равен $f_{T_n'}(z) = z(z-1)^{n-1}$. Вершину v можно окрасить в любой цвет, отличный от цвета u, поэтому имеем $z - 1$ способов приписать какой-либо цвет v. По правилу произведения получаем

$$f_{T_{n+1}}(z) = (z-1) f_{T_n'}(z) = z(z-1)^n.$$

Индукционный шаг доказан.

Докажем достаточность. Пусть у графа G

$$f_G(z) = z(z-1)^{n-1}.$$

Так как коэффициент при z ненулевой, то по теореме 3.2.12, утверждение 6, $k = 1$, т. е. G связен. Далее, из разложения

$$f_G(z) = z(z-1)^{n-1} = z(z^{n-1} - (n-1)z^{n-2} + C_{n-1}^2 z^{n-3} - \cdots) =$$
$$= z^n - (n-1)z^{n-1} + C_{n-1}^2 z^{n-2} - \cdots$$

следует, что коэффициент при z^{n-1} равен $-(n-1)$, поэтому по теореме 3.2.12, утверждение 3, граф имеет $n-1$ рёбер. Из теоремы 3.1.10, следует, что G — дерево. ■

3.2.3.3. Число k-раскрашенных графов

В этом пункте будет выведена формула числа помеченных k-раскрашенных графов порядка n. Пусть $n_1, n_2, \dots, n_k$ — натуральные числа, образующие композицию числа n:

$$\sum_{i=1}^{k} n_i = n. \qquad (3.2.1)$$

Теорема 3.2.14 (теорема Рида)

Число $C_n(k)$ помеченных k-раскрашенных графов порядка n равно

$$C_n(k) = \frac{1}{k!} \sum_{\substack{\langle n_1, n_2, \dots, n_k \rangle \\ 0 < n_i < n \\ n_1 + n_2 + \cdots + n_k = n}} P(n_1, n_2, \dots, n_k)\, 2^{(n^2 - \sum n_i^2)/2}, \qquad (3.2.2)$$

где $P(n_1, n_2, \dots, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}$ — число перестановок с повторениями.

Доказательство

Число помеченных k-раскрашенных графов с фиксированными k цветами равно $k!\, C_n(k)$. Поэтому будем считать цвета фиксированными. Количество способов раскрасить n вершин в k цветов так, чтобы в i-й цвет было окрашено n_i вершин, равно числу перестановок n_1 одинаковых пометок цвета 1, n_2 — цвета 2 и так далее, т. е. числу перестановок с повторениями $P(n_1, n_2, \dots, n_k)$. Очевидно, что существуют

$$C_n^2 - \sum_{i=1}^{k} C_{n_i}^2$$

пар вершин разного цвета. Преобразуем последнее выражение:

$$C_n^2 - \sum_{i=1}^{k} C_{n_i}^2 = \frac{n(n-1)}{2} - \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2} = \frac{n^2}{2} - \frac{n}{2} -$$

$$-\sum_{i=1}^{k} \frac{n_i^2}{2} + \sum_{i=1}^{k} \frac{n_i}{2} = \frac{n^2}{2} - \sum_{i=1}^{k} \frac{n_i^2}{2} = \frac{n^2 - \sum n_i^2}{2}$$

(здесь было использовано условие (3.2.1)). Поскольку каждая пара вершин может быть либо смежной, либо нет, то $2^{(n^2-\sum n_i^2)/2}$ равно общему числу графов с n_i вершинами цвета i, $i = 1, 2, \dots, k$. А с учётом возможностей вариации вершин одного цвета получаем

$$P(n_1, n_2, \dots, n_k) 2^{(n^2-\sum n_i^2)/2}$$

k-раскрашенных помеченных графов с n_i вершинами i-го цвета. Суммируя эти числа по всем упорядоченным решениям уравнения (3.2.1) в натуральных числах, получаем количество k-раскрашенных помеченных графов с фиксированными k цветами, т. е. $k!\,C_n(k)$:

$$k!\,C_n(k) = \sum_{\substack{\langle n_1, n_2, \dots, n_k \rangle \\ 0<n_i<n \\ n_1+\dots+n_k=n}} P(n_1, n_2, \dots, n_k)\, 2^{(n^2-\sum n_i^2)/2},$$

откуда и следует доказываемая формула. ■

Следствие

Величину $C_n(k)$ можно вычислять рекурсивно по формуле

$$C_n(k) = \frac{1}{k} \sum_{i=1}^{n-1} C_n^i 2^{i(n-i)}\, C_i(k-1). \qquad (3.2.3)$$

Утверждение доказывается непосредственной подстановкой (3.2.2) в (3.2.3).

3.2.4. Ациклические орграфы

3.2.4.1. Расширения ациклических орграфов

Орграф, не имеющий контуров, называется *ациклическим.* На рис. 3.2.20 представлены примеры диаграмм ациклических орграфов. Решим более простую задачу перечисления помеченных ациклических орграфов. Эта же проблема для непомеченных орграфов гораздо сложнее и требует привлечения методов теории Пойа.

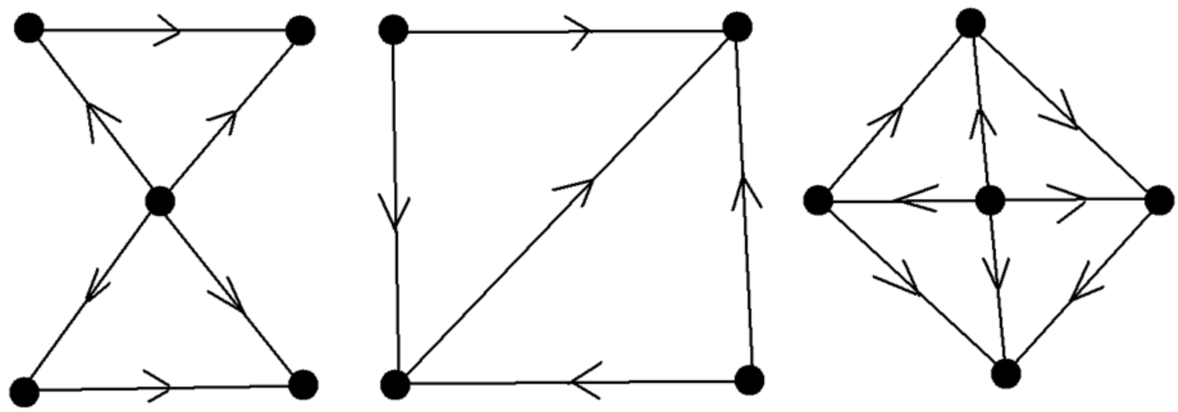


Рис. 3.2.20 Ациклические орграфы

Орграф $\hat{G}$ называется *расширением* орграфа G, если G является подорграфом $\hat{G}$, порождённым подмножеством вершин $\hat{G}$, имеющих положительные полустепени захода. Рассмотрим расширения ациклических орграфов. Нетрудно доказать, что любой ациклический орграф имеет по крайней мере одну вершину с нулевой полустепенью захода. Следовательно, каждый нетривиальный (имеющий хотя бы одну дугу) ациклический орграф является расширением некоторого собственного подорграфа. Будем считать, что он есть расширение единственного собственного ориентированного подграфа, порождённого максимальным подмножеством вершин с положительными полустепенями захода.

Пусть G — ациклический орграф, имеющий $k \geq 1$ вершин v_1, $v_2, \ldots, v_k$ с нулевыми полустепенями захода, остальные вершины (т. е. имеющие положительные полустепени захода) обозначим u_1, $u_2, \ldots, u_s$ ($k + s = n$, n — число вершин). Построим расширение G, содержащее ровно l вершин с нулевой полустепенью захода. Для этого добавляем к G вершины $w_1, w_2, \ldots, w_l$ и дуги такие, что каждая из вершин w_i может быть смежна любой вершине G, но при этом она должна быть начальной (естественно, для того, чтобы полустепени захода w_i были нулевыми, они не должны быть смежны друг другу); кроме того, каждая из k вершин v_i смежна некоторой вершине w_i и при этом является конечной. Таким образом, построенный орграф $\hat{G}$ представляет собой расширение G, содержащее ровно l вершин с нулевой полустепенью захода. Очевидно, что $\hat{G}$ является ациклическим орграфом.

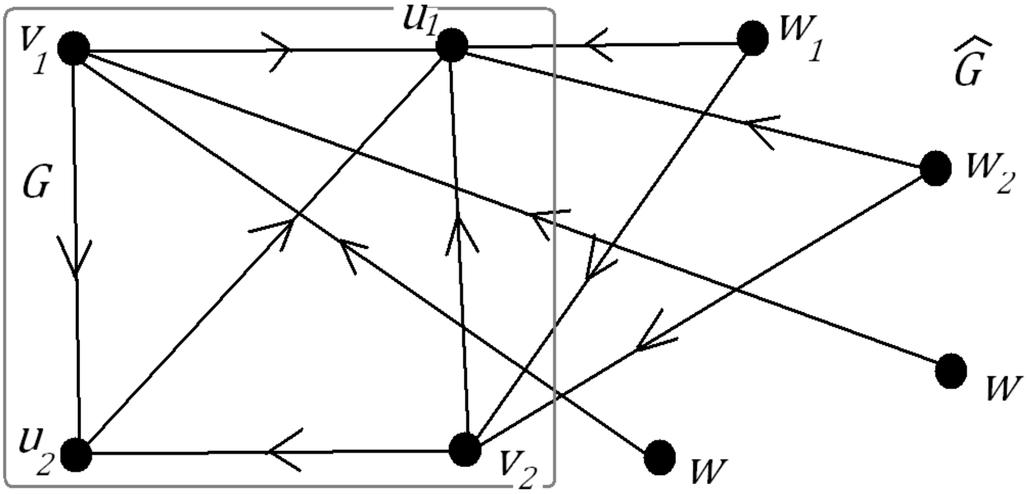


Рис. 3.2.21. Расширение ациклического орграфа

На рис. 3.2.21 показано такое расширение одного из орграфов с рис. 3.2.20. Таким образом, каждому ациклическому орграфу соответствует бесконечное множество расширений, являющихся ациклическими орграфами. Следовательно, все ациклические орграфы порядка n могут быть получены расширением ациклических орграфов порядков, меньших n.

3.2.4.2. Число помеченных ациклических орграфов

Пусть A_n — число помеченных ациклических орграфов порядка n, $A_{n,k}$ — количество таких же орграфов с k вершинами нулевой полустепени захода. Очевидно, что

$$A_n = \sum_{k=1}^{n} A_{n,k}$$

($A_{n,n} = 1$, так как единственный ациклический орграф, в котором все вершины имеют нулевые полустепени захода, — вполне несвязный граф). Если найти эффективный метод вычисления $A_{n,k}$, то задача будет решена. Этот метод, вернее, рекуррентную формулу, даёт следующая теорема.

Теорема 3.2.15

Число $A_{n,k}$ помеченных ациклических орграфов порядка n с k вершинами нулевой степени захода удовлетворяет рекуррентному соотношению

$$A_{n,k} = C_n^k \sum_{i=1}^{n-k} (2^k - 1)^i 2^{k(n-i-k)} A_{n-k,i}.$$

Доказательство

Пусть $i \leq n - k$. Найдём число помеченных расширений с помощью k новых вершин всех $A_{n-k,i}$ ациклических орграфов порядка $n - k$, имеющих i вершин с нулевыми полустепенями захода. Пусть G является одним из таких орграфов, к нему добавляются вершины w_1, $w_2, \dots, w_k$. Всего в расширенном орграфе будет $n - k + k = n$ вершин. Расставить пометки новым вершинам можно C_n^k способами.

Далее, каждая из новых вершин может быть смежна или несмежна с фиксированной вершиной v_j нулевой полустепени захода. Поскольку при этом v_j должна быть конечной, то имеем 2^k способов направить дуги от $w_1, w_2, \dots, w_k$ к v_j. При этом один способ, при котором ни одна дуга не направляется, не годится, так как v_j должна быть смежна по крайней мере одной из новых вершин, следовательно, имеем $2^k - 1$ способов для v_j. Так как всего в G i вершин с нулевыми полустепенями захода, по правилу произведения получаем $(2^k - 1)^i$ способов соединить дугами новые вершины с v_j, $j = 1, 2, \dots, i$.

Теперь подсчитаем способы направлений дуг от новых вершин к вершинам G с положительными полустепенями захода. Любая вершина w_p может быть смежна либо несмежна с каждой из $n - i - k$ вершин u_j. Так как направление дуг задано (от w_p), то имеем 2^{n-i-k} способов их направления от w_p, $p = 1, 2, \dots, k$, и поскольку всего добавлено k новых вершин, то получаем $(2^{n-i-k})^k = 2^{k(n-i-k)}$ способов для всех вершин.

Комбинируя способы расстановки пометок (C_n^k) новым вершинам, направления дуг от них к вершинам с нулевыми полустепенями захода ($(2^k-1)^i$) и с положительными полустепенями ($2^{k(n-i-k)}$), по правилу произведения получаем $(2^k-1)^i 2^{k(n-i-k)} C_n^k$ способов расширить G добавлением k новых вершин. Следовательно, для всех $A_{n-k,i}$ орграфов получится

$$(2^k-1)^i 2^{k(n-i-k)} C_n^k A_{n-k,i}$$

расширений. Если теперь просуммировать эти величины по всем i от 1 до $n-k$, то придём к доказываемой формуле. ■

3.2.5. Теорема Пойа и перечисление графов

В данной главе обзорно изложены основные результаты, полученные в области перечислительных методов теории графов с помощью теоремы Пойа. Целью данного обзора является демонстрация возможностей теоремы перечисления Пойа как мощного средства решения комбинаторных задач, связанных с подстановками данного множества.

3.2.5.1. Перечисление корневых деревьев

Напомним, что деревом называется связный граф без циклов, корневым деревом называется дерево с выделенной вершиной — корнем. Примером корневого дерева может служить дерево поиска в теории алгоритмов. Корень — точка начала поиска.

Пусть Y — множество всех корневых деревьев. Введём для них скалярную (одномерную) весовую характеристику, полагая вес дерева равным числу его вершин. Тогда производящая функция весовой спецификации фигур множества Y имеет вид

$$F(z) = \sum_{n=1}^{\infty} a(n) z^n,$$

где $a(n)$ — число различных корневых деревьев с n вершинами.

На рис. 3.2.22 показаны все корневые деревья с четырьмя вершинами, $a(4) = 4$.

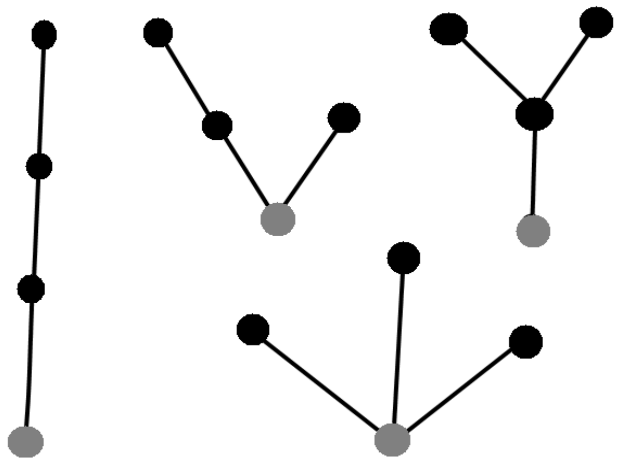


Рис. 3.2.22. Корневые деревья с четырьмя вершинами

Очевидно, что каждому корневому дереву, в котором корень инцидентен m рёбрам, можно поставить во взаимно однозначное соответствие m корневых деревьев, полученных удалением корня с инцидентными ему рёбрами. Корнями новых деревьев являются смежные корню исходного дерева вершины. На рис. 3.2.23 слева показано корневое дерево с тремя инцидентными корню вершинами, а справа — соответствующие ему три «расщеплённых» дерева.

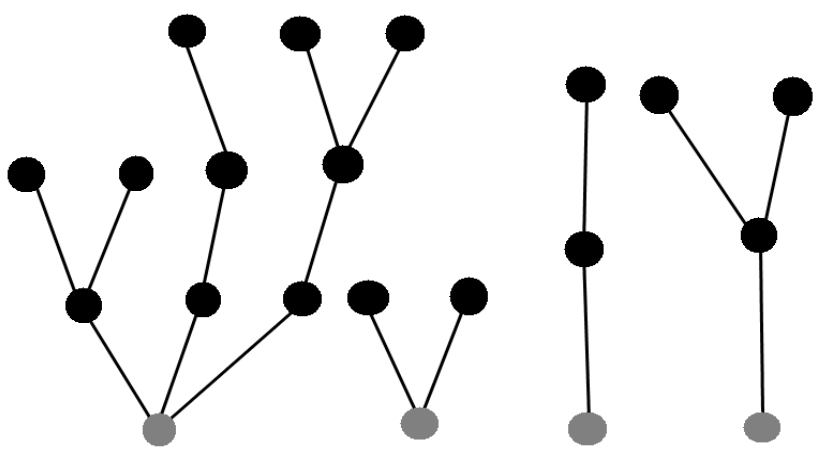


Рис. 3.2.23. Расщепление корневого дерева

Поэтому каждому корневому дереву взаимно однозначным образом соответствует класс эквивалентности на Y^X, $X = \{1, 2, \ldots, m\}$, порождённый симметрической группой $\mathfrak{S}_m$ степени m. Тогда производящая функция весовой спецификации неэквивалентных конфигураций имеет вид

$$\Phi_m(z, \mathfrak{S}_m) = \sum_{n=m+1}^{\infty} b_m(n) z^n,$$

где $b_m(n)$ — число корневых деревьев с n вершинами и m инцидентными корню рёбрами. По теореме Пойа эта функция выражается через цикловой индекс симметрической группы $\mathfrak{S}_m$ и производящую функцию весовой спецификации фигур формулой

$$\Phi_m(z, \mathfrak{S}_m) = z P_{\mathfrak{S}_m}\big(F(z), F(z^2), \ldots, F(z^m)\big), \qquad (3.2.4)$$

где множитель z появляется вследствие необходимости добавления корневой вершины к m корневым деревьям для получения одного корневого дерева.

Пусть $C_{\mathfrak{S}_m}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ — количество подстановок группы $\mathfrak{S}_m$ циклового класса $1^{\alpha_1} 2^{\alpha_2} \ldots m^{\alpha_m}$, $\alpha_1 + 2\alpha_2 + \cdots + m\alpha_m = m$. Производящая функция чисел $C_{\mathfrak{S}_m}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ называется *цикловым индикатором* группы $\mathfrak{S}_m$:

$$F_C(z_1, z_2, \ldots, z_m; \mathfrak{S}_m) = \\ = \sum_{\substack{\langle \alpha_1, \alpha_2, \ldots, \alpha_m \rangle \\ 0 \le \alpha_i \le m \\ \alpha_1 + 2\alpha_2 + \cdots + m\alpha_m = m}} C_{\mathfrak{S}_m}(\alpha_1, \alpha_2, \ldots, \alpha_m)\, z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_m^{\alpha_m}.$$

Построим экспоненциальную производящую функцию для циклового индикатора группы:

$$E_C(t) = \sum_{n=0}^{\infty} F_C(z_1, z_2, \ldots, z_n; \mathfrak{S}_n) \frac{t^n}{n!}$$

и вычислим её. В пункте 1.1.2.3 была выведена формула (1.1.8) для $C_{\mathfrak{S}_m}(\alpha_1, \alpha_2, \ldots, \alpha_m)$:

$$C_{\mathfrak{S}_m}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \frac{m!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \cdots \cdot m^{\alpha_m} \alpha_1! \, \alpha_2! \cdots \alpha_m!}. \qquad (3.2.5)$$

Запишем следующие формальные равенства:

$$\exp\left(\sum_{j=1}^{\infty}\frac{z_j t^j}{j}\right)=\prod_{j=1}^{\infty}\exp\left(\frac{z_j t^j}{j}\right)=\prod_{j=1}^{\infty}\left(\sum_{\alpha_j=0}^{\infty}\left(\frac{z_j t^j}{j}\right)^{\alpha_j}\frac{1}{\alpha_j!}\right).$$

Здесь было применено разложение функции e^x в степенной ряд:

$$e^x=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots=\sum_{n=0}^{\infty}\frac{x^n}{n!}.$$

Теперь перемножим скобки в правой части последнего равенства и запишем произведение в виде суммы, введя обозначение $1\cdot\alpha_1+$ $+2\alpha_2+\cdots+m\alpha_m=m$:

$$\exp\left(\sum_{j=1}^{\infty}\frac{z_j t^j}{j}\right)=$$

$$=\sum_{m=0}^{\infty}\frac{t^m}{m!}\sum_{\substack{\langle\alpha_1,\alpha_2,\dots,\alpha_m\rangle\\ 0\le\alpha_i\le m\\ \alpha_1+2\alpha_2+\cdots+m\alpha_m=m}}\frac{m!}{1^{\alpha_1}\cdot 2^{\alpha_2}\cdot\cdots\cdot m^{\alpha_m}\alpha_1!\,\alpha_2!\cdots\alpha_m!}\times$$

$$\times z_1^{\alpha_1}z_2^{\alpha_2}\cdots z_m^{\alpha_m}.$$

Из полученного равенства и (3.2.5) следует, что

$$E_C(t)=\exp\left(\sum_{j=1}^{\infty}\frac{z_j t^j}{j}\right).$$

Из этого общего результата сразу же вытекает выражение для производящей функции циклового индекса:

$$\sum_{m=0}^{\infty}P_{\mathfrak{S}_m}(z_1,z_2,\dots,z_m)t^m=\exp\left(\sum_{k=1}^{\infty}\frac{z_k t^k}{k}\right).$$

Из этого равенства, в свою очередь, получаем

$$\sum_{m=0}^{\infty}P_{\mathfrak{S}_m}\left(F(z),F(z^2),\dots,F(z^m)\right)t^m=\exp\left(\sum_{k=1}^{\infty}F(z^k)\frac{t^k}{k}\right).\quad(3.2.6)$$

Подстановка (3.2.4) в (3.2.6) даёт

$$\sum_{m=0}^{\infty} \frac{\Phi_m(z, \mathfrak{S}_m)}{z} t^m = \exp\left(\sum_{k=1}^{\infty} F(z^k) \frac{t^k}{k}\right) \Rightarrow$$

$$\Rightarrow \sum_{m=0}^{\infty} \Phi_m(z, \mathfrak{S}_m) t^m = z \exp\left(\sum_{k=1}^{\infty} F(z^k) \frac{t^k}{k}\right) \qquad (3.2.7)$$

(очевидно, что $\Phi_0(z, \mathfrak{S}_0) = z$). Поскольку

$$F(z) = \sum_{m=0}^{\infty} \Phi_m(z, \mathfrak{S}_m),$$

то, полагая в (3.2.7) $t = 1$, приходим к известному *соотношению Кэли-Пойа*

$$F(z) = z \exp\left(\sum_{k=1}^{\infty} \frac{F(z^k)}{k}\right),$$

представляющему собой функциональное уравнение для производящей функции чисел $a(n)$ корневых деревьев с n вершинами.

3.2.5.2. Перечисление графов

Пусть g_n — перечисляющий многочлен графов порядка n, т. е.

$$g_n(z) = \sum_{m} g_{n,m} z^m,$$

где $g_{n,m}$ — число графов с n вершинами и m рёбрами, суммирование ведётся по всем возможным значениям m (под графами здесь подразумеваются непомеченные простые графы, поэтому m конечно и не превосходит C_n^2). Таким образом, общее число g_n графов порядка n равно $g(1)$.

Перебрав все графы с четырьмя вершинами (рис. 3.2.24), получаем

$$g_4(z) = 1 + z + 2z^2 + 3z^3 + 2z^4 + z^5 + z^6.$$

Всего имеются $1 + 1 + 2 + 3 + 2 + 1 + 1 = 11$ графов порядка 4. Пересчёт всех графов с пятью вершинами даёт

$$g_5(z) = 1 + z + 2z^2 + 4z^3 + 6z^4 +$$
$$+6z^5 + 6z^6 + 4z^7 + 2z^8 + z^9 + z^{10}\ , g_5 = g_5(1) = 34.$$

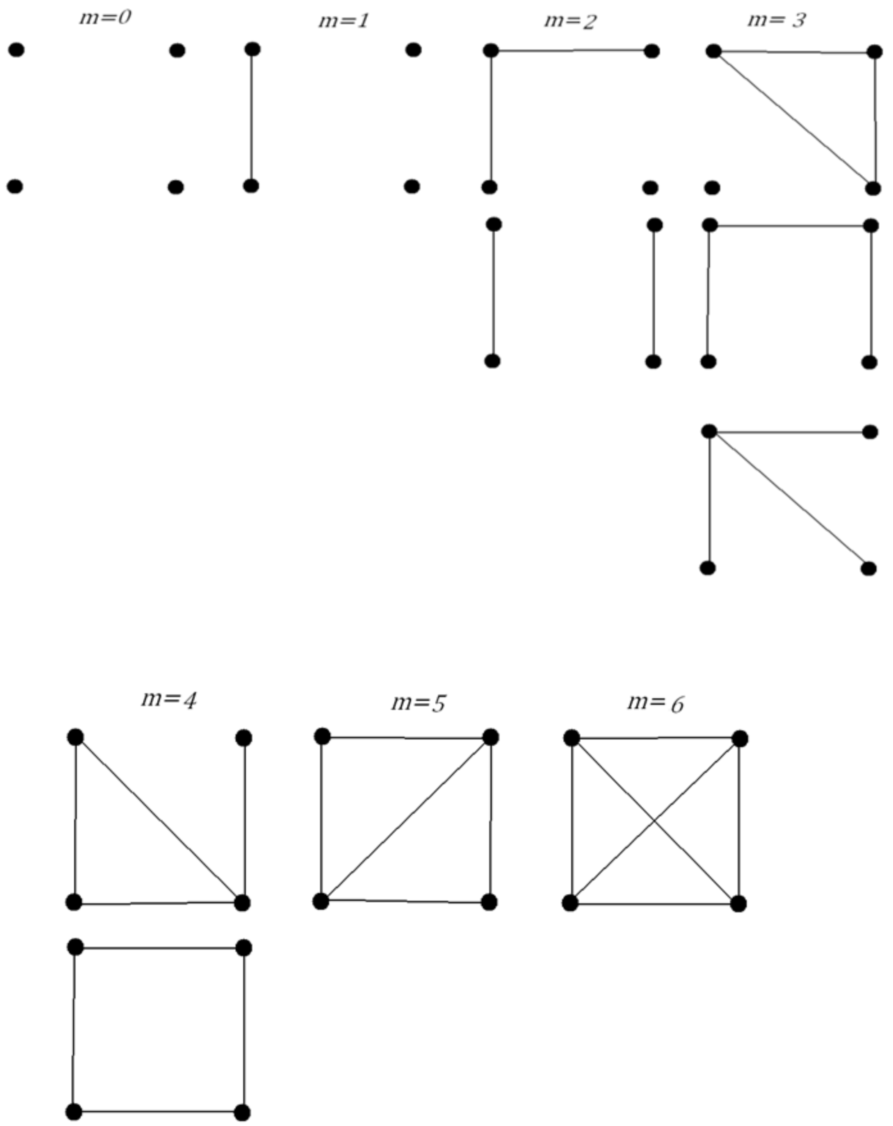


Рис. 3.2.24. Графы с четырьмя вершинами

Опишем метод получения g_n для любого n. Для этого необходимо формализовать граф в терминах отображений множеств. Пусть $V = \{1, 2, \dots, n\}$ — множество вершин графа (вершина v_i для краткости обозначается числом i), $B = \{0, 1\}$, $V^{(2)}$ — множество (2)-подмножеств $\{i, j\}$ $(i \neq j)$ элементов множества V. Определим граф как функцию $f: V^{(2)} \to B$, где $f(\{i, j\}) = 1$, если вершины i и j смежны, т. е. существует ребро, соединяющее i и j, $f(\{i, j\}) = 0$ в противном случае. Вес фигур на B определим как тождественную функцию, т. е. $w(0) = 0$, $w(1) = 1$. Поэтому производящая функция весовой спецификации фигур (перечисляющий ряд для фигур) имеет вид $F(z) =$

$= 1 + z$. Из определения весовой характеристики конфигурации (пункт 1.2.2.1) следует, что вес конфигурации f равен

$$W(f) = z \sum_{\{i,j\} \in V^{(2)}} w\big(f(\{i,j\})\big).$$

Таким образом, вес конфигурации есть число рёбер в графе, соответствующем функции f. Пусть E_2 — тождественная группа, действующая на B, т. е. группа, состоящая из единственной тождественной подстановки $(1)(2)$, $\mathfrak{S}_n$ — симметрическая группа на V. Обозначим через $\mathfrak{S}_n^{(2)}$ парную группу, действующую на множестве $V^{(2)}$, подстановки которой индуцируются группой $\mathfrak{S}_n$, т. е. для каждой подстановки $g \in \mathfrak{S}_n$ существует подстановка $g' \in \mathfrak{S}_n^{(2)}$, для которой $g'(\{i,j\}) = \{g(i), g(j)\}$. Применяя теорему Пойа к группе конфигураций $\mathfrak{S}_n^{(2)}$, получаем следующий результат Пойа.

Теорема 3.2.16

Перечисляющий многочлен для графов с n вершинами g_n получается подстановкой в цикловой индекс $Z_{\mathfrak{S}_n^{(2)}}(z_1, z_2, \dots, z_n)$ группы $\mathfrak{S}_n^{(2)}$ вместо z_k $F(z^k) = 1 + z^k$, где

$$Z_{\mathfrak{S}_n^{(2)}}(z_1, z_2, \dots, z_n) =$$

$$= \frac{1}{n!} \sum_{\substack{\langle j_1, \dots, j_n \rangle \\ 0 \le j_i \le n \\ j_1 + 2j_2 + \dots + nj_n = n}} \frac{n!}{j_1!\, j_2! \cdots j_n!\, 1^{j_1} \cdot 2^{j_2} \cdot \dots \cdot n^{j_n}} \prod_{k=1}^{[n/2]} \left(z_k z_{2k}^{k-1}\right)^{j_{2k}} \times$$

$$\times \prod_{k=0}^{[(n-1)/2]} z_{2k+1}^{k j_{2k+1}} \prod_{k=1}^{[n/2]} z_k^{k C_{j_k}^2} \prod_{1 \le r < s \le n-1} z_{m(r,s)}^{d(r,s) j_r j_s},$$

где $[x]$ — целая часть числа x, $m(r,s)$ — наименьшее общее кратное, $d(r,s)$ — наибольший общий делитель чисел r и s.

3.2.5.3. Перечисление связных графов

Здесь применим другой подход к формализации задачи. Возьмём в качестве множества фигур Y совокупность всех связных графов. Весовая характеристика фигуры (графа) $y \in Y$ — число её вершин. Рассмотрим производящую функцию весовой спецификации множества фигур Y:

$$F_c(z) = \sum_{n=1}^{\infty} c_n z^n, \qquad (3.2.8)$$

где c_n — число связных графов с n вершинами. Пусть $\mathfrak{S}_k$ — симметрическая группа, действующая на множестве $X = \{1, 2, \dots, k\}$ (X — множество мест). Она определяет на Y^X отношение эквивалентности, порождающее классы эквивалентности: f, $f' \in Y^X$ принадлежат одному классу, если $f'(x) = f'(g(x))$ для всех $x \in X$ при некоторой подстановке $g \in \mathfrak{S}_k$. Каждому графу с k компонентами связности ставится во взаимно однозначное соответствие описанный класс эквивалентности на множестве Y^X. Производящая функция весовой спецификации неэквивалентных фигур имеет вид

$$g_k(z) = \sum_{n=k}^{\infty} \tilde{g}_{n,k} z^n,$$

где $\tilde{g}_{n,k}$ — число графов порядка n, имеющих k компонент связности, $\tilde{g}_{0,0} = 1$ (существует единственный граф, не имеющий вершин, — пустой граф). По теореме Пойа

$$g_k(z) = Z_{\mathfrak{S}_k}\big(F_c(z), F_c(z^2), \dots, F_c(z^k)\big). \qquad (3.2.9)$$

Пусть g_n — общее число графов с n вершинами, $g_0 = 1$. Из очевидного равенства

$$g_n = \sum_{k=0}^{n} \tilde{g}_{n,k}$$

следует, что производящая функция чисел g_n равна

$$F_g(z) = \sum_{n=0}^{\infty} g_n z^n = \sum_{k=0}^{\infty} g_k(z). \qquad (3.2.10)$$

Для производящей функции весовой спецификации фигур в пункте 3.2.5.1 было выведено равенство (3.2.6). Применяя его к функциям (3.2.9) и (3.2.10), имеем

$$F_g(z) = \exp\left(\sum_{i=1}^{\infty} \frac{c(z^i)}{i}\right). \qquad (3.2.11)$$

Для коэффициентов разложения функции F_g, определённой формулой (3.2.11), в степенной ряд можно вывести рекуррентные формулы

$$g_n = \frac{1}{n}\sum_{i=1}^{n} i a_i g_{n-i},$$

где

$$a_i = \frac{1}{i}\sum_{d|i} d c_d,$$

суммирование ведётся по всем положительным делителям числа i, величины c_i — коэффициенты разложения (3.2.8). Применяя к последнему равенству формулы обращения, получаем

$$c_n = \sum_{d|n} \frac{\mu(d)}{d} a_{n/d},$$

где

$$a_n = g_n - \frac{1}{n}\sum_{i=1}^{n-1} i a_i g_{n-i},$$

μ — используемая в теории чисел функция Мёбиуса, определяемая равенствами

$$\mu(n) = \begin{cases} 1, n = 1, \\ (-1)^k, n = p_1 p_2 \cdots p_k, \\ 0, n \neq p_1 p_2 \cdots p_k, \end{cases}$$

$p_1, p_2, \dots, p_k$ — некоторые различные простые числа. По этим формулам можно найти число c_n связных графов с n вершинами через общее количество g_n графов порядка n.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Акимов О. Е.* Дискретная математика: логика, группы, графы / О. Е. Акимов. — М. : Лаборатория Базовых Знаний, 2003. — 376 с.

2. *Аляев Ю. А.* Дискретная математика и математическая логика / Ю. А. Аляев, С. Ф. Тюрин. — М. : Финансы и статистика, 2006. — 368 с.

3. *Асеев Г. Г.* Дискретная математика / Г. Г. Асеев, О. М. Абрамов, Д. Э. Ситников. — Ростов : Феникс, 2003. — 144 с.

4. *Виленкин Н. Я.* Комбинаторика / Н. Я. Виленкин. — М. : Наука, 1969. — 328 с.

5. *Виленкин Н .Я.* Комбинаторика / Н. Я. Виленкин, А. Н. Виленкин, П. А. Виленкин. — М. : ФИМА – МЦНМО, 2006. — 400 с.

6. *Гаврилов Г .П.* Задачи и упражнения по дискретной математике / Г. П. Гаврилов, А. А. Сапоженко. — М. : ФИЗМАТЛИТ, 2004. — 416 с.

7. *Горбатов В. А.* Дискретная математика / В. А. Горбатов, А. В. Горбатов, М. В. Горбатова. — М. : АСТ, 2003. — 448 с.

8. *Емеличев В. А.* Лекции по теории графов / В. А. Емеличев, О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич. — М. : Наука, 1990. — 384 с.

9. *Кристофидес Н.* Теория графов. Алгоритмический подход / Н. Кристофидес. — М. : Мир, 1978. — 432 с.

10. *Кук В.* Компьютерная математика / В. Кук, Г. Бейз. — М. : Наука, 1990. — 384 с.

11. *Куратовский К.* Теория множеств / К. Куратовский, А. Мостовский. — М. : Мир, 1970. — 416 с.

12. *Лавров И .А.* Задачи по теории множеств, математической логике и теории алгоритмов / И. А. Лавров, Л. А. Максимова. — М. : ФИЗМАТЛИТ, 2004. — 256 с.

13. *Матросов В. Л.* Лекции по дискретной математике / В. Л. Матросов, В. Н. Стеценко. — М. : МПГУ, 1997. — 220 с.

14. *Нефёдов В. Н.* Курс дискретной математики / В. Н. Нефёдов, В. А. Осипова. — М. : МАИ, 1992. — 264 с.

15. *Новиков Ф. А.* Дискретная математика для программистов / Ф. А. Новиков. — СПб. : Питер, 2009. — 384 с.

16. *Оре О.* Теория графов / О. Оре. — М. : Либроком, 2009. — 354 с.

17. *Оре О.* Графы и их применение / О. Оре. — М. : ЛКИ, 2008. — 168 с.

18. *Пак В .Г.* Сборник задач по дискретной математике. Теория множеств. Комбинаторика / В. Г. Пак. — СПб. : Изд-во БГТУ, 2008. — 108 с.

19. *Пак В. Г.* Сборник задач по дискретной математике. Комбинаторный анализ / В. Г. Пак. — СПб. : Изд-во БГТУ, 2010. — 201 с.

20. *Риордан Дж.* Введение в комбинаторный анализ / Дж. Риордан. — М. : Изд-во иностранной литературы, 1963. — 287 с.

21. *Риордан Дж.* Комбинаторные тождества / Дж. Риордан. — М. : Наука, 1982. — 255 с.

22. *Рыбников К. А.* Введение в комбинаторный анализ / К. А. Рыбников. — М. : Изд-во МГУ, 1985. — 312 с.

23. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики / В. Н. Сачков. — М. : МЦНМО, 2004. — 424 с.

24. *Свами М.* Графы, сети и алгоритмы / М. Свами, К. Тхуласираман. — М. : Мир, 1984. — 455 с.

25. *Соболева Т. С.* Дискретная математика / Т. С. Соболева, А.В. Чечкин. — М. : Академия, 2006. — 255 с.

26. *Судоплатов С. В.* Дискретная математика / С. В. Судоплатов, Е. В. Овчинникова. — М. : Инфра-М, 2007. — 256 с.

27. *Судоплатов С. В.* Элементы дискретной математики / С. В. Судоплатов, Е. В. Овчинникова. — М. : Инфра-М, 2002. — 288 с.

28. *Уилсон Р.* Введение в теорию графов / Р. Уилсон. — М. : Мир, 1977. — 208 с.

29. *Фудзисава Т.* Математика для радиоинженеров. Теория дискретных структур / Т. Фудзисава, Т. Касами. — М. : Радио и связь, 1984. — 240 с.

30. *Хаггард Г.* Дискретная математика для программистов / Г. Хаггард, С. Уайтсайдс, Дж. Шлипф. — М. : БИНОМ. Лаборатория знаний, 2010. — 627 с.

31. *Хаггарти Р.* Дискретная математика для программистов / Р. Хаггарти. — М. : Техносфера, 2003. — 320 с.

32. *Харари Ф.* Теория графов / Ф. Харари. — М. : УРСС, 2006. — 296 с.

33. *Харари Ф.* Перечисление графов / Ф. Харари, Э. Палмер. — М. :

Мир, 1977. — 324 с.

34. *Холл М.* Комбинаторика / М. Холл. — М. : Мир, 1970. — 424 с.

35. *Шапорев С. Д.* Дискретная математика / С. Д. Шапорев. — СПб. : БХВ-Петербург, 2006. — 396 с.

36. *Яблонский С. В.* Введение в дискретную математику / С. В. Яблонский. — М. : Высшая школа, 2003. — 384 с.

ПРИЛОЖЕНИЯ

Приложение 1

УКАЗАТЕЛЬ ПРИНЯТЫХ ОБОЗНАЧЕНИЙ

Для каждого обозначения указана страница, на которой она встречается в первый раз.

$A, B, C, \dots, A_1, A_2, \dots$	множества, 11
$a, b, c, \dots, a_1, a_2, \dots$	элементы множеств, 11
$a \in A$	элемент a принадлежит множеству A, 11
$a \notin A$	элемент a не принадлежит множеству A, 11
$A = B$	равенство множеств A и B, 11
$A \neq B$	неравенство множеств A и B, 11
$A \subseteq B$	A — подмножество B, 11
$\emptyset$	пустое множество, 11
$A \subset B$	A — собственное подмножество B, 11
$\mathbb{U}$	универсальное множество (универсум), 11
2^A	булеан множества A, 12
$A = \{a_1, a_2, \dots, a_n\}$	A состоит из элементов a_1, a_2, ... , a_n, 12
$P(a)$	свойство, которым обладает элемент a, 12
$\{a \mid P(a)\}$	множество элементов a, обладающих свойством P, 12
$\mathbb{N}$	множество натуральных чисел, 13
$A \cup B$	объединение множеств A и B, 13
$A \cap B$	пересечение множеств A и B, 14

$A \setminus B$	разность множеств A и B, 14
$\overline{A}$	дополнение множества A, 14
$A \dot{-} B$	симметрическая разность множеств A и B, 14
$\mathcal{A}, \mathcal{B}, \dots$	формулы алгебры множеств, 15
$\{A_1, A_2, \dots, A_n\}$	покрытие или разбиение множества A, 18
$\|A\|$	мощность конечного множества A, 19
(n)-множество	множество, содержащее n элементов, 19
C_n^m	число бесповторных (m)-сочетаний из элементов (n)-множества, 20
$\mathbb{N}_0$	множество неотрицательных целых чисел, 21
$\langle a_1, a_2, \dots, a_n \rangle$	упорядоченная совокупность элементов a_1, a_2, … , a_n, 22
$A_1 \times A_2 \times \dots \times A_n$	декартово произведение множеств A_1, A_2, … , A_n, 22
A^n	n-я декартова степень множества A, 22
$\overline{A}_n^m$	число повторных (m)-размещений из элементов (n)-множества, 25
A_n^m	число бесповторных (m)-размещений из элементов (n)-множества, 25
P_n	число (n)-перестановок, 26
$\hat{A}$	мультимножество, порождённое множеством A, 27
$a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$	первичная спецификация (m)-

$y = f(x)$	элемент y является значением функции f при аргументе x, 35
$f\|A$	сужение функции f на множество A, 35
B^A	совокупность функций из A в B, 35
$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$	функция $f: A \to B$, $A = \{a_1, a_2, \dots, a_n\}$, 36
$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{pmatrix}$	функция $f: A \to A$, $A = \{a_1, a_2, \dots, a_n\}$, 36
a/R	класс эквивалентности элемента a по эквивалентности R, 43
A/R	фактор-множество A по эквивалентности R, 43
$\leq$	отношение частичного порядка, 44
$\geq$	двойственный к $\leq$ порядок, 44
$\sup B$	точная верхняя грань подмножества $B \subseteq A$, 47
$\inf B$	точная нижняя грань подмножества $B \subseteq A$, 47
$\mathbb{Q}$	множество рациональных чисел, 48
$\alpha(p_{i_1}, p_{i_2}, \dots, p_{i_s})$	количество элементов, обладающих свойствами $p_{i_1}, p_{i_2}, \dots, p_{i_s}$, 47
$\alpha(p_1, \dots, p_s, \overline{p}_{s+1}, \dots, \overline{p}_m)$	количество элементов, обладающих свойствами $p_1, p_2, \dots, p_s$ и не обладающих свойствами $p_{s+1}, \dots, p_m$, 48
D_n	число беспорядочных перестановок элементов (n)-множества, 51
$D_n(r)$	число перестановок элементов

μ	функция Мёбиуса, 64
$x \nleq y$	неверно, что $x \leq y$, 64
$x < y$	$x \leq y$ и $x \neq y$, 64
$\mathfrak{m}(x)$	мера элемента x, 70
$\mathfrak{m}(X)$	мера множества X, 71
(P)-свойство	элемент обладает (P)-свойством, если он обладает всеми свойствами из совокупности P, 71
$g(P)$	мера множества элементов A, обладающих $(\overline{P})$-свойством, где $\overline{P} = P_m \backslash P$, $P_m = \{p_1, \dots, p_m\}$ — набор свойств, 71
$f(P)$	суммарная мера элементов, обладающих $(\overline{P})$-свойством и, может быть, другими свойствами из P, 71
$\{a_n\}_{n=0}^{N}$	конечный вектор $\langle a_0, a_1, \dots, a_N \rangle$, 72
$\{a_n\}$	бесконечный вектор $\langle a_0, a_1, \dots \rangle$, 72
F_a	производящая функция (ряд) последовательности $\{a_n\}$, 72
f_a	функция, к которой сходится ряд F_a, также называется производящей функцией, 72
E_a	экспоненциальная производящая функция (экспоненциальный ряд) последовательности $\{a_n\}$, 73
e_a	функция, к которой сходится экспоненциальный ряд E_a, также называется экспоненциальной

E_a^{-1}	экспоненциальный ряд, обратный относительно умножения к ряду E_a, 85
$F_{a/b}$	ряд, являющийся частным производящих функций F_a и F_b, 86
$E_{a/b}$	экспоненциальный ряд, являющийся частным экспоненциальных производящих функций E_a и E_b, 86
$\hat{A}_m$	число (m)-векторов с координатами из (n)-множества A, в которых присутствует хотя бы по одному экземпляру каждого элемента A, 100
φ	n-местная операция на множестве A, 102
$a = \varphi(a_1, a_2, \dots, a_n)$	элемент a ставится в соответствие вектору $\langle a_1, a_2, \dots, a_n \rangle$ при операции φ, 102
Φ	сигнатура множества, 102
$\mathcal{A}(A, \Phi)$	алгебра с основным множеством A и сигнатурой Φ, 102
$\cdot$	бинарная операция (умножение) на A, 102
$+$	бинарная операция (сложение) на A, 102
a^{-1}	элемент, обратный к элементу a, 103
$\varphi(A')$	образ подмножества $A' \subseteq A$ при операции φ, 104
I	нейтральный относительно операции $\cdot$ элемент абстрактной ал-

$\mathcal{K}(K, +, \cdot)$	кольцо вычетов по модулю m, 111
$GF(p)$	конечное поле порядка p, 112
$\mathfrak{F}_n$	симметрическая полугруппа степени n, 113
$\mathfrak{S}_n$	симметрическая группа степени n, 113
s_i	сужение подстановки s на орбиту A_i, 116
$\left(a, s_i(a), s_i^2(a), \dots, s_i^{n_i-1}(a)\right)$	цикл длины n_i на орбите A_i, $a \in$ $\in A_i$, 116
(a, b)	транспозиция, 117
$1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}$	цикловой класс, 117
$C(\alpha_1, \alpha_2, \dots, \alpha_n)$	число подстановок в цикловом классе $1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}$, 118
$C(n, k)$	число подстановок степени n, имеющих k циклов, 119
$s(n, k)$	числа Стирлинга первого рода, 120
$\sigma(n, k)$	числа Стирлинга второго рода, 120
$(z)_n$	факториальная функция, 121
δ_{nk}	символ Кронекера, 121
$k_i(g)$	число циклов длины i в подстановке g, 121
$P_{\mathcal{G}}(z_1, z_2, \dots, z_n)$	цикловой индекс группы подстановок $\mathcal{G}$, 121
$\mathcal{C}_n$	циклическая группа подстановок степени n, все элементы которой являются степенями подстановки $C = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{pmatrix}$, 123
$\mathcal{G}(a)$	стабилизатор элемента $a \in A$ от-

	ствующих (m)-мультимножествам первичной спецификации ${y_1}^{\alpha_1}{y_2}^{\alpha_2}\dots{y_n}^{\alpha_n}$, не эквивалентных относительно $\mathcal{G}$, 136
$\Phi_m(z_1, z_2, \dots, z_n;\ \mathcal{G})$	производящая функция чисел $C_m(\alpha_1, \alpha_2, \dots, \alpha_n; \mathcal{G})$, 136
$G = \langle V, X\rangle$	граф (орграф) с множеством вершин V и множеством рёбер (дуг) X, 142
$x = \{u, v\}$	ребро, соединяющее вершины u и v, 142
$x = \langle u, v\rangle$	дуга, направленная от вершины u к вершине v, 142
Λ	пустой граф, 143
K_n	полный граф порядка n, 143
$\delta(v)$	звезда вершины v, 144
$\deg(v)$	степень вершины v, 144
$\delta_+(v)$	полустепень захода вершины v, 144
$\delta_-(v)$	полустепень исхода вершины v, 144
$K_{3,3}$	граф Куратовского, 145
$\Omega(G)$	матрица смежности вершин графа (орграфа) G, 147
$\varepsilon(G)$	матрица инцидентности графа (орграфа) G, 148
$v_0x_1v_1x_2v_2 \dots v_{l-1}x_lv_l$	маршрут от вершины v_0 к вершине v_l, 149
(u, v)-маршрут	маршрут от вершины u к вершине v, 149
$X(V')$	множество рёбер (дуг) графа (орграфа) G, обе концевые вершины

	которых принадлежат $V' \subseteq V$, 152
$G' = \langle V', X(V') \rangle$	подграф (подорграф), порождённый подмножеством $V' \subseteq V$, 152
$G \backslash x$	подграф (подорграф) графа (орграфа) G, полученный удалением из него ребра (дуги) x, 153
μ	цикломатическое число графа, 159
$G^{\wp} = \langle V, X, \wp \rangle$	помеченный граф (орграф), 160
Q_n	число помеченных графов порядка n
$\Gamma(G)$	группа автоморфизмов графа (орграфа) G, 164
$s(G)$	порядок группы $\Gamma(G)$, 164
$l(G)$	число способов пометить граф G, 164
$\widehat{\Omega}(G)$	матрица $-\Omega(G)$, в которой элементы главной диагонали заменены на $\deg(v_i)$, 166
$M_-(G)$	диагональная матрица, у которой i-й диагональный элемент равен $\delta_-(v_i)$, 173
$C_-(G)$	матрица $M_-(G) - \Omega(G)$, 173
$M_+(G)$	диагональная матрица, у которой i-й диагональный элемент равен $\delta_+(v_i)$, 173
$C_+(G)$	матрица $M_+(G) - \Omega(G)$, 173
T_+	остовное корневое подордерево, входящее в вершину v, 173
T_-	остовное корневое подордерево, исходящее из вершины v, 173
$C(G)$	матрица $C_+(G)$ (совпадающая с

	$C_{-}(G)$) для эйлерова орграфа G, 177
$e(G)$	число эйлеровых контуров в помеченном эйлеровом орграфе G, 177
$G^C = \langle V, X, R^C \rangle$	раскрашенный граф (орграф), 184
$\chi(G)$	хроматическое число графа (орграфа) G, 184
$G + \{u, v\}$	граф G, к которому добавлено ребро $\{u, v\}$, соединяющее несмежные в G вершины u и v, 186
f_G	хроматический многочлен графа (орграфа) G, 187
T_n	помеченное дерево с n вершинами, 188
$C_n(k)$	число помеченных k-раскрашенных графов порядка n, 189
$\hat{G}$	ациклическое расширение ациклического орграфа G, 191
A_n	число помеченных ациклических орграфов порядка n, 192
$A_{n,k}$	число помеченных ациклических орграфов порядка n с k вершинами нулевой полустепени захода, 192
$a(n)$	число корневых деревьев с n вершинами, 194
$b_m(n)$	число корневых деревьев с n вершинами и m инцидентными корню рёбрами, 196
$g_{n,m}$	число графов с n вершинами и m рёбрами, 198

$m(r, s)$	наименьшее общее кратное чисел r и s, 200
c_n	число связных графов с n вершинами, 201
$\tilde{g}_{n,k}$	число графов с n вершинами, состоящих из k компонент связности, 201

Приложение 2

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ